Дэвид КАН
ВЗЛОМЩИКИ КОДОВ

DAVID KAHN
THE CODEBREAKERS

Анонс

В книге подробнейшим образом прослеживается тысячелетняя история криптоанализа — науки о вскрытии шифров. Ее события подаются автором живо и доходчиво и сопровождаются богатым фактическим материалом. Кто был первым библейским криптоаналитиком, какое влияние криптоанализ оказывает на исход политических событий военных операций и судьбы известных исторических личностей, как он позволяет бороться с преступностью — обо всем этом рассказывает известный американский журналист и военный историк.

Содержание

Предисловие

Дешифрование является одним из наиболее важных способов добывания разведывательных данных в современном мире. Оно дает намного больше достоверной информации, чем традиционная агентурная разведка, оказывая значительное влияние на политику правительств. Тем не менее у дешифровальных спецслужб нет своего летописца.

А они остро нуждаются в таком летописце. Хотя официально было признано, что американские дешифровальщики сократили сроки окончания войны на Тихом океане примерно на год, в научных трудах по истории это отражено лишь мимоходом, что приводит к неправильному взгляду на ход исторических событий в мире. Более того, криптоанализ сам может только выиграть, как и другие области человеческой деятельности, зная своих гениев и основные направления развития, свои ошибки и извлеченные из них уроки.

Я сделал попытку написать серьезную историю криптоанализа, и в первую очередь — разъяснить

обществу ту важную роль, которую дешифрование сыграло в жизни человечества. Для любознательных читателей эта книга может послужить надежным проводником в прошлое криптоанализа. А для историков она будет полезна тем, что обратит их внимание на скрытое влияние дешифрования на историю.

Начиная эту книгу, я, подобно другим, хорошо осведомленным криптологам-любителям, считал, будто знаю обо всем, что напечатано по криптоанализу. Но как же мало нам было известно! Ни мы, любители, ни даже профессионалы не имели представления о том, какое большое количество ценной информации содержится в научных журналах. Мы не обращались к дешифровальщикам с просьбой поделиться своими воспоминаниями. Мы не пытались воспользоваться огромным богатством архивов. Мы не пробовали изучать вопросы, которые в настоящее время представляются нам главными. Я думаю, что не ошибусь, если заявлю, что по сравнению с ранее опубликованными материалами в моем труде содержится от 85 до 90% совершенно нового.

И это далеко не все. Из-за необоснованной секретности недоступна большая часть документов, относящихся к недавнему прошлому. Чтобы рассказать о криптоаналитических разработках этого периода полностью, потребуется еще одна такая же книга. Даже, к примеру, в XVIII веке можно обнаружить массу неизученных рукописей.

В моей книге я старался придерживаться двух принципов. Первый — по возможности использовать первоисточники. Часто я не мог поступить иначе, так как по некоторым вопросам еще ничего не было опубликовано. Второй — при оценке роли криптоанализа, будь то на поле брани или на дипломатическом поприще, я пытался никогда не забывать об иных важных факторах, сыгравших свою роль. Если книга создает впечатление, что все события в истории зависели от тех, о ком написана эта книга, то это не история, а ее искажение. Такой подход особенно широко распространен в литературе о шпионах, но от него не застрахован и криптоанализ. Я считаю, что хотя и пытаюсь уравновесить рассказ об истории дешифрования упоминанием других факторов, тем самым я не уменьшаю интереса к книге. Просто мое повествование становится от этого достовернее и поэтому заслуживает более серьезного внимания.

У каждой профессии есть свой словарь. Словарь криптоаналитика достаточно сложен, поэтому небольшое по объему введение в общепринятую криптоаналитическую терминологию значительно облегчит понимание изложенного в этой книге. Определения в нем являются нестрогими и преследуют лишь цель пояснения того или иного термина. Исключения игнорируются, а множество редко употребляемых терминов и вовсе не определены — в процессе чтения книги их значение становится ясным из контекста.

Открытый текст — сообщение, подлежащее засекречиванию. В результате применения методов *шифрования* сообщение делают непонятным для посторонних, используя два основных способа преобразования открытого текста.

В случае *перестановки* знаки открытого текста перемешиваются, нарушается их нормальный порядок следования. Перетасовать буквы слова *«секрет»* так, чтобы получить *«еткрсе»,* и означает сделать перестановку.

При *замене* знаки открытого текста замещаются другими знаками. Так, слово *«секрет»* может быть заменено на *19 5 3 18520.*

Системы замены основаны на идее *шифралфавита* — перечня эквивалентов, используемых для преобразования открытого текста в шифрованный.

Иногда шифралфавит предусматривает несколько замен одного знака. Например, знак открытого текста «с» не всегда замещается числом *16,* а может быть заменен одним из чисел *16, 21, 35, 74.* Этот выбор называется *гомофоном.* Время от времени в шифралфавит включаются символы, которые ничего не означают. Такие символы зовут *пустышками.*

В том случае, когда используется только один шифралфавит, система замены называется *одноалфавитной.* Но когда применяются два или большее число шифралфавитов по какому-то заранее определенному правилу, система замены становится *многоалфавитной.*

Среди систем замены следует делать различия между *кодами* и *шифрами.* Код состоит из тысяч слов, фраз, букв и слогов и соответствующих им *кодовых слов* или *кодовых обозначений,* которые заменяют эти элементы открытого текста. По существу, код является огромным шифром замены, в котором основными единицами открытого текста служат слова и фразы. В шифрах же основная единица — это знак, иногда пара знаков.

В течение 450 лет, начиная примерно с 1400 г. и до 1850 г., в шифровальной практике доминировали системы, которые являлись наполовину кодом и наполовину шифром. В них обычно был отдельный шифралфавит, включавший гомофоны и кодоподобный перечень имен, слов и слогов.

От этого перечня, первоначально состоявшего только из имен, и произошло название для таких систем — *номенклатор.*

Во многих шифрах используется *ключ,* который определяет порядок следования знаков в шифралфавите, или порядок перемешивания знаков в перестановке, или начальные установки в шифрмашинах. Когда слово, или фраза, или число служат ключом, они, естественно, называются *ключевым словом, ключевой фразой* или *ключевым числом.*

Проведение соответствующих преобразований открытого текста в шифрованный называется *шифрованием* или *кодированием* открытого текста. То, что получается в результате, носит название *шифртекста* или *кодтекста.*

Окончательно обработанное и отосланное секретное сообщение называется *криптограммой.* Термин «шифртекст» обращает внимание на результат зашифрования, в то время как термин «криптограмма» подчеркивает сам факт передачи сообщения и является аналогом слова «телеграмма».

Расшифрование (раскодирование) означает проведение обратных преобразований шифртекста (кодтекста) лицами, владеющими на законном основании ключом и системой шифрования (кодирования), для получения открытого текста. Этот процесс следует отличать от *криптоанализа,* который ставит своей целью прочтение открытого текста (или, другими словами, *дешифрование)* криптограммы людьми, не имеющими в своем распоряжении ни ключа, ни системы, то есть лицами, являющимися третьей стороной, «противником». Разница между ними, безусловно, огромная, хотя начиная с того времени, когда возникло слово «криптоанализ», термины «расшифровать» или «раскодировать» часто использовались и в смысле «дешифровать».

Успешный криптоанализ шифра или кода часто именуют его *вскрытием* или *взломом.*

Сообщения, посылаемые без предварительного зашифрования, называются *незашифрованными* или отправляемыми *клером.* Иногда говорят еще, что они передаются *открытым текстом.*

Наконец, *криптология* — это наука, охватывающая составление шифров *(криптографию)* и криптоанализ.

ПЕРВЫЕ 3000 ЛЕТ

Почти четыре тысячи лет тому назад в древнеегипетском городе Менет-Хуфу на берегу Нила один опытный писец нарисовал иероглифы, рассказавшие историю жизни его господина. Сделав это, он стал родоначальником документально зафиксированной истории криптографии.

Его система не является тайнописью в том виде, в каком она известна современному миру. Для засекречивания своей надписи он не использовал никакого полноценного шифра. Эта надпись, вырезанная им примерно в 1900 г. до нашей эры на гробнице знатного человека по имени Хнумхотеп, лишь в отдельных местах состоит из необычных иероглифических символов вместо более привычных иероглифов. Большинство их встречается в ее последних двадцати столбцах, в которых перечисляются монументы, созданные Хнумхотепом на службе у египетского фараона Аменемхета II. Неизвестный писец старался не затруднить чтение текста, а придать ему важность, подобно тому, как это делается в каком-нибудь заявлении по торжественному поводу, в котором пишут «в год одна тысяча восемьсот шестьдесят третий от Рождества Христова», вместо того чтобы просто и без затей написать «в 1863 году». Таким образом, хотя писец применил не тайнопись, он, бесспорно, воспользовался одним из существенных элементов шифрования — умышленным преобразованием письменных символов. Это самый древний известный нам текст, который претерпел такие изменения.

По мере расцвета древнеегипетской цивилизации и совершенствования ее письменности росло количество усыпальниц почитаемых умерших и все более изощренными становились преобразования текстов, которые вырезались на камнях гробниц. Со временем писцы стали заменять обычную иероглифическую форму буквы, например, рот, изображенный анфас, иной формой, например, ртом, изображенным в профиль. Они вводили в употребление новые иероглифы, первый звук произношения которых выражал желательную букву, как, например, изображение свиньи. Иногда произношение двух иероглифов различалось, но их изображение напоминало друг друга. Время от времени писцы использовали иероглиф по принципу ребуса, подобно тому, как, например, в английском языке изображение пчелы может означать букву «В». Эти преобразования были изначально свойственны обычному египетскому письму: именно с их помощью иероглифы приобрели свои звуковые значения. В дальнейшем они лишь усложнялись и делались все более искусственными.

Такие преобразования были обнаружены во многих местах — в надгробных надписях,

восхвалявших пройденный путь умерших, в гимне в честь Тота* и на саркофагах фараона Сети I. В них нет ничего такого, что преследовало бы цель скрыть смысл текста. И действительно, большинство надписей повторяются в обычной форме рядом с измененной. Для чего же тогда делать преобразования? Часто с той же целью, что и в гробнице Хнумхотепа, а именно — чтобы произвести впечатление на читателя. Иногда — чтобы показать хорошую каллиграфию или ради украшения. Реже — чтобы отразить соответствующее тому времени произношение.

Тот — бог Луны, письма, счета и письменности в Древнем Египте.

Но постепенно многие надписи начинают преследовать другую, важную для криптографии цель — секретность. В некоторых случаях секретность была нужна для усиления тайны и, следовательно, колдовской силы поминальных текстов. Гораздо чаще секретность проистекала из понятного желания древних египтян заставить прохожего прочитать их эпитафии и тем самым выразить умершим благословения, которые содержались в надгробных надписях. В Древнем Египте, с характерной для него непоколебимой верой в загробную жизнь, количество надписей быстро выросло до такой степени, что внимание к ним прохожих пошатнулось. Чтобы возродить их интерес, писцы нарочно делали надписи несколько туманными. Они ввели криптографические знаки, дабы привлечь внимание читателя, заставить его задуматься и вызвать у него желание разгадать их смысл. Но эти приемы совершенно не удались. Вместо того чтобы заинтересовать читателя, они губили даже малейшее желание прочитать набившие всем оскомину эпитафии. А посему вскоре после появления «надгробной» криптографии от нее отказались.

Итак, добавление элемента секретности в преобразование иероглифов породило криптографию. Правда, это напоминало скорее игру, поскольку преследовалась цель задержать разгадку только на самое короткое время. Поэтому криптоанализ также заключался всего лишь в раскрытии головоломки. Таким образом, древнеегипетский криптоанализ был квазинаукой, в отличие от этой современной, чрезвычайно серьезной области научных знаний. Однако всем великим делам свойственны скромные начинания. Иероглифы Древнего Египта действительно включали, хотя и в несовершенной форме, два элемента — секретность и преобразование письма, которые составляют основные атрибуты криптографии.

Так родилась криптология. В течение первых 3000 лет ее развитие не было неуклонным. В одних местах криптология появилась самостоятельно и потом умерла вместе с породившими ее цивилизациями. В других она выжила, проникнув в литературу. Опираясь на ее литературную основу, следующее поколение могло карабкаться к новым высотам криптологии. Но продвижение к ним было медленным и прерывистым. Больше было потеряно, чем сохранено. Значительная часть древней истории криптологии представляет собой плохо подобранный букет, составленный из расцветающих, распустившихся и увядающих цветов. Накопленные знания получили простор только в начале эпохи европейского Возрождения.

В Индии, стране с древней высокоразвитой цивилизацией, люди с незапамятных времен пользовались несколькими разновидностями тайнописи. В классическом древнеиндийском трактате об искусстве управлять государством, написанном между 321-м и 300 гг. до нашей эры, рекомендуется, чтобы глава шпионской спецслужбы давал своим агентам задания с помощью тайнописи. Там же дипломатам дается совет прибегать к криптоанализу для получения разведывательных данных: «При невозможности беседовать с людьми пусть посол осведомится о происходящем у врага из речей нищих, пьяных, сумасшедших, спящих или из условных знаков, надписей, рисунков в храмах и местах паломничества». И хотя автор трактата не дает никакого намека, как именно нужно читать тайнопись, тот факт, что он знает о возможности ее дешифрования, свидетельствует о некоторой искушенности в области криптоанализа. Более того, впервые в истории человечества здесь упоминается о криптоанализе в политических целях.

Не избежала соприкосновения с шифрами (или, если говорить точнее, с предшественниками шифров, так как в ней нет элемента секретности) и Библия. Как в случае с иероглифами на гробнице Хнумхотепа, преобразования письма сделаны в Библии без какого-либо явного желания скрыть содержание текста. Главной причиной, очевидно, было стремление переписчика обессмертить себя путем изменения текста, который позднее будет снова тщательно переписан и позволит пронести частицу его личности через века.

Самая знаменитая «криптограмма» в Библии связана с историей о том, как в разгар пира у вавилонского царя Валтасара человеческая рука стала писать на стене зловещие слова: «мене, текел, упарсин». Однако тайна заключается не в том, что означают эти слова. Непонятно, почему мудрецы

царя не смогли разгадать их смысл.

Сами слова «мене», «текел» и «упарсин» взяты из арамейского языка, родственного древнееврейскому, и означают «исчислил», «взвешен» и «разделено». Когда Валтасар вызвал к себе пророка Даниила, последний без труда прочитал надпись и дал толкование этих трех слов: «мене — исчислил Бог царство твое и положил конец ему; текел — ты взвешен и найден очень легким; фарес — разделено царство твое и отдано мидянам и персам». При этом было обыграно значение слова «фарес», которое в арамейском языке идентично слову «упарсин».

«Надпись «мене, текел, упарсин» может также означать названия денежных единиц — мина, текел (1/60 мины) и фарес (1/2 мины). Их перечисление именно в такой последовательности символизирует крушение Вавилонской империи.

Учитывая возможность всех этих интерпретаций, кажется странным, что вавилонские священники не сумели прочитать зловещую надпись на стене. Возможно, они боялись сообщить Валтасару плохую новость, или, может быть, Господь открыл глаза только Даниилу. Как бы там ни было, одному Даниилу удалось разгадать эту загадку, и в результате он стал первым известным криптоаналитиком. А поскольку это библейское сказание, то и награда за успешный криптоанализ, согласно Библии, намного превзошла какие-либо более поздние вознаграждения за аналогичные успехи в дешифровании: «Тогда... облекли Даниила в багряницу, и возложили золотую цепь на шею его, и провозгласили его третьим властелином в царстве».

В Европе криптография находилась в состоянии застоя вплоть до наступления эпохи Возрождения. Применявшиеся шифрсистемы были предельно просты — фразы писались по вертикали или в обратном порядке, гласные заменялись точками, использовались иностранные алфавиты (например, древнееврейский и армянский), каждая буква открытого текста заменялась следовавшей за ней буквой. Кроме того, в течение всех этих лет криптология была поражена болезнью, которая сохранилась до более позднего времени, а именно — убежденностью многих людей в том, что криптография и криптоанализ являются разновидностями черной магии.

С первых дней своего существования криптография преследовала цель спрятать содержание важных разделов письменных документов, имевших отношение к таким сферам магии, как гадание и заклинание. В одной из рукописей о магии, датируемой III веком, используется шифр, чтобы скрыть важные части колдовских рецептов. Криптография часто была на службе магии во времена средневековья, и даже в эпоху Возрождения с помощью шифров алхимики засекречивали важные части формул получения философского камня.

Сходство между магией и криптографией подчеркивалось и другими факторами. Помимо криптографии, таинственные символы использовались в таких понятных лишь посвященным областях магических знаний, как астрология и алхимия, где, подобно знакам открытого текста, каждая планета и каждое химическое вещество имели специальный знак. Как и зашифрованные слова, заклинания и магические формулы, вроде «абракадабры», походили на чепуху, но в действительности были сильны скрытым значением.

Вдобавок многие люди, которые хвастались своей способностью разгадывать шифры, одновременно похвалялись и умением слышать человеческие голоса, будучи глубоко под землей, или даром телепатии. Естественно, что впоследствии эти две области стали обсуждаться вместе — поскольку, мол, они всегда развивались бок о бок.

Мнение о том, что криптоанализ является по своей природе черной магией, происходит и от поверхностного сходства между криптоанализом и гаданием. Извлечение смысла из шифртекста казалось точно таким же делом, что и получение знаний путем изучения расположения звезд и планет, длины линий и мест их пересечения на ладони, внутренностей овец, положения кофейного осадка в чашке. Видимость брала верх над реальностью. Простодушные усматривали магию даже в обычном процессе расшифрования. Другие, более искушенные, видели ее в криптоанализе, так как вскрытие чего-то глубоко спрятанного казалось им непостижимым и сверхъестественным.

Ни в одном из упомянутых выше случаев применения тайнописи нет подтверждения существованию криптоанализа как науки. Время от времени факт дешифрования текста имел место. Подтверждением тому служат истории с пророком Даниилом или с какими-нибудь египтянами, которые разгадали отдельные иероглифические надписи на могильных памятниках. Но научного криптоанализа не существовало ни в Египте с Индией, ни в Европе в период до 1400 г. Была только криптография.

Первыми открыли и описали методы криптоанализа арабы. Этот народ создал одну из самых развитых цивилизаций, которую когда-либо знала история. Арабская наука процветала. Медицина и математика у арабов стали самыми лучшими в мире. Распространились ремесла. Мощная

созидательная энергия арабской культуры, которую ислам лишил живописи и скульптуры, дала плоды на ниве литературы. Получило широкое распространение составление словесных загадок, ребусов и каламбуров. Грамматика стала главным учебным предметом и включала в себя тайнопись.

Интерес к криптографии у арабов проявился рано. В 855 г. арабский ученый по имени Абу Бакр тамед бен-Али бен-Вахшия ан-Набати включил несколько классических шифралфавитов в свою «Книгу о большом стремлении человека разгадать загадки древней письменности». Один такой шифралфавит, называвшийся «дауди» (по имени израильского царя Давида), использовался для зашифрования трактатов по черной магии. Он был составлен из видоизмененных букв древнееврейского алфавита. Другой — сохранился до более позднего времени: в 1775 г. он был использован в письме шпиона, направленном регенту Алжира.

Познания арабов в области криптологии были подробно изложены в произведении Шехаба Калкашанди, которое представляет собой громадную 14-томную энциклопедию, написанную в 1412 г. для того, чтобы дать систематический обзор всех важных областей знания. Раздел под общим заголовком «Относительно сокрытия в буквах тайных сообщений» содержал две части: одна касалась символических действий и намеков, а другая была посвящена симпатическим чернилам и криптологии. Первый раз за всю историю шифров в энциклопедии приводился список как систем перестановки, так и систем замены. Более того, в пятом пункте списка впервые упоминался шифр, для которого была характерна более чем одна замена букв открытого текста. Однако каким бы замечательным и важным этот факт ни был, он затмевается первым в истории описанием криптоаналитического исследования шифртекста.

Его истоки, очевидно, следует искать в интенсивном и скрупулезном изучении Корана многочисленными школами арабских грамматиков. Наряду с другими исследованиями, они занимались подсчетом частоты встречаемости слов, пытаясь составить хронологию глав Корана, изучали фонетику слов, чтобы установить, являлись ли они подлинно арабскими или были заимствованы из других языков. Большую роль в обнаружении лингвистических закономерностей, приведших к возникновению криптоанализа у арабов, сыграло также развитие лексикографии. Ведь при составлении словаря автору фактически приходилось учитывать частоту встречаемости букв, а также то, какие буквы могут стоять рядом, а какие — никогда не встречаются по соседству.

Калкашанди начинает изложение криптоаналитических методов с главного: криптоаналитик должен знать язык, на котором написана криптограмма. Поскольку арабский язык, «самый благородный и самый прекрасный из всех языков», является «одним из наиболее распространенных», далее дается пространное описание его лингвистических характеристик. Приводятся перечни букв, которые никогда не стоят вместе в одном слове, и букв, которые редко появляются по соседству, а также буквенные комбинации, которые в словах встретить невозможно. Последним идет список букв в порядке «частоты их использования в арабском языке в свете результатов изучения священного Корана». Автор даже отмечает, что «в произведениях, не связанных с Кораном, частота использования может быть иной».

Калкашанди продолжает:

«Если вы хотите прочесть сообщение, которое вы получили в зашифрованном виде, то прежде всего начните подсчет букв, а затем сосчитайте, сколько раз повторяется каждый знак, и подведите итог в каждом отдельном случае. Если изобретатель шифра был очень внимателен и скрыл в сообщении все границы между словами, то первая задача, которая должна быть решена, заключается в нахождении знака, разделяющего слова. Это делается так: вы берете букву и работаете, исходя из предположения, что следующая буква является знаком, делящим слова. И таким образом вы изучаете все сообщение с учетом различных комбинаций букв, из которых могут быть составлены слова... Если получается, тогда все в порядке; если нет, то вы берете следующую по счету букву и т. д., пока вы не сможете установить знак раздела между словами. Затем нужно найти, какие буквы чаще всего встречаются в сообщении, и сравнить их с образцом частоты встречаемости букв, о котором упоминалось прежде. Когда вы увидите, что одна буква попадается чаще других в данном сообщении, вы предполагаете, что это буква «Алиф». Затем вы предполагаете, что следующая по частоте встречаемости будет буквой «Лам». Точность вашего предположения должна подтверждаться тем фактом, что в большинстве контекстов буква «Лам» следует за буквой «Алиф»... Затем первые слова, которые вы попытаетесь разгадать в сообщении, должны состоять из двух букв. Это делается путем оценки наиболее вероятных комбинаций букв до тех пор, пока вы не убедитесь в том, что вы стоите на правильном пути. Тогда вы глядите на их знаки и выписываете их эквиваленты всякий раз, когда они попадаются в сообщении. Нужно применять точно такой же принцип по отношению к трехбуквенным словам этого сообщения, пока вы не убедитесь, что вы на что-то напали. Вы

выписываете эквиваленты из всего сообщения. Этот же принцип применяется по отношению к словам, состоящим из четырех и пяти букв, причем метод работы прежний. Всякий раз, когда возникает какое-либо сомнение, нужно высказать два, три предположения или еще больше и выписать каждое из них, пока оно не подтвердится на основании другого слова».

Дав это четкое разъяснение, Калкашанди приводит пример вскрытия шифра. Дешифруемая криптограмма состоит из двух стихотворных строк, зашифрованных с помощью условных символов. В заключение Калкашанди отмечает, что восемь букв не было использовано и что это как раз те самые буквы, которые стоят в конце перечня, составленного по частоте встречаемости. Он отмечает: «Однако это простая случайность: буква может быть поставлена не на то место, которое она должна занимать в вышеупомянутом перечне». Такое замечание свидетельствует о наличии большого опыта в области криптоанализа. Чтобы расставить все точки над «i», Калкашанди приводит второй пример криптоанализа довольно длинной криптограммы. Этим примером он и заканчивает раздел о криптологии.

История умалчивает о том, в какой степени арабы использовали свои блестящие криптоаналитические способности, продемонстрированные Калкашанди, для вскрытия военных и дипломатических криптограмм или какое воздействие это оказало на мусульманскую историю. Однако совершенно ясно, что вскоре эти познания перестали применяться на практике и были забыты. Один эпизод, произошедший почти 300 лет спустя, ярко показывает эту деградацию.

В 1600 г. марокканский султан Ахмед аль-Мансур направил к английской королеве Елизавете I посольство во главе с доверенным человеком — министром Абдель Вахид ибн Масуд ибн Мухаммед Ануном. Посольство должно было заключить с Англией союз, направленный против Испании. Анун отправил на родину зашифрованную простой заменой депешу, которая вскоре после этого каким-то образом попала в руки одного араба. Араб тот был, возможно, умным человеком, но, к сожалению, он ничего не знал о великом арабском наследии в области криптоанализа. Свидетельством тому — памятная записка, в которой он написал:

«Хвала Аллаху! Относительно письма министра Абдель Вахид ибн Масуд ибн Мухаммед Ануна.

Я нашел письмо, написанное его рукой, в котором он с помощью тайных знаков изложил некоторые сведения, предназначенные для нашего покровителя Ахмеда аль-Мансура. Эти сведения касаются султанши христиан (да покарает их Аллах!), которая жила в стране под названием Лондон... С того момента, как это письмо попало ко мне, я постоянно время от времени изучал содержавшиеся в нем знаки. Прошло примерно 15 лет, пока не наступило то время, когда Аллах позволил мне понять эти знаки, хотя никто не обучал меня этому...»

Пятнадцать лет! Подобную задачу Калкашанди решил бы за несколько часов. Такова история человеческой цивилизации!

ПОДЪЕМ НА ЗАПАДЕ

Западноевропейская цивилизация начала использовать криптографию с тех самых пор, как возникла из недр средневекового феодализма. Правда, первоначально тайнопись находилась в эмбриональном состоянии, ее применение было редким и непостоянным. Даже церковные системы шифрования пребывали в зачаточном виде, хотя тогда Церковь пользовалась наибольшим влиянием в обществе. Все же именно с этого времени криптография развивается без продолжительных периодов стагнации и регресса, ее совершенствование становится неуклонным.

Самый древний шифрованный документ, хранящийся в архивах Ватикана, представляет собой небольшой список имен, составленный в 1326-1327 гг., когда в Италии шла борьба между гвельфами* и гибеллинами**. В нем гибеллины называются «египтянами», а гвельфы — «детьми Израилевыми». В архивах Венеции можно отыскать шифр, датируемый 1226 г. Суть его заключается в том, что точки и кресты заменяют гласные в нескольких словах, находящихся в разных местах послания.

* Гвельфы — сторонники Папы Римского.

** Гибеллины — приверженцы императора Священной Римской империи.

В 1379 г. антипапа Климентий VII, за год до этого бежавший во французский город Авиньон, чтобы внести раскол в Римскую Католическую Церковь, объявив себя законным владельцем папского трона, повелел своей канцелярии ввести в действие новые шифры. Секретарь антипапы Габриэли Лавинде, работавший в его представительстве в одном из североитальянских городов-государств,

изготовил индивидуальные ключи для всех 24 корреспондентов антипапы. Ключи Лавинде, самые древние среди сохранившихся на Западе, сочетают в себе элементы кода и шифра. Помимо шифралфавита замены с пустышками, почти каждый такой ключ включает небольшой список из более десятка широко распространенных слов или имен, которым ставятся в соответствие двухбуквенные кодовые эквиваленты. Это самый ранний образец номенклатора — гибридной системы шифрования, которой в последующие 450 лет суждено было распространиться по всей Европе.

Сначала западные шифралфавиты предусматривали только однозначную замену каждой буквы открытого текста. Первый известный Западу случай многозначной замены имел место в шифре, который был изобретен в 1401 г. в Мантуанском герцогстве. Секретарь герцога ввел в шифр гомофоны для гласных букв, чтобы создать препятствия для любого человека, который попытался бы дешифровать перехваченное сообщение. Тот факт, что гомофоны применялись не для всех букв, а только по отношению к гласным, свидетельствует о знании криптоаналитических методов, основанных на частоте встречаемости знаков шифртекста.

Откуда взялись эти познания? Возможно, они самостоятельно родились в Западной Европе. Хотя верно и то, что соприкосновение с мусульманской цивилизацией во время крестовых походов вызвало на Западе бурное развитие естественных наук и что арабские математические трактаты нередко попадали в Европу через Испанию. Однако нет никаких документальных доказательств того, что криптоанализ попал в христианский мир из исламского. У арабов криптоанализ считался скорее разделом грамматики, чем частью естественных наук или математики, поскольку по традиции был тесно связан с языком Корана. Во всяком случае, труды Калкашанди, в которых давалось подробное объяснение методов дешифрования, так и не были переведены с арабского на европейские языки.

Развитие криптоанализа на Западе оказалось в прямой зависимости от расцвета дипломатии. С тех пор как государства стали поддерживать постоянные дипломатические отношения друг с другом, их послы, которых иногда иронично называли «почетными шпионами», регулярно отправляли к себе на родину пространные послания. Существовавшие между государствами соперничество и подозрительность вынуждали дипломатов зашифровывать свои депеши, поскольку их нередко перехватывали и вскрывали. К концу XVI столетия криптоанализ стал играть настолько важную роль, что в большинстве европейских государств были введены должности секретарей по шифрам, которые полный рабочий день были заняты зашифрованием и расшифрованием сообщений, а также дешифрованием перехваченных депеш.

Первым знаменитым западным криптоаналитиком стал венецианец Джованни Соро, в 1506 г. назначенный секретарем по шифрам Венецианской республики. Он прославился тем, что с успехом вскрывал шифры многочисленных европейских княжеств. Слава Соро была столь велика, что начиная с 1510 г папская курия присылала ему для вскрытия шифры, с которыми не могли справиться в Риме. В 1526 г. Папа Климентий VII* дважды направлял Соро перехваченные депеши для дешифрования, и оба раза Соро добился успеха. А когда одно из посланий Климентия попало в руки его противников, тот воскликнул: «Соро может вскрыть любой шифр!» — и направил Соро копию этого послания, чтобы выяснить, надежно ли оно зашифровано. Климентий успокоился, только когда Соро сообщил, что не может его прочесть. Хотя кто знает, не пытался ли Соро преднамеренно ввести Папу в заблуждение ложными заявлениями о надежности его шифра.

* Не путать Папу Климентия VII с аптипапой, носившим такое же имя.

В 1542 г. Соро получил двух помощников. С этого времени Венеция имела уже трех квалифицированных криптоаналитиков. Их помещение находилось во дворце венецианского правителя, где они работали за запертыми дверями. Никому не дозволялось их беспокоить, а им самим, по слухам, не разрешалось покидать свое рабочее помещение, пока не будет найден открытый текст очередной перехваченной криптограммы. Криптоаналитики также писали трактаты, в которых разъясняли методы своей работы. Труд Соро о дешифровании переписки на латинском, итальянском, испанском и французском языках, написанный им в начале XVI века, утерян. Но уцелели отрывочные записи его преемника, а также исследования в этой области других венецианских секретарей по шифрам.

Венеция была не единственным местом обитания искусных криптоаналитиков в эпоху европейского Возрождения. Римский Папа Павел III, сменивший Климентия VII, быстро сообразил, что не в его интересах посылать шифры для вскрытия за границу. В 1555 г. в папской курии была учреждена должность секретаря по шифрам. Первый успех пришел только через два года — в 1557 г.

папские криптоаналитики вскрыли шифр испанского короля Филиппа II, который тогда воевал с Папой Римским. А в 1567 г. отличился викарий собора Святого Петра в Риме, который менее чем за шесть часов сумел прочитать криптограмму, написанную «на большом листе бумаги на турецком языке, на котором викарий не знал и четырех слов».

Во Флоренции Пирро Музефили, граф Сассетский, с 1546-го по 1557 г. прочел множество шифрованных сообщений, вскрыв среди прочих номенклаторы, использовавшиеся в переписке между французским королем Генрихом II и его послом в Дании. Криптоаналитическая экспертиза Музефили была настолько квалифицированной, что многие приезжали к нему, как и к Соро, с просьбой вскрыть для них шифры. Среди клиентов Музефили был и король Англии, который прислал ему криптограмму, найденную в подметках пары золотых туфель, доставленных к его двору из Франции.

Жестокие и решительные герцоги Сфорца, правители Милана, также широко пользовались услугами криптоаналитиков. В 1474 г. один из секретарей Сфорца по имени Чикко Симонетта написал первый в мире трактат, посвященный исключительно криптоанализу. В нем Симонетта установил 13 правил вскрытия шифров простой замены, в которых сохранены разделители слов. Рукопись, написанная на трех кусках пергамента, начинается со слов:

«Первое необходимое условие состоит в выяснении того, написан ли документ на латинском или на местном языке, а это можно установить следующим образом: выясните, имеют ли слова в данном документе только пять различных окончаний, меньше или больше. Если их только пять или меньше, вы правы, считая, что документ написан на местном языке...»

В XVI веке не только итальянские дворы славились своими криптоаналитиками. Во Франции в дешифровании перехваченных депеш наиболее преуспел Филибер Бабу, занимавший пост первого государственного секретаря при короле Франциске I. Один наблюдатель описывает, как Бабу, «не имея алфавита, часто дешифровывал многие перехваченные депеши на испанском, итальянском и немецком языках, хотя он не знал ни одного из этих языков или знал очень плохо*, причем он упорно работал над сообщением дни и ночи напролет в течение трех недель, прежде чем разгадывал одно слово. После того как брешь была проделана, остальное происходило очень быстро и напоминало разрушение стен». Следует заметить, что в то время как Бабу не покладая рук работал на короля, король с удовольствием принимал у себя любовницу — прелестную жену Бабу. Бабу получил много милостей от короля, но трудно сказать, за что он их удостоился — за криптоаналитические ли успехи или за позволение наставлять рога.

* Дешифровать криптограмму на «неизвестном» языке можно при условии, что «незнание» означает только то, что человек не понимает смысла слов, как это имеет место в данном случае. Чтобы добиться вскрытия, у криптоаналитика должно быть общее представление об образовании и структуре слов языка. Очевидно, что чем лучше он знает язык, тем легче ему дешифровать криптограммы, открытый текст которых написан на этом языке. Если криптоаналитик никогда не виде ни одного предложения на данном языке, то чтение криптограммы почти невозможно, хотя чередование гласных и согласных, общее для всех языков, все же может подсказать некоторые пути к решению задачи.

В 1589 г. королем Франции стал Генрих IV, который сразу же был вынужден вступить в ожесточенную борьбу со Священной лигой — фракцией католиков, которые наотрез отказывались согласиться с тем, что протестант может носить европейскую корону. Священная лига во главе с герцогом Майеннским контролировала столицу и все другие крупные города Франции, получая большие подкрепления в виде живой силы и денег от испанского короля Филиппа II. Генрих был со всех сторон окружен противником. Но именно в это тяжелое для него время в его руки попала часть переписки Филиппа с испанским военачальником Хуаном Морео.

Письма Филиппа были зашифрованы, но у Генриха в то время работал некий Франсуа Виет, 49-летний адвокат, член тайного совета короля. В течение многих лет любимым развлечением Виета была математика. В наши дни Виета помнят как человека, которому обязана своим происхождением современная алгебра. В 1588 г. он прочел шифрованную испанскую депешу, адресованную Алессандро Фарнезе, герцогу Пармы, который командовал испанскими войсками Священной лиги. С тех пор Генрих передавал Виету все новые перехваченные депеши, чтобы выяснить, сможет ли он повторить свой успех.

Очередной крупный успех пришел к Виету только 15 марта 1590 г. В этот день он отправил королю Генриху полностью дешифрованное письмо Морео Филиппу II, которое содержало

подробности переговоров Морео с герцогом Майеннским. Письмо было зашифровано с помощью нового номенклатора, который Филипп специально дал Морео перед его отъездом во Францию. Но Виет не знал, что за день до этого Генрих разбил превосходящие силы герцога в битве при реке Иври, к западу от Парижа, придав несколько упражненческий характер задаче дешифрования письма Морео.

Тем не менее в письме Генриху, которое содержало открытый текст шифрованной депеши Морео, Виет, в частности, хвастливо написал: «Не волнуйтесь из-за того, что для Ваших врагов это будет повод сменить свои шифры и еще больше замаскироваться. Они неоднократно меняли их, и тем не менее их уловки были и всегда будут раскрыты». Из-за этой своей самонадеянности Виет однажды и попал в ловушку, благодаря которой один зарубежный дипломат выудил из Виета конфиденциальную информацию так же ловко, как это делал сам Виет, разгадывая секретный смысл таинственных иностранных символов. Венецианский посол во Франции Джованни Мочениго написал, что однажды он имел следующую беседу с Виетом:

«Он* только что сказал мне, что было перехвачено большое количество шифрованных писем испанского короля, а также императора** и других государей, которые он дешифровал. Когда я выразил большое изумление, он сказал мне:

— Я представлю вашему правительству веские доказательства этого.

* Виет

** Священной Римской империи

Он немедленно принес мне толстую пачку писем от упомянутых государей, которые он дешифровал, и добавил.

— Я хочу, чтобы вы также знали, что я знаю их шифр.

— Я не поверю этому, — сказал я, — пока не увижу сам.

Поскольку у меня было три моих шифра — обычный, которым я пользовался, второй, который я не применял, и третий под названием «dalle caselle»*, он раскрыл мне, что знает первый шифр. Затем, чтобы лучше разобраться в таком серьезном деле, я сказал ему:

— Вы, несомненно, знаете наш шифр «dalle caselle»?

* В буквальном переводе с итальянского — «из квадратиков»

— Чтобы его узнать, нужно изрядно попрыгать, — ответил он, подразумевая под этим, что ему известны только части шифра.

Я попросил его показать мне несколько наших дешифрованных писем. Он обещал мне, но затем больше не разговаривал на эту тему, а после того как он ушел, я уже ни разу не встречал его».

Мочениго доложил о разговоре с Виетом в Венецию, и вскоре по приказу из Венеции все действующие венецианские шифры были заменены.

Между тем из перехваченных им французских писем Филипп узнал, что Виет вскрыл шифр, который в Испании считался неуязвимым. Это рассердило Филиппа. Решив причинить хлопоты французам безо всякого ущерба для себя, он сообщил Папе, что Генрих вскрыл папские шифры с помощью черной магии, и попросил сурово наказать его за колдовство. Но такая тактика причинила ущерб престижу самого Филиппа. Папа, доверяя своим криптографам и зная от них о ненадежности испанских шифров, ничего не предпринял в отношении просьбы короля Испании. Сам же Филипп был осмеян всеми, кто прослышал об этой истории.

Одним из тех, кто, должно быть, смеялся больше всех, был фламандский дворянин Филипп ван Марникс, барон де Сент-Альдегонд, правая рука Вильгельма Оранского, стоявшего во главе объединенного восстания голландцев и фламандцев против Испании. Марникс, автор мелодии современного национального гимна Голландии, был также блестящим криптоаналитиком и только что закончил работу по вскрытию испанского шифра. Шифрованное письмо испанцев, прочитанное Марниксом, было перехвачено Генрихом IV во время осады Парижа. Отправителем письма был опять неудачливый Морео, а его адресатом — снова король Филипп.

Французский король лично передал эту испанскую криптограмму своему фламандскому союзнику-протестанту. Прочитав ее, Марникс обнаружил в ней оскорбительные выпады против герцога Пармы, который был также испанским губернатором Голландии. В августе 1590 г. Генрих повелел Марниксу отправить герцогу Пармы как саму криптограмму Морео, так и ее открытый текст, надеясь тем самым раздуть разногласия между ними. Однако герцог посчитал ниже своего

достоинства отвечать на клеветнические выпады испанского военачальника и не предпринял никаких ожидавшихся Генрихом действий против Морео.

Это был не первый случай вскрытия Марниксом испанских шифров: за 13 лет до этого он добился результата, который привел в действие цепь событий, завершившихся на плахе палача.

В 1577 г. Голландией правил испанский губернатор дон Хуан Австрийский, единокровный брат короля Филиппа. Честолюбивые замыслы дона Хуана не ограничивались крошечной Голландией. Он мечтал пересечь пролив Ла-Манш, высадиться с войсками в Англии, свергнуть королеву Елизавету, а затем жениться на обольстительной королеве Шотландии Марии и вместе с ней носить английскую корону. Филипп дал брату согласие на вторжение и на женитьбу. Правда, и то и другое должно было произойти лишь после того, как дон Хуан восстановит мир и спокойствие в Голландии.

Но Англия не дремала. Через своих шпионов на Европейском континенте министр Елизаветы Фрэнсис Уолсингем пронюхал о том, что против Англии замышляется что-то недоброе. Его подозрения оставались неподтвержденными до тех пор, пока в июне 1577 г. во Франции не были перехвачены несколько шифрованных писем дона Хуана. Письма были переправлены Марниксу, который через месяц вскрыл испанский шифр, использованный для их зашифрования. Особенность этого шифра заключалась в том, что каждая гласная открытого текста помимо буквенной и цифровой замен имела еще одно обозначение в виде завитушки. Если в открытом тексте согласная предшествовала гласной, то эту завитушку писали вместе с шифрованным знаком согласной, так что получался комбинированный символ, представлявший обе эти буквы.

11 июля Вильгельм Оранский сообщил содержание писем дона Хуана, дешифрованных Марниксом, Даниэлю Роджерсу, одному из агентов Уолсингема. Роджерс так написал об этом в своем докладе Уолсингему:

«Принц* сказал мне, что ее величество может понять, как было достигнуто соглашение между доном Хуаном и папским нунцием, если она ознакомится с письмами, написанными доном Хуаном и Эсковедо** в апреле прошлого года и перехваченными теперь. Затем он вызвал г-на де Сент-Альдегонда и поручил ему принести письма... Сент-Альдегонд принес девять писем. Все они были написаны по-испански. Большая часть каждого письма, за исключением одного, была зашифрована. Три письма были написаны доном Хуаном, причем два были адресованы королю***, а одно — министру короля Антонио Пересу. Автором остальных писем был Эсковедо, и они предназначались королю. Принц также показал мне письмо ла Ну****, в которое были вложены все вышеупомянутые письма, так как последний перехватил их во Франции. Я счел нужным сделать некоторые выписки по главным темам, содержавшимся в них».

* Вильгельм Оранский
** Эсковедо — секретарь дона Хуана
*** Испании
**** Франсуа де ла Ну. генерал гугенотов

Уолсингем, несомненно, был прельщен возможностями, открывшимися перед ним, когда через Роджерса он ознакомился с результатами работы Марникса по дешифрованию испанской корреспонденции. Поэтому он незамедлительно принял меры, чтобы обеспечить себе больший приток информации и при этом не зависеть от иностранных криптоаналитиков. С этой целью он направил в Париж одного талантливого юношу, который очень ловко расправлялся с шифрованными депешами. Это был Томас Фелиппес, первый знаменитый криптоаналитик из Англии.

В качестве курьера Уолсингема Фелиппес много путешествовал по Франции. По возвращении он стал одним из наиболее доверенных помощников Уолсингема. Фелиппес одинаково умело дешифровывал переписку на латинском, французском, итальянском и испанском языках. Единственное описание его внешности вышло из-под пера королевы Шотландии Марии Стюарт. Согласно ей, Фелиппес — блондин со светлой бородой, «низкого роста, весьма стройный, лицо изрыто оспинками, близорук, на вид ему можно дать 30 лет».

Эти нелестные замечания Марии выдают ее подозрения в отношении Фелиппеса — подозрения, которые не были безосновательными, ибо Фелиппес и его хозяин Уолсингем пристально следили за Марией по причинам, которые, в свою очередь, в равной мере являлись оправданными. Мария была бесспорной наследницей английского трона. Номинально она считалась также королевой Шотландии, хотя и была оттуда изгнана. Это была выдающаяся женщина: красивая, обладавшая даром большого личного обаяния, умевшая внушать преданность своим подданным, храбрая католичка, непоколебимо преданная своей религии, но вместе с тем неблагоразумная, упрямая, капризная.

Различные католические группировки не раз замышляли возвести ее на английский трон и таким образом восстановить господство римской Церкви. Многие годы Мария прожила пленницей в английских замках, и все это время Уолсингем настойчиво искал возможность раз и навсегда покончить со смертельной угрозой, которую для королевы Елизаветы представляла Мария.

Такая возможность представилась в 1586 г. Бывший паж Марии Энтони Бабингтон приступил к подготовке заговора. Вовлеченные в заговор придворные должны были убить Елизавету, организовать широкое восстание католиков в Англии и короновать Марию. Бабингтон также заручился поддержкой Филиппа II, который обещал прислать войска на помощь, как только Елизавета будет мертва. Чтобы получить согласие Марии, Бабингтон был вынужден вступить с ней в переписку.

Эта задача была не из легких. Мария была отрезана от внешнего мира и находилась под домашним арестом в загородном поместье. Один бывший семинарист по имени Гилберт Гиффорд, которого Бабингтон завербовал в качестве посыльного, придумал способ тайной доставки корреспонденции Марии в бочонке с пивом.

В основном эта корреспонденция посылалась в зашифрованном виде. Зашифровывал письма Марии один из ее двух доверенных секретарей. Мария часто отдавала им распоряжения о внесении изменений в используемые номенклаторы для повышения их стойкости. Кроме того, чтобы обеспечить безопасность своей переписки, Мария настояла на том, чтобы все письма сочинялись в ее апартаментах, зачитывались ей перед зашифрованием и опечатывались в ее присутствии.

Но ни Мария, ни Бабингтон не знали того, что, несмотря на тщательно разработанные меры предосторожности, их письма сразу же после написания доставлялись прямо Фелиппесу. Гилберт Гиффорд был двойным агентом и работал не только на Бабингтона, но и на Уолсингема. Шифрованные послания Марии читались Фелиппесом почти сразу же после того, как он их получал.

Уолсингем умышленно не препятствовал дальнейшему развитию заговора и прохождению тайной корреспонденции, надеясь на то, что Мария окажется замешанной в государственном преступлении. Его ожидания полностью оправдались. В начале июля Бабингтон в своем письме к Марии упомянул о планируемом вторжении испанцев, ее собственном скором освобождении и «казни соперницы, незаконно захватившей власть». Мария думала над ответом в течение недели. После тщательного составления ответа она поручила секретарю зашифровать его. Письмо было отправлено Бабингтону 17 июня. Оно оказалось роковым, поскольку в нем Мария подтверждала существование заговора и давала советы Бабингтону о способах «его успешного доведения до конца». Как только Фелиппес дешифровал письмо, он сразу же расценил его как смертный приговор Марии.

Но Уолсингем все еще не знал имен шести молодых придворных, которые должны были совершить убийство Елизаветы. Поэтому, когда письмо Марии попало к Бабингтону и тот его расшифровал, в конце письма была приписка, содержавшая просьбу сообщить имена «тех шести джентльменов, которые должны осуществить план». Автором подделки был Фелиппес.

Хитроумная затея Фелиппеса оказалась лишней. По предложению Уолсингема Бабингтону, как бы случайно, показали записку с требованием его ареста. Бабингтон спешно бежал, чтобы спасти себе жизнь. Узнав о его побеге, скрылись и шестеро молодых джентльменов, о которых шла речь. В течение месяца и они, и Бабингтон были пойманы. Суд приговорил их к смертной казни. Перед казнью Бабингтона заставили выдать шифр, которым он пользовался в переписке с Марией.

Этот шифр и письма Марии послужили главным обвинительным материалом на заседаниях суда, который признал Марию виновной в государственной измене. С величавым спокойствием встретила Мария объявление о том, что Елизавета подписала ей смертный приговор. 8 февраля 1587 г. в 8 часов утра она, еще раз проникновенно заявив о своей невиновности и помолившись вслух о благополучии своей Церкви и сына, с гордо поднятой головой взошла на эшафот, встала на колени и мужественно приняла от палача три удара топором. Так окончилась короткая жизнь Марии, королевы Шотландии, насильственную смерть которой ускорил криптоанализ.

О ПРОИСХОЖДЕНИИ ВИДА

«Мы с Дато гуляли в папских садах в Ватикане и переходили от одной темы к другой, изумляясь человеческой изобретательности, пока Дато не выразил своего неподдельного восхищения людьми, которые могут использовать то, что называют шифрами», — написал Леон Альберти в начале своего 25-страничного трактата, являющегося самой старинной из сохранившихся на Западе рукописей по криптоанализу.

Альберти был не только пионером в области криптоанализа, но и первым разработал вид шифров, к которому принадлежит большинство современных шифрсистем. Это многоалфавитная замена. Ее изобретение явилось большим шагом вперед, хотя она и не смогла вытеснить номенклаторы в течение более четырех столетий с момента своего появления на свет. Почему? Да потому, что по сравнению с номенклаторами многоалфавитная замена отнимала тогда у людей слишком много времени, а малейшая ошибка при письме была сопряжена с такими искажениями, что получатель сообщения не мог правильно расшифровать его даже при наличии верного ключа.

Альберти родился в 1404 г. Незаконнорожденный, но любимый сын в семье богатых флорентийских купцов, Альберти обладал выдающимися способностями. Его семья со щедрой заботой культивировала их, дав ему юридическое образование в университете в Болонье. После тяжелой болезни Альберти переключил свое внимание с юриспруденции на искусство и науку. Его талант был универсален. Он рисовал, сочинял музыку и считался одним из лучших органистов своего времени. Из-под его пера регулярно выходили поэмы, басни, комедии и научные трактаты.

Среди друзей Альберти был и секретарь Папы Леонардо Дато, который во время той памятной прогулки по ватиканским садам перевел разговор на криптоанализ.

«Вы всегда интересовались секретами бытия, — сказал Дато. — Что вы думаете о дешифровальщиках? Вы не пробовали свои силы в этом занятии?»

Альберти улыбнулся в ответ. Он знал, что в обязанности Дато входила работа с шифрами.

«Вы начальник папского секретариата, — поддразнил он Дато. — Не приходится ли и вам иногда пользоваться услугами дешифровальщиков в делах очень важных для его святейшества?»

«Поэтому я и заговорил об этом, — откровенно ответил Дато. — Занимая свою должность, я хочу научиться делать это самостоятельно, не прибегая к помощи посторонних лиц. Так что, пожалуйста, если у вас есть какие-нибудь новые идеи на этот счет, расскажите мне о них».

Альберти пообещал Дато подумать над его просьбой, и в результате в 1466 г. на свет появился трактат по криптоанализу. Он начинается с описания характерных особенностей латинского языка:

«Сначала я рассмотрю вопрос о количестве букв и те явления, которые зависят от количественных закономерностей. Здесь гласные претендуют на первое место... Без гласной нет и слога. Поэтому, если вы возьмете страницу какого-либо стихотворного или прозаического латинского текста и отдельно подсчитаете в строках гласные и согласные, то вы наверняка убедитесь, что гласных очень много... Если все гласные на одной странице будут насчитывать, скажем, 300 букв, то количество всех согласных, вместе взятых, составит около 400 букв. Я заметил, что среди гласных буква «О» хотя и встречается не менее часто, чем согласные, но реже других гласных... Когда в конце слова согласные следуют за гласной, этой конечной согласной всегда будет «Т», «S» и «Х», к которой может быть добавлена «С».

Затем Альберти коротко останавливается на особенностях итальянского языка и переходит к решению задачи вскрытия шифра на основе анализа повторяемости букв в тексте. Оставшаяся часть трактата посвящена вопросу повышения стойкости шифров.

В дальнейшем преклонный возраст не позволил Альберти развить идеи из области криптоанализа, изложенные им в своем трактате. Это за него сделал молодой одаренный человек по имени Джованни Порта.

Порта родился в Неаполе в 1535 г. Его воспитанием занимался образованный дядя. Уже в возрасте десяти лет Джованни сочинял очерки на латинском и итальянском языках. После путешествия по Европе он возвратился в Неаполь для завершения образования. Порте было всего лишь 28 лет, когда он опубликовал книгу под названием «О тайной переписке». Ее первые два раздела посвящены криптографии, а в оставшихся двух излагаются основы криптоанализа и рассматриваются лингвистические особенности, которые помогают при вскрытии шифров. Книга Порты содержит первое в Европе описание того, как следует вскрывать шифр простой замены, когда шифртекст не разделен на слова или разделен неправильно. Порта также предвосхитил всех других авторов, описав то, что считается вторым по значимости приемом в современном криптоанализе:

«..Когда тема переписки известна, исследователь может сделать проницательные предположения относительно слов, которые обычно употребляются в таком контексте. Эти слова можно без большого труда обнаружить, подмечая в текстах количество знаков, а также сходство и различие букв... Каждой теме характерны некоторые общие слова, которые сопутствуют ей, будучи необходимы. Например, в любви — это страсть, сердце, огонь, пламя, сгорать, жизнь, смерть, жалость, жестокость; на войне — это солдат, командир, генерал, лагерь, оружие, бороться и т. д. Таким образом, этот прием вскрытия, который не основан на анализе самих документов или на попытке разбить текст на гласные или согласные, может облегчить задачу».

В своей книге Порта также дал один мудрый совет, который и сегодня полезен криптоаналитику в той же степени, в какой он был уместен в Италии эпохи Возрождения:

«Необходимы самая полная сосредоточенность и усердие, чтобы свободная от посторонних мыслей голова, когда все остальное отложено в сторону, была всецело занята единственной задачей доведения начатого дела до успешного завершения. И все-таки, когда такая задача требует чрезмерного напряжения и необычных затрат времени, напряжение не должно быть непрерывным, не следует изнурять мозг сверх меры, ибо слишком большие усилия и продолжительная умственная нагрузка приводят к нервному истощению, после которого голова уже менее пригодна для подобных вещей и из нее уже не выжмешь ничего...»

А далее Порта делится с читателем своим собственным практическим опытом работы:

«Кроме того, далеко немаловажно, чтобы сообщение было написано рукой автора или искусного писца, ибо если перехваченное сообщение будет скопировано неправильно или если оно выйдет из-под руки человека незнакомого с искусством шифра, то в результате, поскольку правописание нарушено, любая интерпретация сообщения будет блокирована».

Подобный опыт приходит только к криптоаналитику, имеющему дело с сообщениями, в которых буквы часто бывают пропущены, переставлены или заменены на другие. Это случается лишь при обработке настоящих криптограмм. Задачи, встречающиеся в книгах по криптоанализу того времени, всегда безукоризненно составлены с точки зрения правописания и поэтому легко решаются. Скорее всего, Порта регулярно занимался криптоанализом, выполняя поручения папской курии.

В полной мере замечательные способности Порты проявились при решении наиболее трудной проблемы криптоанализа эпохи Возрождения — вскрытии многоалфавитных шифров. Несмотря на высокую оценку, которой эти шифры тогда были повсеместно удостоены, Порта отказался признать их неуязвимость и разработал для них методы вскрытия. Хотя эти методы и не универсальны, их основная ценность состоит в примененном Портой смелом подходе, который и привел его к успеху.

Для начала Порта попытался прочесть шифртекст, который его современники получали на специальном приспособлении для шифрования. Это приспособление состояло из внутреннего неподвижного диска, на который по часовой стрелке был нанесен алфавит открытого текста, и из внешнего подвижного с рядом причудливых шифрзнаков. Внешний диск после зашифрования очередной буквы поворачивался по часовой стрелке на один шаг. Порта заметил, что если в каком-либо слове открытого текста три буквы подряд стояли в алфавитной последовательности, один и тот же шифрзнак троекратно повторялся в получаемом шифртексте. Это помогло ему прочитать одну замысловатую криптограмму.

Затем Порта модифицировал разработанный им метод, чтобы дешифровать другую сложную многоалфавитную криптограмму. Она была составлена в соответствии с принципом, изложенным в 1553 г. итальянцем Джованни Белазо. Тот опубликовал брошюру под названием «Шифр синьора Джованни Белазо», в которой предложил использовать легко запоминаемый ключ. Буквы такого ключа последовательно выписывались над буквами открытого текста. Ключевая буква, которая стояла в паре с данной буквой открытого текста, указывала на шифралфавит, который следовало использовать для ее зашифрования.

По мнению Порты, в исследуемой им криптограмме троекратное повторение буквы шифртекста сигнализировало о том, что ключом с тремя буквами, расположенными в обычном алфавитном порядке, зашифрован открытый текст, в котором было три буквы в порядке, противоположном алфавитному. Рассуждая по этому поводу, Порта вплотную подошел к универсальному методу вскрытия многоалфавитных шифров, найти который он так стремился: «Поскольку... между первыми тремя «М» и этими же тремя буквами, повторенными в 13-м слове, находится 51 буква, я прихожу к выводу, что ключ повторен три раза, и правильно считаю, что он содержит 17 букв». Правда, Порта так и не извлек практическую выгоду из этого своего наблюдения. В результате многоалфавитный шифр продолжал считаться надежным в течение трех последующих столетий.

Многоалфавитные шифры, вероятно, время от времени все же вскрывались. Иногда удавалось просто угадать ключ. Существенную помощь оказывало и сохранение в криптограмме первоначального деления слов. Тогда криптоаналитик делал предположения о словах в открытом тексте и в результате восстанавливал часть использованного ключа. Далее он мог пытаться выписать остальную его часть или, если из этого ничего не выходило, стараться дешифровать другие места криптограммы. Такие эпизодические вскрытия многоалфавитных шифров нельзя считать вне пределов досягаемости людей эпохи европейского Возрождения.

В XVII веке авторы работ по криптоанализу иногда обращались к теме вскрытия многоалфавитных шифров. Правда, делали они это в весьма туманных выражениях, что

свидетельствовало об отсутствии знаний в данной области. Так, например, автор брюссельского «Трактата о шифрах», который продемонстрировал свои незаурядные криптоаналитические способности, вскрыв в 1676 г. французский королевский код для испанского короля, оказался бессилен, когда столкнулся с многоалфавитностью. Он смог лишь предложить метод опробования одной буквы открытого текста за другой до тех пор, пока в определяемом им ключе не появится имеющее смысл слово. Разумеется, он не сумел проиллюстрировать свой метод на практике: количество перебираемых комбинаций настолько велико, что он и сейчас продолжал бы заниматься опробованием букв. Слабая сторона предложенного им метода находится в заметном контрасте с техническим мастерством, продемонстрированным в остальной части его «Трактата о шифрах».

Время и место написания «Трактата о шифрах», неудача его автора с многоалфавитностью и работа на испанского короля позволяют сделать предположение, что это был криптоаналитик по имени Мартин, который фигурировал в другом инциденте, показавшем, насколько редким и случайным было вскрытие многоалфавитного шифра. Французский кардинал Рец поведал в своих «Мемуарах», как 8 августа 1654 г. он сбежал из замка в городе Нанте после двух лет заключения по политическим мотивам. Он, между прочим, писал о шифрах:

«У нас... был один шифр, который мы называли невскрываемым, так как нам всегда казалось, что никто не сможет проникнуть в его тайну, не зная согласованного между нами слова. Мы настолько доверяли ему, что никогда не боялись писать свободно и пересылать самые важные и самые конфиденциальные сведения с обычным курьером. Именно этим шифром я написал, что 8 августа совершу побег... Принц*, у которого был один из лучших дешифровальщиков в мире, его звали, кажется, Мартином, пользовался этим шифром вместе со мной.. Он сказал мне, что, по признанию Мартина, шифр был невскрываемым... Впоследствии с ним справился Ги Жоли**, который, хотя и не был профессиональным дешифровальщиком, сумел найти ключ и сообщил мне о нем...»

* Конде (Луи II Бурбон), французский полководец.
** Жоли Ги— советник трибунала в Париже и один из единомышленников Реца

Здесь Рецу явно хотелось показать, как мало можно доверять шифрам. Но тот факт, что счастливая догадка близкого друга Реца была единственным случаем вскрытия, скорее повышает ценность этого шифра, чем свидетельствует о его ненадежности.

Самое интересное вскрытие многоалфавитного шифра в годы господства номенклаторов принадлежит знаменитому человеку, имя которого стало нарицательным совсем в другой области: он был настолько одержим женщинами, что заставил служить своей страсти даже криптоанализ.

В 1757 г. он беседовал о магии и алхимии с одной знакомой дамой, некой мадам д'Юрфе. Она показала ему зашифрованную рукопись, в которой говорилось о превращении простых металлов в золото, и сказала, что ей не нужно держать эту рукопись под запором, поскольку ключ находится только у нее. Д'Юрфе дала ему рукопись со словами, что не верит в криптоанализ. Позже он написал в своих мемуарах:

«Через пять или шесть недель она спросила меня, расшифровал ли я эту рукопись с описанием процесса превращения. Я ответил, что расшифровал. Однако мадам д'Юрфе скептически заметила:

— Без ключа? Простите, но я считаю это невозможным.

— Не хотите ли вы, мадам, чтобы я назвал ваш ключ?

— Сделайте одолжение.

Затем я назвал ей слово — НАВУХОДОНОСОР* — и увидел ее удивление. Она заявила мне, что это невозможно, ибо она считала себя единственным обладателем этого слова, которое она держала в памяти и никогда не записывала.

* Навуходоносор — царь Вавилонии (с 605 г. до нашей эры), о котором упоминается в Библии как о жестоком деспоте, наказанном Богом за прегрешения скитаниями по пустыне на грани истощения.

Я мог бы сказать ей правду о том, что те же самые предположения, которые помогли расшифровать рукопись, дали мне возможность найти и это слово. Но, повинуясь какому-то капризу, я сказал ей что мне открыл его мой гений. Это выдуманное признание привязало мадам д'Юрфе ко мне. В тот день я стал господином ее души и не замедлил злоупотребить своей властью. Вспоминая об этом, я каждый раз испытываю чувство горечи и стыда...»

Однако «чувство горечи и стыда» не помешало ему изумить даму фокусом с ключевым словом

«НАВУХОДОНОСОР», а через некоторое время распрощаться с ней, «унося с собой ее душу, ее сердце, ее ум и все хорошие чувства, которые она оставила».

Кто же был этот криптоаналитик? Джакомо Казакова*.

* Казакова Джакомо — итальянский авантюрист и писатель, автор мемуаров с описаниями любовных похождений.

Может показаться, что множество случаев дешифрования должно было развеять миф о невскрываемости многоалфавитных шифров задолго до того, как в 1863 г. отставной майор прусской пехоты впервые опубликовал универсальный метод их вскрытия. Но это были изолированные случаи, отделенные друг от друга десятками, а иногда и сотнями лет. Многоалфавитность оставалась редким явлением, и сама ее непопулярность служила ей защитой. Если бы многоалфавитностью пользовались чаще, то, возможно, криптоаналитики давно бы проложили путь к общему решению. Но мир твердо остановил свой выбор на номенклаторе, поэтому мифу была суждена долгая жизнь.

Что касается человека, который в середине XIX века произвел переворот в криптоанализе, то о нем известно только то, что содержится в его послужном списке. В течение почти всей своей служебной карьеры Фридрих Казиский был офицером 33-го пехотного полка. Он родился 29 ноября 1805 г. в местечке Шлохау в Западной Пруссии, которое теперь называется Члухув и находится на территории Польши. В возрасте 17 лет Казиский поступил в полк. Через три года он был произведен в офицеры и получил чин лейтенанта, в котором прослужил 14 лет. Старшим лейтенантом он пробыл недолго, а затем получил звание капитана и должность командира роты, на которой находился 9 лет. Казиский вышел в отставку в 1852 г. в звании майора. В 1863 г. в Берлине вышла в свет его небольшая книга «Искусство тайнописи и дешифрования», ознаменовавшая начало новой эпохи в криптоанализе. Однако в то время она почти не вызвала откликов, и Казиский утратил интерес к криптоанализу. Он сделался рьяным любителем-антропологом, принимал активное участие в раскопках древних могил и писал о своей работе в научные журналы. Казиский умер 22 мая 1881 г., даже не догадываясь о том, что произвел настоящую революцию в криптоанализе.

ЭРА «ЧЕРНЫХ КАБИНЕТОВ»

Реальмон был осажден. Армия французского короля под командованием принца Конде окружила его на рассвете 19 апреля 1628 г. Однако гугеноты, укрывшиеся за зубчатыми стенами этого небольшого города на юге Франции, оказывали упорное сопротивление. Они с презрением отвергали все требования о капитуляции, заявляя, что скорее умрут, чем сдадутся.

Вскоре королевские солдаты захватили городского жителя, который пытался доставить зашифрованное сообщение войскам гугенотов за пределами Реальмона. Никто в окружении принца не сумел его прочесть. Только через неделю выяснилось, что перехваченное сообщение гугенотов может дешифровать юный отпрыск влиятельной семьи в городе Альби в десяти милях от Реальмона. Этот молодой человек, по слухам, интересовался шифрами.

Криптограмма была отвезена в Альби. Молодой человек прочитал ее сразу же. Выяснилось, что защитники Реальмона отчаянно нуждались в боеприпасах и что, не получив их, они будут вынуждены в скором времени капитулировать. Это была важная новость, потому что город по-прежнему отважно сопротивлялся, не показывая никаких признаков грядущей капитуляции. Осада города была продолжена, и 30 апреля 1628 г. Реальмон сдался. Так было положено начало карьеры человека, которому суждено было стать первым профессиональным криптоаналитиком во Франции. Это был Антуан Россиньоль.

Когда весть о роли Россиньоля в покорении Реальмона дошла до хитрого и предприимчивого кардинала Франции Ришелье, он немедленно присоединил Россиньоля к своей свите. Как раз вовремя. Армия католиков под командованием Ришелье, окружившая главный бастион гугенотов — крепость Ла-Рошель, перехватила несколько зашифрованных писем. Их легко прочитал молодой дешифровальщик из Альби. Его высокопреосвященству было доложено, что голодающие горожане с нетерпением ожидают помощи, которую англичане обещали прислать морем. Когда английский флот с продовольствием прибыл, он был настолько напуган превосходившими его по силе французскими кораблями, охранявшими подходы к Ла-Рошели, что даже не предпринял попытки пробиться к осажденным силой. Через месяц город капитулировал. Так был заложен фундамент великой традиции во французском криптоанализе.

Очень скоро Россиньоль перешел на королевскую службу. К 1630 г. его работа принесла ему

капитал, достаточный для того, чтобы выстроить себе элегантный особняк с очаровательным садом. Здесь для встреч с молодым криптоаналитиком неоднократно останавливался сам король Людовик XIII, когда возвращался в Париж из загородной резиденции.

Россиньоль необычайно плодотворно служил на поприще криптоанализа как при дворе этого монарха, так и в свите Людовика XIV. Например, взятие крепости Эден королевской армией было ускорено благодаря тому, что Россиньоль прочитал зашифрованную просьбу ее защитников о помощи, а после этого тем же шифром составил ответ, в котором жители города извещались о тщетности их надежд. Он тогда не рассказывал о том, сколько других городов вынудил сложить оружие и сколько предательств раскрыл среди высшей знати. Из-за этой скрытности некоторые придворные утверждали, что на самом деле Россиньоль не вскрыл ни одного шифра и что кардинал распространяет слухи о его способностях с целью отбить охоту у потенциальных заговорщиков. На смертном одре Людовик XIII охарактеризовал Россиньоля как человека, от которого зависит благополучие его подданных. Неудивительно, что через два года, 18 февраля 1645 г., преемник Ришелье кардинал Мазарини назначил Россиньоля государственным советником. Как и Ришелье, Мазарини пересылал ему перехваченные шифрсообщения. Например, в 1656 г. он направил зашифрованное письмо кардинала Реца с указанием Россиньолю прочесть его. При Людовике XIV Россиньоль часто работал в комнате, непосредственно прилегающей к кабинету короля в Версальском дворце. Отсюда шел поток дешифрованных сообщений, которые помогали королю определять политику Франции.

Одним из лучших друзей Россиньоля был поэт Буаробер, инициатор идеи создания Французской академии. Когда Буаробер попал в немилость при дворе, он пожаловался на свалившееся на него несчастье в стихотворении, адресованном своему влиятельному другу-криптоаналитику. Россиньоль показал это стихотворение Мазарини, который во время следующей аудиенции во всеуслышание похвалил Буаробера. Позже из чувства благодарности Буаробер написал 66-строчное стихотворение, в котором воспел Россиньоля. Это первая стихотворная ода, посвященная криптоаналитику. Некоторые ее строки звучат так:

31 Под небом нет ничего,
Что может скрыться от твоих глаз;
Эти глаза Линса*, которые, я думаю,
Проникают в наши самые сокровенные мысли.
35 Как изумительно твое искусство и ярко.
И как важна сила твоего мастерства!
Ибо с его помощью приобретаются провинции,
Раскрываются секреты всех королей,
И с малыми усилиями оно
40 Вынуждает сдаваться города и форты
……..
57 Действительно, твое мастерство
выше моего понимания,
И я никогда не постигну
Твой секрет; но я сейчас могу сказать,
60 Что оно служит тебе очень хорошо,
Что ты заслуживаешь этого. Не опасайся,
Твое мастерство будет благоприятствовать тебе годами
И судьба будет тебе улыбаться,
Пока войны омрачают землю.

* Линс — аргонавт, взгляд которого был настолько пронзителен, что проникал в недра земли.

Работа Россиньоля сделала его видной фигурой при дворе Людовика XIV. Россиньоль стал первым человеком, прославившимся исключительно благодаря своим криптоаналитическим способностям. Шарль Перро, который больше известен как автор сказок, включил краткую* биографию Россиньоля в свою книгу «Знаменитые люди, появившиеся во Франции в нынешнем веке», наряду с жизнеописанием Ришелье. Возникла даже легенда о том, что успехи Россиньоля во вскрытии шифров были настолько непостижимы для современников, что приспособление, с помощью которого открывают замок, когда ключ утерян, до сих пор называют во Франции

«россиньолем». Хотя сам факт такого употребления слова «россиньоль» имеет место, приписываемое ему происхождение ложно. В данном конкретном значении «россиньоль» появился в уголовном жаргоне почти за два века до рождения знаменитого криптоаналитика. Поскольку это слово также означает «соловей», не исключено, что взломщики приспособили его вместо слова «отмычка», поскольку щелканье и дребезжание воровского инструмента звучали для их ушей подобно пению птицы.

** На двух страницах.

Власть, богатство и королевская благосклонность, которые окружали Россиньоля при дворе, совершенно вскружили голову этому выходцу из провинции. Ведь это что-то значит — расхаживать по галереям королевского дворца с надменными принцами Франции, носить дорогие кружевные костюмы с огромными манжетами и чулки из самого белого шелка, играть в бильярд с самим королем и видеть это запечатленным на гравюре, а потом возвращаться домой во всем блеске своей славы. «Монсиньор, — сказал он однажды Ришелье о своих соседях с плохо скрываемой радостью, — они не смеют приближаться ко мне. Они считают меня фаворитом, меня, который живет с ними так же, как и раньше. Они изумляются моей любезности».

Тем не менее достижения Россиньоля действительно неоспоримы. С предельной ясностью он показал правителям Франции важность дешифрованных депеш для формирования их политики. Его работа демонстрировала это настолько эффективно, что королевский военный министр Лувуа энергично поощрял каждого, кто мог предоставить полученную таким образом информацию. Сохранилось письмо Лувуа, в котором он выражает благодарность за добытый шифр неприятеля, заверяя, что человеку, который может помочь прочесть несколько шифрованных писем, «его величество пожалует все, что он попросит».

Будучи в курсе успехов собственных дешифровальщиков, французские правители прекрасно осознавали необходимость повышения надежности своих шифрсистем. Их осмотрительность была нелишней. В 1774 г. Людовику XV был доставлен пакет из Вены. Когда французский король вскрыл его, он обнаружил там копии открытых текстов своей шифрованной корреспонденции. Людовику сообщили, что пакет прибыл от аббата Жоржеля, секретаря французского посла в Австрии. В Вене Жоржель встретился в полночь с человеком в маске, который в обмен на тысячу дукатов передал ему этот пакет и за дополнительное щедрое вознаграждение пообещал два раза в неделю передавать аббату все находки так называемого «черного кабинета» в Вене, в котором тайно вскрывалась и дешифровалась корреспонденция других стран.

В XVIII веке «черные кабинеты» стали распространенным явлением в Европе, а венский пользовался репутацией самого лучшего среди них. Он функционировал очень эффективно. Мешки с почтой, которая должна была доставляться утром посольствам в Вене, в 7 часов утра ежедневно привозили в помещение «черного кабинета». Там письма вскрывали, растапливая печати над свечой, отмечали порядок расположения страниц в конверте и передавали их помощнику директора. Он читал их и давал указания о снятии копий с самых важных документов. Длинные письма для экономии времени копировались под диктовку с использованием до четырех стенографистов одновременно. Если письмо было на незнакомом помощнику директора языке, он передавал его служащему кабинета, знавшему этот язык. Имелись переводчики со всех европейских языков, а когда появлялась потребность в новом языке, один из служащих срочно выучивал его. После копирования письма укладывались обратно в конверты, которые опечатывались поддельными печатями и возвращались на почту не позже 9.30 утра.

Через полчаса в «черный кабинет» прибывала новая почта. Она обрабатывалась таким же образом, хотя и с меньшей поспешностью, поскольку была транзитной. Как правило, эта корреспонденция возвращалась на почтовую станцию к 2 часам дня, хотя иногда ее задерживали и до 7 часов вечера. В 11 часов утра прибывала почта, перехваченная полицией. А в 4 часа дня курьеры привозили письма, которые отправляли зарубежные посольства. Эти письма снова вливались в поток отправляемой из Вены почтовой корреспонденции к 6.30 вечера. Скопированный материал попадал на стол к директору «черного кабинета», который отбирал особо интересную информацию и направлял ее заинтересованным лицам — ко двору, полицейским чиновникам, дипломатам и военачальникам. Таким образом венский «черный кабинет» со штатом всего в десять человек обрабатывал в среднем сотню писем за день.

Поражает то обстоятельство, что проворные пальцы сотрудников венского «черного кабинета» почти никогда не вкладывали письма в чужие конверты. Лишь однажды перехваченное письмо для

герцога Моденского было ошибочно опечатано очень похожей печатью правителя Пармы. Когда герцог заметил подлог, он отправил его в Парму с ироничной пометкой: «Не совсем мне, но и не вам». Оба государства заявили протест, но Вена отреагировала на него проявлением полнейшего недоумения. Тем не менее многие представители зарубежных стран при австрийском дворе знали о существовании в Вене «черного кабинета». Его наличие косвенно признали даже сами австрийцы. Когда английский посол с юмором пожаловался, что он получает копии вместо оригинальной корреспонденции, австрийский канцлер холодно заметил: «Как неловки эти люди!»

Перехваченная зашифрованная корреспонденция подвергалась криптоанализу. В нем венцы достигли замечательных успехов, которыми были обязаны своей прогрессивной системе работы с персоналом. За исключением чрезвычайных случаев, австрийские криптоаналитики одну неделю работали, а другую — отдыхали, чтобы избежать переутомления от интенсивной умственной нагрузки. Хотя их заработная плата была невысокой, за вскрытие шифров выдавались значительные премии. Несколько меньшая премия полагалась за дешифрование по украденным ключам. Например, в 1833 г. криптоаналитики получили 3/5 суммы, предназначенной для премий, за чтение шифровок французского посланника. В течение одной ночи ключ к его шифру был тайно изъят, скопирован и снова водворен в шкаф в спальной комнате секретаря французской дипломатической миссии в Вене.

Существенным стимулом в работе было и королевское признание выдающихся заслуг австрийских криптоаналитиков. Карл VI вручал им премии лично, а эрцгерцогиня Мария-Терезия часто беседовала с сотрудниками «черного кабинета» о надежности используемых шифров и о достижениях других стран в криптоанализе.

Подготовка криптоаналитиков также была нацелена на получение от них максимальной отдачи. Для работы в «черном кабинете» набирали молодых людей в возрасте примерно двадцати лет с высокими моральными качествами. Они должны были бегло говорить по-французски и по-итальянски, знать математику. Сначала их держали в полном неведении относительно подлинного характера предстоящей деятельности и обучали созданию надежных шифров, а затем подвергали испытанию — смогут ли они вскрыть разработанные ими же шифры. Неспособным подыскивали другую государственную службу, а остальных посвящали в секреты криптоаналитического мастерства и посылали в другие страны для лингвистической практики. После вскрытия первого шифра их жалованье удваивалось. Кроме того, для молодого человека открывалась перспектива стать квалифицированным специалистом, который за достигнутые успехи получает аудиенцию у монарха со всеми вытекающими отсюда привилегиями.

Хорошую возможность взглянуть на достижения венского «черного кабинета» дают письма барона Игнаца Коха, который руководил им с 1749-го по 1763 г. Например, 4 сентября 1751 г. он послал австрийскому послу во Франции некую дешифрованную корреспонденцию, позволявшую, по его словам, «гораздо лучше понять основные политические принципы, которыми руководствуется правительственный кабинет во Франции». А еще через две недели он написал: «Это восемнадцатый шифр, который мы вскрыли в течение года... К сожалению, нас считают чересчур способными в этом искусстве, и мысль о том, что мы можем вторгнуться в их корреспонденцию, побуждает иностранные дворы непрерывно менять ключи, иначе говоря, посылать каждый раз более трудные в смысле дешифрования сообщения». К достижениям венского «черного кабинета» относится чтение шифрованной переписки Наполеона, Талейрана, множества других зарубежных политических деятелей и дипломатов.

В XVIII веке в Англии также функционировал свои «черный кабинет». В отличие от венского, он не имел собственного помещения. Поэтому его небольшой штат экспертов работал большей частью дома, получая материалы через посыльных. У английского «черного кабинета» отсутствовала четкая организационная структура, старший дешифровальщик был в нем просто первым среди равных. Финансирование «черного кабинета» осуществлялось за счет денег, отпускавшихся министерству почт Англии из дополнительных доходов парламента. Во всей стране только около тридцати человек знали о том, что «черный кабинет» читает иностранную дипломатическую переписку. С ней знакомились только король и несколько его главных министров. Однако несмотря на соблюдаемую секретность, большинство деловых людей в Англии предусмотрительно шифровало свою корреспонденцию или доверяло ее частным посыльным. И немудрено — ведь английский закон о почте от 1711 г. давал правительственным служащим право вскрывать любые почтовые отправления на основании ордеров, которые они же себе и выдавали.

Английский «черный кабинет» прочитывал в среднем две или три шифрованные депеши за неделю. Его криптоаналитики успешно вскрывали шифры Австрии, Греции, России, Турции, Франции, а также Неаполя, Саксонии, Сардинии и других итальянских государств. Позднее к этим

странам присоединились и Соединенные Штаты Америки. К примеру, архив французской корреспонденции, перехваченной в XVIII-XIX веках, состоит из пяти томов, насчитывающих в общей сложности более 2000 страниц. К ним дополнительно прилагаются еще три тома ключей к французским шифрам. Испанское досье состоит из трех томов на 872 страницах. В нем собраны сообщения, перехваченные англичанами с 1719-го по 1839 г. Не все испанские шифровки были прочитаны непосредственно после того, как были перехвачены. Многие ждали своей очереди до тех пор, когда их накапливалось достаточно много для успешного дешифрования или когда появлялась необходимость в их чтении.

В 1723 г. два криптоаналитика английского «черного кабинета» выступили в качестве свидетелей в палате лордов, где судили епископа Фрэнсиса Эттербери по обвинению в заговоре. Поскольку главные изобличающие Эттербери улики были найдены в дешифровках Эдварда Уиллеса и Энтони Корбире, лорды «сочли уместным вызвать в суд этих дешифровальщиков, дабы убедиться в достоверности их дешифрования». Уиллес и Корбире показали под присягой, что переписка Эттербери была дешифрована ими независимо друг от друга, поскольку один из них находился в провинции, а другой — в столице, и тем не менее результаты дешифрования совпали.

Эттербери попытался поставить под сомнение достоверность открытых текстов, представленных Уиллесом и Корбире. Подсудимый поднял такой шум, что ему и его адвокату было приказано удалиться, а лорды проголосовали за предложение о том, «что, по мнению палаты, любые вопросы дешифровальщику, которые могут привести к раскрытию способов или тайн дешифрования, противоречат общественной безопасности». Голосование было положительным, и дешифрованные тексты были приняты в качестве доказательства виновности Эттербери. Он был отрешен от должности и изгнан из королевства.

Эра «черных кабинетов» в Европе была недолгой. Бурные политические события середины XIX века привели к ограничению абсолютной власти европейских монархов и их полицейских ведомств. Провозглашенные принципы свободы и равенства были несовместимы с цензурой переписки. В июне 1844 г. волна протестов со стороны общественности по поводу перлюстрации писем вынудила английское правительство прекратить перехват дипломатической переписки. В Австрии двери венского «черного кабинета» закрылись в 1848 г. А во Франции «черный кабинет», который уже со времен Великой французской революции дышал на ладан, в этот год также прекратил свое существование.

За океаном не было ни «черных кабинетов», ни платных криптоаналитиков. Тем не менее и там криптоанализ сыграл положительную роль — помог американским колониям занять достойное место среди других стран мира.

Эта история началась в августе 1775 г. Булочника Годфри Венвуда навестила в Ньюпорте его бывшая любовница. Она попросила Венвуда помочь передать одно письмо английским офицерам. У патриота-повстанца Венвуда зародилось сомнение. Он уговорил любовницу отдать письмо для доставки по назначению и уехать, прежде чем его невеста узнает о ее посещении. Но Венвуд не отослал письмо, а вскрыл его и обнаружил три страницы, заполненные странными символами и цифрами. Это укрепило его подозрения.

В конце сентября Венвуд прибыл в штаб генерала Джорджа Вашингтона, чтобы показать ему письмо. Главнокомандующий повстанческими войсками не сумел прочитать криптограмму и распорядился допросить бывшую любовницу Венвуда. Она призналась, что письмо ей передал ее очередной любовник — доктор Бенджамин Черч. Вашингтон был поражен. Черч являлся генеральным инспектором госпиталей. Процветающий бостонский врач, он только накануне просил об отставке с поста директора госпиталей. Вашингтон отклонил эту просьбу из-за своего «нежелания расстаться с хорошим инспектором». Мог ли такой известный человек состоять в тайной и, возможно, предательской переписке?

Когда Черча допросили, он с готовностью признался, что письмо принадлежит ему и адресовано брату Флемингу, который находится в Бостоне. Если письмо расшифровать, то обнаружится, что в нем нет ничего криминального. И хотя Черч неоднократно торжественно заверял в своей преданности делу освобождения из-под английского колониального гнета, он не изъявил готовности дословно изложить содержание письма.

Вашингтон занялся поисками людей, которые смогли бы прочесть письмо Черча. Когда стало известно, что Вашингтону нужны криптоаналитики, несколько человек с готовностью предложили свои услуги. 3 октября Вашингтон получил от них открытый текст письма. В нем Черч доносил английскому главнокомандующему о снабжении американцев боеприпасами, их продовольственных запасах и численности войск. Письмо заканчивалось словами: «Соблюдайте всяческую

предосторожность, не то я погиб».

Черча заключили в тюрьму, а затем в 1780 г. выслали в Вест-Индию. Небольшая шхуна, на которой он плыл, пропала без вести. Так первый американец, лишившийся свободы в результате умелого использования криптоанализа, потерял вдобавок и жизнь.

В то время как в ходе американской революции появлялись все новые и новые шифровальные системы, криптоанализ переживал период застоя. Главная причина крылась в том, что за редким исключением, как, например, в случае с Черчем, криптограммы не удавалось перехватить. И лишь когда война с англичанами близилась к своему завершению, было захвачено достаточное количество сообщений для криптоанализа. Большинство из них было дешифровано Джеймсом Ловеллом, которого можно по праву назвать отцом американского криптоанализа.

Ловелл родился 31 октября 1737 г. в Бостоне. В 1756 г. он окончил Гарвардский университет и в течение 18 лет преподавал в средней школе. В 1777 г. Ловелл был избран депутатом конгресса и вскоре стал известен благодаря своему рвению и трудолюбию.

Криптоаналитические успехи Ловелла пришлись очень кстати. Осенью 1781 г. заместитель английского главнокомандующего в Америке Чарльз Корнуоллис перебросил свои войска на север — из Каролины в Вирджинию. Будучи убежден, что для того, чтобы удержать южные земли, сначала нужно овладеть севером, он выступил по направлению к побережью в надежде получить подкрепления по морю от своего шефа, генерала Генри Клинтона, находившегося в Нью-Йорке. Корнуоллис планировал подчинить себе Вирджинию, затем покорить Каролину и известить его величество, короля Георга III, о том, что с восстанием в Америке покончено.

Именно в это время американский командующий на юге Натаниэль Грин направил конгрессу несколько перехваченных английских криптограмм, которые в его штабе никто не мог прочитать, присовокупив их к своему общему донесению. Эта шифрованная английская корреспонденция оказалась перепиской между Корнуоллисом и некоторыми из его подчиненных.

Донесение Грина было зачитано в конгрессе 17 сентября. Четырьмя днями позже Ловелл расшифровал приложения к донесению. К сожалению, из-за быстрого развития событий добытая Ловеллом информация не принесла много пользы. Но найденные Ловеллом ключи вполне могли пригодиться когда-нибудь в будущем. В своем письме Вашингтону Ловелл написал: «Не исключено, что противник намерен и далее зашифровывать свою переписку... Если это так, то Ваше превосходительство, возможно пожелает извлечь для себя пользу, дав Вашему секретарю указание снять копию ключей и замечаний, которые я через Вас направляю...»

Более проницательным Ловелл быть не мог. Вскрытый им шифр действительно служил также и для связи между Корнуоллисом и Клинтоном. К тому времени Корнуоллис отошел к Йорктауну, чтобы дождаться подкреплений от Клинтона. Но Вашингтон с 16-тысячным войском окружил город, а французский адмирал граф де Грасс с 24 кораблями блокировал помощь англичанам с моря. 6 октября Вашингтон писал Ловеллу: «Мой секретарь снял копии с шифров и с помощью одного из алфавитов сумел расшифровать параграф недавно перехваченного письма лорда Корнуоллиса сэру Клинтону». Эта информация помогла Вашингтону оценить реальное положение дел в английском лагере.

Тем временем для связи с Корнуоллисом Клинтон снарядил два небольших судна, которые он отправил из Нью-Йорка 26 сентября и 3 октября. Оба они были захвачены повстанцами. При этом одно из них прибило к берегу, где англичанин, который вез пачку шифрованных депеш, спрятал их под большим камнем, прежде чем его захватили в плен. Потом, как выразился один американец, «в результате непродолжительной беседы и пообещав прощение», повстанцы уговорили англичанина отыскать спрятанные депеши. Поиски заняли около двух дней.

Ловелл получил эти депеши 14 октября и тотчас же принялся за дело. Успех не заставил себя долго ждать, так как к своей радости Ловелл обнаружил, что они зашифрованы тем же шифром, что и остальная переписка Корнуоллиса. В одной из прочитанных Ловеллом депеш, в частности, говорилось:

«Милостивый государь! Ваша светлость может быть уверена, что я делаю все, что в моих силах, чтобы оказать вам помощь непосредственными действиями, а полученные мной сегодня от адмирала Грейвса* заверения дают мне основание полагать, что к 12 октября мы сумеем преодолеть трудности, если позволит ветер и не произойдет ничего непредвиденного. Это, безусловно, не исключает неудачного исхода, а посему, если я получу от вас известие, ваши пожелания будут для меня руководящими, и я буду настойчиво придерживаться своей идеи непосредственного действия...»

* Грейвс — командующий английским флотом у берегов Америки.

Через пять дней после того, как Ловелл закончил дешифрование, Корнуоллис капитулировал. Но победа повстанцев была не совсем полной. Вашингтон понял это, когда на следующий день он наконец получил от Ловелла копии дешифрованных депеш. Не теряя ни минуты, Вашингтон переправил их де Грассу, корабли которого должны были воспрепятствовать попытке оказания помощи Корнуоллису Грейвсом и Клинтоном. Будучи предупрежден, французский адмирал основательно подготовился к нападению англичан. 30 октября он заставил английский флот отступить и тем самым приблизил окончательную победу американцев в Войне за независимость.

КАК ИЗБИРАЛИ АМЕРИКАНСКОГО ПРЕЗИДЕНТА

В декабре 1863 г. начальник почтового отделения Нью-Йорка Абрам Уэйкман, просматривая корреспонденцию перед отправлением, наткнулся на письмо, адресованное некому Александру Кейту в город Галифакс в Новой Шотландии. Про Кейта было известно, что он часто переписывается с агентами южан. Поэтому Уэйкман передал письмо Кейта военному министру, который, вскрыв конверт, установил, что письмо зашифровано.

В течение двух дней сотрудники военного министерства тщетно пытались разгадать таинственные знаки перехваченной криптограммы. Затем она была передана трем шифровальщикам президента Линкольна — Бейтсу, Чэндлеру и Тинкеру, которые вызвались ее прочитать. Они быстро установили, что неизвестный автор письма использовал для его зашифрования как обычный алфавит, так и 5 различных шифралфавитов. Но он поступил неблагоразумно, разделив слова письма запятыми и ограничившись одним алфавитом в пределах каждого слова. Бейтс, Чэндлер и Тинкер нашли слово, состоявшее из 6 букв, в котором вторая и шестая буквы повторялись. Затем следовало слово из 4 букв, за которым, в свою очередь, шла фраза, посланная клером: «reaches you»*. Они решили, что за этой последовательностью шифрзнаков должна скрываться фраза «before this»**. Бейтс предположил, что в письме использован шифр, подобный тому, который применялся для обозначения цен в магазине в Питтсбурге, где он когда-то давно работал посыльным.

* «Дойдет до вас»
** «Прежде чем это»

Эта догадка позволила значительно продвинуть вперед процесс дешифрования криптограммы. Выявление знаков, обозначавших место отправления и дату сообщения — «Нью-Йорк, 18 декабря 1863 г.», также дало ощутимые результаты. Действуя таким образом, три шифровальщика в присутствии президента Линкольна, который нетерпеливо прохаживался около них, за четыре часа прочли шифрованное письмо, которое, в частности, гласило:

«Нью-Йорк, 18 декабря 1863 г.

...Два парохода отбудут отсюда примерно на Рождество... 12 тысяч нарезных мушкетов пришли точно по адресу и отправлены в Галифакс в соответствии с инструкциями. Мы сможем захватить еще два парохода, как намечено... прежде чем это* дойдет до вас. Цена 2000 долларов. Нам нужно больше денег... Пишите как прежде...»

* Письмо

Два дня спустя была перехвачена и быстро дешифрована еще одна криптограмма, адресованная Кейту. В ней говорилось: «Передай Мемминджеру*, что у Хилтона все станки находятся в собранном виде и все матрицы будут готовы к отправке 1 января. Гравировка печатных форм превосходная». Таким образом, из письма явствовало, что формы для печатания денег южан изготовлялись в Нью-Йорке. Гравера Хилтона легко нашли в Манхэттене. В последний день года полицейские совершили налет на его жилище, захватили печатные станки и матрицы, а также уже отпечатанные деньги на сумму в несколько миллионов долларов. Конфедерация лишилась оборудования для изготовления бумажных денег, в которых она остро нуждалась. Главную роль во всем этом деле сыграли криптоаналитические способности, проявленные тремя молодыми шифровальщиками Линкольна. За это каждый из них получил прибавку к жалованью в размере 25 долларов в месяц.

* Мемминджер Кристофер — министр финансов Конфедерации

А что же южане? Учитывая то, что они порой не могли правильно расшифровать свои собственные сообщения, неудивительно, что им не удалось прочесть ни одного шифрованного сообщения северян. Хотя конфедераты перехватывали телеграфные сообщения Севера и их кавалерия время от времени захватывала одновременно открытый и шифрованный тексты этих сообщений, а также сами шифры, южане так и не смогли разобраться в шифрпереписке янки. Этому факту было бы трудно поверить, если бы конфедераты сами не признали его, напечатав в своих газетах несколько шифрованных сообщений с просьбой дешифровать их.

Последовавшая капитуляция южан отнюдь не приостановила криптоаналитических разработок, начатых еще во время Гражданской войны. Триумф одной из них ознаменовался появлением сенсационной статьи, напечатанной 7 октября 1878 г. газетой «Нью-Йорк трибюн». В заметке, помещенной под броским заголовком «Перехваченные шифрованные телеграммы», приводился открытый текст нескольких криптограмм. Впервые в истории США криптоанализ был призван сыграть решающую роль в американской политике.

Дело в том, что в результате подсчета голосов, поданных на выборах президента в 1876 г., впереди оказался кандидат от Демократической партии Самуэль Тилден, получивший на четверть миллиона голосов больше, чем его соперник от Республиканской партии Рутерфорд Хейс. Но как распределятся решающие голоса выборщиков — это зависело от того, какие из противоречивых результатов голосования, проведенного дважды во Флориде, Луизиане, Южной Каролине и Орегоне, будут признаны действительными. Конгресс создал специальную комиссию для решения этого вопроса. А комиссия приняла решение отдать все спорные голоса выборщиков Хейсу. Это обеспечило ему большинство всего в один голос в коллегии выборщиков и пост президента страны.

На сессии конгресса, последовавшей за выборами президента, была назначена еще одна специальная комиссия для расследования упорно распространявшихся демократами слухов о покупке республиканцами голосов выборщиков. В ходе расследования комиссия конфисковала более 600 шифртелеграмм, которые были посланы различными политическими деятелями и их доверенными людьми во время избирательной кампании в четырех штатах. Остальные американская телеграфная компания «Вестерн юнион» к тому времени уже успела уничтожить, чтобы показать, что гарантирует тайну доверенной ей переписки. В 1878 г. 27 шифртелеграмм были тайно переданы в прореспубликанскую газету «Нью-Йорк трибюн» в надежде на то, что, будучи дешифрованы, они поставят демократов в затруднительное положение.

За несколько недель до этого один из самых близких политических советников Тилдена Мэнтон Марбл написал открытое письмо в нью-йоркскую газету «Сан», печатный орган демократов. В нем Марбл противопоставлял темным делам республиканцев открытость Тилдена. Поэтому редактор «Нью-Йорк трибюн» Уайтлоу Рейд не раздумывая согласился, когда председатель Республиканской партии предложил ему включить в редакционные статьи газеты шифртелеграммы демократов в качестве ответа на письмо Марбла в «Сан». Демократы почувствовали себя весьма неуютно, когда сотрудники «Нью-Йорк трибюн» на ее страницах стали отпускать злые шутки по поводу этих загадочных документов, вопрошая, где же хваленая открытость демократов.

Но Рейд решил не ограничиваться публикацией шифртелеграмм своих политических противников. Полагая, что предание гласности содержания переговоров, которые демократам приходилось вести под покровом шифра, поставит их в затруднительное положение, он взялся за его вскрытие.

Многие читатели, движимые намеками, содержавшимися в редакционных статьях газеты, предлагали свои варианты дешифрования опубликованных шифртелеграмм, но при проверке все они оказались неверными. Рейд даже попытался обратиться к самому Тилдену, когда он случайно встретился с ним в августе 1878 г.: «Я сообщил ему, что у нас имеется вся шифрпереписка, которая проходила между его домом и Флоридой, и шутливо попросил его указать ключ. Я сказал ему, что мы не можем прочитать ее, и выразил пожелание, чтобы он помог нам. Он улыбнулся, покраснел, как невинный ребенок, и прошел мимо». Дело не сдвигалось с мертвой точки.

Между тем газета «Детройт пост» сумела узнать от одного из демократов о том, каким шифром пользовались его соратники по партии во время предвыборной кампании в Орегоне. Шифровальщик отыскивал нужное слово в «Домашнем английском словаре», который был издан в Лондоне в 1876 г., определял порядковый номер этого слова на странице, отсчитывал 4 страницы назад и брал на ней соответствующее слово в качестве кодового обозначения. Для расшифрования полученного сообщения его адресат поступал наоборот.

4 сентября один из редакторов «Нью-Йорк трибюн» Джон Хассард, основываясь на открытии газеты «Детройт пост», опубликовал несколько открытых текстов дешифрованных криптограмм, из

которых следовало, что в Орегоне демократы стремились подкупить одного республиканского выборщика и что сделка не удалась только из-за задержек с передачей ему денег.

Но «Домашний английский словарь» мало помогал в дешифровании сообщений демократов, присланных из других трех штатов. Не рассчитывая больше на постороннюю помощь, Рейд предложил своим сотрудникам как следует заняться их дешифрованием. За дело взялись Хассард и Уильям Гросвенор, экономический обозреватель «Нью-Йорк трибюн». Причем Хассард работал над криптограммами столь упорно, что простудился, заболел туберкулезом и последующие десять лет, оставшиеся ему до смерти, думал лишь о своем выздоровлении.

Позднее Рейд вспоминал: «Оба они работали чрезвычайно хорошо, работали независимо друг от друга, честно сравнивая результаты и прекрасно сотрудничая друг с другом... Хассард несколько раньше начал работать в этой области и заслуживает особой похвалы. Но Гросвенор был в равной степени способным и, как я сейчас припоминаю, достиг почти такого же успеха. Иногда он и Хассард подходили к дешифрованию одной и той же криптограммы с различных сторон и после неоднократных неудач, наконец, находили решение в один и тот же вечер...»

Одновременно с Хассардом и Гросвенором над чтением криптограмм, которые Рейд привел в редакционных статьях «Нью-Йорк трибюн», работал молодой математик из военно-морской обсерватории США в Вашингтоне Эдвард Холден. В своих мемуарах Холден написал по этому поводу: «К 7 сентября 1878 г. я открыл закономерность, с помощью которой можно было безошибочно найти любой ключ к самым трудным и хитроумным из этих телеграмм». Он обратился в «Нью-Йорк трибюн», которой понравилась идея нанять профессионального математика. Хассард выслал ему большое количество криптограмм. Однако к тому времени Хассард и Гросвенор независимо от Холдена разработали свои криптоаналитические методы и сумели опередить его в чтении некоторых криптограмм*. Рейд утверждает, что ни одну из дешифрованных Холденом криптограмм «Нью-Йорк трибюн» не получила раньше, чем эти же самые криптограммы были прочитаны Хассардом и Гросвенором. Поэтому результаты работы Холдена рассматривались лишь как подтверждение правильности дешифровок Хассарда и Гросвенора.

* Дешифрование сообщений демократов Хассардом, Гросвенором и Холденом стало возможным благодаря наличию большого количества телеграмм, зашифрованных с помощью одного и того же ключа.

Результат превзошел все ожидания. Общественность негодовала по поводу непорядочности демократов и восхищалась изобретательностью дешифровальщиков. Тысячи читателей расшифровывали криптограммы с помощью ключей, опубликованных в «Нью-Йорк трибюн», и с удовлетворением отмечали правильность решений. К тому же до выборов в конгресс оставалось всего несколько недель. На них республиканцы одержали внушительную победу.

Часть дешифрованных телеграмм была адресована на дом Тилдену — его племяннику У.Т. Пелтону. И хотя Тилден клялся, что совсем не знал, чем занимается у него в доме племянник, и что все было сделано без его разрешения, репутация Тилдена была навсегда запятнана. Это разоблачение положило конец его надеждам стать президентом. Газета «Сан» была вынуждена печально заметить: «Г-н Тилден уже никогда не будет кандидатом в президенты ни от какой партии». Даже биограф Тилдена, питавший к нему большую симпатию, признал, что «в результате дешифрования телеграмм демократов республиканцы получили преимущество, которое обеспечило им победу на президентских выборах в 1880 г.». Так криптоанализ помог избрать американского президента.

ДВА ГЕНИЯ

В любой научной дисциплине найдется очень немного работ, которые по праву можно назвать гениальными. На протяжении XIX столетия непревзойденными трудами по криптологии считались работы Альберта и Порта. Изложенные ими концепции оставались актуальными потому, что в криптологии не происходило никаких существенных изменений. Связь поддерживалась с помощью гонцов, и поэтому основным видом засекречивания сообщений оставался номенклатор. Но с изобретением телеграфа эти концепции быстро устаревают. Новые условия потребовали новых идей. И в 1883 г. криптология получила их в форме труда под названием «Военная криптография». Его автором был Жан Вильгельм Губерт Виктор Франсуа Александр Огюст Керкхофф фон Ньювенгоф, родившийся 19 января 1835 г. в голландском городе Нуте в семье богатого помещика, принадлежавшего к одной из самых древних фамилий фламандского герцогства.

После окончания семинарии Керкхофф отправился в Англию для изучения английского языка. Там он пробыл полтора года, а затем переехал во Францию, где поступил в Льежский университет. Получив две ученые степени, одну — в области литературы, другую — в области науки, Керкхофф в течение четырех лет преподавал в Голландии. В 1863 г. он возглавил кафедру современных языков в высшей школе в Мелуне, крупном городе к юго-востоку от Парижа. В течение всех этих лет он активно занимался разнообразной научной деятельностью, которая отражает широту его интересов. Он читал лекции по истории литературы, организовал курсы по изучению английского и итальянского языков, представлял французское археологическое общество на международном конгрессе в Бонне. Познания Керкхоффа были настолько разносторонними, что в разные периоды жизни он преподавал латинский, немецкий и греческий языки, историю и математику.

«Военная криптография» впервые была опубликована двумя частями в журнальном варианте в январе и феврале 1883 г., а позднее в том же году была переиздана в виде отдельной брошюры. Керкхофф обладал уникальной способностью выделять главное в любом предмете и всего на 64 страницах своей книги сумел найти ответы на многие вопросы, которые встали перед криптографией в результате возникновения новых условий. При этом предложенные им решения были разумными и хорошо обоснованными.

Его второе достижение заключается в подтверждении принципа, состоящего в том, что только дешифровальщики могут со знанием дела судить о надежности шифра. Разумеется, об этом догадывались и до него. Поэтому-то криптоаналитик Россиньоль и создал довольно стойкий номенклатор, а в XVII веке в Англии составлением номенклаторов занимались исключительно дешифровальщики. Но после закрытия «черных кабинетов» об этом принципе все как-то позабыли. Во всяком случае, данный критерий оценки надежности номенклатора не применялся к более сложным шифрам, которые предлагались в XIX веке. Их изобретатели, вместо того чтобы вынести свои шифры на суд криптоаналитиков, обладавших большим практическим опытом, стремились оценить их стойкость сами. Они подсчитывали, сколько веков уйдет на опробование всех ключей, или доказывали, что практически невозможно пробиться через какой-либо элемент шифра. Керкхофф изучил это негативное явление и вынес о нем такое суждение:

«Я поражен тем, что наши ученые и профессора преподают и рекомендуют для применения в военное время системы, ключи к которым, несомненно, менее чем за час откроет самый неопытный криптоаналитик. Такое чрезмерное доверие к некоторым шифрам можно объяснить лишь недостатком научных исследований в области шифровального дела после упразднения «черных кабинетов»... Можно также полагать, что многочисленные утверждения некоторых авторов, а также отсутствие серьезных работ по искусству прочтения тайнописи способствовали распространению самых ошибочных идей о стойкости наших шифрсистем».

Выступая против этого, Керкхофф показал, что единственным средством просвещения в шифровальном деле является криптоанализ и что только карабкаясь вверх по крутой и тернистой тропе криптоанализа можно получить истинное представление о стойкости шифров. Вся его книга проникнута именно этой идеей и поэтому является, по существу, работой по криптоанализу. В ней Керкхофф доказал, что в новых условиях криптоанализ — единственное верное средство испытания надежности шифров. Такого мнения продолжают придерживаться до сих пор.

Если бы Керкхофф на этом остановился, то он и тогда бы оставил глубокий след в истории криптоанализа. Но он сделал больше, разработав криптоаналитические методы, играющие важную роль в современной теории дешифрования. Один из них называется наложением, или перекрытием, и представляет собой способ дешифрования многоалфавитных систем замены. Данный способ не ставит никаких ограничений, нужно только иметь несколько сообщений, зашифрованных одним и тем же ключом. Криптоаналитик выписывает эти сообщения одно под другим так, чтобы буквы, зашифрованные одной и той же буквой ключа, образовывали единую колонку. Каждую такую колонку можно потом дешифровать как обыкновенную одноалфавитную замену.

Таковы многочисленные поразительные достоинства книги «Военная криптография», которая стоит первой в ряду крупных трудов по криптологии. Это место она занимает благодаря ясности изложения, солидной научной основе и предложенным криптоаналитическим методам. Ее мог написать только человек с такими широкими теоретическими познаниями, как Керкхофф.

В отличие от выдающегося теоретика криптоанализа Керкхоффа, француз Этьен Базери был великим практиком. Шифры буквально плавились под действием интенсивной работы его мозга. Архивные криптограммы, правительственные шифры, тайная переписка заговорщиков — ничто не выдерживало неукротимого напора Базери.

Базери родился 21 августа 1846 г. в семье полицейского в маленькой рыбацкой деревушке на

берегу Средиземного моря. Его отец хотел, чтобы он посвятил свою жизнь сельскому хозяйству. Однако через пять дней после того, как ему минуло 17 лет, Базери записался рекрутом во французскую армию. Во время франко-прусской войны он сражался на фронте и был взят в плен, но бежал, переодевшись каменщиком. После окончания войны Базери медленно, но неуклонно продвигался вверх по служебной лестнице.

Интерес к криптоанализу возник у Базери, когда он пытался прочесть криптограммы, помещаемые в газетах в колонках для личной переписки. Пикантными подробностями этой переписки он развлекал своих сослуживцев. Однажды в 1890 г., когда его эскадрон стоял в Нанте, Базери заявил во всеуслышание своим друзьям-офицерам в штабе корпуса, что известный ему французский военный шифр можно читать без ключа. Раздался взрыв общего смеха. Не рассмеялся только один человек. Это был командир корпуса генерал Шарль Фэй, один из лучших офицеров своего времени. Он принял брошенный Базери вызов и прислал ему несколько телеграмм, зашифрованных с помощью этого шифра. Базери дешифровал их. Все были изумлены, а военное министерство спешно изготовило новый шифр. Ознакомившись с криптограммами, подготовленными с использованием нового шифра, Базери вскрыл его еще до того, как он был введен в действие.

Слава Базери достигла Парижа, и в августе 1891 г. армейское командование направило его в распоряжение криптобюро французского МИД. Именно в эти годы жизни Базери больше всего времени посвящал криптоанализу. Едва только новые шифры появлялись на свет, как он вскрывал их. Базери начал заниматься шифрами прошлого, когда начальник генерального штаба попросил его помочь в прочтении шифрованных сообщений для изучения военных кампаний Людовика XIV. Базери успешно справляется с поставленной задачей, но на этом не останавливается — заодно ему удается вскрыть номенклаторы Франциска I, Франциска II, Генриха IV, Мирабо и Наполеона. Обнаружив, что шифры французского военного гения XIX века были чрезвычайно слабыми, в заголовке своей монографии о них Базери презрительно поставил слово «шифры» в кавычки. А в 1892 г., когда французские власти арестовали и предали суду группу анархистов, в числе доказательств фигурировали дешифрованные Базери криптограммы.

В 1899 г., даже после того, как Базери официально вышел в отставку, министерство иностранных дел Франции продолжало пользоваться его услугами. В том же году оно рекомендовало его полиции как человека, который может прочесть шифрованные сообщения, захваченные в апартаментах некого Шевильи, участвовавшего в заговоре с целью восстановления монархии. Благодаря серии правильных догадок в отношении вероятных слов Базери в конце концов дешифровал эти сообщения. О них Базери позднее дал показания на судебном процессе по делу заговорщиков. Умер Базери в 1931 г. в возрасте 85 лет.

ДЕЛО ДРЕЙФУСА

15 октября 1894 г. капитан французского генерального штаба Альфред Дрейфус прибыл к 9.00 в здание военного министерства в Париже. Он пришел туда на заседание, в котором, кроме него, приняли участие еще несколько старших офицеров. Вскоре после начала заседания Дрейфус написал под диктовку несколько строк. Его почерк оказался похожим на почерк, каким был написан имевшийся в распоряжении участников заседания документ, в котором разглашались секретные сведения военного характера. Один из присутствовавших офицеров поднялся и торжественно произнес: «Капитан Дрейфус, именем закона я арестовываю вас. Вы обвиняетесь в государственной измене». На этом заседание было закрыто, а арестованного отправили в тюрьму.

Сперва арест хранился в тайне. Продолжалось это недолго, и 1 ноября парижская «Либр пароль» опередила все остальные газеты, поместив сообщение под кричащим заголовком «Государственная измена. Арест офицера-еврея А. Дрейфуса». В нем указывалось, что Дрейфус являлся шпионом Германии или Италии.

2 ноября 1894 г. произошло другое важное событие, которое впоследствии оказало большое влияние на ход дела Дрейфуса. Военный атташе Италии полковник Александр Паницарди телеграфировал в Рим. Сообщение Паницарди было зашифровано. Эта шифртелеграмма стала самым сенсационным секретным донесением тех лет, когда для освещения помещений все еще применялась газовая лампа. В переводе с итальянского выглядела она примерно так:

«Рим. Генштаб
913 44 7836 527 3 88 706 6458 71 18 0288 5715 3716 7567 7943 2107 0018 7606 4891 6165

Паницарди».

Мало меняла она свой вид и в переводе на многие другие европейские языки.

На парижском телеграфе с шифртелеграммой Паницарди поступили точно так же, как и со всеми другими дипломатическими криптограммами, проходившими через столичный телеграф французского министерства почт: сняли копию и отправили в МИД для возможного дешифрования.

В ноябре 1894 г. криптоаналитическое бюро (криптобюро) французского МИД состояло из семи человек. Его начальник Шарль-Мари Дармье, которому через две недели после того, как туда поступила шифртелеграмма Паницарди, исполнилось 59 лет, пришел в архивный отдел министерства в самом начале своей карьеры сорок лет назад, проработал в нем три года, а затем перешел в криптобюро французского МИД. Заместителем Дармье был Альбин-Шризостом Марно 54 лет от роду, который попал на эту должность в тот же день, когда Дармье был назначен начальником мидовского криптобюро. Двое других сотрудников имели стаж работы в нем более двадцати лет, а остальные — менее семи. Три более пожилых сотрудника являлись кавалерами ордена Почетного легиона, а остальные четверо имели ученые степени в области права.

После ознакомления с шифртелеграммой на языке оригинала французские криптоаналитики высказали предположение, что Паницарди применил итальянский коммерческий код, изданный несколько ранее в том же 1894 г. инженером Паоло Баравелли. Этот код под названием «Словарь для шифрованной переписки» состоял из четырех разделов: таблицы I, в которой гласные буквы и знаки препинания были представлены цифрами от 0 до 9; таблицы II, где согласные буквы, грамматические конструкции и вспомогательные глаголы были обозначены парами цифр; таблицы III, состоявшей из слогов, заменяемых на трехзначные цифровые группы, и таблицы IV — собственно словарной части кода, в которой слова и фразы представлялись четырехзначными цифровыми группами. Некоторые четырехзначные цифровые группы могли быть оставлены пустыми, с тем чтобы пользователь кода заполнил их по своему усмотрению.

На мысль о коде Баравелли мидовских криптоаналитиков навел один забавный случай, который произошел за несколько месяцев до описываемых событий. В июне началась таинственная ежедневная шифрованная переписка по телеграфу между племянником короля Италии графом Туринским и герцогиней Грациоли, высокой темпераментной итальянкой, проживавшей в фешенебельном отеле «Виндзор» в Париже. Руководитель военной разведки полковник Жан Сандгерр сразу учуял подозрительный запах шпионажа. Помощник министра иностранных дел Франции Морис Палеолог, в обязанности которого входил также контроль за работой сотрудников криптобюро МИД, напротив, заявил, что от этой шифрпереписки пахло только любовными отношениями. На том и разошлись.

Вскоре Сандгерр ворвался в кабинет Палеолога с тоненькой книжечкой в руках. От книжечки пахло отнюдь не любовными отношениями, а просто женскими духами. Но важнее оказался не источаемый запах, а ее содержимое. Это был код Баравелли. Один из агентов Сандгерра выкрал код, обнаружив его в доме герцогини, когда она была на скачках. А через два дня Палеолог получил переводы открытых текстов прочитанных шифртелеграмм. По его словам, в них выражались «лишь простые, элементарные, естественные чувства». Все же одна четырехзначная группа, которая повторялась в большинстве шифртелеграмм, осталась недешифрованной. По-видимому, это была пустая группа кода Баравелли, которую влюбленные заполнили сами. Романтически настроенный Палеолог и его криптоаналитики решили для себя, что это мистическое число из четырех цифр означало нечто необычное, незабываемое и возвышенное. Опровержения от влюбленной пары не последовало.

Приобретенный опыт криптоанализа зашифрованной по Баравелли переписки оказался очень поучительным для французских криптоаналитиков из МИД. Они уяснили для себя суть уловки, которую Баравелли предусмотрел для обеспечения секретности кода, имевшегося в свободной продаже. Однако дело осложнялось тем, что каждый пользователь кода Баравелли мог применить эту уловку по-своему, и это требовало от криптоаналитиков дополнительного приложения сил и времени для определения содержания уловки в каждом конкретном случае. Первая же предпринятая ими попытка прочитать шифртелеграмму Паницарди показала, к их великому огорчению, что итальянский полковник этой уловкой воспользовался.

Заразившись всеобщим возбуждением, вызванным разоблачением Дрейфуса, криптоаналитики без труда пришли к выводу, что в криптограмме должна фигурировать фамилия арестованного капитана. Элементы открытого текста, имевшиеся в коде Баравелли, позволяли разбить слово «ДРЕЙФУС» для зашифрования только следующим однозначным способом: «ДР», «Е», «Й», «ФУС»

были найдены в таблице III. В закодированном виде слово «ДРЕЙФУС» выглядело бы так: «227 1 98 306». И в шифртелеграмме Паницарди имелась аналогичная последовательность кодовых групп, составленных из одно-, двух- и трехзначных чисел: «527 3 88 706».

С помощью этого наблюдения криптоаналитики МИД уже 3 ноября получили предварительный вариант дешифровки, который гласил: «...арестован... капитан Дрейфус, который не был в сношениях с Германией...». Этот весьма предположительный текст, в котором единственным точно определенным словом являлась фамилия Дрейфус, был показан Сандгерру, поддерживавшему тесные контакты с дешифровальщиками МИД. Тот сразу же им заинтересовался, ибо, будучи дешифрованной, шифртелеграмма Паницарди могла подтвердить или опровергнуть виновность центральной фигуры сенсационного скандала, в котором оказалась замешана и служба Сандгерра.

К 6 ноября криптоаналитики пришли к варианту открытого текста шифртелеграммы, который они полагали точным, за исключением конца. Этот вариант гласил: «Если капитан Дрейфус не состоял в сношениях с вами, было бы целесообразно... сделать официальное опровержение... Наш агент предупрежден». Последняя его часть о том, что итальянский агент предупрежден, как раз и полагалась предположительной. Тем не менее Сандгерр, склонный считать Дрейфуса предателем, попросил на время рабочие материалы дешифровальщика с последовательно выписанными вариантами под каждой кодовой группой и с вопросительными знаками, указывавшими на предположительный характер последних трех слов. Он доложил о прочитанной шифртелеграмме начальнику генштаба Шарлю Буадеффру, сказав при этом: «Ну, генерал, вот еще одно доказательство виновности Дрейфуса». Но Сандгерр поторопился. К 10 ноября криптоаналитики выписали, наконец, окончательный текст криптограммы: «Если капитан Дрейфус не состоял в сношениях с вами, было бы целесообразно поручить послу сделать официальное опровержение, чтобы избежать комментариев в печати».

Эта версия, которая никоим образом не говорила о виновности Дрейфуса, была доведена до сведения Сандгерра 28-летним подчиненным Палеолога Полем Генри Филиппом Горацием Делорош-Верне, служившим связным между дешифровальщиками МИД и армией (в 1908 г. его назначат начальником мидовского криптобюро, и он будет занимать эту должность в течение пяти лет). Сандгерр был недоволен новой версией. Он сообщил о ней своим начальникам, заметив при этом, что, «когда имеешь дело с министерством иностранных дел, никогда нельзя быть уверенным в отношении всего этого — у них немного не хватает точности». Тогда у одного из подчиненных Сандгерра, 38-летнего артиллерийского майора Эрнста Маттона, который служил армейским связным с МИД, появилась идея, навсегда положившая конец всякому скептицизму. Он предложил пойти на хитрость и вынудить Паницарди послать шифртелеграмму, открытый текст которой был бы известен французам. Ее дешифрование подтвердило бы или опровергло правильность вскрытия шифрованного сообщения Паницарди о Дрейфусе. Маттон составил сообщение, включив в него слова которые предположительно встречались в открытом тексте шифртелеграммы Паницарди, а также имена собственные, которые можно было разбить при шифровании на отдельные слоги или буквы только однозначно. Он искусно придал этому сообщению такой важный характер, что Паницарди не мог не обратить на него внимания и не телеграфировать о нем в Рим. В сообщении говорилось о неком А., который находился в городе Б. и должен был через несколько дней отбыть в Париж, имея при себе мобилизационные документы, которые он достал во французском генеральном штабе. Маттон попросил одного двойного агента подбросить это сообщение итальянскому военному атташе.

Паницарди попался на уловку, зашифровав сообщение почти дословно и отослав его по телеграфу в Рим 13 ноября. Криптоаналитики из МИД, не зная, что в генштабе имелся открытый текст, дешифровали эту шифртелеграмму и передали полученную информацию, ввиду ее военного характера, в генштаб. Когда Поль Генри-и-так-далее Делорош-Верне принес туда дешифрованный текст шифртелеграммы Паницарди от 13 ноября, Маттон сказал: «Одну минуточку, сейчас достану оригинал». Он пошел в кабинет и принес текст собственноручно написанного им сообщения. Оба текста были почти идентичны.

Тем не менее Буадеффр отказался разрешить представить открытый текст шифртелеграммы Паницарди на первом судебном процессе по делу Дрейфуса в качестве доказательства, заявив прокурору, что поскольку в процессе дешифрования возникло несколько вариантов, а последующие варианты были точнее предыдущих, то это обстоятельство сводило на нет ценность шифртелеграммы как доказательства. Дрейфуса признали виновным.

Итак, сам факт существования шифртелеграммы Паницарди скрыть не удалось. Тогда настроенные против Дрейфуса офицеры подсунули на последующих судебных процессах и

заседаниях апелляционного суда фальшивую версию ее открытого текста, которая подтверждала виновность Дрейфуса: «Капитан Дрейфус арестован, военный министр имеет доказательства его связей с Германией. Заинтересованные лица информированы под большим секретом. Мой агент предупрежден». Эта версия была сфабрикована исходя из различных предположений, содержавшихся в рабочих материалах дешифровальщика, взятых на время Сандгерром. Ее истинность опровергалась наличием слов «доказательства» и «связи» которые никак не могли быть эквивалентом открытого текста для группы «0288» в криптограмме.

Наконец, 27 апреля 1899 г. шифртелеграмму Паницарди дешифровали заново по решению суда. Результат был, конечно, тот же, что получился первоначально. Правда, одно наличие правильного открытого текста шифртелеграммы итальянского военного атташе не могло служить доказательством невиновности Дрейфуса. Понадобилось еще семь лет, чтобы полностью восстановить его в правах. Но демонстрация того, как были использованы неправильные варианты дешифрования с целью раздуть дело против Дрейфуса, явно помогла реабилитировать этого французского офицера.

ЛИТЕРАТУРНЫЙ КРИПТОАНАЛИЗ

Первые шаги литературного криптоанализа связаны с появлением рассказа американского писателя Эдгара По «Золотой жук». Этот рассказ и по сей день остается непревзойденным художественным произведением на тему о дешифровании.

Про По можно сказать, что он неизбежно должен был заинтересоваться криптоанализом. Хотя По неоднократно пространно рассуждал о логике и писал рассказы с логично построенными сюжетами, он увлекался и такими иррациональными предметами, как френология и гипноз. А поскольку криптоанализ обладал качествами, которые импонировали По в науках, и вместе с тем от криптоанализа исходил неземной свет мистики, двойственный характер этой области человеческих знаний пришелся впору раздвоенной натуре По. Научность импонировала интеллекту писателя, а таинственность была созвучна его эмоциям.

Первое упоминание о криптоанализе у По появилось в статье «Загадочное и головоломное», опубликованной в номере филадельфийской газеты «Александерс уикли мессенджер» от 18 декабря 1839 г. После напечатания загадки, поставившей в тупик одного из читателей газеты. По написал:

«Мы сочувствуем нашему корреспонденту, оказавшемуся в затруднительном положении, и спешим помочь ему, особенно поскольку мы сами имеем склонность к загадкам. Несмотря на анафемы, провозглашаемые умниками, мы считаем хорошую загадку стоящей вещью. Решение загадок дает наилучшее средство упражнения аналитических способностей... Для обоснования этой идеи можно написать солидную статью в журнал. Было бы весьма полезно также показать, в какой большой степени строгий метод пронизывает процесс решения загадки. Это утверждение верно настолько, что можно дать свод правил, с помощью которых любая в мире загадка может быть решена очень быстро. Возможно, это звучит странно. Но это не более странно, чем общеизвестный факт, что действительно существуют правила, с помощью которых легко дешифровать любые виды иероглифического письма, то есть письма, где вместо букв алфавита используются произвольные знаки».

А в сноске к этому замечанию По читаем:

«Например, вместо «а» поставьте «+» или любой другой произвольный знак, вместо «b» поставьте «а» и т. д. Замените таким образом весь алфавит, а затем используйте получившийся алфавит для письма. Написанное будет прочтено путем использования надлежащего метода. Можете проверить это. Пусть кто-нибудь напишет нам такое письмо. Мы обещаем прочитать его незамедлительно, независимо от того, насколько необычными или произвольными будут в нем знаки».

В редакцию газеты посыпались письма. Корреспонденты зашифровывали тексты сумбурным набором звездочек, вопросительных знаков, цифр, знаков параграфа, а один прислал «самые безобразные и смешные иероглифы, какие только можно придумать (в типографии газеты не оказалось ни одного печатного знака, который хотя бы отдаленно напоминал какой-нибудь из них)». Поток писем был столь обилен, что По обратился к своим читателям: «Неужели люди считают, что у нас нет других занятий, кроме чтения иероглифов? Или, может быть, думают, что мы бросим свои дела и превратимся в колдунов? Кто нам подскажет, как решить эту дилемму? Если мы не справимся со всеми присланными задачами, их составители подумают, что мы не можем решить их, а мы как раз можем. Если же решать их все, то нам вскоре придется выпускать газету, в десять раз превосходящую объем «Бразер Джонатан»*. До этого дело не дошло, а большое количество присланных в редакцию

писем предоставило По возможность объяснить, почему он предпочел бросить вызов именно шифрам: «Мы говорили, что можем вскрыть и раскроем любой шифр определенных свойств, который нам пришлют, и мы сдержали наше обещание более чем десятикратно».

* «Бразер Джонатан» — нью-йоркская газета с форматом полосы 60x90 см.

Всего в 15 номерах газеты «Александерс уикли мессенджер» По опубликовал открытые тексты 11 дешифрованных им криптограмм. Для 16 криптограмм он дал только ответы, про 3 другие он просто сообщил, что они дешифрованы, а 6 не дешифровал: одну потерял, с одной не успел ознакомиться, одна была написана карандашом и стерлась, две оказались «подделками»*, а в одной число различных шифрзнаков составляло 51, и поэтому она нарушала принцип однозначности, который По изложил в своей статье от 18 декабря 1839 г.

* Ложные криптограммы

За все эти месяцы По ни разу не проговорился об используемых методах дешифрования криптограмм, хотя читатели неоднократно просили его поделиться своим секретом: «Откройте же нам вашу тайну, мы так любим чудеса». А По поддразнивал их: «А что мы получим взамен? Это удивительный секрет, и он вполне стоит того, чтобы за него заплатили. Пусть нам пришлют список сорока подписчиков с деньгами, и мы подробно объясним весь наш метод работы». По понимал, что именно тайна разжигала интерес у читателей, и в следующем номере газеты отказался от своего первоначального намерения: «Поразмыслив, мы решили пока не раскрывать нашего метода дешифрования».

Открытые тексты криптограмм, опубликованные в «Александерс уикли мессенджер», стали тем фундаментом, на котором покоится слава По-криптоаналитика. Однако надо признать, что легенда о почти сверхъестественной криптоаналитической одаренности По была создана людской молвой и его способностями по части саморекламы, с помощью которых он непомерно преувеличил значение своих довольно рядовых побед. Например, один из друзей По написал в газету о том, как По дешифровал криптограмму «за гораздо меньшее время», чем потребовалось для ее зашифрования, и По сразу же опубликовал это письмо. Через год после смерти По легенда о нем разрослась до невероятных размеров. Некий священнослужитель из Массачусетса рассказал, как По прочитал криптограмму «за пятую часть времени, потребовавшеюся на ее запись», и выразил мнение, что «самым глубоким знатоком и самым большим мастером дешифровального дела всех времен был, несомненно, Эдгар Аллан По».

Прошло время, и миф о «большом мастере дешифровального дела всех времен» растаял. Однако о его былой славе криптоаналитика нет-нет да и вспоминают. Один из современных исследователей жизни и творчества По, например, утверждает, что криптоаналитические способности По были «весьма незаурядными». Конечно, они были незаурядными по сравнению с обычными людьми. Ограничившись вскрытием простейших шифров, По не поднялся выше уровня простого любителя. Спорить о том, почему он избрал такой путь — из-за боязни потерпеть крах с более сложными шифрами или из-за нехватки времени, бесполезно.

В мае 1840 г. По ушел из «Александерс уикли мессенджер». Через год, когда он стал редактором выходившего в Филадельфии журнала «Грэхемс мэгэзин», По снова принялся разрабатывать «золотую жилу», которую открыл в «Александерс уикли мессенджер». В своих «Заметках о знаменитостях Франции», опубликованных в номере за апрель 1841 г., По почти в тех же выражениях, что и три года назад, вызвался дешифровать любую из криптограмм, которые читатели пожелают ему прислать.

В ожидании реакции на свой вызов По написал статью «Несколько слов о тайнописи» и поместил ее в июльском номере «Грэхемс мэгэзин». Статья представляет собой мешанину сведений по криптологии, преподнесенных живо и бойко, однако содержит очень мало нового. Примечательным является разве что афоризм, ставший классикой криптоанализа: «Человеческая изобретательность не в состоянии создать шифр, который человеческая же изобретательность не смогла бы вскрыть».

1 июля друг По писатель Ф. Томас, проживавший в Вашингтоне, прислал ему две криптограммы, полученные от своего приятеля, который принял вызов, брошенный По в апрельском номере «Грэхемс мэгэзин». Одну из них По дешифровал сразу же, а другую несколькими днями позже. 4 июля, окрыленный успехом, По отослал Томасу открытый текст криптограмм, потребовав взамен хвалебных отзывов. Славословия в адрес По не заставили себя долго ждать и были включены им в

августовский номер «Грэхемс мэгэзин».

Из всего написанного По в бытность журналистом наибольшим успехом пользовалась тема вскрытия шифров. Поэтому он прекрасно понимал, что рассказ, в котором фигурирует шифрованная переписка, уже сам по себе покажется необычным. Если же в нем хоть чуть-чуть потолковать про методы криптоанализа, то есть раскрыть тайну, которой По два года терзал своих читателей, рассказу обеспечен верный успех.

«Золотой жук» впервые был опубликован в 1843 г. и явился вершиной литературной работы По с привлечением криптоанализа. С тех пор По больше ничего не писал на эту тему, хотя в течение еще двух лет он читал криптограммы, присылавшиеся ему читателями. Потом он перестал заниматься и этим, жалуясь в письме другу, что, «отдавшись вскрытию шифров, я потерял времени больше чем на тысячу долларов».

На первых страницах «Золотого жука» описывается жизнь главного героя рассказа Уильяма Леграна, ведущего уединенный образ жизни на острове. С ним живет старый слуга-негр по имени Юпитер. Легран увлекается естественными науками и обнаруживает новый вид насекомого — золотистого жука. На подобранном на берегу обрывке пергамента он рисует находку для своего друга, который в первом лице и рассказывает об этих событиях. Рассказчик случайно оказывается возле огня с обрывком пергамента. Рассматривая обрывок, он замечает красноватый рисунок человеческого черепа. Познакомившись с рисунком, Легран погружается в задумчивость. В течение следующего месяца он ведет себя все более и более странно. Однажды к рассказчику приходит Юпитер, и по просьбе Леграна, все они, вооружившись лопатами, отправляются в лес. Остановившись у большого дерева, Легран заставляет Юпитера влезть на него, отыскать череп на конце ветви и опустить золотого жука в глазницу. Определив с помощью жука и дерева направление, они роют землю и извлекают спрятанное Киддом* сказочное сокровище. Таинственные обстоятельства отыскания Леграном сокровища проясняются, когда он объясняет, как с помощью огня проявил на пергаменте криптограмму, написанную невидимыми чернилами, а затем дешифровал ее.

* Киддом — шотландский пират, грабивший английские суда, казнен в Лондоне в 1701 г.

Рассказ изобилует нелепостями и ошибками. Кусок пергамента был найден возле «остатков лодки, походившей на большую корабельную шлюпку», которая, «видимо, пролежала здесь очень долго, ибо сходство с деталями шлюпки едва улавливалось». Это была шлюпка, на которой Кидд доставил свое сокровище на берег. Мог ли пергамент долгие годы оставаться на одном и том же месте? А если и мог, то разве на нем, как на дереве шлюпки, не сказалось бы действие разрушительных сил?

По указал, что невидимые чернила — это «кобальтовый королек, растворенный в нашатырном спирте». Но к сожалению, такой раствор дает азотнокислый кобальт, который легко растворяется в воде. Разве после многих десятилетий, в течение которых пергамент валялся на берегу, могли на нем остаться какие-либо следы чернил? Даже если бы они и сохранились, то они стерлись бы, когда Легран мыл пергамент в теплой воде, чтобы очистить его от грязи.

Легран обнаружил череп с точки, находящейся на холме, рассмотрев его сквозь просвет в деревьях. Как только он отходил от этой точки, череп исчезал. По утверждает, что именно по этой причине пираты выбрали эту точку, это дерево и эту ветвь. Но как мог этот узкий просвет остаться неизменным на протяжении 150 лет?

Первые следы чернил случайно проявились, когда рука рассказчика, державшая пергамент, опустилась к огню. Но ведь жар, который нужен для проявления чернил, наверное, вызвал бы ожог на руке рассказчика. И наконец, можно усомниться, стал бы Кидд прибегать к такому нелепому способу обозначения места сокровища и был ли он настолько неосторожным, что потом потерял запись его расположения.

Все эти критические замечания в адрес «Золотого жука» По обоснованны. Они показывают, что автор заботился не столько о точности, сколько о видимости точности и что он претендовал на ученость, которой не обладал. Если пренебречь этими соображениями и встать на точку зрения читателя, то все замечания оказываются несущественными. Никто из читателей просто не замечает несуразностей, отдавшись во власть стремительного потока повествования, характерного для рассказа. Как зачарованный читатель следит за появлением звеньев цепи логических рассуждений. Одним из орудий этих рассуждений служит криптоанализ, который выглядит больше как разновидность прорицания. Загадочные знаки текста на пергаменте скрывают тайну огромного

богатства, а прочитавший их человек заставляет землю разверзнуться и выдать спрятанное сокровище. Эти же действия характерны для прорицателей и заклинателей духов. Иными словами, По окружил криптоанализ ореолом волшебства.

По был первопроходцем в деле популяризации криптоанализа. Небывалый успех его рассказа гораздо больше способствовал ознакомлению широкой публики с имевшимися знаниями о дешифровании, чем это можно было сделать с помощью учебника. «Золотой жук» стал первым общедоступным курсом криптоанализа. Это свое предназначение рассказ По сохраняет и поныне. Люди по-прежнему читают его, учатся по нему и черпают в нем вдохновение. Естественно, что вклад в криптоанализ людей, нашедших к нему дорогу благодаря «Золотому жуку», не поддается точной оценке, но каким бы он ни был, этим вкладом криптоанализ обязан По.

Следуя примеру По, и другие писатели ввели тайнопись в свои рассказы. Немалую их часть по справедливости можно было бы назвать «Возвращение золотого жука», поскольку это были повествования на ту же тему. В них почти всегда фигурировали простейшие шифры, так как для объяснения сложного метода вскрытия пришлось бы существенно замедлить темп повествования. В ряду героев рассказов, в которых можно найти упоминание о криптоанализе, особняком стоит Шерлок Холмс Конан Дойла, самый знаменитый из детективов, оживших на книжных страницах.

В своей литературной жизни Холмсу по крайней мере дважды приходилось иметь дело с шифрами. Когда в рассказе «Долина страха» великому сыщику передали послание, закодированное сообщником его заклятого врага, профессора Мориарти, детектив с помощью блестящих логических построений приходит к выводу о том, какая именно книга использовалась для кодирования. В «Долине страха» Холмс дешифрует криптограмму только благодаря своим удивительным способностям к дедуктивному мышлению и поэтому совершенно не нуждается в знании криптоаналитических методов.

Свое глубокое знание этого предмета, равно как и всех других, с которыми он сталкивается в избранном им занятии, Холмс проявил в рассказе «Пляшущие человечки». Пляшущие человечки — это маленькие, изображенные палочками фигурки, руки и ноги которых занимают различные положения. Они представляют собой знаки шифра. Американский гангстер Аб Слени, «самый опасный бандит в Чикаго», зашифровывает этим шифром записки с угрозами, адресуя их Илси, жене английского эсквайра*, в которую он был влюблен в пору молодости. Эсквайр переписывает эти послания, написанные мелом на подоконниках его дома и сарая, и передает их Холмсу. Тот вскрывает шифр и дешифрует криптограммы, но не успевает предотвратить трагедию: во время перестрелки Слени убивает сквайра и скрывается. Холмс, зная о местопребывании Слени из дешифрованных записок, посылает ему записку, написанную его шифром, с просьбой «прийти немедленно». Наивно считая, что этим шифром владеют только Илси и друзья-гангстеры, Слени приходит в дом эсквайра, и его тут же арестовывают.

* Эсквайр — низший дворянский титул в Англии.

Холмс говорит: «Я превосходно знаком со всеми видами тайнописи и сам являюсь автором научного труда, в котором проанализировано 160 различных шифров, однако я вынужден признаться, что этот шифр для меня совершенная новость». И действительно, перед Холмсом стояла значительно более сложная задача, чем перед каким-либо другим литературным криптоаналитиком, так как Холмсу пришлось иметь дело с очень коротким текстом, насыщенным именами. Весь перехваченный материал состоял из пяти сообщений, написанных на телеграфном английском языке:

1) «Am here Abe Slaney»*; 2) «At Elriges»**; 3) «Come Elsie»***; 4) «Never»****; 5) «Elsie prepare to meet thy God»*****.

* «Я здесь. Аб Слени».
** «У Элриджа».
*** «Приходи, Илси».
**** «Никогда».
***** «Илси, готовься к встрече с Богом».

В самом начале у Холмса была лишь одна записка. С ней он сделал первые шаги, а весь шифр вскрыл по этой и по следующим трем запискам общим объемом в 38 букв, из которых 8 встречаются только по одному разу. В этих записках 4 слова из 9 приходятся на имена, а остальные 5 не входят в число 10 самых частых английских слов, которые обычно составляют четвертую часть текста на

английском языке.

Трудность вскрытия шифра в таких условиях свидетельствует о силе и гибкости ума знаменитого детектива. Холмс начинает дешифрование криптограммы со своих обычных строгих логических построений, то есть с анализа частот встречаемости знаков. В первой записке было 15 пляшущих человечков. Из них четыре — с распростертыми руками и ногами, а у трех фигурок была согнута левая нога. Холмс сразу же выделяет четыре фигурки как букву «е». Но при коротких текстах нельзя полностью полагаться на законы статистики. Поэтому было вполне вероятно, что букву «е» скрывают три фигурки с согнутой левой ногой, или что эта буква кроется в любой из одиночных фигурок, или даже что в первой записке совсем нет буквы «е». Вряд ли Холмс этого не знал. Тем не менее «с некоторой уверенностью» он закрепляет именно эту фигурку за «е».

Холмс, конечно, был прав. Определив, что фигурки с флажками означают концы слов, Холмс заметил, что две из выделенных им четырех фигурок держат флажки, и тотчас же связал это с известным фактом, что слова в английском языке чаще всего оканчиваются на букву «е». Его быстрый ум, видимо, уловил разнообразие соседних с «е» знаков. Но все это пронеслось в его мозгу на уровне подсознания, чем и объясняется характерная для Холмса быстрота логических рассуждений. Поэтому детали его рассуждений отсутствуют в объяснениях другому герою серии рассказов Конан Дойла о великом сыщике — доктору Ватсону. А может быть, Холмс просто не хотел обременять Ватсона скучными подробностями.

Холмс понимает, что трудно чего-либо добиться, имея лишь одну записку. После получения еще трех он убеждается, что анализ частот встречаемости букв не срабатывает при таком коротком тексте. Не преуспев со своим любимым методом дедукции, Холмс ловко переключается на индукцию. Действует он блестяще: догадавшись сначала, что пятизначное слово с буквой «е» на втором и четвертом местах, которое представляет собой самостоятельное сообщение, должно быть словом «never», сыщик затем приходит к мысли, что в записках встречается имя «Elsie», и находит его. Оказавшись на верном пути, Холмс прилагает дополнительные энергичные усилия и успешно завершает процесс дешифрования.

Некоторые посмеивались над тем фактом, что для дешифрования этих криптограмм Холмс в течение двух часов покрывал «цифрами и буквами страницу за страницей». Но при таком коротком и трудном тексте потраченное Холмсом время не только приемлемо, но и удивительно мало. Более того, пляшущие человечки выделывают совершенно непонятные антраша, если их разместить в алфавитном порядке. Даже если их упорядочить и заставить заниматься хореографией, то в соответствующих им буквах опять не видно никакой закономерности. Члены клуба почитателей Шерлока Холмса, в том числе и президент США Франклин Делано Рузвельт, провели многие вечера в поисках закономерностей построения фигурок. Их усилия были напрасными. То обстоятельство, что при составлении записки к Слени с текстом «Come here at once»* Холмс ограничился уже прочитанными буквами открытого текста, наводит на мысль, что он не нашел никакой закономерности, которая дала бы ему больше свободы в выборе слов при ее составлении.

* «Приходи немедленно».

В заключение остается выяснить источник ошибок, допущенных при воспроизведении шифрованного текста посланий Слени и встречающихся во всех изданиях «Пляшущих человечков». В самой первой публикации рассказа Конан Дойла в этих криптограммах используется одна и та же человеческая фигурка для буквы «v» в слове «never» и для буквы «p» в слове «prepare», а также одинаковая фигурка для буквы «b» в слове «Abe» и для буквы «r» в слове «never». Высказывалось предположение о том, что ошибки «встречаются в записках злодея, и при желании их можно объяснить замешательством и отчаянием бедняги». Однако никто не увидел возможности того, что сквайр мог сделать ошибки, когда переписывал записки Слени, чтобы доставить их Холмсу.

В действительности же ни Слени, ни муж Илси не делали этих ошибок, поскольку никаких ошибок не было, когда Холмс дешифровывал криптограммы. Если бы одни и те же знаки употреблялись для обозначения букв «v» и «p» в оригиналах записок, то Холмс после угадывания слова «never» записал бы частичный открытый текст в пятой записке в виде «vrevare» вместо «?re?are», как у него, где две буквы «p» неизвестны. Аналогично этому, если бы буквы «r» и «b» были спутаны в оригинале, Холмс записал бы частично дешифрованный текст в виде «?re» (вместо правильного «Abe»), а он записал его как «??e», где буква «b» все еще неизвестна. Таким образом, рассуждения Холмса доказывают, что в оригиналах записок ошибок не было. И хорошо, что их не было, ибо они встречаются в критических для криптоанализа местах и могли бы привести к тому, что

прочитать криптограммы было бы почти невозможно даже Холмсу. Поэтому эти ошибки были допущены, скорее всего, доктором Ватсоном, поведавшим миру историю пляшущих человечков.

РУССКАЯ КРИПТОЛОГИЯ

Хотя появление тайнописи в России датируется XII-XIII веками, использование криптографии для засекречивания государственной переписки началось лишь в эпоху правления Петра I. Чрезвычайная осторожность, которую русские проявляли в вопросах криптографии, свидетельствует о том, что в России криптографы приобретали навыки работы единственно правильным путем — практикуясь в криптоанализе. В XVIII веке Россия переняла у Запада одно из его полезных нововведений — «черные кабинеты». Так же, как в Англии и Австрии, у русских они размещались в почтовых отделениях. В число сотрудников «черных кабинетов» входили специалисты по вскрытию конвертов и подделке печатей, переводчики и дешифровальщики.

«Черные кабинеты» действовали в царской России со времен правления императрицы Елизаветы. Посол Франции маркиз Шетарди определенно знал, что русские вскрывают его корреспонденцию. Однако текст его писем был зашифрован, и Шетарди чувствовал себя в полной безопасности, так как был уверен, что русские недостаточно образованны, чтобы вскрыть его шифр. Неизвестно, насколько он был прав в отношении русских, но для трех немцев, работавших в русском «черном кабинете», это был отнюдь не крепкий орешек. Шетарди допустил ошибку, когда в письме домой неуважительно отозвался о русской императрице, написав, что она «полностью находится во власти своих прихотей» и является «довольно фривольной и распутной женщиной». Это письмо попало в руки канцлера императорского двора графа Алексея Бестужева-Рюмина, который только и ждал случая, чтобы отомстить Шетарди, который сплел вокруг Бестужева сеть интриг в связи с англофильскими настроениями графа. Письмо было показано Елизавете, которая, будучи ослепленной своими симпатиями к Франции, отказалась ему поверить до тех пор, пока оно не было дешифровано в ее присутствии. На следующий день. 17 июня 1744 г., когда Шетарди прибыл в свою резиденцию, ему была вручена нота, в соответствии с которой в течение 24 часов французский посол должен был покинуть пределы России. Шетарди заявил протест. Тогда русские начали зачитывать ему его же собственные письма. «Достаточно», — сказал он и отправился упаковывать вещи.

В конце XVIII века информация, получаемая с помощью криптоанализа, по-прежнему продолжала служить источником ценных сведений для министерства иностранных дел России. 26 марта 1800 г. министр иностранных дел Панин писал из Петербурга своему послу в Берлине: «В нашем распоряжении есть шифры, с помощью которых король* переписывается со своим поверенным в делах в России. В случае, если у вас возникнут подозрения в вероломстве министра иностранных дел Пруссии графа Кристиана фон Хаугвитца, то ваша задача будет состоять в том, чтобы под каким-нибудь предлогом заставить его написать сюда письмо по интересующему нас вопросу. Сразу же, как только будет дешифровано его письмо или письмо его короля, я проинформирую вас о его содержании».

* Пруссии.

Спустя 12 лет после этого русские дешифровальщики внесли свой вклад в достижение победы над Наполеоном. Французский полководец определенно не придавал большого значения криптографии. Во время почти всех своих военных кампаний, в том числе и русской, Наполеон использовал один довольно простой шифр. Даже если бы его генералы не злоупотребляли лишь частичным зашифрованием своих посланий, то и тогда их криптограммы все равно были бы дешифрованы русскими криптоаналитиками. Русский император Александр I обильно процитировал переписку генералов Наполеона в своих воспоминаниях о войне. А однажды, во время званого обеда, данного им в Париже в честь французских маршалов через несколько лет после окончания войны с Наполеоном, Александр упомянул о том, что читал секретную французскую переписку. Маршал Макдональд, вспомнив, что один из французских генералов оказался перебежчиком, сказал: «Ваше величество, нет ничего удивительного в том, что вы смогли дешифровать нашу переписку, ведь кто-то передал вам ключи». Александр отверг это утверждение. Приняв серьезный вид и положив одну руку на сердце, а вторую подняв вверх, он сказал: «Нет. Я даю вам мое честное слово». Русские криптоаналитики могли гордиться тем, что их достижения пропагандировал сам царь.

В XIX веке криптоанализ постепенно превратился в орудие царского деспотизма. По всей стране нарастало движение за свободу. Одним из методов, с помощью которых «охранка»* следила за

подпольщиками, было использование «черных кабинетов» для ознакомления с содержанием писем и телеграмм подозреваемых лиц.

* «Охранка» — царская тайная полиция.

Постоянно функционирующие «черные кабинеты» были созданы при почтовых отделениях Петербурга, Москвы, Варшавы, Одессы, Киева, Харькова, Риги, Вильно, Томска и Тифлиса. Кроме них, были еще временные, которые создавались в других городах по мере необходимости. Большинство сотрудников «черных кабинетов» были иностранцами, являвшимися подданными России. В основном это были немцы, говорившие на русском языке с большим акцентом, поскольку в целях собственной безопасности они вели изолированный образ жизни. Для вскрытия писем, как правило, использовался пар или горячая проволока, с помощью которых снималась восковая печать. Начальник киевского «черного кабинета» Карл Зиверт, впоследствии осужденный как австрийский шпион, изобрел устройство, которое полностью исключало возможность случайной поломки или обгорания печати, свидетельствовавших о том, что конверт был распечатан. Это устройство представляло собой тонкую круглую отполированную палочку размером с вязальную спицу, расщепленную примерно до половины. Зиверт вводил палочку под клапан конверта, разрезом захватывал письмо, наматывал его на палочку и извлекал из конверта, не оставляя после себя каких-либо видимых повреждений.

«Черные кабинеты» направляли добытые воровским путем криптограммы в «охранку», где был квалифицированный специалист по криптоанализу, некто, Иван Зыбин, обладавший почти сверхъестественными способностями. Начальник «охранки» в Москве П. Заварзин вспоминает, что это был высокий худой, смуглый 40-летний мужчина с длинными волосами, расчесанными на пробор, имевший живой и проницательный взгляд. «По отношению к своей работе он был фанатиком, если не маньяком. Чтобы вскрыть простой шифр, ему было достаточно увидеть его только один раз. Если же ему приходилось иметь дело со сложным шифром, то он почти впадал в состояние транса, из которого выходил лишь тогда, когда шифр был вскрыт», — писал Заварзин.

Однажды в 1911 г. Заварзину пришлось привлечь Зыбина к работе над перехваченным письмом, в основном состоявшим из дробей. Зыбин приехал из Петербурга и, успев только поздороваться с Заварзиным, попросил дать ему письмо. Чиновник дал ему копию, но Зыбин хотел получить оригинал. Он уже было направился за ним на почту, когда ему сказали, что письмо отправлено. Заварзин уступил гостю свой стол, и вскоре Зыбин с головой ушел в работу, быстро заполняя разложенные перед ним листы бумаги. Когда Заварзин вернулся, чтобы пригласить Зыбина на обед, то ему пришлось обратиться к Зыбину дважды, прежде чем его слова были услышаны. За обеденным столом, все еще находясь в состоянии транса, Зыбин поел супа, затем перевернул тарелку и попытался писать на ней. Но так как карандаш на тарелке не был виден, он начал писать на манжетах, не обращая ни на кого внимания. Вдруг он вскочил со стула и закричал: «Тише едешь — дальше будешь»!

После этого Зыбин сел, отдохнул и съел обед, как нормальный человек. Он объяснил Заварзину, что повторения букв в письме дали ему ключ к шифру. Выкрикнутая им фраза «Тише едешь — дальше будешь» и была искомым ключом. В дешифрованном письме шла речь о пересылке в Киев нескольких картонных коробок. В этих коробках, вероятно, находилась взрывчатка, так как в то же самое время русский император планировал совершить туда поездку. Заварзин немедленно установил наблюдение за адресатами письма и помешал им организовать покушение на императора.

Зыбин рассказывал, что только однажды не смог вскрыть шифр, которым было написано письмо, посланное австрийским шпионом. «Но это было очень давно, — признался он Заварзину. — Сейчас это исключено». Начальник «охранки» Алексей Васильев также поделился своими воспоминаниями о Зыбине. Однажды во время налета на один из домов в Севастополе был найден лист бумаги, исписанный цифрами. Васильев передал его Зыбину, который тут же предложил затребовать из Севастополя все книги, найденные в этом доме. Вскоре после их прибытия, выяснив, что для шифрования была использована повесть Куприна «Поединок», Зыбин вручил Васильеву полученный открытый текст. За эту работу Зыбин получил повышение по службе и был отмечен наградой. В другом случае прочесть письмо террористов Зыбину помогло знание цены одного фунта динамита, которую ему сообщил Васильев.

Перед Первой мировой войной Россия провела одну из крупнейших для того времени разведывательных операций, вынудив полковника Редля выдать ей стратегические планы генштаба Австро-Венгрии. Боясь появления в России доморощенного Редля, начальник армейского

шифровального бюро полковник Андреев вплоть до последней минуты перед началом боевых действий воздерживался от рассылки копий нового шифра, предназначенного для использования в период войны. Эта мера предосторожности привела к печальным последствиям.

Русскими планами ведения военной кампании против Германии предусматривалось вторжение двух армий на территорию Восточной Пруссии. Армия под командованием генерала Раненкампфа должна была вести наступление строго в западном направлении и боевыми действиями сковать немцев. Перед армией генерала Самсонова, располагавшейся южнее, была поставлена задача обойти Мазурские болота, выйти в тыл немцам и, блокировав пути отхода, уничтожить их. Естественно, что успешное решение этой задачи предполагало согласованное и тщательное взаимодействие двух русских армий.

К сожалению, российская служба связи совершенно не отвечала предъявлявшимся к ней требованиям. Когда армии Раненкампфа и Самсонова оказались разделенными Мазурскими болотами и стали осуществлять связь друг с другом в основном по радио, выяснилось, что в армии Раненкампфа новый шифр получили и старый уничтожили, а у Самсонова все еще действовал старый шифр. В результате переговоры между ними некоторое время велись по радио в открытую.

К этому надо добавить, что и материальное обеспечение русских армий было налажено из рук вон плохо. В распоряжении армии Самсонова находилось немногим более шестисот километров провода, который был вскоре израсходован. Такое скудное обеспечение резко отличалось от снабжения вооруженных сил Англии и Франции, которые на Западном фронте ежедневно расходовали почти в десять раз больше провода. В то же время средства радиосвязи использовались только в штабах обеих русских армий и в штабах подчиненных им корпусов. Штабы дивизий и штабы более низкого звена радиосвязи не имели. Поэтому штабы корпусов для связи с дивизиями были вынуждены использовать проводные средства. А штабы армий, в свою очередь, потратили мизерные запасы провода для связи с тыловым командованием. В результате радио осталось единственным средством связи между штабами корпусов и армий.

Содержание их радиопереписки не представляло тайны для противника. Общая неэффективность проведенной Россией мобилизации пагубно сказалась и на доведении до войск новых военных шифров и ключей к ним. Например, 13-й корпус армии Самсонова не имел ключей для чтения криптограмм, поступавших от его соседа, 6-го корпуса. По прошествии двух недель после начала войны русские связисты даже не пытались шифровать свои сообщения, а передавали их по радио открытым текстом.

Восточная Пруссия уже в то далекое время в буквальном смысле слова была опутана телефонными проводами. С любой захудалой фермы немцы могли докладывать о продвижении русских армий прямо в свои штабы. Русская военная разведка обнаруживала потайные телефоны в погребах и даже в пчелиных ульях. В отсутствие достаточных запасов телефонного провода командование российских войск пыталось вести переговоры по телефону из квартир местных жителей, что отнюдь не способствовало сохранению содержания этих переговоров в тайне.

В соответствии со стратегическими планами, армия под командованием Раненкампфа 17 августа начала продвижение в глубь Восточной Пруссии. Для ее обороны немцы оставили только одну армию, так как в их стратегические планы входил, в первую очередь, быстрый разгром Франции. Эта немецкая армия не уступала ни одной из двух русских армий, но была слабее их объединенных сил, и поэтому германским генеральным штабом предусматривалось поочередное нанесение ударов по русским армиям.

После боя с Раненкампфом при Гумбиннене немцы оставили свои позиции и начали поспешный отход. Им удалось остановиться только тогда, когда они уже отошли на тридцать километров. Все же немецкие войска до некоторой степени потрепали армию Раненкампфа, и тот, вместо развития успеха, на время остановил свое наступление.

Перепуганный немецкий командующий уже был готов оставить пределы Восточной Пруссии. О своих намерениях он доложил верховному командованию, которое начало подыскивать ему замену. Но его талантливый начальник штаба М. Гофман сообщил, что армия Самсонова очень далеко вклинилась на территорию Пруссии, и убедил своего шефа в необходимости нанесения удара по этому флангу русских войск. Он предложил снять с фронта два немецких корпуса, действовавших против Раненкампфа, перебросить их по отличным железным дорогам Германии на южное направление и нанести внезапный удар по южной группировке под командованием Самсонова.

Перевозки уже начались, когда прибыли новый командующий немецкими войсками Гинденбург и его начальник штаба Людендорф. Они оставили план операции без изменений. В северной части линии фронта Людендорф поставил кавалерийский заслон для прикрытия отхода войск с занимаемых

позиций и наблюдения за войсками Раненкампфа. Распыление сил являлось нарушением стратегической военной доктрины Германии, в основу которой был положен принцип их концентрации. Когда 24 августа в немецком штабе шло обсуждение всех плюсов и минусов варианта Гофмана, мотоциклист привез две перехваченные русские радиограммы. Они были присланы начальником радиостанции крепости Кенигсберг. Подчиненные ему операторы у которых было мало документов для передачи, чтобы как-то развлечься, стали прослушивать работу русских радиостанций.

Обе радиограммы поступили от штаба 13-го корпуса армии генерала Самсонова и были переданы открытым текстом, так как штаб этого корпуса все еще не получил соответствующие ключи к шифрам. В них точно указывались пункты назначения частей корпуса, ожидаемое время их прибытия и планы действий. Эти данные полностью совпали с содержанием директивы, обнаруженной накануне в сумке убитого русского офицера. Перехваченные сообщения не дали главного — информации о намерениях Раненкампфа. Но, несмотря на это, Людендорф решил, что при наличии таких сведений ради достижения полной победы над Самсоновым стоило пойти на риск. Был отдан приказ о передислокации остальных немецких войск.

На следующее утро после совещания в немецком штабе появился документ, который положил конец сомнениям Гинденбурга и Людендорфа. Это была перехваченная радиограмма. Раненкампф передал ее открытым текстом своему 4-му корпусу. В ней, в частности, было сказано, что его армия будет продолжать наступление, и обозначался рубеж, на который она собиралась выйти. Немцам стало ясно, что Раненкампф намеревался и далее продвигаться вперед черепашьим шагом.

Поспешный уход немцев, следы которого обнаружил генерал Раненкампф, когда неторопливо проезжал по оставленным ими позициям, лишний раз утвердил его в ошибочности мнения о всеобщем отступлении немецких войск после Гумбиннена. Он не намерен был оказывать на немцев сильное давление, так как боялся отбросить их из Восточной Пруссии раньше, чем Самсонов сможет их разбить.

Немцы, в свою очередь, сразу же сделали вывод, что Раненкампф своевременно не выйдет ни на один из рубежей, чтобы нанести удар по тылам немецких войск раньше предполагаемого разгрома Самсонова. Получив передышку, они решили бросить все свои силы против армии Самсонова.

В то же утро связист вручил Гофману еще одну перехваченную радиограмму, также переданную открытым текстом. Самсонов отправил ее в шесть утра злополучному 13-му корпусу, у которого не было шифра. В ней содержалась полная характеристика обстановки с подробным описанием последующих действий войск армии Самсонова. Равного этому прецедента не было во всей военной истории.

При разработке своих планов немцы учли слабости в расположении русских войск. Генеральное сражение началось 26 августа, а к 30 августа немецкие войска взяли русских в железное кольцо, из которого смогли уйти только две тысячи человек. Армия Самсонова перестала существовать. Мертв был и ее командующий, в отчаянии покончивший жизнь самоубийством. После одержанной победы Гинденбург стал настолько популярен, что был назначен верховным главнокомандующим, а после войны — президентом.

Гофман, подавший идею этой блестящей операции, указал причину ее сокрушительного успеха в своей книге «Война упущенных возможностей»: «Русская радиостанция передала приказ в нешифрованном виде, и мы перехватили его. Это был первый из ряда бесчисленных других приказов, передававшихся у русских в первое время с невероятным легкомыслием... Такое легкомыслие очень облегчало нам ведение войны на Востоке, иногда лишь благодаря ему и вообще возможно было вести операции». Сказано ясно. Перехват незашифрованных сообщений русских войск позволил немцам одержать победу в первой битве в мировой истории, на исход которой решающим образом повлияла несостоятельность в вопросах криптографии.

Хотя в начале войны Россия испытывала большие трудности в обеспечении своих войск всем необходимым, в том числе и средствами связи, уже в первой половине сентября 1914 г. ей удалось полностью снабдить их шифровальными средствами. 14 сентября российская ставка верховного главнокомандования отдала распоряжение о том, что все военные приказы подлежат зашифрованию.

Принятая шифрсистема основывалась на многоалфавитном шифре цифровой замены, в котором допускалось зашифрование нескольких букв подряд по одному алфавиту. Этот шифр представлял собой таблицу, в верхней части которой в строку были выписаны буквы русского алфавита. Сама таблица состояла из восьми строк двузначных цифровых групп, выписанных в произвольном порядке. Строки отличались друг от друга порядком расположения в них этих групп. Слева они были бессистемно пронумерованы. При зашифровании эти строки использовались поочередно: сначала под

номером один, потом два и так далее. Каждая из строк применялась для зашифрования нескольких знаков открытого текста. Количество знаков, подлежащих шифрованию данной строкой, определялось самим шифровальщиком. Для того чтобы адресат мог расшифровать полученное сообщение, в его заголовке пять раз проставлялась цифра, соответствующая количеству знаков, которые были зашифрованы каждой из строк. Когда в процессе шифрования оператор хотел изменить это число, он вставлял в текст шифровки пятизначную группу, элементами которой была одна и та же цифра, соответствующая новому числу знаков, шифруемых одной и той же строкой. Таким образом, шифртелеграммы русской армии состояли из групп букв, зашифрованных одним и тем же алфавитом. Длина каждой группы букв определялась однозначно по пятизначной цифровой группе, состоявшей из одной и той же цифры.

Уже к 19 сентября молодой одаренный начальник русского отделения дешифровальной службы Австро-Венгрии капитан Герман Покорный вскрыл эту систему и полностью восстановил все строки. Дело в том, что такие шифрсистемы не представляли непреодолимых преград для криптоаналитиков, поскольку в шифртексте зачастую сохранялась структура наиболее часто встречавшихся в открытом тексте слов, таких, как «атака» и «дивизия», которые полностью шифровались одной строкой таблицы. К тому же поначалу русские связисты нередко вставляли открытый текст в шифрованный. Вскоре одновременное использование открытых и шифрованных текстов в сообщениях было запрещено, но было уже слишком поздно, и оно сыграло свою негативную роль.

Первую важную шифртелеграмму Покорный прочитал 25 сентября. Это было длинное донесение генерала Новикова о результатах разведки с примечанием в конце: «Я принял решение не форсировать Вислу». Шифртелеграмма была отправлена в 8.40 утра, а в 16.00 офицер связи австрийских войск довел до сведения немецкого штаба ее содержание. Знание решения, принятого генералом Новиковым, обеспечило успех действий австро-немецких войск в начальной стадии битвы на реке Висле.

Чтение другой шифрпереписки тоже оказало большое влияние на ход боевых действий. Из телеграммы полковника русской кавалерийской дивизии князя Ингалищева немцы узнали о готовившемся наступлении на крепость Перемышль. Предупрежденный об этом комендант крепости успешно отражал атаки, пока наступление австрийских войск не вынудило нападавших в середине октября снять осаду крепости. Во время этого наступления группа Покорного читала ежедневно до тридцати шифртелеграмм противника.

Примерно в это же время русские впервые сменили шифр. Сами строки остались без изменений, переменился порядок выбора строк для шифрования. Новый шифр был вскрыт Покорным в течение нескольких минут: все трудности отпали, когда одна из русских радиостанций передала зашифрованную новым шифром телеграмму, переданную еще до смены шифра.

Продолжали развивать свою дешифровальную службу и немцы. Профессор филологии Кенигсбергского университета Людвиг Дойбнер был зачислен в народное ополчение Германии в качестве переводчика русского языка. Он начал свою службу на поприще криптоанализа с перевода перехваченных сообщений, переданных в открытую. По мере появления в этих текстах зашифрованных слов он пытался прочитать и их. Постепенно у профессора накопился такой опыт работы в этой области, что он мог читать и полностью зашифрованные тексты противника.

В середине сентября 1914 г. Дойбнер был вызван я штаб и назначен руководить переводчиками, отобранными для обучения криптоанализу. После подготовки из них была образована дешифровальная группа при штабе. Каждый вечер к 11 часам она направляла Людендорфу уже прочитанные криптограммы. Тот ожидал их с большим нетерпением и часто спрашивал у своих подчиненных, есть ли дешифрованные криптограммы противника. Приказы, которые Людендорф отдавал на следующий день, в значительной мере основывались на информации, полученной от дешифровальщиков. Если же прочитанные криптограммы не доставлялись вовремя, он сам отправлялся в дешифровальную группу, чтобы выяснить причины задержки. А когда в перехваченных и обработанных радиограммах противника не содержалось ценных данных, Людендорф выражал недовольство по поводу того, что дешифровальная группа работает недостаточно внимательно. Однако такое случалось редко.

Вскоре была установлена прямая телефонная связь между группами Покорного и Дойбнера. Они совместно читали почти все русские шифрсообщения, полученные на постах перехвата. Из радиообмена стало известно о планировавшемся русском наступлении на Силезию, являвшуюся промышленным центром Центральной Европы. К концу сентября перед Гинденбургом и Людендорфом лежала информация о составе, дислокации, численности и планах русских войск, которая почти ничем не отличалась от плана, разработанного в русской ставке. Неизвестна была

только дата начала наступления, но немцы решили взять инициативу в свои руки и нанести упреждающий удар.

И вот 11 октября армия под командованием Маккензена вклинилась в русскую оборону. В 14.10 следующего дня начальник штаба одной из русских армий, по которым был нанесен удар, передал по радио длинную шифровку. Кроме даты запланированного наступления, в шифровке указывалась наиболее уязвимая зона в боевом порядке этой армии — стык между ее войсками и армией соседа. На следующий день дешифрованная и переведенная радиограмма уже лежала в штабе немецких войск Восточного фронта, а ее содержание было незамедлительно передано Маккензену. В 19.30, имея перед собой карту со схемой расположения русских, он отдал приказ о переходе подчиненных ему войск в наступление по всему фронту с нанесением главного удара в стык двух армий.

К этому времени русские уже ежедневно меняли порядок использования шифралфавитов, но по-прежнему оставляли без изменений сами шифралфавиты. В результате дешифровальщики противника без перебоев читали их шифрпереписку. Поток информации, добываемой с помощью криптоанализа, не сокращался. Немцы уже настолько привыкли к этому, что 19 октября Маккензен не отдавал приказов до тех пор, пока не были получены сведения от дешифровальщиков.

Следующий день стал черным для немецкой дешифровальной группы. В перехваченной шифртелеграмме 4-й русской армии содержалось предупреждение о том, что немцы имеют ключи к русскому шифру: русские сумели захватить ключи к немецкому и предположили, что аналогично мог поступить и противник. В действие был введен новый шифр, на этот раз — с заменой всех элементов шифрсистемы. На Восточный фронт опустился занавес молчания. Лишенные глаз и ушей, войска Маккензена к 21 октября оказались в «мешке». Русские предвкушали победу и уже заказали поезда для вывоза военнопленных. Но на следующий же день группа Покорного вскрыла новый шифр, и в немецкий штаб вновь пошел поток ценной информации. Из него немцам стало известно слабое место в кольце русских войск. К 25 октября кольцо окружения было успешно прорвано.

К весне 1915 г. в русских войсках полностью отказались от старой системы шифров и стали применять простой шифр Цезаря. Большое количество таблиц, использовавшихся в условиях ведения активных боевых действий, и ежедневная смена ключей ставили непосильную задачу перед связистами. В этих условиях вскрытие очередного русского шифра для дешифровальных служб Австро-Венгрии и Германии не составило почти никакого труда.

Чтение русских криптограмм позволило странам германского блока принимать время от времени такие меры, которые были единственно правильным тактическим решением в данной ситуации. Российский генеральный штаб был озадачен прозорливостью противника. Однажды немцы оставили занимаемые ими позиции за два дня до начала большого наступления русских войск. Одним из объяснений точного соответствия решений германского командования создавшейся обстановке русские считали использование им аэрофотосъемки.

Но постепенно крепло убеждение, что противник читает русскую шифрпереписку. Когда немецкое весеннее наступление второго года войны достигло апогея, русские опять сменили шифр. Но эта смена доставила больше хлопот им самим, так как почти все шифровки, переданные по радио в первые два дня после смены шифров, из-за допущенных ошибок так и не были прочитаны адресатами.

В июне 1916 г. вновь произошло изменение способа шифрования — русские ввели свой первый код. Возможно, это было сделано под влиянием Франции, которой из дешифрованных немецких криптограмм стало известно, что немцы читают русские шифрсообщения, или под воздействием собственной службы перехвата, которая начала функционировать в 1916 г.

Нараставшая дезорганизация русской армии оказывала отрицательное воздействие и на ее службу связи. Пропорционально снижению дисциплины в войсках росла болтливость радистов. В начале 1917 г. только в течение одного дня австрийская дешифровальная служба прочла более трехсот русских шифртелеграмм, из чего следовало, что служба обеспечения безопасности связи России быстро разваливалась.

Укрепление советской власти позволило Ленину и его соратникам заняться не только решением трудных проблем, связанных с управлением первым в мире социалистическим государством, но и традиционной для коммунистов деятельностью по разжиганию классовой борьбы во всем мире. Большевики считали себя вправе вести широкомасштабную кампанию по дестабилизации политической обстановки за рубежом, а также задействовать любые пропагандистские и агитационные методы с целью насаждения коммунизма в других странах.

Большую часть советских агентов составляли члены национальных коммунистических партий, которые ставили почти религиозное преклонение перед идеологией коммунизма выше интересов

своей родины. Они отсылали в Москву огромное количество информации и получали оттуда необходимые инструкции. При этом для связи с Центром советские агенты использовали самые разнообразные шифры.

Например, в 1919 г. в самолете, летевшем из Германии в Советский Союз и совершившем аварийную посадку в Латвии, местные пограничники обнаружили три шифрованных сообщения. Не сумев их дешифровать, правительство Латвии передало эти сообщения в распоряжение американского консула в Риге, который, в свою очередь, переправил их в США. Там они были довольно быстро прочитаны. Оказалось, что сообщения послали в Москву немецкие коммунисты, которые применили для их засекречивания шифр вертикальной перестановки, а в качестве ключа использовали строки из стихотворения немецкого поэта Генриха Гейне «Лорелея». В шифровках содержалась просьба прислать побольше денег, обсуждался провал съезда коммунистов в Голландии и говорилось об аресте известной немецкой коммунистки Клары Цеткин.

Примерно в это же самое время министерство юстиции США приступило к внедрению своих агентов в Коммунистическую партию Соединенных Штатов. Секретный агент министерства Фрэнсис Морроу, ставший секретарем районного комитета американской компартии в городе Камден в штате Нью-Джерси, занимался сбором информации о противоправных деяниях своих соратников. Он завел дружеские связи с одним из организаторов партийной ячейки района, который однажды в состоянии легкого опьянения привлек Морроу для расшифровки полученного им сообщения. Так в руки Морроу попал шифр, который использовался в переписке руководства компартии с партийными организациями на местах. Его основу составлял бланк американского денежного перевода, наличие которого у частного лица было вполне обычным делом и не могло вызвать никаких подозрений. Шифрованный текст представлял собой арифметические дроби, числители которых соответствовали номерам строк текста на обратной стороне бланка почтового перевода, а знаменатели — номерам букв в этих строках. Применяемая американскими коммунистами система шифрования во многом напоминала так называемый «дробный» шифр русских революционеров, с которым они активно работали при царском режиме. Вполне вероятно, что эта шифрсистема была позаимствована именно у них, впрочем, как и многие другие методы ведения подпольной деятельности. Например, у американских коммунистов в ходу было кодовое слово «дубок», означавшее укромное место, которое служило почтовым ящиком. Это кодовое слово использовалось русскими подпольщиками еще до революции.

Руководство ведением разведывательной работы против США было поручено сотрудникам российской торговой корпорации «Амторг», которая в 1924 г. учредила свои представительства в Нью-Йорке. Вся переписка «Амторга» была зашифрована, и применявшаяся шифрсистема надежно скрывала секреты ее агентуры в США от американских контрразведывательных спецслужб. В 1930 г. по распоряжению Гамильтона Фиша, председателя комитета конгресса, занимавшегося расследованием подрывной коммунистической деятельности в США, более трех тысяч перехваченных шифртелеграмм «Амторга» были переданы в военно-морское ведомство с целью получения более полной информации об этой деятельности. Дешифровальщики, которые получили шифртелеграммы для криптоанализа, вскоре сообщили, «что шифр, используемый «Амторгом», является очень сложным» и что «для его вскрытия их собственных знаний недостаточно». Тогда Фиш передал криптограммы в военное министерство. Через два года Фиш пожаловался на очередном заседании конгресса: «За период от 6 до 12 месяцев ни один специалист не смог прочитать ни слова из этих шифртелеграмм, хотя они заверяли меня, что легко вскроют шифр».

Однако Советский Союз был не до такой степени увлечен работой по совершенствованию своих собственных шифров, чтобы не следить за достижениями других стран в этой области. Напротив, он постоянно занимался так называемым практическим криптоанализом, который имеет другое, более прозаическое наименование — воровство шифров. Украсть чужой шифр всегда было значительно легче и быстрее, чем пытаться вскрыть его чисто аналитическим путем. Правда, стоило это, несомненно, дороже, да вдобавок еще было чревато потерей доступа ко всякой полезной информации, если противник установит, что его шифр был выкраден.

В соревнованиях по краже шифров победу одерживала то одна, то другая сторона. В 1926 г. в Марселе была арестована французская коммунистка, у которой при обыске обнаружили код французской армии. Этот код, вместе с кодом министерства внутренних дел Франции, был выкраден из тюрьмы в городе Мелуне, где печатались французские коды, одним заключенным-коммунистом, который спрятал их при выходе из тюрьмы в грамматике английского языка.

На следующий год Советский Союз завербовал эксперта по шифрам кабинета министров Ирана. К этому времени на СССР уже работал и шифровальщик одной из бригад иранской армии,

дислоцировавшейся вблизи русской границы. Кроме того, советская разведка сумела заполучить ключ к шифрам дашнаков*. Деятельностью дашнаков руководили из-за границы — из города Тебриза, расположенного на территории Ирана. Советский резидент в Тебризе установил связь с одним из чиновников почтовой службы Ирана и скоро имел в своем распоряжении достаточную информацию, позволявшую ему своевременно узнавать обо всех планируемых мероприятиях дашнаков. А в 1930 г. высокопоставленный сотрудник румынской полиции в знак протеста против своего несправедливого понижения в должности передал советской разведке секретный код Румынии.

* Дашнаки — члены антикоммунистической партии в Советской Армении.

Противник тоже не сидел сложа руки. В 1925 г исчезли шифрдокументы из советского посольства в Шанхае. Русский белогвардеец, подозреваемый в краже, при невыясненных обстоятельствах исчез с корабля, на котором он отплыл из Шанхая. В 1935 г советский служащий выкрал шифры из посольства СССР в Праге, и, хотя они впоследствии были вежливо возвращены чешской полицией их законным владельцам, ничто не могло поколебать уверенности работников посольства в компрометации этих шифров.

Летом 1936 г. русская военная разведка получила доступ к шифрпереписке военного атташе Японии в Берлине с японским военным министерством в Токио. Фотокопии шифртелеграмм были предоставлены в распоряжение московского эксперта, владевшего японским языком. Он дешифровал их с помощью кодовою блокнота, добытого советской разведкой, и перевел на русский язык. Прочитанные японские шифровки касались деятельности стран, присоединившихся к так называемому антикоминтерновскому пакту, что, несомненно, представляло огромный интерес для родины III Интернационала.

В 1937 г. жертвой охотников за чужими шифрами в очередной раз стал Советской Союз: был выкраден код применявшийся для засекречивания переписки между Москвой и министерством национальной обороны испанских республиканцев, получавших помощь из СССР для борьбы против режима Франко. В 1938 г. вновь пострадал Советский Союз. Высокопоставленный сотрудник советской тайной политической полиции генерал Г.С. Люшков, отвечавший за ведение контрразведывательной работы в армии, дислоцированной на Дальнем Востоке, убежал к японцам и передал им подробные сведения об организации армейской службы секретной связи. Правда, ущерб, причиненный СССР бегством Люшкова, не был слишком большим, поскольку советские агенты за рубежом своевременно информировали Москву о тех сведениях, которые стали достоянием японцев. Однако в 1939 г. урон, нанесенный СССР, был более значительным: еще один перебежчик, дезертировавший на Запад, выдал очень ценного советского агента — капитана Джона Кинга, сотрудника шифровального отделения министерства иностранных дел Англии. Англичане приговорили Кинга к десяти годам тюремного заключения.

Это постоянное воровство друг у друга шифрматериалов в конце концов привело к нелепому судебному процессу, который состоялся в 1939 г. Двое русских эмигрантов Владимир и Мария Азаровы в 1939 г. тайком вывезли из Советского Союза, как потом было указано в материалах судебного следствия, «секретную кодовую книгу, которая содержала действующий в Советском Союзе код, предусмотренный для ведения переписки». Их вещи, в том числе и кодовая книга, сначала были доставлены на борт грузового судна, а затем выгружены в Риге, в результате чего были безвозвратно утеряны. Азаровы в судебном порядке предъявили пароходной компании иск на 511900 долларов: 11900 долларов — за утерянное личное имущество, а остальные полмиллиона — за код, что, как заявил Владимир Азаров на суде, «точно соответствовало рыночной стоимости кодовой книги на момент ее пропажи». Дело было улажено вне суда. Поэтому никто так и не узнал, какая сумма была выплачена Азаровым в порядке возмещения стоимости практически не поддающейся оценке кодовой книги.

Советский «практический криптоанализ» не ограничивался одной только кражей шифров. Разведка СССР была также чрезвычайно заинтересована в добывании открытых текстов, наличие которых помогало советским криптоаналитикам добиваться значительных успехов во вскрытии шифров. Хорошей иллюстрацией этого тезиса служат события вокруг так называемых «бумаг в тыкве», которые, как следовало из публичного заявления бывшего американского коммуниста Уиттейкера Чэмберса, были вручены ему Элджером Хиссом для последующей передачи агентам советской разведки. Хотя в силу сложившихся обстоятельств Чэмберс так и не отдал советскому разведчику полковнику Борису Быкову катушки с пленкой, на которую были засняты пресловутые

«бумаги в тыкве», они составляли лишь малую часть огромного количества сфотографированных секретных документов, которые Чэмберс уже успел переправить в Москву и которые он якобы получил от Хисса. Например, среди этих бумаг была телеграмма американского посольства в Париже, датированная 13 января 1938 г. и имевшая отметку «Строго конфиденциально. Лично государственному секретарю». И хотя большая часть дипломатических телеграмм, которые попали в руки советской разведки через Чэмберса, была зашифрована несекретным кодом, остальные, как заявил в 1938 г. помощник государственного секретаря США Самнер Уэллес, «возможно, были отправлены с использованием одного из наиболее секретных кодов, бывших тогда в употреблении». Когда Уэллеса спросили, а не является ли наличие открытого текста сообщения и соответствующего ему шифрованного текста необходимыми подсобными материалами для вскрытия кода, тот ответил: «По-моему, именно так оно и есть». По крайней мере, один из известных экспертов по Советскому Союзу — Исаак Левин (американский журналист, родившийся в России) после неоднократных бесед с начальником военной разведки СССР в странах Западной Европы генералом Вальтером Кривицким, бежавшим из России, в середине 1939 г. пришел к выводу, что советская дешифровальная служба успешно вскрывала самые стойкие американские коды, применявшиеся для засекречивания дипломатической переписки.

Вполне естественно, что советских секретных агентов в США интересовали и вопросы безопасности собственной шифрпереписки. Рассказывают, что однажды в годы Второй мировой войны помощник президента Рузвельта Лочлин Кэрри, якобы работавшая на разведку СССР, явилась в дом другого советского агента Джорджа Сильвермана и сообщила ему, что Соединенные Штаты близки к вскрытию советского кода. Но когда Сильверман спросил Кэрри: «Какого именно кода?», то она так и не смогла вразумительно ответить на этот вопрос. Впоследствии Кэрри отрицала, что эти сведения могли исходить от нее, заявив о том, что ей ничего не было известно об успехах США в области криптоанализа и что она никогда не была агентом советской разведки.

Советские агенты не брезговали никакими сведениями, которые могли бы оказаться полезными для работы дешифровальных служб СССР. Когда зимой 1945 г. сотрудники американского управления стратегических служб ворвались в нью-йоркское отделение прокоммунистического журнала «Амеразия», то среди около двух тысяч подлинных конфиденциальных документов США ими был обнаружен и совершенно секретный доклад о вскрытии американцами японских кодов.

Советский Союз занимался успешным вскрытием кодов и шифров других стран, опираясь на нелегальные операции за рубежом двух своих ведомств — тайной политической полиции и военной разведки.

В задачу тайной полиции, с помощью которой коммунистическое правительство держало в подчинении народы, населявшие Советский Союз, входило как ведение внешней разведки, так и обеспечение внутренней безопасности страны. Таким образом, в СССР тайная полиция выполняла функции и ЦРУ, и ФБР. Возможно, что такое положение дел сложилось еще в царские времена, когда большое количество русских революционеров находилось за границей. В тот период царская «охранка» занималась внедрением своей агентуры за пределами России. Ее преемник при коммунистическом режиме поступал точно таким же образом с высланными или убежавшими из СССР людьми, ведущими борьбу против советской власти. Эта деятельность, как средство защиты коммунистического режима, вскоре естественным образом распространилась на капиталистические страны Запада, превратившись в политическую разведку.

Созданная Лениным всего месяц спустя после сформирования им своего правительства советская тайная политическая полиция имеет чрезвычайно запутанную историю. Многочисленные реорганизации (слияния и разделения) нашли свое отражение в частой смене ее наименований — ЧК, ВЧК, ГПУ, ОГПУ, НКВД, НКГБ, МГБ, МВД, КГБ.

Другим ведомством, занимавшимся в СССР вскрытием зарубежных шифров, являлась военная разведка, по своему назначению и функциям примерно соответствовавшая разведывательному управлению министерства обороны США. Основанная первым советским военным министром Львом Троцким, она, как и тайная полиция, в ходе многочисленных реорганизаций неоднократно меняла свое наименование и структуру. Чисто теоретически военная разведка должна была заниматься исключительно военными вопросами, а тайная полиция — только ведением политического сыска. Однако на практике данное правило соблюдалось далеко не всегда, и, возможно, это делалось преднамеренно. Было время, когда на короткий срок оба разведывательных ведомства были объединены в единую систему. В настоящее время орган советской военной разведки носит название Главного разведывательного управления (сокращенно — ГРУ).

Одной из задач тайной полиции являлась защита диктатуры пролетариата от самих пролетариев,

которые не обрели обещанного счастья при новоявленных диктаторах. Сразу же после своего создания по распоряжению Ленина ЧК занялась вскрытием почтовых отправлений и чтением телеграмм. В дальнейшем цели и задачи этого вида деятельности, которая при царе была прерогативой «черных кабинетов», оставались практически неизменными, а все внесенные в нее впоследствии усовершенствования касались лишь практических методов работы. В начале 50-х годов перлюстрация писем была возложена на 3-й отдел 2-го специального управления МВД, сотрудники которого проверяли благонадежность советских граждан, используя для этого разнообразные средства ведения наблюдения — миниатюрные электронные устройства для подслушивания, утонченные методы слежки, разветвленную сеть осведомителей. Представители 3-го отдела в почтовых отделениях вскрывали корреспонденцию, поступавшую из-за рубежа, а также читали письма, адресованные подозрительным лицам, и выборочно — всю другую переписку.

Перехваченные сообщения передавались в главное криптоаналитическое управление Советского Союза — в так называемый Спецотдел, основное назначение которого состояло в чтении шифрпереписки других стран. Хотя Спецотдел формально входил в состав управления по иностранным делам советской тайной полиции, в действительности же он отчитывался о своей деятельности только перед ЦК Коммунистической партии, являвшимся в СССР главным правящим органом. В 1938 г. после реорганизации Спецотдел был переименован в 5-е управление.

Спецотдел возглавлял старый большевик и друг Ленина Глеб Иванович Бокий, который одновременно был членом Верховного суда СССР. Бокий родился в 1879 г. и принимал активное участие в революционном движении. Он неоднократно подвергался арестам и был приговорен к трем годам ссылки Сибирь. Во время революции Бокий работал секретарем большевистской ячейки в Петрограде. Затем Бокий руководил ЧК в Туркестане, где он навел такой страх на местных жителей, что даже после его отъезда о нем еще долго ходили различные легенды. Например, рассказывали, что он питался мясом собак и пил кровь людей. Все это больше похоже на выдумки врагов советской власти. Однако не лишены основания слухи о том, что, уже будучи начальником Спецотдела, Бокий во время своих отпусков, которые он проводил на даче около Батуми, устраивал дикие оргии, на которые приглашались тщательно отобранные люди. Дверь его кабинета всегда была плотно закрыта, и через специально вмонтированный в нее глазок Бокий пристально изучал посетителей, прежде чем впустить их к себе. Высокий и сутулый, со злым выражением лица и холодными голубыми глазами, у своих собеседников Бокий создавал впечатление, что уже само их присутствие было ему ненавистно. Он приводил в трепет ночных дежурных, когда выходил из своего кабинета и заводил с ними разговор. Бокий никогда не носил шляпу, но всегда, независимо от сезона, надевал плащ. Он был скорее администратором, чем криптологом. В 1937 г. Бокия казнили во время большой чистки, устроенной Сталиным. Позже было установлено, что в нарушение социалистической законности Бокий хранил у себя большое количество золотых и серебряных монет.

Спецотдел занимался как вопросами шифрования, так и вопросами дешифрования. В 1933 г. шифровальщики Спецотдела работали в большой комнате на четвертом этаже обширного здания бывшей страховой компании на улице Лубянке в Москве. А дешифровальщики занимали верхний этаж бывшего здания Министерства иностранных дел на углу улиц Лубянка и Кузнецкий мост. Тот факт, что нижние этажи здания посещались частными лицами и членами дипломатического клуба, использовался для маскировки. В 1935 г. и шифровальщики, и дешифровальщики переехали в новое здание на улице Дзержинского, которая была названа так в честь первого главы советской тайной политической полиции Феликса Дзержинского.

Шифровальный отдел был разделен на несколько отделений, которые занимались обеспечением секретной связи с региональными управлениями тайной полиции, с ее пограничными частями и воинскими формированиями, с администрациями тюрем и лагерей, с нелегальной заграничной агентурой и с «легальными» резидентурами за рубежом. За секретную связь с «легальными» резидентурами отвечало отделение под номером 6. Его начальник по фамилии Козлов был снят с должности во время чистки в 1937 г. А после того, как преемник Козлова был отправлен в качестве шифровальщика в Соединенные Штаты, начальником 6-го отделения стал человек, чье имя приобрело впоследствии скандальную известность. Это был Владимир Петров, который в 1954 г. вместе с женой Евдокией получил политическое убежище в Австралии*.

* Петров назвал фамилии трех человек, которые числились среди его начальников, пока он возглавлял 6-е отделение. Ими были Ильин, Дегтярев и Шевелев. Неизвестно, являлись ли они начальниками 5-го управления или возглавляли шифровальный отдел, в который входило 6-е отделение. Учитывая частую смену руководства 5-го управления, наиболее вероятным является

первое предположение. Преемник Бокия, некто Шапиро, продержался на своем посту до ареста в течение всего одного-двух месяцев. Следующие три или четыре начальника 5-го управления также были арестованы.

Рост 6-го отделения может служить показателем расширения советской разведывательной деятельности. В 1933 г., в момент прихода Петрова в это отделение, оно насчитывало в своем составе 12 человек. К 1951 г. число его сотрудников выросло до 50. Этим людям доверялись самые большие тайны наиболее секретного учреждения в СССР, и поэтому они относились к элите советского общества. Однако их работа в «раю трудящихся» была какой угодно, но только не божественной. Операции по расшифрованию сообщений выполнялись вручную, и Петрову часто приходилось задерживаться на работе до полуночи, чтобы успеть вовремя обработать всю массу шифртелеграмм, поступивших к нему в течение дня. Позже, уже будучи заместителем начальника 6-го отделения, Петров сам не занимался непосредственно шифрованием или расшифрованием, а читал, корректировал и подписывал открытые тексты шифртелеграмм.

Иногда шифровальщикам давались поручения, выходящие далеко за рамки их прямых обязанностей, как это случилось, например, с Боковым — высоким, молчаливым сотрудником, обладавшим необычайной физической силой. Ему было поручено убить советского посла в одной из стран Ближнего Востока, что он и сделал в кабинете последнего, проломив ему череп одним ударом металлического бруска. Чтобы отвести от себя подозрение в убийстве, Боков в течение года продолжал работать шифровальщиком в этом посольстве, а затем вернулся в Россию, где за удачно проведенную операцию был награжден орденом Красной Звезды.

Дешифровальный отдел* был разбит на отделения по географическому и языковому принципу — китайское, англо-американское и т. д.** Будущая г-жа Евдокия Петрова, в течение двух лет изучавшая японский язык в московской спецшколе, попала на работу в японское отделение. Ее коллегами по работе были Вера Плотникова, дочь профессора японскою языка, который в течение многих лет был резидентом японской разведки в Москве, Галина Подпалова, настолько влюбленная во все японское, что, придя домой, она неизменно облачалась в кимоно, Иван Калинин, который время от времени приглашался в качестве консультанта, а также пожилой, но полный сил и энергии профессор Шунгский — главный авторитет отделения по вопросам японского языка. Однажды профессор нежно поцеловал Дусю (уменьшительное имя будущей г-жи Петровой) в щечку, когда на заключительном экзамене после четырехлетнего обучения, которым руководил сам Шунгский, она сумела правильно перевести на русский язык очень трудное японское предложение.

* Им руководил некто Гусев; возможно, это был С.И. Гусев, старый революционер, с !922 г. являвшийся членом ЦК Компартии, а с 1930 г. — членом президиума Коминтерна. Репрессирован в 1938 г.

** В 1933 г в состав дешифровального отдела на правах отделения входила также группа военной разведки во главе с полковником Харкевичем, который передавал добытую разведывательную информацию руководству спецотдела и в Генеральный штаб Красной Армии. Впоследствии эта группа была ликвидирована, а сам Харкевич подвергся чистке в 1938 г.

Шунгский служил еще в царской армии. Вообще, среди личного состава дешифровального отдела было довольно много бывших русских аристократов, в том числе графов и баронов. Это вопиющее противоречие с государственным укладом того времени объяснялось серьезной нехваткой лингвистов, которые требовались для ведения дешифровальных работ. А сама профессия дешифровальщика была настолько редкой, что даже тогда, когда представители этой профессии попадали в тюрьму, их все равно привлекали к работе по специальности.

Владимир Кривош, отец первого мужа Дуси Романа Кривоша, занимал высокий пост в царской «охранке». После революции его неоднократно то арестовывали, то освобождали. Но, даже находясь в заключении в Бутырской тюрьме в Москве, он выполнял секретные задания Спецотдела. В конце концов был арестован и его сын Роман, которого поместили в ту же тюрьму, что и отца, а начальник одного из дешифровальных отделений, входивших в состав 5-го управления тайной полиции, приносил туда обоим работу, что называется, «на дом», то есть в камеру.

Понятно, что в отношении заключенных дешифровальщиков никаких проблем, связанных с обеспечением режима секретности, не возникало. Однако в отношении остальных эти проблемы всегда стояли очень остро. Им категорически запрещалось говорить, в каком учреждении они работают и где оно расположено. Об этом никогда не рассказывала своим родителям и Дуся.

Сотрудникам Спецотдела даже запрещалось посещать любые рестораны, ибо там их разговоры могли быть подслушаны иностранными шпионами и врагами советской власти.

Была ли их работа успешной?

Несомненно. Например, в середине 1929 г. Спецотдел составил многостраничный отчет о прочитанных за неделю криптограммах других государств и разослал его начальникам управлений тайной полиции и членам ЦК Коммунистической партии. В конце 30-х годов события стали развиваться еще более быстрыми темпами. Дуся вспоминает, что в этот период она совместно с несколькими другими сотрудницами была с утра до ночи занята одной только сверкой отпечатанных на машинке открытых текстов, составлявших ежедневную порцию дешифрованных криптограмм, с написанными от руки черновиками. По свидетельству высокопоставленного партийного руководителя, Спецотдел «прекрасно справлялся с работой по вскрытию кодов», а подчиненные Бокия являлись «первоклассными специалистами, которых довольно часто отмечали как передовиков социалистического соревнования».

Советские военные не имели таких богатых традиций и ресурсов, чтобы их успехи в области криптоанализа были сравнимы с достижениями тайной полиции. Включение группы военной радиоразведки в состав Спецотдела в 1933 г. свидетельствует о том, что она занимала подчиненное по отношению к нему положение. Во всяком случае, известно о ней значительно меньше. Возможно, это объясняется тем, что каждый вид Вооруженных Сил СССР вел работы по дешифрованию переписки только одного, соответствующего ему вида вооруженных сил других государств. Например, дешифровальщики Красной Армии работали против сухопутных войск Англии, Германии, США, Японии и других стран. Аналогичным образом действовали ВМФ и ВВС Советскою Союза. Поскольку криптоанализ является составной частью любой разведывательной деятельности, ГРУ, будучи основным органом военной разведки, имело в своем составе криптоаналитическую спецслужбу в виде 8-го оперативного отдела, который занимался добыванием разведывательных данных, используя для этого как легальные, так и нелегальные методы. В 1943 г. в распоряжении военной разведки было несколько вспомогательных производств, включая фабрику, занимавшуюся изготовлением фотобумаги, продукция которой почти целиком доставлялась в белый двухэтажный особняк, расположенный во дворе комплекса зданий ГРУ. Этот особняк принадлежал фотолаборатории, в которой обрабатывались фоотопленки, используемые для связи с агентурой за границей.

На Воробьевых горах находился Особый радиодивизион (ОРД), с помощью которого ГРУ поддерживало радиосвязь со своими секретными агентами, разбросанными по всему миру. Официально это учреждение называлось Научно-исследовательским институтом по проблемам золотодобычи. Специалисты ОРД принимали криптограммы от советских агентов и передавали им распоряжения за подписью «Директор». Для агентов это было практически единственным надежным средством связи с ГРУ, по приказам которого они рисковали своими жизнями. В ОРД имелись специалисты, которые разрабатывали частотные расписания для обеспечения наилучшей слышимости при проведении сеансов связи из различных точек земного шара, а также сотрудники, занимавшиеся распределением радиопозывных среди зарубежной агентуры.

Шифровальная служба в ГРУ была представлена специальным отделом, которым руководил подполковник Кравченко. Среди сотрудников отдела числился и Игорь Гузенко, скандально прославившийся впоследствии. «Я хорошо помню первую телеграмму, которую мне дали в ГРУ для расшифрования, — вспоминает Гузенко. — Она пришла из города Харбина в Маньчжурии. Телеграмма по своему содержанию напоминала страницу из авантюрного романа. В ней давалось подробное описание тайника, где была спрятана рация агента (этот тайник располагался недалеко от дворца генерал-губернатора), а также весьма подробно характеризовались жители прилегающего района. Следующая телеграмма была передана мне для зашифрования. В ней содержались инструкции по проведению встречи с агентом ГРУ в Харбине. В инструкциях указывались основные и запасные места этой встречи, ее время и дата, а также приметы агента и пароль». Гузенко и его сослуживцы, работая с криптограммами, могли реально представить себе опасность, которая ежеминутно грозила жизни агентов советской военной разведки за рубежом.

Советские военные шифровальщики учились своей профессии в целом ряде учебных заведений. Гузенко изучал основы шифрования в Военно-инженерной академии имени Куйбышева, где заместителем начальника академии по политической части был бывший опытный шифровальщик Масленников, по прозвищу Криптус, который слыл хорошим преподавателем и отменным знатоком шифровального дела. Далее Гузенко продолжил свое обучение в Высшей школе Красной Армии, более известной как Разведывательная академия. Среди других предметов шифровальное дело

изучалось также и в электроминной школе в Кронштадте. Здесь в течение двух лет учился шифровальному делу Петров, при этом курс его обучения включал и криптоанализ. После этого Петров два года служил в качестве старшего шифровальщика на борту эсминца «Володарский», где работал в маленькой каюте под капитанским мостиком. По окончании срочной воинской службы Петров демобилизовался и поступил на работу в Спецотдел.

Советская шифровальная служба в основном учла плачевный опыт своей российской предшественницы времен Первой мировой войны. Об этом свидетельствует следующий полный драматизма обмен радиограммами между советскими воинскими частями 22 июня 1941 г. Сразу же после внезапного нападения Германии на Советский Союз один из передовых постов Красной Армии передал по радио открытым текстом: «Нас обстреливают. Что нам делать?» На что последовал следующий ответ: «Вы с ума сошли! Почему ваше сообщение не зашифровано?»

Во время Второй мировой войны шифровальная служба Красной Армии использовала в основном коды с перешифровкой. Советское военное командование часто заменяло коды тактического звена, но отмечались случаи, когда код, который использовался на одном участке большого фронта, через некоторое время начинал применяться на другом. У советских погранвойск и тайной полиции были свои собственные шифрсистемы. Кроме того, в распоряжении советских криптографов находилось несколько полученных по ленд-лизу экземпляров американского шифратора «М-209», которые они использовали в качестве прототипов для создания своих собственных шифрмашин, хотя об их применении на практике ничего достоверно не известно.

При достаточной интенсивности обмена шифрованными сообщениями коды с перешифровкой, безусловно, могут вскрываться. Одним из первых, кто вскрыл советский военный код, был шведский криптолог Арне Берлинг. В период ожесточенных боев финнов с русскими зимой 1939/40 г. Швеция передавала своему соседу разведывательные данные, полученные путем чтения советской шифрпереписки.

Советская стратегия ведения войны против финнов предусматривала нанесение ударов по пяти направлениям в глубь территории Финляндии. Одна из группировок Красной Армии должна была атаковать финнов в районе небольшой деревушки Суомусалми, а другая, расположенная севернее, должна была действовать в направлении деревни Салла. Однако разведывательная информация, полученная шведами из дешифрованной переписки этих группировок, помогла финнам отразить оба удара.

Финский маршал Маннергейм сумел разгромить советские войска под Суомусалми в основном благодаря тому, что он заблаговременно получил сведения о выдвижении туда 44-й Московской ударной моторизованной дивизии. Имея на руках эти сведения, Маннергейм направил в Суомусалми необходимые подкрепления. Через два дня после того, как по приказу Маннергейма пять батальонов прибыли на место, финские солдаты в белых маскировочных халатах, словно привидения, атаковали позиции советских войск, сломили их сопротивление и вынудили отступить по льду замерзшего озера Каянтоярви. Затем финские лыжники отрезали пути отхода 44-й дивизии и уничтожили ее по частям в ходе боев, которые продолжались вплоть до начала 1940 г. Финнами было захвачено большое количество советского военного имущества. Маннергейм писал: «Потери противника нельзя подсчитать хотя бы приблизительно из-за выпавшего глубокого снега, который похоронил под собой убитых и раненых».

Стояли 56-градусные морозы, когда шведы дешифровали несколько перехваченных советских криптограмм. Попавшие в окружение солдаты радировали своему командованию о том, что они сожгли все документы и бумаги, а также о том, что в ближайшее время они собираются съесть последнюю оставшуюся в живых лошадь и что это их последнее сообщение. И действительно, никаких новых радиограмм дальше не последовало, а вскоре шведские криптоаналитики узнали, что финны ликвидировали эту группу окруженных советских солдат.

Затем один из советских батальонов передал шифрованное сообщение, в котором указывалось, что его запас боеприпасов и продуктов почти исчерпан и что ближайшей ночью будут разведены три костра, дабы указать место, куда самолетам советских ВВС следовало сбросить на парашютах необходимое снаряжение. Шведы дешифровали это сообщение и довели его содержание до сведения финнов, которые разожгли костры недалеко от указанного в сообщении места и с нескрываемым удовольствием наблюдали, как с советских военно-транспортных самолетов к ним сбрасывались тюки с продовольствием и боеприпасами.

Шведскими криптоаналитиками было прочитано большое количество криптограмм советских ВВС. Многие из них содержали приказы по нанесению бомбовых ударов по столице Финляндии. Очень часто эти криптограммы дешифровались еще до момента вылета советских бомбардировщиков

с аэродромов, расположенных в Латвии и Эстонии всего в 20 минутах полета от Хельсинки. Благодаря этому финские власти имели достаточный запас времени, чтобы заблаговременно предупредить население города о готовившихся воздушных налетах, и в результате число жертв среди гражданского населения города было незначительным, учитывая количество сброшенных советских бомб.

Однако маленькая Финляндия не могла сравниться по своей военной мощи и ресурсам с Советским Союзом, и, несмотря на значительную помощь, оказываемую соседями (в том числе и в криптоанализе), в марте 1940 г. она была вынуждена подписать не совсем выгодный для себя мирный договор. Поэтому когда годом позже Германия напала на Советский Союз, Финляндия с готовностью приняла участие в начавшихся боевых действиях и приступила к активному взаимодействию со своим новым союзником в области ведения шифрперехвата.

Немецкая радиоразведка против Советского Союза была малоэффективной. В стратегическом отношении она вообще не имела ни одного сколько-нибудь заметного успеха. Немцы оказались не в состоянии вскрыть шифрсистемы, применявшиеся для засекречивания переписки высшего советского военного командования. По всей вероятности, к 1941 г. в СССР были внесены необходимые изменения в применяемые методы шифрования, и поэтому немцы не смогли добиться такого же успеха, как шведы двумя годами ранее. Таким образом, немецкая дешифровальная служба мало способствовала тому, чтобы в распоряжении верховного командования Вермахта было как можно более полное представление о советской стратегии ведения войны против Германии.

Это, однако, ничуть не мешало немцам собирать обильный урожай разведывательных сведений тактического характера. В середине 1940 г., когда Гитлер принял решение напасть на СССР, у немцев на Востоке не было никаких радиоразведывательных средств. Спустя год, когда Германия напала на Советский Союз, созданная с нуля служба радиоперехвата уже добывала важную информацию о советских войсках. Например, в июне 1941 г. захваченный немцами в плен советский летчик выдал им одну из шифрсистем, применявшихся в переписке советских ВВС. В результате полученная из дешифрованных сообщений информация помогла «Люфтваффе» уничтожить сотни советских самолетов на земле и в воздухе в ходе большого сражения в небе над Минском.

Используя свое превосходство в воздухе, внезапность нападения, скорость передвижения и другие факторы, немецкие войска победоносно продвигались в глубь советской территории. К 1942 г. в результате массированных наступательных действий немцы захватили обширные районы Советского Союза. Но зимой 1942/43 г. осажденный Сталинград выстоял, а 6-я немецкая армия капитулировала. Одновременно немцы были вынуждены снять двухлетнюю блокаду Ленинграда. К лету следующего года стало очевидно, что германский нацизм не сможет одержать победу над советским большевизмом, но войска Германии все еще надеялись удержать захваченную территорию. Немецкое высшее военное командование решило сломить наступательную мощь Красной Армии путем ведения ограниченных боевых действий. С ликвидацией превосходства своей авиации в воздухе немцы стали в меньшей степени надеяться на ведение разведки с воздуха и в большей — на действия своей радиоразведки. Во время ожесточенных сражений в октябре 1943 г. начальник штаба 48-го немецкого танкового корпуса заявил: «Лучшим и наиболее надежным источником получения разведывательных данных в настоящее время является наша служба радиоперехвата».

Несколько месяцев спустя 48-й танковый корпус участвовал в боевых действиях в районе города Радомышля в составе группы немецких армий «Юг» — одной из трех основных военных группировок Германии на Восточном фронте, перед которой стояла задача сорвать планировавшееся советское наступление. Этот корпус должен был разгромить 60-ю армию советских войск. Авиаразведка не смогла добыть какую-либо полезную информацию, а чтобы не насторожить противника, командование корпуса приняло решение группы войсковой разведки не высылать. Наступление, развернутое немцами в 6 часов утра 6 декабря 1943 г., оказалось для советских войск совершенно неожиданным, и они начали беспорядочный отход.

«В те дни, — писал начальник штаба 48-го танкового корпуса полковник Меллентин, — мы успешно осуществляли перехват радиосообщений русских. Эти сообщения немедленно дешифровывались, и их содержание своевременно докладывалось командованию корпуса. Мы всегда были в курсе действии русских, которые предпринимались в ответ на передислокацию наших сил, и в каждом конкретном случае мы вносили соответствующие изменения в наши планы. Вначале русские недооценили важность нанесенного по ним удара и подбросили на наш участок слишком малое количество противотанковых пушек. Затем постепенно русское командование начало проявлять заметное беспокойство. В эфире стали появляться встревоженные запросы: «Срочно уточните, откуда наступает противник». Ответ: «Узнайте у чертовой бабушки. Как я могу узнать, откуда наступают

немцы?» (Всякий раз, когда в русских радиограммах упоминаются черт и его ближайшие родственники, можно предположить, что назревают серьезные события.) К середине дня 60-я армия русских перестала выходить в эфир, но это уже не имело особого значения, поскольку вскоре наши танки разгромили ее штаб».

К вечеру того же дня немцы оттеснили советские войска на 40 километров, и в результате к ночи 9 декабря запланированное советское наступление расстроилось. В течение последующих нескольких дней по советским войскам была нанесена еще целая серия ударов. Меллентин писал: «Русские были определенно поражены этими ударами, наносимыми неизвестно откуда, а их радиопереписка неоспоримо свидетельствовала о царившем среди них замешательстве и беспокойстве».

Победа немцев в битве под Радомышлем задержала, но не сорвала наступление советских войск. В рождественские дни группа армий «Юг» была вынуждена начать свое отступление с Украины. Несколько месяцев спустя советские войска уже отбросили немцев на расстояние более чем тысяча километров.

Меллентин отмечал: «Красная Армия периода Второй мировой войны значительно отличалась от императорской русской армии 1914-1917 гг., однако в двух отношениях русские ничуть не изменились. Они продолжают отдавать предпочтение массированным наступлениям и не перестают проявлять чрезвычайное безразличие к обеспечению безопасности своей радиосвязи». Это замечание, по моему глубокому убеждению, справедливо только для оперативно-тактического звена советских войск, а определение «чрезвычайное» можно применить для характеристики действий русских в период их панического отступления под напором превосходящих сил противника.

Дешифрованные советские сообщения, как сообщалось в докладе об итогах работы немецкой дешифровальной службы за февраль 1944 г., «позволили получить сведения об оперативной обстановке, о районах сосредоточения, командных пунктах, потерях и подкреплениях, порядке подчинения и рубежах для атаки (смотри, например, радиограммы 122-й бронетанковой бригады от 14-го и 17 февраля). Кроме того, содержание этих сообщений дало возможность выявить семь танковых частей противника и их номера, а также установить наличие еще двенадцати танковых частей. За редким исключением, весь материал обрабатывался своевременно, и полученные сведения использовались на практике».

Эти сведения тактического характера могли в лучшем случае способствовать достижению успехов сугубо местного значения. Явная неспособность немецких криптографов вскрыть советские стратегические шифрсистемы, с помощью которых засекречивалась самая важная информация, вынудила одного немецкого криптографа признать, что, хотя Россия и проиграла Первую мировую войну в эфире, во время Второй мировой войны она сумела взять реванш за свое поражение.

В его изречении содержится доля правды. Советские криптологи достигли больших успехов как в обеспечении безопасности своей радиопереписки, так и в дешифровании немецких криптограмм. В 1942 г. они научились читать криптограммы, зашифрованные с помощью немецкого дискового шифратора «Энигма». Немецкие связисты отдали должное успехам советских криптоаналитиков, когда в решении, принятом на конференции офицеров связи в 1943 г., записали: «Запрещается каким-либо образом выделять передаваемые по радио послания фюрера».

В то же время Советский Союз надежно обеспечил безопасность своей дипломатической переписки, применяя для ее зашифрования одноразовые шифрблокноты, которые использовались начиная с 1930 г. Следовательно, важные сообщения Министерства иностранных дел СССР не читались ни врагами, ни нейтральными странами, ни союзниками. Поэтому любые планы, которые Советский Союз мог вынашивать против тех, кто в конце войны должен был стать их марионетками или противниками, так и остались наиболее неприкосновенными из его секретов.

В период Второй мировой войны агенты советской тайной полиции и ГРУ вели активные поиски ценной информации во многих точках земною шара. Три шпионские группы обеспечивали почти непрерывное поступление разведывательных данных в Москву. Легендарная сеть «Люси» в Швейцарии, «Красный оркестр» в Германии и группа Зорге в Японии добывали для Кремля нескончаемый поток подробных и достоверных разведывательных сведений.

Шифрпереписка советских разведчиков не поддавалась дешифрованию. Большинство из них использовало стандартную для советской агентуры того времени шифрсистему, которая была триумфом шифровальной техники. Она представляла собой доведенную до совершенства старую систему, применявшуюся русскими революционерами, и объединяла в себе шифр равнозначной замены с одноразовой «гаммой». В Москве обоснованно считали ее абсолютно стойкой.

Другие советские агенты пользовались слегка измененным вариантом стандартной агентурной шифрсистемы, который хотя и являлся более сложным, но в то же время был несколько ненадежнее.

Этот вариант предусматривал получение знаков «гаммы» из текста обычной книги путем его шифрования с помощью шифртаблицы. В частности, данный вариант использовался агентами из «Красного оркестра». Он также применялся членами швейцарской сети «Люси» и Бертилем Эриксоном, советским агентом, арестованным в Швеции в 1941 г. Для шифрования Эриксон заимствовал тексты из книги Ярослава Гашека «Похождения бравого солдата Швейка», изданной в Швеции в 1940 г. Данный вариант стандартной советской агентурной шифрсистемы не является невскрываемым. Применение текстовой «гаммы» позволяет криптоаналитику восстанавливать как саму «гамму», так и первичный шифртекст.

Каким же образом эта стандартная советская шифрсистема, такая простая, но в то же время и столь надежная, использовалась советской агентурой за рубежом в годы Второй мировой войны?

Доктор Рихард Зорге, высокий, крепкого сложения человек с недоброжелательным взглядом, работал в Японии в качестве корреспондента германской газеты «Франкфуртер цайтунг». Член нацистской партии, он был в близких отношениях с послом Германии в Японии Ойгеном Оттом, с которым сдружился, когда Отт был еще только помощником военного атташе. Зорге даже состоял на службе в германском посольстве в качестве пресс-секретаря и каждый день, сидя за завтраком рядом с Оттом, просматривал газеты и обсуждал с ним последние новости и политические проблемы. После этого он передавал полученную информацию врагу Германии — Советскому Союзу. Опытные немцы как-то не обратили должного внимания на тот факт, что дед Зорге работал секретарем у Карла Маркса, а сам Зорге одно время был убежденным коммунистом.

С 1929-го по 1931 г. Зорге возглавлял советскую шпионскую сеть в Шанхае. Проявленные им способности и его интерес к Дальнему Востоку побудили ГРУ через два года направить его в Японию под видом журналиста. Задание Зорге состояло в выяснении стратегических планов Японии, которая обладала достаточным военным потенциалом, чтобы вести успешные боевые действия против СССР. Зорге кропотливо налаживал свои собственные каналы получения информации и вербовал агентов среди японцев. Самой важной его находкой оказался Хоцуми Одзаки, бывший в дружеских отношениях с принцем Коноэ, премьер-министром Японии. В дополнение к Одзаки более двух десятков других агентов-японцев поставляли ему важные сведения военного и экономического характера. Таким образом, Зорге черпал свои разведывательные данные в высших правительственных кругах Японии и одновременно имел прямой доступ к ценнейшей информации относительно планов ее европейскою союзника.

Добытую информацию Зорге переправлял на фотопленках в СССР с помощью курьеров, а также передавал по радио. Его радистом был Макс Клаузен, приземистый немец с приятными чертами лица и вьющимися волосами, который в годы Первой мировой войны служил радистом в германских войсках связи и впоследствии работал вместе с Зорге в Шанхае. В качестве прикрытия Клаузен вел бойкую торговлю копировальным оборудованием. Он владел частным предприятием, имевшим такой большой коммерческий успех, что иногда Клаузену приходилось уделять делам своего предприятия больше внимания, чем заданиям Зорге. Например, в 1941 г Клаузенотправил всего лишь треть от общего количества сообщений Зорге. Однако найти полноценную замену Клаузену как радисту оказалось делом слишком сложным. Тем более, что тот проявлял чудеса изобретательности при поддержании радиосвязи на большие расстояния с помощью портативного передатчика, сконструированного им самим. Перед началом работы Клаузен собирал свой передатчик, а после окончания каждого сеанса радиосвязи разбирал его на части и укладывал в большой портфель, в котором переносил с места на место.

Однажды вечером Клаузен был на грани провала, когда его и другого агента остановил полицейский, а у них в портфеле был разобранный передатчик. «У меня сжалось сердце от мысли, что нас выследили, — вспоминал Клаузен. — Но полицейский почему-то лишь заметил: «У вас фары не горят, будьте осторожны» — и отошел, не обыскав нас и не осмотрев портфель».

С приближением войны группа Зорге значительно активизировала свою деятельность. С 1938 г. ее радиопередачи стали вестись регулярно: по нечетным дням и воскресеньям сеанс связи начинался в 3 часа дня, в остальные дни — в 10 часов утра. Клаузен передавал информацию советской радиостанции, имевшей условное название «Висбаден» и находившейся где-то на Дальнем Востоке. Оттуда сообщения ретранслировались в Москву. Сначала Клаузен только передавал уже зашифрованные сообщения, но после того, как в 1938 г. Зорге на своем мотоцикле попал в аварию, из Москвы поступило распоряжение обучить Клаузена шифровальному делу. Впоследствии Клаузен писал:

«Я всегда занимался шифрованием и расшифрованием, сидя дома в комнате, которой пользовался только я один. О нежданных посетителях меня всегда предупреждал звонок над входной

дверью, что давало возможность спрятать все мои бумаги. В трех случаях японские служащие видели шифр, но, кажется, не придали этому должного значения. Однажды, когда я находился в постели и занимался шифрованием*, в комнату неожиданно вошел доктор, которого обычно впускала моя служанка. Он подозрительно взглянул на шифровальную таблицу, но ограничился всего лишь замечанием: «Вам не следует ничего писать до полного выздоровления». Затем доктор произвел обычный медицинский осмотр и удалился. В течение нескольких дней я опасался того, что он известит полицию, но в этот раз все закончилось благополучно».

* С апреля по август 1941 г врачи обязали Клаузена соблюдать постельный режим из-за обострившейся болезни сердца.

Зорге составлял все свои сообщения только на английском или на немецком языках, никогда не пользуясь для этой цели русским языком, чтобы не выдать истинной национальной принадлежности своей разведывательной группы.

Зорге сумел узнать не только о том, что Германия собирается совершить нападение на СССР, но даже установил приблизительную дату этого нападения. Сталин не придал значения информации Зорге и был захвачен врасплох. С началом войны наступил тот момент, ради которого Зорге и члены его группы очутились в Японии. Они прилагали все свои силы ради получения конкретной информации, которую Советское правительство считало жизненно важной для успешного продолжения войны и, фактически, для самого существования страны. Намерена ли Япония совершить нападение на СССР, чтобы «пожать руку» Германии на Урале, или она займется осуществлением своего давно разработанного плана захвата Малайи и голландской Восточной Индии, богатых каучуком и нефтью?

Япония сделала свой выбор 2 июля 1941 г. в обстановке глубочайшей секретности на заседании кабинета, на котором присутствовал японский император. По мере того как сведения об этом выборе постепенно становились достоянием все более широкого круга лиц в правительстве Японии, группа Зорге наращивала объем пересылаемой в СССР информации. Японская контрразведка перехватывала значительную часть радиопередач Зорге. В министерстве связи Японии, в бюро связи в Токио и в Осаке, а также в бюро связи японского генерал-губернатора Кореи знали о том, что с 1938 г. на территории Токио нелегально работает радиопередатчик. Однако японская радиопеленгаторная служба оказалась не в состоянии засечь его местонахождение, а дешифровальщики так и не смогли прочитать перехваченные шифровки. Эти две неудачи помешали японцам своевременно обезвредить группу Зорге.

Различные соображения привели Зорге к мысли, что Япония твердо решила не предпринимать наступления, в результате которого могла бы состояться упомянутая выше встреча с Германией на Урале. В течение лета, когда колонны немцев неуклонно продвигались по направлению к столице СССР, Зорге передавал в Москву информацию о дальнейшем наиболее вероятном развитии событий на Дальнем Востоке. В конце концов Одзаки предоставил Зорге сведения о решении Японии наступать в южном направлении и не начинать пока войну с Советским Союзом. Поэтому в начале октября 1941 г. Зорге передал свое окончательное заключение по этому вопросу: «Вступление Японии в войну против СССР не ожидается по крайней мере до весны следующего года».

По мере получения все более обнадеживающих сообщений от Зорге Советский Союз стал снимать войска со своих восточных границ. Как раз в это же самое время немцы предприняли решительное наступление с целью захвата Москвы до начала зимы. Советское военное командование, не опасаясь удара в спину со стороны Японии, постепенно уменьшило свою Дальневосточную армию на 15 пехотных и 3 кавалерийские дивизии, на 1700 танков и 1500 самолетов. Эти войска перебрасывались по территории самого крупного в мире государства с востока на запад. Свежие подкрепления, а также надвигающаяся зима замедлили продвижение немцев, но они все же продолжали находить слабые места в обороне советской столицы, нанося по этим местам улары своим большим «бронированным кулаком». 2 декабря 1941 г. немцы достигли окраины подмосковного города Химки, откуда в свинцовом небе были видны купола соборов Кремля. На следующий день с помощью свежих резервов маршал Георгий Жуков предпринял яростную контратаку и отбросил полузамерзших на тринадцатиградусном морозе немцев от стен столицы. Через пять дней Берлин сообщил о приостановлении своего наступления на Востоке. Москва выстояла.

Чего нельзя было сказать про Зорге. Полиция арестовала одного японца по подозрению в коммунистической деятельности. Этот японец не являлся членом разведывательной группы Зорге, но

для того, чтобы выгородить себя, он донес на другую женщину. Эта женщина действительно была членом группы Зорге, и ее признания позволили в конце концов арестовать Одзаки. Он был задержан 15 октября, Зорге и Клаузен — 18 октября. В ходе допроса Клаузен во всем признался и посвятил японцев в тонкости работы с шифрсистемой, которая применялась им и Зорге для засекречивания радиопереписки с Москвой. Японцы смогли, наконец, прочитать злополучные криптограммы Зорге, которые послужили основным обвинением на состоявшемся судебном заседании. Клаузена приговорили к пожизненному заключению, а Одзаки и Зорге были повешены 7 ноября 1944 г. с интервалом в 50 минут. Их трагическая, но великая миссия была завершена.

Вероятно, самой разветвленной советской разведывательной сетью была организация, вошедшая в историю под именем «Красный оркестр». Щупальца «Красного оркестра» проникли в самое логово нацизма, а его филиалы функционировали на территории и Германии, и оккупированной Европы. Постоянное гудение, издаваемое радиопередатчиками, прозванными немцами «музыкальными шкатулками», послужило причиной, по которой советскую разведывательную сеть окрестили «Красным оркестром».

Зашифрованная информация поступала в Москву от 300 агентов «Красного оркестра», находившихся в Берлине, Брюсселе, Марселе, Париже и в других европейских городах. Дирижировал «Красным оркестром» Харро Шульце-Бойзен — лейтенант немецких ВВС, работавший в дешифровальной службе министерства авиации. Он был выходцем из безупречной немецкой семьи, в родстве с которой состоял сам адмирал фон Тирпиц. Своеобразным концертмейстером «Красного оркестра» был Арвид Харнак, племянник влиятельного немецкого историка-теолога Адольфа Харнака. А на должности импресарио состоял Леопольд Треппер, профессиональный советский резидент, который обосновался в Париже под прикрытием главы корпорации «Симекс».

Организация, которую Треппер создал во главе с Шульце-Бойзеном и Харнаком, оставалась законсервированной вплоть до того момента, когда 22 июня 1941 г. немцы перешли советскую границу. И сразу Москва потребовала от «Красного оркестра» информацию о планах немцев. Вскоре радиопередатчики заполнили эфир, почти непрерывно передавая пятизначные группы шифровок. Первая криптограмма была перехвачена 26 июня 1941 г. немецкой службой радиоконтрразведки в городе Кранце в Восточной Пруссии. Но расшифровать и эту, и все последующие перехваченные криптограммы «Красного оркестра» не удалось. В то время служба радиоконтрразведки имела в своем распоряжении только шесть пеленгаторов дальнего действия, и нехватка оборудования сильно затрудняла слежение за передатчиками.

Только в октябре 1941 г. стало известно, что перехваченные сообщения предназначались для Москвы, а в декабре была запеленгована первая радиостанция «Красного оркестра». 13 декабря отряд солдат, неслышно ступая сапогами, поверх которых были надеты носки, бесшумно поднялся на второй этаж дома 101 по улице Аттребатов в Брюсселе. Они ворвались в одну из комнат и арестовали там радиста-шифровальщика Михаила Макарова — лейтенанта советских ВВС, родственника министра иностранных дел Вячеслава Молотова. Одновременно были арестованы два других советских агента. В этот момент в доме появился Треппер. Он разговаривал с невероятным апломбом и, выдав себя за продавца кроликов, ловко сумел избежать ареста.

В камине немцы обнаружили обугленный клочок бумаги, исписанный цифрами. Ясно, что это были записи, сделанные в процессе шифрования какого-то сообщения, и немецкие дешифровальщики немедленно принялись за его изучение. Фраза, записанная на найденном клочке бумаги, была на французском языке и больше походила на часть ключа, чем на открытый текст. В этой фразе присутствовало слово «ПРОКТОР». Служба радиоразведки допросила хозяйку, наивную пожилую вдову, которая перечислила одиннадцать книг, которые читал ее постоялец. На 286-й странице научно-фантастического романа французского писателя Ги де Терамона «Чудо профессора Вальмара» дешифровальщики нашли действующее лицо с именем Проктор. Они сумели правильно понять важность этого совпадения. Роман Терамона дал им возможность прочесть 120 шифровок, которые принадлежали одной из самых активных радиостанций «Красного оркестра». В прочитанных сообщениях говорилось о весеннем наступлении немцев на Кавказе, давались данные о состоянии немецких ВВС, сообщались сведения о потреблении горючего, о потерях и содержалась некоторая другая важная информация. Но все имена разведчиков, упомянутых в этих сообщениях, были псевдонимами, а три арестованных на улице Аттребатов агента не хотели или не могли дать о них информацию. Служба радиоконтрразведки удвоила усилия.

После своего мелодраматического побега Треппер немедленно предупредил остальных членов «Красного оркестра» о провале. Курьеры доставили из Москвы новые ключи, и вскоре «Красный оркестр» «заиграл» с удвоенной силой. Многие исполненные им номера звучали по заявкам из

Москвы.

«Жильберту* от Директора.

Проверьте, действительно ли Гудериан** собирается прибыть на Восточный фронт. Под его ли командованием находятся 2-я и 3-я армии? Доложите о 26 бронетанковых дивизиях, которые формируются во Франции».

* Жильберт — кличка Треппера

** Гудериан Хайнц — генерал танковых войск Германии.

Разведывательные сведения стекались от информаторов, работавших в различных областях. Шульце-Бойзен обосновался в дешифровальной службе министерства авиации. Харнак занимал высокий пост в министерстве экономики. У «Красного оркестра» были также ценные источники информации в министерстве иностранных дел, в контрразведке ВВС, в министерстве труда и пропаганды, а также в армейской криптографической службе. Монотонное звучание радиопередатчиков было для Москвы лучше всякой музыки. Благодаря «Красному оркестру» там узнали о немецком плане блокады Ленинграда, о точном времени выброски многих парашютных десантов, о ежемесячном производстве самолетов, о найденном в финском городе Петсамо советском коде, о потерях ВВС Германии, о производстве военных самолетов, о технических данных нового истребителя «мессершмитт», о создании синтетического горючего, о немецких внешнеполитических акциях, о внутренней оппозиции нацизму и о передвижениях немецких войск вдоль реки Днепр.

Но «Красный оркестр» играл не только для Москвы Немецкая служба радиоперехвата внимательно слушала издаваемые «Красным оркестром» звуки, казавшиеся ей отвратительной какофонией. И хотя криптограммы оставались неразгаданными, их источник можно было попытаться выследить. 30 июня 1942 г. на территории Бельгии была выявлена другая советская разведывательная группа, во главе которой стоял агент с большим стажем работы Йоган Венцель, за отличные знания в области радиотехники получивший прозвище Профессор. Он был схвачен рядом с еще теплым радиопередатчиком. Венцелем занялось гестапо, и дело, начавшееся с психологической встряски от ареста, довершило грубое физическое воздействие на человеческую плоть. Широкая осведомленность Профессора о системе шифрованной связи советских агентов позволила немецкой радиоразведке прочесть ранее перехваченные криптограммы «Красного оркестра». В одном из сообщений почти годичной давности ей удалось обнаружить настоящие адреса Шульце-Бойзена и Харнака. Так «Красный оркестр» остался сразу и без «дирижера», и без «концертмейстера», что не замедлило сказаться на качестве исполняемых им «мелодий».

Среди всех советских разведывательных сетей, действовавших во время Второй мировой войны, самой важной была швейцарская. Эта сеть поставляла в Центр исключительно ценную информацию благодаря тому, что своим плацдармом она избрала нейтральную Швейцарию, где в течение длительного времени была недосягаемой для немцев. Там чрезвычайно плодотворно трудился советский агент по кличке Люси, которого многие считают величайшим разведчиком военного времени. Под этой агентурной кличкой скрывался Рудольф Росслер — маленький и неприметный издатель католических книг на немецком языке. Среди источников, которыми пользовался Росслер, числились десять его товарищей по Первой мировой войне. Все они были немецкими офицерами, причем пятеро из них в ходе войны стали генералами и заняли высшие военные посты. Например, Фриц Тиль возглавлял шифровальный отдел верховного командования Вермахта. Пользуясь техническими средствами, имевшимися в его распоряжении, Тиль организовал канал оперативной радиосвязи с Росслером, чтобы передавать тому свежайшие разведывательные данные, которые добывал, находясь в самом центре управления немецкими войсками.

Главой разведывательной сети «Люси» являлся Шандор Радо, профессиональный картограф. Он был венгерским коммунистом, засланным в Швейцарию в 1936 г. для вербовки агентуры. Помощником Радо и его основным радистом был Александр Фут — невозмутимый, похожий на медведя 35-летний англичанин, который жил в Швейцарии на собственные средства, якобы уклоняясь от службы в английской армии.

В середине июня 1941 г., ночью Фут отправил в Центр короткую, но важную радиограмму:

«Директору от Доры* через Тейлора**.

Гитлер окончательно принял решение совершить нападение на Россию 22 июня».

* Дора — агентурная кличка Ш. Радо

** Тейлор — курьер.

На Сталина эти данные не произвели никакого впечатления, как, впрочем, и информация, полученная от Зорге. Сталин посчитал, что заинтересованность Германии в покорении Англии и расчленении ее империи значила гораздо больше, чем разведывательные сведения из этих двух источников. Данный случай хорошо иллюстрирует одну из самых сложных проблем в оценке информации, поставляемой разведкой, — проверку ее достоверности.

Вначале Фут связывался с Центром только дважды в неделю, но после нападения Германии на Советский Союз Центр потребовал вести радиопередачи круглые сутки. В результате Фут, работавший без помощников, еле-еле справлялся со своей работой. После ночи, проведенной за радиопередатчиком, он вставал в 10 часов и проводил свое утро, как это положено делать английскому эмигранту, а после полудня в уединенном месте встречался с курьером. «Вернувшись после встречи, — писал он, — я обычно весь вечер занимался шифрованием». Согласно полученным из Центра наставлениям, шифрование сообщений можно было осуществлять только после наступления темноты и за запертой дверью. Но Центр постоянно торопил с отправкой накопленных разведывательных сведений, и Футу очень часто «приходилось шифровать сообщения в любую свободную минуту». За все время своей работы в качестве шифровальщика Радо Фут в общей сложности отправил более 2 тысяч шифрованных радиограмм — примерно по шесть радиограмм в сутки, в каждой из которых было примерно по 100 слов.

Связь с Центром поддерживалась на определенных частотах. Центр отвечал на своих собственных частотах. Затем обе станции меняли частоты и позывные для вечерней работы. «Обычно я передавал свою информацию в час ночи, — писал Фут. — Если условия передачи были хорошими, а радиограммы — небольшими, мне удавалось закончить работу уже через пару часов. Если же, как это сплошь и рядом случалось, радиограммы были длинными, а атмосферные условия — плохими, я должен был терпеливо дожидаться. пока атмосфера придет в норму, и только тогда начинать передачу радиограмм. Часто в подобных ситуациях мне приходилось засиживаться за своим передатчиком до 6 часов утра, а раз или два — до 9 часов. Такая продолжительная работа нарушала все меры предосторожности в отношении радиоперехвата. Но это был шанс для передачи наших разведывательных данных, и Центр шел на риск, несмотря на неоднократные предостережения с моей стороны и со стороны Радо».

По мере продвижения немцев к Москве поддерживать связь с Центром становилось все труднее и труднее. Совершенно неожиданно, предупредив только вышестоящее руководство и никак не проинформировав своих агентов, с которыми поддерживалась радиосвязь, Центр покинул Москву и переместился в Куйбышев*. Такое перемещение чуть не погубило швейцарскую группу.

* Ныне — Самара.

«19 октября, — писал Фут, — Центр прервал передачу на половине сообщения. Я и Радо по ночам вызывали Центр, но в ответ — ни слова. Радо был в отчаянии и поговаривал о переходе к англичанам. И вдруг однажды ночью в урочное время — после шести недель молчания — Центр откликнулся. Как ни в чем не бывало он закончил передачу телеграммы, прерванную полтора месяца назад».

Информация, которую Центр получал от своей сети в Швейцарии, была очень важна. Росслер снабжал советский Генеральный штаб ни больше ни меньше, как ежедневными боевыми приказами немцев. Советскому командованию это давало возможность совершенно точно определять, какие силы противостоят их войскам. Насколько в Москве верили этой информации, показывает случай, когда там использовали сообщение «Люси», в которое вкралась ошибка или которое было сфальсифицировано (как это случилось, неизвестно до сих пор). В сообщении говорилось о передислокации немецких войск и, по словам Директора, «это обошлось нам в несколько сотен тысяч убитыми под Харьковом и привело к тому, что немцы дошли до Сталинграда».

Как и в случае с разведывательной группой Зорге и «Красным оркестром», шифр, который применялся для засекречивания передаваемых в Москву сообщений, так и не был вскрыт противником. Немецкая радиоконтрразведка и швейцарская полиция перехватили сотни шифрованных сообщений Радо, но не смогли прочесть ни одного из них. Немцы установили абсолютно точно, что радиопередачи велись из Швейцарии. Однако там они не имели права производить аресты, а швейцарская полиция, у которой было на это право, на первых порах не желала предпринимать какие-либо активные действия против антифашистской группы. Однако в конце концов давление со стороны Германии заставило полицейских действовать более решительно.

В октябре 1943 г. швейцарцы напали на след двух радиопередатчиков. 20 ноября в 1.15 ночи Фут принимал очень длинную радиограмму из Центра. Вдруг раздался сильный грохот, и комната заполнилась полицейскими. Фута арестовали, и последнее звено, связывавшее разведывательную сеть «Люси» с Центром, было ликвидировано. Сеть перестала существовать, выполнив задание Центра. И хотя до капитуляции Германии оставалось еще целых полтора долгих года, исход войны не вызывал сомнений — будущее сулило полную победу СССР.

Страны-союзницы СССР во время Второй миро вой войны были постоянными объектами его разведывательной деятельности, а окончание войны позволило эту деятельность активизировать. Наибольших успехов Советский Союз достиг, завербовав так называемых «атомных шпионов» — Клауса Фукса и Аллана Мэя, но советские мастера разведки не брезговали и «мелкой рыбешкой». С началом «холодной войны» советские агенты стали вербоваться еще более интенсивно. Разведывательная сеть СССР покрыла весь мир. Для того чтобы руководить этой сетью и получать сведения от агентуры, требовалось создать развитую систему надежной связи. Чаще всего центрами разведывательной сети СССР служили советские посольства, через которые, в частности, осуществлялась связь агентов с Центром.

В посольстве СССР в Канаде криптографические ключи, которыми пользовался шифровальщик Игорь Гузенко, хранились в специальном опечатанном портфеле. Этот портфель каждую ночь клали в стальной сейф, находившийся в одной из восьми комнат отдельной квартиры. В этой комнате были двойные стальные двери, а окна защищены металлическими щетками и стальными ставнями. Сама комната находилась на втором этаже отдельного крыла посольского здания, которое, в свою очередь, было обнесено очень высоким забором.

В советском посольстве в Австралии, где Владимир Петров шифровал разведывательные сведения, полученные от агентов КГБ, ключ от сейфа с шифрдокументами хранился в опечатанном восковой печатью конверте в главном посольском сейфе. Шифровальный отдел посольства располагался в четырех комнатах. Две из них, наружные, использовались посольством для своей обычной работы по зашифрованию и расшифрованию дипломатической переписки, а в двух внутренних потайных комнатах шифровались разведывательные данные. В столе старшего шифровальщика, стоявшем в наружной комнате, Петров видел четыре револьвера. В обоих посольствах были печи, где за ненадобностью уничтожались секретные материалы.

В 60-х годах в посольстве СССР в Вашингтоне всегда наготове были специальные химикаты, которые за несколько секунд уничтожали толстую кипу бумаги. С помощью этих химикатов избавиться от секретных бумаг можно было значительно быстрее, чем путем их простого сжигания в печи. Насколько серьезно в СССР относились к вопросам обеспечения безопасности, показывает следующий случай. Накануне нового 1956 г. советские дипломаты предпочли, чтобы их посольство в Оттаве сгорело дотла, но не допустили канадских пожарных на его территорию, чтобы те случайно не увидели посольские шифры и коды.

Документы, подлежащие отправке в Москву, фотографировались на пленку и посылались дипломатической почтой в непроявленном виде, чтобы они засветились, если почтовое отправление будет вскрыто посторонним лицом. Такой процедуре подвергались и все материалы, поступавшие в посольство. Когда из Москвы доставлялась фотопленка, она проявлялась, с каждого кадра печатался один увеличенный снимок, а затем негатив уничтожался. В свою очередь, после того как Москва подтверждала получение фотопленки из посольства, все подлинники в нем немедленно уничтожались. Фотопленка, предназначенная для советских органов государственной безопасности, запечатывалась в конверт, на котором проставлялись буквы «П. М. В.» (Палата мер и весов).

В конце 50-х годов для транспортировки непроявленной пленки стали использоваться запираемые контейнеры. При попытке вскрыть такой контейнер на хранимую в нем пленку автоматически впрыскивалась кислота. Новые шифровальные ключи пересылались дипломатической почтой. Они помещались в конверт с фамилией шифровальщика. Затем этот конверт запечатывался и клался в другой конверт, адресованный лично послу. Ключи представляли собой одноразовые шифрблокноты, которые использовались для засекречивания переписки советских зарубежных представительств — дипломатических, государственной безопасности, военных, торговых и партийных. Все телеграммы, поступавшие в советскую дипломатическую миссию, выглядели совершенно одинаково — они представляли собой длинную последовательность групп из пяти цифр. Старший шифровальщик расшифровывал самую последнюю группу и получал, скажем, 66666, что в один день обозначало принадлежность сообщения ГРУ, в другой — КГБ, а в третий — торговому представительству.

Донесения разведчиков писались на русском языке открытым текстом с использованием

шпионского жаргона: слово «упаковка» означало шифрование, «открытая упаковка» — открытый текст, «банк» — тайник и т. д. Кроме того, в подобных письмах широко применялись клички. Например, в Канаде советский военный атташе полковник Заботин имел кличку Грант, Аллан Мэй — Алек. Насколько эффективна была эта предосторожность, видно из доклада канадской комиссии о деятельности советской разведывательной группы. В нем говорилось о том, что члены комиссии так и не смогли установить личности агентов, фигурировавших под псевдонимами Галя, Гини, Голия, Грин и Саренсен, хотя со всей определенностью было выяснено, что они являлись агентами Заботина.

Шифровальщик переписывал сообщение, заменяя в нем имена на клички, а наиболее секретные места — на специальные обозначения (№ 1, № 2 и т. д.). В таком виде письмо фотографировалось. Секретные места, замененные номерами, шифровались отдельно с помощью одноразового шифрблокнота. Полученный цифровой шифртекст, записанный на обычной бумаге, вместе с фотопленкой пересылался дипломатической почтой.

Например, Владимир Петров, проявив фотопленку, полученную из Москвы 25 ноября 1952 г., прочитал: «Просим вас в следующий раз сообщить всю информацию относительно № 42, который фигурирует в папках департамента в связи с № 43, а также в связи с ее № 44 в Спарте.

В зависимости от наличия всех подробностей о № 42 и ее № 44 в Спарте мы будем рассматривать вопрос о № 45 в Суданию одного из наших планировщиков № 46 новатора под видом № 44 к № 42».

Петрову было известно, что на шпионском жаргоне «багаж» означает почту, «департамент» — консульство, «планировщик» — кадровый работник. Далее по списку кодовых обозначений Петров выяснил, что «Спарта» — это СССР, «Судания» — Австралия, «новаторы» — секретные агенты. Дешифровав прилагаемый к фотопленке шифртекст, Петров узнал, что в этом фотописьме «№ 42» — Казанова, «№ 43» — последнее завещание, «№ 44» — родственники, «№ 45» — засылка, «№ 46» — в качестве.

Таким образом, после расшифрования и перевода приведенный выше параграф стал выглядеть примерно следующим образом:

«Просим вас в следующий раз сообщить всю известную вам информацию о Казановой*, которая фигурирует в папках консульства в связи с ее завещанием и родственниками в СССР**.

* Казанова — пожилая русская женщина, проживавшая в Сиднее.

** Которых она пожелала увидеть.

В зависимости от наличия всех подробностей о Казановой и ее родственниках в СССР мы будем рассматривать вопрос о засылке в Австралию одного из наших кадровых работников в качестве секретного агента под видом родственника Казановой».

Применение подобной гибридной шифрсистемы вместо полного зашифрования было обусловлено соображениями удобства. Шифровка всего сообщения отнимала слишком много сил и требовала значительных временных затрат, поскольку шифровальщик осуществлял ее вручную.

Для своих агентов за границей Советский Союз использовал свои самые лучшие средства шифрования. С криптографической точки зрения он никак не рисковал своими агентами или их связями, поскольку для засекречивания их переписки применялись лишь очень стойкие шифрсистемы. Это придавало советским агентам больше уверенности, так как им не следовало бояться дешифровальной службы противника.

Основным шифром советских разведчиков являлся одноразовый шифрблокнот. Его внешний вид был различным. Он мог представлять собой толстую прямоугольную брошюру размером с почтовую марку, а иногда — свернутые полоски бумаги размером с сигаретный окурок. Причем во внешнем виде советских шифрблокнотов отчетливо просматривалась тенденция к уменьшению. Так, шифрблокнот, захваченный в 1954 г., содержал 40 строк по 8 групп из 5 цифр. В другом шифрблокноте, доступ к которому был получен в 1958 г., имелось 30 строк по 10 групп. В шифрблокнотах, захваченных в 1957-м и 1961 гг., было 20 строк по 4 и 5 групп соответственно. Группы, строки и страницы были пронумерованы. Еще один шифрблокнот состоял из 250 страниц, изготовленных из материала, напоминавшего металлическую фольгу. Обычно одна половина шифрблокнота печаталась красным шрифтом, а другая — черным. Вероятно, это делалось, чтобы различать «гамму», применяемую для зашифрования и расшифрования.

Размножение шифрблокнотов производилось простым фотографированием, которое считалось наилучшим способом скопировать «гамму» для агента. Более того, бумага, из которой изготавливались шифрблокноты, делалась из нитроклетчатки — материала, который применялся для производства фотопленки на заре кинематографа. Этот материал очень легко воспламеняется, а с

помощью марганцовокислого калия, который у шпионов всегда под рукой, обычное горение можно было превратить почти во взрыв, который быстро и полностью уничтожал шифрблокнот, не оставляя даже скрытого изображения на пепле.

Интересно, что оригиналы некоторых шифрблокнотов готовились не с помощью высокоточных и производительных печатных механизмов, а на простой пишущей машинке. Это видно из-за наличия в них подтирок и повторных ударов, чего не может быть при полиграфическом способе изготовления.

Более важные наблюдения можно сделать при статистическом анализе цифр, содержавшихся в захваченных шифрблокнотах. В одном из таких шифрблокнотов, например, количество групп, в которых цифры от 1 до 5 чередуются с группами цифр от 6 до 0, было в 7 раз большее по сравнению со случайным распределением. Это наводит на предположение, что машинистка работала поочередно левой рукой (печатая цифры от 1 до 5) и правой (печатая цифры от 6 до 0). Кроме того, вместо половинного количества групп, начинающихся с цифр от 1 до 5, таких групп наблюдается ¾. Это, вероятно, происходило из-за того, что пробел машинистка делала правой рукой, а новую группу печатала левой. Удвоений и утроений отмечается меньше, чем этого следовало ожидать согласно случайному распределению. Возможно, машинистки, которым было приказано печатать цифры наугад, понимали, что повторения неизбежны, но в целях конспирации сводили их число к минимуму. Кроме перечисленных особенностей, в шифрблокноте было слишком мало закономерностей для успешного проведения криптоанализа.

Одноразовые шифрблокноты были захвачены при аресте нескольких советских агентов. Рудольф Абель пользовался шифрблокнотом в форме брошюры размером с почтовую марку. Сотрудники ФБР обнаружили его 21 июня 1957 г. в мусорной корзине в комнате отеля «Латам» в Нью-Йорке в ходе обыска, последовавшего за арестом Абеля. Абель, выдававший себя за художника, спрятал шифрблокнот в выемке обитого наждачной бумагой куска дерева, который прятал в корзине для мусора.

В начале 1961 г. в пригороде Лондона было найдено с полдюжины шифрблокнотов в виде свернутых трубочек бумаги. Английские полицейские отыскали их в зажигалке на даче Елены и Петра Крюгер — двух советских агентов, выдававших себя за семейную американскую пару Лону и Мориса Коэн. Остальные шифрблокноты извлекли из другой зажигалки, обнаруженной на лондонской квартире их руководителя — советского резидента в Англии, известного под вымышленным именем Гордона Лонсдейла.

Английский ученый-атомщик Джузеппе Мартелли, которому было предъявлено обвинение в шпионаже против Англии в пользу Советского Союза, носил при себе два шифрблокнота, спрятанные в пачке сигарет и обнаруженные в 1963 г. при его аресте в лондонском аэропорту. Семь сигарет в пачке были нетронуты, а шесть других были склеены друг с другом и частично вырезаны, чтобы освободить место для блокнотов.

У Абеля в его художественной студии в Бруклине был коротковолновый передатчик, а в отеле «Латам» приемник. Он говорил своему помощнику о том, что записывает поступающую из Центра информацию на магнитофон, затем переписывает ее на бумагу и расшифровывает. После ареста Абеля американские контрразведчики следили за радиопередачами в соответствии с расписанием, найденным у Абеля в полом конце карандаша, и дважды перехватывали радиограммы, состоявшие из пятизначных цифровых групп.

Наряду с шифрблокнотами английская полиция обнаружила в зажигалке Крюгера расписание радиопередач. В соответствии с этим расписанием, настроившись на частоту 17080 килогерц, 9 января 1961 г. в 12.32 по Гринвичу полиция услышала позывной «277». Через 18 минут тот же самый позывной был принят на частоте 14755 килогерц. 18 января в 6.38 по Гринвичу на частоте 6340 килогерц снова был услышан позывной «277». Меньше чем через час этот позывной был замечен на волне 8888 килогерц. Пеленгаторы установили, что источник радиопередач находится в Москве. Лонсдейл имел высокоскоростной радиопередатчик, который посылал 240 слов в минуту. Советский разведчик записывал свои сообщения на пленку и затем на большой скорости передавал их в эфир.

Радиообмен советских агентов был довольно интенсивным. Крюгер осуществлял контакты с Центром по радио во вторник, среду, пятницу и субботу. Такая частота сеансов связи объясняет, почему при аресте Абеля и четы Крюгер их застали за шифрованием донесений в Центр. При аресте Абель попытался засунуть шифровку в рукав, а г-жа Крюгер перед тем, как выйти из дома, попросила у конвоиров разрешение затопить печь. Однако после того как из ее сумочки был изъят конверт с листом бумаги, на котором были напечатаны цифры, она потеряла всякий интерес к печи.

Для передачи разведывательной информации советские агенты наряду с радио часто применяли микроточки. У Лонсдейла был прибор для чтения микроточек, который он держал в банке с тальком.

Абель изготовлял микроточки, уменьшая размер кадра 35-миллиметровой фотопленки с помощью линзы с очень малым фокусным расстоянием. Чтобы сохранить четкость при таком уменьшении, он использовал фотопленку с самой высокой разрешающей способностью из тех, которые продавались в магазинах. Для пересылки подготовленного материала Абель расшивал журналы по домоводству и садоводству, помещал в их корешок микроточки, снова переплетал эти журналы и посылал их по определенному адресу в Париж. По каким-то причинам эта скрытая информация не дошла до адресата, и Москва попросила Абеля прекратить отправку подобных сообщений. Однако он по-прежнему продолжал получать инструкции из Центра в виде микроточек.

Как уже отмечалось выше, советским агентам не грозит опасность быть разоблаченными из-за слабости применяемых ими шифровальных средств. Возьмем, к примеру, шифр, который использовал помощник Абеля Рейно Хейханен. В течение двух лет толстый, ленивый и безответственный Хейханен, проживавший в Нью-Йорке, лично не встречался с Абелем, а связывался с ним, оставляя сообщения в тайниках — таких, как трещина в цементной стене между 165-й и 167 улицами в Бронксе, или за вынимающимся кирпичом под мостом в Центральном парке, или под фонарными столбами в парках и на улицах. Сообщения были на так называемой мягкой микропленке, которую собственноручно изготавливал Абель. Он растворял твердую основу пленки и оставлял только мягкий эмульсионный слой, который легко было поместить в потайное место. В качестве контейнеров для сообщений, оставляемых в тайниках, Абель и курьеры из Москвы использовали высверленные карандаши, болты, батарейки и монеты. Даже будучи случайно обнаруженными, они не вызвали бы особых подозрений. Горизонтальная отметка голубым мелом в заранее обусловленных местах на заборах и на станциях метро означала, что сообщение находится в тайнике. Вертикальная отметка сигнализировала о том, что сообщение уже изъято. Эти отметки нужно было проверять ежедневно. 21 октября 1952 г., вскоре после прибытия Хейханена в Нью-Йорк, он оставил в одном из тайников свое первое сообщение. Москва ответила ему шифровкой на мягкой микропленке, помещенной в полую монету выпуска 1948 г. В шифровке говорилось.

«1. Поздравляем с благополучным прибытием. Подтверждаем получение вашего письма, адресованного V, и прочтение письма № 1.

2. Для организации прикрытия дано указание переслать вам 3 тысячи в местной валюте. Посоветуйтесь с нами перед тем, как вложить эти средства в какое-нибудь дело.

3. Согласно вашей просьбе, мы вышлем вам формулу изготовления мягкой микропленки и другую дополнительную информацию вместе с письмами вашей матери.

4. Пока еще слишком рано передавать вам одноразовые шифрблокноты. Короткие письма шифруйте, а при работе с длинными письмами применяйте вставки*. Шифровки не должны содержать данные о вас, вашем месте работы, адресе и т. д. Вставки также высылайте отдельно.

* Вероятно, по технологии, описанной Петровым.

5. Посылка была лично вручена вашей жене. В вашей семье все в порядке. Желаем удачи. Привет от товарищей.

№1, 3 декабря».

Однако полая монета заблудилась. Скорее всего, Хейханен, который отличался небрежностью, просто истратил ее. Монета ходила среди миллионов подобных ей монет, и никто не догадывался о ее содержимом. Но однажды жарким летним утром 1953 г. разносчик газет Джеймс Бозарт, который только что получил сдачу 50 центов в виде пяти монет в Бруклине, уронил их на лестницу. Когда он наклонился, чтобы поднять монеты, то увидел, что одна из них распалась пополам. В половинке этой монеты находилась микропленка, завернутая в папиросную бумагу. Бозарт передал эту микропленку полицейским, которые переправили ее в ФБР. Там попытались расшифровать попавший к ним в руки материал, однако предпринятая попытка потерпела полный провал.

Четыре года спустя Хейханен явился с повинной в американское посольство в Париже, где он оказался, следуя на «заслуженный отдых» в СССР, куда его отправил Абель, разочаровавшийся в своем помощнике. Хейханен передал в ФБР применявшиеся им в переписке с Москвой шифрсистемы и ключи. Летом 1957 г. эксперт ФБР Майкл Леонард применил полученные от Хейханена сведения для чтения материала на микропленке, найденной Бозартом, и убедился, что попытки ФБР вскрыть используемую Хейханеном шифрсистему, имея на руках один только шифртекст, были абсолютно тщетными.

Таково состояние дел в русской криптографии. Представляет интерес поразмышлять о ее успехах. Россия сама по себе остается загадкой, овеянной тайной из тайн. То же самое касается и ее

средств связи. Одноразовые шифрблокноты обеспечивают надежную защиту для сообщений российских разведчиков, военных, дипломатов и работников тайной политической полиции. Грамотно сконструированные шифраторы навечно сохраняют в секрете от врагов России ее наиболее важную дипломатическую, агентурную и военную переписку. В период «холодной войны» русские сумели вскрыть шифры американского посольства в Москве. Такие подвиги свидетельствуют об их осведомленности, базирующейся на глубоком понимании шифровального дела и криптоанализа. Исходят ли эти знания из врожденной способности русских к естественным наукам, что позволило им первыми запустить искусственные спутники Земли, или же из большого опыта в области криптологии, которая исправно служила коммунистическим диктаторам в России в их борьбе за власть, или же из привычки, которая впиталась в кровь всякому жителю тоталитарного общества, на каждом шагу видеть и разгадывать секреты, или из врожденной любви славян ко всему таинственному в природе, но так или иначе русские вознесли достижения своей страны в криптологии до высоты полета ее космических спутников.

КОМНАТА 40

Рано утром 5 августа 1914 г., в один из первых дней мировой войны, которая до основания потрясла всю Европу и унесла миллионы человеческих жизней, произошло на первый взгляд малозначительное событие, которому тем не менее суждено было войти в историю. Глава английской военно-морской разведки контр-адмирал Генри Оливер отправился позавтракать к Альфреду Юингу, ведавшему в Адмиралтействе вопросами военно-морской подготовки. Во время завтрака Оливер случайно упомянул, что Адмиралтейство в большом количестве получает шифрованные немецкие сообщения, перехваченные военно-морскими и коммерческими радиостанциями, и что эти сообщения скапливаются у него, так как в его распоряжении нет отдела, который мог бы заняться их дешифрованием. Юинг проявил большую заинтересованность и попросил как можно скорее продемонстрировать ему вражеские шифровки. Когда после полудня Юинг увидел их воочию, он тотчас высказал предположение, что перед ним военно-морские радиограммы противника. Добавив, что их чтение могло бы иметь огромное значение для победы над врагом, Юинг попросил именно ему доверить решение этой сложной задачи.

В 1914 г. Юингу исполнилось 59 лет. Это был небольшого роста, коренастый шотландец с голубыми глазами, густыми бровями, тихим голосом и манерами доброго доктора. Три года назад он получил дворянский титул за выдающийся вклад в науку и за заслуги перед обществом, среди которых особо было отмечено его плодотворное руководство военно-морской подготовкой. И вот теперь, несмотря на преклонный возраст, Юинг вознамерился основать криптоаналитическое бюро, которому предстояло оказать непосредственное и весьма ощутимое влияние на ход мировой истории.

Юинг начал с тщательного изучения криптографических материалов, имевшихся в книгохранилищах библиотеки Британскою музея. Потом он перешел к изучению кодов на городском центральном почтамте, где хранились экземпляры коммерческих кодовых книг. Одновременно Юинг приобщил к своей деятельности четырех преподавателей военно-морских колледжей. Все они были его друзьями, хорошо знали немецкий язык и, собравшись вместе за столом в кабинете Юинга, изучали непонятные строки букв и цифр, имея лишь самое общее представление о том, с чего начать работу над вскрытием шифров.

Среди первых перехваченных немецких сообщений было одно, которое, если бы его удалось разгадать, сразу бы направило течение войны совсем в иное русло. Оно находилось в первой партии телеграмм, показанных Оливером Юингу 5 августа. Это сообщение было составлено верховным командованием военно-морских сил Германии 4 августа в 1.35 ночи и немедленно передано командующему на Средиземном море адмиралу Вильгельму Сушону. В сообщении говорилось: «3 августа заключили соглашение о союзе с Турцией. Немедленно следуйте в Константинополь». На тяжелом крейсере «Гебен» в сопровождении легкого крейсера «Бреслау» Сушон направился из центральной части Средиземноморья на восток. Английская средиземноморская эскадра, будучи абсолютно уверена, что Сушон попытается прорваться через Гибралтарский пролив, усердно бороздила море к западу от Сицилии. Когда английский крейсер, наконец, обнаружил Сушона, идущего курсом на восток, англичане предприняли отчаянную попытку настичь и уничтожить «Гебен» с «Бреслау». Однако те все же сумели ускользнуть, затерявшись среди греческих островов. В воскресенье, 10 августа, «Гебен» на полных парах вошел в Дарданеллы, неся с собой, по словам главы английского Адмиралтейства лорда Уинстона Черчилля, «больше кровопролития, страданий и разрушений, чем когда-либо причинял один военный корабль». Проведенный «Гебеном» мощный

артиллерийский обстрел русских портов на Черноморском побережье помог втянуть в войну Турцию. В результате Россия оказалась изолированной от своих союзников, что в значительной мере способствовало ее последующей капитуляции со всеми вытекающими последствиями. Если бы английское Адмиралтейство оказалось в состоянии прочесть шифрованные приказы Сушону из Берлина, Англия, скорее всего, выиграла бы роковую игру в прятки с «Гебеном» и «Бреслау», и это имело бы более важные последствия, чем любой другой единичный успех в Первой мировой войне.

Об этой упущенной возможности повлиять на ход войны в самом ее начале Юинг так никогда и не узнал. Интересно, что в то самое воскресенье, когда «Гебен» вошел в Дарданеллы, Юинг написал своей семье в Шотландию: «Нахожусь в самой гуще специальной работы, выходящей за рамки моих обычных занятий». К этому времени им были изучены коды нескольких немецких коммерческих фирм, но проделанная работа была выполнена, как вскоре выяснилось, впустую. Ненамного полезнее оказался и сигнальный код, который использовался немецкими кораблями сторожевого охранения и был реквизирован на немецком торговом судне, захваченном в Австралии. Никто из небольшой группы английских пионеров-дешифровальщиков не мог похвастать основательными знаниями из области криптоанализа, и поэтому в первые недели войны их успехи были ничтожны.

Тем не менее «специальная работа» настолько увлекла Юинга, что лишь в воскресенье 25 октября он устроил себе день отдыха. Юинг старался не зря: в сентябре Англии представился счастливый случаи, который дал такой мощный толчок ее усилиям наладить криптоанализ перехваченных криптограмм противника, что в течение всего оставшегося периода войны она намного опережала своих противников в дешифровании. О том, что произошло, лучше всех рассказал в своих мемуарах Черчилль:

«В начале сентября 1914 г. на Балтийском море был потоплен немецкий легкий крейсер «Магдебург». Несколько часов спустя русские выловили из воды тело утонувшего немецкого младшего офицера. Окостеневшими руками мертвеца он прижимал к груди кодовые книги ВМС Германии, а также разбитые на мелкие квадраты карты Северного моря и Гельголандской бухты. 6 сентября ко мне с визитом прибыл русский военно-морской атташе. Из Петрограда он получил сообщение с изложением случившегося. Оно уведомляло, что с помощью кодовых книг русское Адмиралтейство в состоянии дешифровать по меньшей мере отдельные участки немецких военно-морских шифртелеграмм. Русские считали, что Адмиралтейству Англии, ведущей морской державы, следовало бы иметь эти книги и карты. И если бы мы прислали корабль, то русские офицеры, в ведении которых находились книги, доставили бы их в Англию. Мы незамедлительно отправили такой корабль, и октябрьским вечером принц Луи* и я получили из рук наших верных союзников слегка попорченные морем бесценные документы».

* Принц Луи Баттельбергский, первый морской лорд Англии.

Это произошло 13 октября. Но даже поразительная, неожиданная удача с кодовыми книгами «Магдебурга» (пожалуй, самая счастливая во всей истории криптоанализа) не дала группе Юинга возможность немедленно приступить к чтению немецких военно-морских шифрсообщений, так как в них впрямую не использовались кодовые обозначения из этих книг. Чтение началось только тогда, когда офицер английской интендантской службы Чарльз Роттер, ведущий эксперт по Германии, обнаружил, что кодовые группы дополнительно перешифровывались по довольно простому алгоритму. Нахождение такой перешифровки не является слишком трудной проблемой, если в распоряжении криптоаналитика имеется кодовая книга. Как и в обычном открытом тексте, отдельные кодовые обозначения повторяются чаще других. В сходных сочетаниях буквы одного кодового обозначения повторяются в других кодовых обозначениях, но в ином расположении. Самим кодовым обозначениям присуща определенная структурная система: в случае с немецким военно-морским кодом, полученным англичанами от русских, согласные чередовались с гласными. Когда характерные особенности кода известны, умелый криптоаналитик может эффективно использовать их для снятия перешифровки.

Но английские криптоаналитики были еще настолько неопытны, что им потребовались почти три недели, чтобы начать читать отдельные участки некоторых немецких военно-морских донесений. Эти донесения, по утверждению Черчилля, «носили, главным образом, характер текущей служебной переписки: «В 8 часов вечера один из наших торпедных катеров выходит в квадрат 7» и так далее. Однако скрупулезное накопление этих отрывочных сведений составляло основу информации, по которой с достаточной степенью точности можно было определять характер военных приготовлений противника в Гельголандской бухте, прилегающей к северо-западному побережью Германии».

В октябре 1914 г. количество сотрудников группы Юинга выросло настолько, что они до отказа заполнили служебный кабинет своего начальника. Их постоянно раздражало, что приходится откладывать работу, когда Юинг принимает посетителей по вопросам военно-морской подготовки. Поэтому приблизительно в середине ноября вся криптоаналитическая группа перебралась в большую комнату под номером 40, расположенную в старом здании Адмиралтейства. К комнате прилегало маленькое помещение, в котором стояла походная кровать для отдыха. Расположена комната 40 была очень удачно: она находилась в стороне от наиболее оживленных помещений Адмиралтейства и в то же время — сравнительно близко к оперативному отделу, который получал от нее дешифровки радиограмм противника. И хотя группа стала официально именоваться 25-м отделением разведывательного отдела, название «комната 40» оказалось настолько удобным и безобидным, что вскоре стало олицетворять общепринятое название отделения. Это название сохранилось даже тогда, когда отделение перевели в другое, более просторное помещение.

В конце декабря 1914 г. английский траулер выловил тяжелый ящик, в котором были обнаружены различные книги и документы на немецком языке. Ящик был выброшен за борт с немецкого эскадренного миноносца, потопленного более двух месяцев назад в ходе сражения в Гельголандской бухте. Среди прочего в ящике находился важный немецкий код, которого недоставало в магдебургской находке. Криптоаналитики комнаты 40 немедленно использовали его для чтения сообщений, которые передавал немецкий крейсер, препятствовавший английскому судоходству. Идентичный код использовался для засекречивания телеграфной переписки между Берлином и немецкими военно-морскими атташе за границей, однако об этом в комнате 40 узнали только несколько месяцев спустя.

С увеличением потока сообщений на работу в комнату 40 принимались все новые и новые сотрудники, причем часто это делалось в чисто английской манере. Однажды вечером Фрэнсис Той, который во время войны работал администратором тюрьмы для военнопленных и переводчиком, а после ее окончания стал известным музыкальным критиком, присутствовал на обеде в лондонской квартире видного финансиста Макса Бонна. Среди гостей оказался один из сотрудников комнаты 40 — Фрэнк Тиаркс, компаньон банковской фирмы «Дж. Шредер энд К°» и директор Английского банка.

Той вспоминает:

«Мы долго беседовали, а после обеда Тиаркс отозвал меня в сторону и спросил, не хотел бы я перейти в Адмиралтейство. Выразив уместное и совершенно неподдельное удивление, я ответил, что не вижу, какую пользу могут принести мои услуги Адмиралтейству.

— Макс только что сообщил мне, что вы очень хорошо знаете немецкий, — ответил он. — Очевидно, вы умны и, судя по вашей характеристике, внушаете доверие. Есть сотни людей с одним из этих качеств, несколько человек — с двумя и очень мало таких, у которых все эти три качества присутствуют одновременно. Что вы на это скажете?

— А как же с моей работой в военном министерстве?

— Если вы придете к нам на работу, вы можете во всем положиться на нас.

— Ну, конечно, я приду, если я действительно так нужен.

— Очень хорошо, я наведу о вас справки, и вам сообщат в надлежащее время...

Примерно две недели спустя меня вызвал начальник и молча протянул телеграмму военного министерства: «Лейтенант-переводчик Той должен как можно быстрее прибыть в Адмиралтейство для выполнения особого задания». Каковы же могущество и быстрота действий английского Адмиралтейства, коль оно так скоро приняло решение! Подумайте, сколько бюрократических преград пришлось ему преодолеть за какие-то две недели!»

Тем временем английская военно-морская разведка бурно развивала деятельность, сопутствующую криптоанализу. На побережье были сооружены крупные радиопеленгаторные станции. Получаемые данные они передавали в Адмиралтейство, оказывая огромную помощь в определении местонахождения немецких кораблей и подводных лодок. Безусловно, немцы понимали, что, кроме как сохранять полное радиомолчание, другого пути избежать радиопеленгации не было. Учитывая это, Англия даже не пыталась держать в секрете свою деятельность в области радиопеленгации, используя ее в качестве дымовой завесы для ведения менее явной для противника и более ценной криптоаналитической работы.

Другими источниками радиоразведки являлись опознавание радиопозывных вражеских кораблей и определение «почерка»* их радиооператоров. Например, если Адмиралтейству становилось известно, что позывной, переданный по радио в Северном море, принадлежал 12-орудийному линкору «Вестфален», оно выбирало несколько иную тактику действий, нежели если бы он исходил

от подводной лодки «У-20». Данные радиоразведки вместе с дешифровками и другой информацией, поступавшей в Адмиралтейство, систематизировались и интерпретировались адмиралом Артуром Вильсоном, которому Черчилль поручил доводить основное содержание получаемых данных до сведения высших английских военачальников. Результаты не заставили себя долго ждать.

* «Почерк» — отличительные особенности в передаче азбуки Морзе.

14 декабря 1914 г. в 7 часов вечера Вильсон прибыл к Черчиллю, чтобы доложить о том, что разведка сообщила о боевом выходе немецких кораблей, направлявшихся к английскому побережью. Не прошло и трех часов, как Адмиралтейство отдало приказ кораблям английского флота немедленно следовать в «пункт, где они наверняка смогут перехватить корабли противника на их обратном пути». В результате, пока эскадра немецких крейсеров обстреливала английские прибрежные города, четыре линейных крейсера и шесть самых мощных в мире линкоров расположились восточнее этого района, отрезав немецким кораблям пути отхода. Когда после завершения бомбардировки немцы пошли обратным курсом на свою базу, погода резко испортилась, и шторм ухудшил видимость. Но разведка Адмиралтейства настолько точно расположила легкий крейсер «Саутгемптон» на пути движения немецких кораблей, что в 10.30 утра командир «Саутгемптона» У. Гудинаф увидел их перемещавшиеся в тумане контуры. Чтобы убедиться, что перед ним корабли противника, он передал им свой световой опознавательный сигнал. Поскольку должного ответа не последовало, Гудинаф приказал открыть по ним огонь. Однако вскоре из-за плохой погоды контакт с вражескими кораблями был потерян.

Два часа спустя крупные силы англичан снова обнаружили противника. Но когда командующий немецкими легкими крейсерами увидел гигантские контуры английских линейных кораблей, смутно вырисовывавшиеся сквозь моросящий дождь, он, проявив смекалку, передал световой опознавательный сигнал, который незадолго до этого получил от Гудинафа. Затем немцы свернули в сторону и скрылись за пеленой тумана прежде, чем обман был обнаружен и огонь английских орудий разнес их корабли на клочки.

Разочарованию, воцарившемуся в английском военно-морском флоте, который буквально рвался в бой с немецким, не было конца и края. Утешение пришло лишь немногим более месяца спустя, когда у англичан снова появилась реальная возможность помериться силами с немцами. В полдень 23 января 1915 г. в кабинет Черчилля вошел Вильсон и сообщил: «Первый лорд, они опять выходят в море». — «Когда?» — спросил Черчилль. «Сегодня вечером, — ответил Вильсон. — У нас как раз достаточно времени, чтобы послать туда Битти»*.

* Битти Давид — английский вице-адмирал

Далее Вильсон объяснил Черчиллю, что главным источником его разведывательных данных явилась полученная из комнаты 40 дешифровка криптограммы, направленной в 10.25 утра того же дня немецкому контр-адмиралу Францу Хипперу. В ней говорилось: «1-я и 2-я поисковые группы, старший офицер эсминцев и две флотилии, которые будут отобраны старшим офицером поисковых сил, должны провести рекогносцировку... Им следует выйти из порта сегодня вечером с наступлением темноты».

Англичане решили прибегнуть к прежней тактике: их корабли под командованием Битти немедленно вышли в море, чтобы блокировать обратный путь немецких кораблей. На этот раз им повезло больше. На следующий день в 7.30 утра противник был обнаружен. Когда Хиппер увидел перед собой многочисленные силы англичан, он тут же пустился наутек, а англичане на своих быстрых линкорах начали преследование. К 9 часам вечера линкор «Лайон», на борту которого находился Битти, смог открыть прицельный огонь по кораблям противника. Вскоре завязался бой между четырьмя английскими и четырьмя немецкими крупными боевыми кораблями. Однако замешательство в английской эскадре, возникшее после того, как вражеский снаряд повредил ее флагман, позволило немецким кораблям скрыться.

Это морское сражение окончательно укрепило доверие Адмиралтейства к информации, получаемой из комнаты 40, и вскоре Юингу была предоставлена полная свобода действий относительно всего, что он считал необходимым сделать для улучшения своей работы. Юинг увеличил штат сотрудников, улучшил оборудование на своих радиоперехватывающих и радиопеленгаторных станциях, довел их число до полусотни.

В итоге, когда немецкий вице-адмирал Рейнхард Шеер, раздраженный своей вынужденной

бездеятельностью, решил заманить часть военных кораблей Англии туда, где без особых помех их могли бы атаковать подводные лодки и флот Германии, отдаваемые Шеером приказы регулярно попадали в умелые руки английских криптоаналитиков. Поэтому, когда 30 мая 1916 г. немецкий флот начал сниматься с якорей, Адмиралтейство быстро оказалось в курсе этого события и уже в 5 часов дня смогло уведомить о нем свои военно-морские силы. После получения уведомления фактически весь английский флот величественно вышел в открытое море. Он должен был принять участие в крупной морской операции, которая в случае успеха обеспечила бы Англии неоспоримое превосходство над противником на морских просторах.

Однако тут произошла одна из многих незначительных ошибок, которые так часто меняют весь ход мировой истории. Сразу после отплытия Шеер поменял позывные, передав позывной своего флагманского корабля портовому военно-морскому центру. В результате командующий объединенным английским флотом адмирал Джон Джелликоу получил уведомление о том, что в 11.10 утра радиостанция направленного действия обнаружила флагманский корабль противника в порту. Три часа спустя, когда Джелликоу полагал, что немцы все еще находятся в порту, английские и немецкие боевые корабли уже встретились в Северном море. Такое неожиданное развитие событий до некоторой степени поколебало веру Джелликоу в разведку Адмиралтейства. Его вере был нанесен еще один удар, когда в соответствии с очередным сообщением Адмиралтейства он нанес на карту местоположение немецкого крейсера «Регенсбург» и обнаружил, что оно оказалось в том же самом месте, в котором в то время находился он сам. Откуда Джелликоу мог знать, что виноват в получении этого абсурдного результата был штурман «Регенсбурга», допустивший ошибку в своих расчетах, а не криптоаналитики комнаты 40?!

В 9.14 вечера после короткого, не имевшего решающего значения боя, получившего громкое название битвы за Ютландию, Шеер отдал приказ своим кораблям начать движение в указанном им направлении. В 9.46 он слегка скорректировал их курс. Обе шифртелеграммы Шеера были быстро прочитаны комнатой 40, и в 10.41 их резюме было получено на борту английского флагманского корабля. Однако к этому времени Джелликоу был сыт разведкой Адмиралтейства по горло. Поэтому он проигнорировал полученную информацию, которая на этот раз была правильной. В результате надежда Англии на решительную победу на море испарилась в сумбуре ошибок, упущенных возможностей и недоверия.

После битвы за Ютландию Германия сделала ставку на ведение подводной войны. Соответственно у комнаты 40 возрос интерес к радиосообщениям немецких подводных лодок. Пытаясь заполучить любые сведения относительно аппаратуры связи, установленной на субмаринах противника, Адмиралтейство обзавелось судном с водолазом, оснащенным специальным оборудованием для обследования затонувших подводных лодок.

Работу водолаза поручили Е. Миллеру — худощавому и бледному, но выносливому молодому инструктору водолазного дела, отличавшемуся необычайной смелостью и способностью выдерживать давление на больших глубинах. Уже во время своего первого погружения через пробоину в корпусе он проник внутрь немецкой подводной лодки и начал поиск в кромешной темноте, натыкаясь на какие-то предметы. После включения фонаря выяснилось, что это были трупы немецких моряков. Пробравшись между ними, Миллер открыл расположенную в кормовой части дверь офицерского кубрика. Внутри помещения он обнаружил железный ящик, в котором находились кодовые книги.

Находка Миллера оказалась настолько ценной, что подводная охота за кодами стала его основным занятием на войне. Согласно его воспоминаниям, это была неприятная работа:

«Акулы всегда держались поблизости и были готовы сожрать кого угодно. В сезон спаривания их, естественно, возмущает любой незваный гость, и очень часто, когда они преследовали меня, я предлагал им свой ботинок, и они обязательно кусали его... Внутри лодок происходили довольно фантастические сцены... Я обнаружил множество огромных морских угрей. Все они усердно питались трупами. Довольно шокирующее зрелище».

Несмотря на отвратительные стороны работы, Миллеру почти каждый раз удавалось обнаружить железный ящик, знакомый ему еще по самому первому погружению. На одной из немецких подводных лодок, внутреннее устройство которых Миллер теперь знал как свои пять пальцев, он обнаружил совершенно новый военно-морской код, в котором криптоаналитики комнаты 40 испытывали острую необходимость. Эта находка Миллера оказала им существенную помощь в чтении увеличивающегося объема шифрпереписки субмарин противника.

С ростом объема читаемой шифрпереписки противника комната 40 перестала просто направлять отредактированные материалы радиоперехвата оперативному управлению Адмиралтейства, а стала

посылать туда ежедневные сводки, включавшие криптоаналитическую, пеленгационную и другую радиоразведывательную информацию. После войны было подсчитано, что с октября 1914 г. по февраль 1919 г. комнатой 40 было перехвачено и прочитано более 15 тысяч немецких шифрсообщений.

Работа велась круглосуточно, даже во время бомбардировок, когда в целях светомаскировки окна задергивали хорошо пригнанными непроницаемыми шторами. Штат сотрудников комнаты 40 еще более расширился за счет раненых офицеров и студентов немецких университетов, с началом мировой войны вернувшихся в Англию. Последним присваивалось офицерское звание в добровольческом резерве английских ВМС, с тем чтобы они могли носить форму во избежание косых взглядов гражданского населения. На работу в комнату 40 были приняты женщины, которые освободили криптоаналитиков от канцелярской работы.

Наиболее важное изменение в штате сотрудников комнаты 40 произошло в связи с отставкой Юинга, которому в мае 1916 г. была предложена должность ректора Эдинбургского университета. Предложение было заманчивым, особенно для Юинга, который в течение 25 лет с успехом занимался сугубо научной деятельностью, прежде чем в 1903 г. перейти в Адмиралтейство. Вдобавок к этому времени Юинг уже принимал мало участия непосредственно в дешифровальной работе, поскольку в комнате 40 появились сотрудники, чьи криптоаналитические способности намного превосходили его собственные. А Юинг превратился в обыкновенного администратора.

Руководство Адмиралтейства заявило Юингу, что не возражает против его перехода, поскольку он настолько хорошо организовал работу комнаты 40, что мог без всякого ущерба делу передать свои полномочия другому лицу. Поэтому Юинг принял эдинбургское предложение, и с 1 октября 1916 г. бразды правления комнатой 40 перешли в твердые руки очень примечательного человека, который производил незабываемое впечатление на всех, с кем встречался.

Начальник военно-морской разведки Англии капитан Уильям Холл почти в буквальном смысле был рожден для разведывательной работы. Его отец был первым начальником отдела разведки Адмиралтейства. В 14 лет Холл поступил на службу в военно-морские силы и к 35 годам был произведен в капитаны. В ноябре 1914 г., после краткого периода командования сначала крейсером, а потом линкором, он возглавил военно-морскую разведку.

Энергичный, живой 45-летний мужчина с куполообразной, преждевременно облысевшей головой и большим крючковатым носом, Холл обладал проницательным, гипнотизирующим взглядом. «Какие глаза у этого человека! — писал президенту США Вудро Вильсону американский посол в Англии Уолтер Пэйдж. — Во время разговора с вами Холл видит вас насквозь и замечает малейшее движение каждого мускула вашей бессмертной души». Из-за нервного тика один глаз у Холла непрерывно дергался, за что он получил прозвище «мигалка».

Энергия и уверенность наполняли весь облик Холла. «Он более всех, кого я когда-либо знал, вызывал желание сделать что-нибудь для него, — вспоминает о Холле Фрэнсис Той. — Когда он разговаривал с вами, вы чувствовали, что сделаете для него все чтобы заслужить его похвалу». Лучше всех краткую характеристику Холлу дает Пэйдж: «Холл — один из тех гениев, которых породила война. Ни в воображении, ни в действительности вы не найдете человека, который мог бы с ним сравниться. Среди его удивительных дел, известных мне, есть несколько, описание которых заняло бы целый волнующий том. Этот человек — гений, бесспорный гений. По сравнению с ним все остальные сотрудники секретной службы — простые любители».

В начале 1917 г. Холлу и Пэйджу предстояло вместе окунуться в мрачный водоворот международных интриг и пропаганды, которые должны были самым решительным образом сказаться на ходе войны. Однако ни тот, ни другой не подозревали обо всем этом, когда осенью 1916 г. Холл официально принял дела у Юинга.

ШИФРТЕЛЕГРАММА ЦИММЕРМАНА

Утром 17 января 1917 г. Уильям Монтгомери, работавший криптоаналитиком в дипломатическом отделении комнаты 40, пришел доложить Холлу о перехваченной немецкой шифртелеграмме, которая показалась ему чрезвычайно важной. Интуиция не подвела Монтгомери. Эта шифртелеграмма, которую он вместе со своим молодым коллегой Найджелом Греем сумел частично прочесть, действительно содержала уникальную информацию, которая при умелом использовании могла существенно повлиять на исход войны.

Шифртелеграмма была очень длинной и состояла примерно из тысячи цифровых кодовых групп. Посланная из Берлина и датированная 16 января, она была адресована немецкому послу в

Соединенных Штатах Иоганну Бернштorффу. Ее открытый текст был закодирован с помощью дипломатического кода, известного английским криптоаналитикам как код 0075. Над ним в комнате 40 работали в течение последних шести месяцев. Там знали, что код 0075 принадлежал к серии неалфавитных кодов, которые немецкое министерство иностранных дел обозначало четырехзначным числом, составленным из двух нулей и двух ненулевых цифр, причем разность между отличными от нуля цифрами всегда равнялась двум. В список аналогичных кодов, которые к тому времени уже были вскрыты в комнате 40, входили коды 0097 и 0086, применявшиеся дипломатическими миссиями Германии в Южной Америке, код 0064, использовавшийся, например, для связи между Берлином и Мадридом, а также коды 0053 и 0042.

Министерство иностранных дел Германии впервые направило код 0075 своим миссиям в Берне, Бухаресте, Вене, Гааге, Константинополе, Копенгагене, Осло, Софии и Стокгольме в июле 1916 г. В ноябре комната 40 начала осуществлять перехват зашифрованных тем же кодом телеграмм посольству Германии в Соединенных Штатах. В результате англичане накопили достаточное количество копий немецких телеграмм, засекреченных с помощью кода 0075, что дало Монтгомери и Грею возможность продвинуться в работе над его вскрытием.

Хотя Монтгомери и Грей смогли прочесть лишь отдельные части большой немецкой шифртелеграммы от 16 января 1917 г., они сумели установить, что она состояла из двух частей и была подписана министром иностранных дел Германии Артуром Циммерманом. Насколько они могли судить об открытом тексте этой шифртелеграммы на основе частичного вскрытия кода 0075, вторая ее часть предположительно гласила:

«Совершенно секретно. Для личной информации Вашего превосходительства и для передачи надежным путем имперскому посланнику в Мехико...

С 1 февраля мы намерены начать неограниченную подводную войну. Поступая таким образом, мы, однако, приложим все усилия к тому, чтобы Америка оставалась нейтральной. Если нам не удастся осуществить это, мы предлагаем Мексике союз на следующей основе: совместное ведение войны, совместное заключение мира...

Вашему превосходительству надлежит секретно проинформировать президента* лишь о том, что мы ожидаем войну с США и, возможно, с Японией, и одновременно попросить его провести переговоры между нами и Японией. Сообщите президенту, что... наши подводные лодки... в течение нескольких месяцев вынудят Англию заключить мир.

Циммерман»

* Мексики

Монтгомери передал эту частично прочитанную шифртелеграмму Холлу, который несколько раз перечитал фразы о «неограниченной подводной войне» и «совместном ведении войны» с Мексикой. Ему сразу же стало ясно, что перед ним дипломатическое оружие с огромными потенциальными возможностями. Он приказал Монтгомери ускорить работу над дальнейшим чтением шифртелеграммы, а также сжечь все ее копии, за исключением подлинника и единственного варианта открытого текста. А сам тем временем занялся анализом сложившегося положения на фронтах Первой мировой войны.

Оно было мрачным, под стать суровому зимнему дню 17 января 1917 г. Война, которая, как все поначалу надеялись, закончится за несколько недель, длилась уже почти три года, и все равно надежды на ее успешное завершение не было почти никакой. В сражении под Верденом Франция потеряла полмиллиона жизней, а удалось ей лишь восстановить ту линию фронта, которая сложилась десятью месяцами ранее. Англия отчаянно пыталась удержать несколько километров сплошь изрытой снарядами земли у французской реки Соммы, но, лишившись 60 тысяч человек всего лишь за один день битвы, обессиленная, была вынуждена отступить. На Востоке Румыния, новый союзник Антанты, была молниеносно разломлена и оккупирована немцами, а Россия уже балансировала на грани военного поражения. Развязывание Германией подводной войны усилило экономическое давление на Англию. Но особенно раздражало англичан то что, несмотря на узы давно сложившихся общих англо-американских интересов, Соединенные Штаты до сих пор упрямо сохраняли нейтралитет. И, судя по всему, собирались придерживаться его и дальше: во главе США недавно снова встал президент, который добился своего переизбрания на выборах под лозунгом «Благодаря мне мы не участвуем в войне».

Не лучше было положение и у Германии. Ее поначалу успешное наступление приостановилось у Марны, и с тех пор немецкие солдаты безвылазно сидели в окопах. Вследствие английской морской

блокады гражданское население питалось исключительно картофелем. Поэтому, как и у стран Антанты, у Германии было мало надежды одержать победу в ближайшем будущем. Кроме одной. «Развернуть неограниченную подводную войну! — твердили генералы. — И вскоре Англия будет задыхаться, как рыба, выброшенная на берег. Блокирующие превратятся в блокированных». В течение долгих месяцев они продолжали упорно насеивать на этом и, наконец, когда голод и всеобщее истощение усилились, сумели навязать свое мнение другим. В частности. их поддержал министр иностранных дел Циммерман, который очень долго возражал против неограниченной подводной войны.

Циммерман прекрасно понимал, что неоднократные потопления американских судов рано или поздно торпедируют нейтралитет Соединенных Штатов. Поэтому он решил предпринять необходимые действия с целью противостоять этой опасности. Циммерман предложил Мексике, настроенной очень враждебно по отношению к своему северному соседу из-за его карательной экспедиции на мексиканской территории, заключить военный союз с Германией. Циммерман сопроводил свое предложение Мексике обещанием щедрого финансирования ее военных затрат, намеком на поддержку со стороны Японии и другими приманками.

Будучи не в состоянии действовать через мексиканского посла, резиденция которого находилась в нейтральной Швейцарии, Циммерман направил предложение о военном союзе с Мексикой немецкому посланнику в этой стране Генриху Эккардту через Вашингтон. Для того чтобы быть уверенным в том, что оно непременно попадет в руки Эккардта, Циммерман послал его по двум каналам связи. Оба они контролировались англичанами.

Один маршрут англичане называли «шведским окольным путем». Швеция, которая формально была нейтральной, но фактически ориентировалась на немцев, с самого начала войны оказывала помощь МИД Германии в преодолении английской блокады, направляя немецкие телеграммы под видом своих собственных. Англичане раскрыли этот обман. Поэтому, когда летом 1915 г. Швеция официально выразила свое недовольство тем, что Англия необоснованно задерживает ее телеграммы, англичане намекнули шведам, что им достоверно известно о кое-какой деятельности Швеции, несовместимой с ее статусом нейтральной страны. В ответ шведское правительство пообещало, что в дальнейшем не будет направлять ни одной немецкой телеграммы в Вашингтон. И сдержало свое обещание: вместо Вашингтона, оно стало отправлять их в Буэнос-Айрес. Здесь шведы передавали полученные телеграммы в руки немцев, и только потом они попадали прямиком в немецкое посольство в Вашингтоне. Это и был пресловутый «шведский окольный путь».

Кабель из Стокгольма в Южную Америку проходил через Лондон. Немцы справедливо опасались, что английская цензура может опознать немецкие кодовые группы в шведских телеграммах. Поэтому МИД Германии скрывало эти группы путем их перешифровки. Перешифровка накладывалась на немецкие телеграммы, отправляемые через Стокгольм в Южную Америку, после зашифрования их кодом 13040. К несчастью для немцев, перешифровка не скрывала всех следов кода 13040. Эти следы вызвали подозрение у криптоаналитиков комнаты 40. Они сняли перешифровку, и на свет появился код 13040. После этого в комнате 40 внимательно присмотрелись и к другим официальным шведским телеграммам. Многие из них на поверку также оказались немецкими. Например, под одной перешифровкой англичане обнаружили код 0075. Но на этот раз Англия не заявила протеста Швеции. Холл был убежден, что выгоднее было подольше послушать, о чем говорят между собой немецкие дипломаты, чем помешать им это делать.

Идея второго маршрута, который Циммерман использовал для передачи своей шифртелеграммы в Вашингтон, зародилась у Эдварда Хауза, близкого друга президента Соединенных Штатов Америки Вильсона. В 1915 г. во время одной из своих поездок в Европу Хауз устроил так, что все кодированные сообщения из американских посольств стали поступать непосредственно в его адрес, минуя государственный департамент США. Когда 27 декабря 1916 г. немецкий посол Берншторфф обсуждал с Хаузом новую мирную инициативу Вильсона, он подчеркнул, что ее шансы на успех значительно возрастут, если правительство Германии сможет связываться через Хауза непосредственно со своим послом в Соединенных Штатах. Хауз доложил об этом президенту. На следующий день Вильсон разрешил немецкому правительству, используя собственный код, передавать телеграммы между Берлином и Вашингтоном под американским дипломатическим прикрытием.

Шифртелеграмма Циммермана была доставлена в посольство США в Берлине 16 января в 3 часа дня. Однако ее нельзя было направить непосредственно в Вашингтон. Поэтому сначала ее отослали в Копенгаген, а затем — в Лондон. И лишь оттуда она могла пойти прямо в Вашингтон. В итоге Англия перехватила и второй экземпляр шифртелеграммы Циммермана. В комнате 40 крайне

удивились, увидев немецкий код в пришедшей из Копенгагена американской телеграмме. Но англичане снова не заявили никакого протеста. Наличие двух копий одной и той же шифртелеграммы помогало избежать искажений, которые затруднили бы работу английских криптоаналитиков, и Грей с Монтгомери приступили к ее вскрытию.

Выпускник престижного Итонского университета Грей в течение семи лет работал переводчиком в одном солидном лондонском издательстве, но потом началась мировая война, и он поступил на военную службу в морскую авиацию. На работу в комнату 40 Грей пришел в 1915 г. в возрасте 29 лег. После Первой мировой войны он стал директором столичного издательства, специализировавшегося на художественных гравюрах и эстампах. В 1939 г. английское правительство вспомнило о его прошлых достижениях в области дешифрования, и он был принят в криптоаналитическое отделение министерства иностранных дел Англии, став вскоре заместителем начальника этого отделения.

Когда шифртелеграмма Циммермана попала в руки Монтгомери, ему было 45 лет. Сын ливерпульского судовладельца, учившийся в частных школах или под руководством репетиторов в Англии, Германии и Франции, Монтгомери получил степень бакалавра богословия в Лондоне. Однако состояние здоровья не позволило ему выполнять обязанности пастора, и Монтгомери переквалифицировался в переводчика, специализировавшегося на истории раннехристианской Церкви. В отзыве на один из его переводов, сделанный в 1910 г., говорилось о том, что «никогда еще работа немецкого автора не была переведена на английский язык так идиоматично и одновременно так достоверно». В 1916 г. Монтгомери поступил на должность цензора и в том же году был переведен на работу в комнату 40. Там криптоанализ увлек его настолько, что после окончания Первой мировой войны Монтгомери продолжил службу в криптоаналитическом отделении министерства иностранных дел вплоть до самой своей кончины в 1930 г.

Когда Монтгомери работал в комнате 40, хорошее знание Библии однажды помогло ему решить проблему, которая поставила в тупик других сотрудников комнаты 40. Некий г-н Джоунд получил из Турции совершенно чистую почтовую открытку, посланную ему по адресу: Шотландия, Тайнабруич, Кингдом-роуд, 184. Джоунд знал, что открытка была от его сына, которого турки взяли в плен. Но в Таинабруиче ни про какую Кингдом-роуд слыхом не слыхивали, а домов было так мало, что нумеровать их никому просто в голову не приходило. Открытка попала в комнату 40, где никто не смог точно ответить, о чем именно сын Джоунда пытался ему сообщить. В конце концов Монтгомери высказал предположение о том, что в адресе на открытке содержится намек на 18-ю главу 4-го стиха «Книги Царств» Библии. Проверка показала, что в этой главе говорится о 50 пророках, которых спрятали в пещере и кормили хлебом с водой. Монтгомери истолковал слова из Библии как весть о том, что сын Джоунда вместе с другими военнопленными находится в безопасности, но нуждается в пище. Впоследствии выяснилось, что догадка Монтгомери была абсолютно правильной.

Однако прочтение шифртелеграммы Циммермана требовало от английских криптоаналитиков значительно большего, чем простое угадывание, поскольку «угадать» надо было значения для 10 тысяч кодовых групп. Работа началась с определения кодовых обозначений для точки. Логично было предположить, что они располагаются в конце шифртелеграммы. Опознавание точки облегчается тем, что при ее кодировании, как правило, используется очень ограниченное число кодовых обозначений. Шифровальщики, часто обращаясь к точке, запоминают всего одну или две соответствующие ей кодовые группы. После этого для кодирования точки они употребляют только эти группы, чтобы все время не рыскать по кодовой книге в поисках подходящего для нее обозначения. Криптоаналитики, хорошо знакомые с шифрперепиской какого-то определенного посольства, часто могут сказать, когда к работе в нем приступает новый шифровальщик, определяя это событие по появлению в перехваченных криптограммах непривычных кодовых эквивалентов для точки.

Нахождение точек позволило выявить структуру шифртелеграммы Циммермана. В немецком языке, где сказуемое очень часто стоит в конце предложения, кодовая группа, непосредственно предшествующая точке, скорее всего, является глаголом. Дополнительную помощь английским криптоаналитикам при вскрытии кода 0075 оказали стереотипные выражения, которые так любили употреблять в своих посланиях немецкие дипломаты: «Имею честь сообщить Вашему Превосходительству, что...»

Первые пробные отождествления фиксировались Монтгомери и Греем при помощи карандаша, чтобы их потом можно было легко исправить или стереть. Назывались они «карандашными группами». Если в дальнейшем прочитанная шифрпереписка подтверждала значение полученных «карандашных групп», то Монтгомери и Грей немедленно превращали их в «чернильные группы».

По мере дальнейшего поступления в комнату 40 перехваченных немецких шифртелеграмм, включая шифрованные сообщения, адресованные Бернсторффу или отправленные им в Берлин, Монтгомери и Грей определяли значения все большего числа кодовых групп кода 0075. 28 января Грей принес Холлу частично прочитанную шифртелеграмму Бернсторффа с выражением протеста против объявления неограниченной подводной войны, о которой ему сообщалось в первой части шифртелеграммы Циммермана от 16 января. В резких выражениях Бернсторфф заявлял, что это сведет на нет все его усилия добиться ослабления напряженности между двумя странами и непременно втянет Соединенные Штаты в войну на стороне Антанты.

И действительно, 3 февраля 1917 г. президент Вильсон заявил, что разрывает дипломатические отношения с Германией, поскольку еще в апреле 1915 г. он обещал сделать это, если Германия возьмет курс на ведение неограниченной подводной войны. У уставшей от войны Англии появилась надежда, что в течение ближайших нескольких дней или, самое большее, через пару недель Соединенные Штаты вступят, наконец, в войну.

Тем временем в комнате 40 продолжалась упорная работа над кодом 0075. В первых числах февраля Грей принес Холлу открытый текст очередной шифртелеграммы Бернсторффа, в которой излагались подробности его беседы с Вильсоном в связи с заявлением о разрыве дипломатических отношений США с Германией. Полученные новые значения кодовых групп кода 0075 были использованы для чтения шифртелеграммы Циммермана. В результате 5 февраля Холл смог представить в министерство иностранных дел ее более полный открытый текст.

С самого первого дня, когда Монтгомери принес ему первый вариант открытого текста шифртелеграммы Циммермана, Холл понял, что в сложившихся условиях публичное разоблачение немецкого заговора против Соединенных Штатов почти наверняка вынудило бы их объявить войну Германии. Это был очень весомый довод в пользу того, чтобы сообщить о нем американцам. Однако имелись и железные аргументы против доведения содержания шифртелеграммы Циммермана до сведения Вильсона.

Во-первых, существование комнаты 40 и ее криптоаналитические возможности являлись одним из самых тщательно скрываемых секретов. Каким образом Англия могла предать гласности содержание шифртелеграммы Циммермана, чтобы Германия не догадалась, что ее коды вскрываются? Можно было бы свести риск до минимума, намекнув, что открытый текст шифровки украден. Однако и в этом случае существовала опасность, что Германия заподозрит неладное, сменит коды и лишит Англию доступа к секретной информации.

Во-вторых, разгласив содержание шифртелеграммы Циммермана, Англия тем самым косвенно признала бы, что контролирует переписку нейтральной Швеции. Американцам не составило бы особого труда сообразить, что заодно со шведской Англия, возможно, осуществляет контроль за перепиской Соединенных Штатов, которые, как и Швеция, работали на немцев в качестве телеграфного курьера и передали в Вашингтон эту шифртелеграмму. США оказались бы в затруднительном положении, что отнюдь не способствовало бы их вступлению в войну на стороне Англии.

В-третьих, шифртелеграмма Циммермана все еще не была прочитана полностью. После предания гласности полученного открытого текста возникли бы обоснованные сомнения в правильности выполненного дешифрования в силу его отрывочности. Например, при частичном вскрытии кода 0075 англичане могли пропустить частицу «не», присутствие которой в открытом тексте совершенно меняло его смысл. Или могли неверно прочесть место, которое представили как свидетельство двуличности Германии. Более того, эти искажения в открытом тексте прямо указывали бы именно на вскрытие кода, не допуская каких-либо отговорок о похищении телеграммы. В результате тайна, которую Англия желала всеми силами сохранить, была бы непременно раскрыта.

Но наиболее веский довод против публичного разоблачения немецкого заговора сводился к тому, что, возможно, сам ход событий сделает этот рискованный шаг ненужным. Отношения между Германией и Соединенными Штатами становились все более натянутыми. Американское общественное мнение стремительно менялось не в пользу Германии. Суда торгового флота США не осмеливались выходить в море, порты были переполнены, людей увольняли, деловая жизнь затихала. Объявление войны казалось делом ближайшего будущего. Поэтому Англия продолжала ждать и надеяться.

Однако Холл не желал сидеть сложа руки. Его работа была бы выполнена наполовину, если бы он заполучил в свое распоряжение лишь открытый текст шифртелеграммы Циммермана, не подготовив почву для его практического использования в интересах Англии. Поэтому Холл составил план, который одним махом помог бы преодолеть неблагоприятные последствия, связанные с

публичным разоблачением немецкого заговора против США в случае, если это понадобится. Холл рассуждал примерно так.

Шифртелеграмма Циммермана в том виде, в котором она была послана в Мексику через шведов, в мелких деталях могла отличаться от его шифртелеграммы, отправленной в Вашингтон через американцев. Почти наверняка у нее была другая дата и, возможно, другой порядковый номер. Кроме того, вероятно, она была снабжена дополнением, предназначенным для Бернштorффа и предписывавшим переслать ее в столицу США. Если бы Холл сумел заполучить экземпляр открытого текста именно для этого варианта шифртелеграммы Циммермана, немцы, вероятно, пришли бы к заключению, что он был украден в Мексике, и кодов своих не заменили бы.

Другие дополнительные штрихи могли бы сделать «мексиканскую легенду» более правдоподобной для американцев. Благодаря чтению немецких шифртелеграмм, проходивших по «шведскому окольному пути», английским криптоаналитикам из комнаты 40 стало известно о том, что дипломатическая миссия Германии в Мексике, не пользовалась кодом 0075. В таком случае Бернштorффу, очевидно, пришлось перешифровать телеграмму Циммермана с использованием другого кода. Поэтому если бы американцы узнали о ее содержании от англичан в том виде, в каком она была послана «шведским окольным путем», то поверили бы, что этот код был скомпрометирован и его вскрытие не представляло для англичан никакого труда или что английские агенты в Мехико получили доступ непосредственно к открытому тексту шифртелеграммы Циммермана. Оба варианта устраивали Холла.

5 февраля Холл предпринял первые попытки заполучить открытый текст шифртелеграммы Циммермана в том виде, в каком он был отправлен в Мексику из Берлина. По заданию Холла английский агент раздобыл на телеграфе в Мехико шифртелеграмму Бернштorффа Эккардту, открытый текст которой дублировал открытый текст шифртелеграммы Циммермана.

Холл оказался прав: у Эккардта не было кода 0075, поэтому Бернштorффу пришлось перешифровать открытый текст шифртелеграммы Циммермана по одному из кодов, которые имелись в распоряжении Эккардта. Это был код 13040, введенный в действие раньше кода 0075* и являвшийся по сравнению с ним более простым. Он представлял собой гибрид алфавитного и неалфавитного кодов.

* Между 1907-м и 1912 гг.

По своей трудности вскрытие гибридного кода занимает промежуточное место между алфавитным и неалфавитным кодами: оно сложнее для первого из них, но легче для второго. Благодаря относительной слабости кода 13040 и наличию большого количества накопленного еще до войны перехвата английские криптоаналитики давно вскрыли большинство кодовых групп кода 13040, которые наиболее часто встречались в перехваченной шифрпереписке. Поэтому в комнате 40 смогли прочесть шифртелеграмму Бернштorффа к Эккардту почти целиком. В тех немногих ее местах, где какая-нибудь кодовая группа встречалась в первый раз, потребовалось провести небольшую дополнительную работу. В результате была подтверждена правильность полученного Монтгомери и Греем варианта открытого текста первоначальной шифртелеграммы Циммермана, отправленной из Берлина в Вашингтон 16 января. Английские криптоаналитики также обнаружили незначительные изменения, внесенные Бернштorффом в исходный открытый текст шифртелеграммы Циммермана.

Теперь его можно было передать американцам с наименьшей вероятностью скомпрометировать источник полученной информации. Однако риск того, что немцы догадаются о нем, был все еще слишком велик. И поскольку дальнейшее развитие событий могло сделать этот риск ненужным, Холл продолжал хранить открытый текст шифртелеграммы Циммермана в секрете и выжидал.

Дни проходили в томительном ожидании. Англия и Франция изнемогали в битве не на жизнь, а на смерть, однако никаких признаков того, что Соединенные Штаты собираются вступить в войну на стороне Антанты, заметно не было. Посол США в Англии Пэйдж, давний друг президента Вильсона и искренний сторонник оказания военной помощи Антанте, раздраженно написал в своем дневнике: «Опасность состоит в том, что с получением всех полномочий, которые он хочет (кроме разве официального объявления войны), президент вновь будет ждать, ждать и ждать — до тех пор, пока не будет торпедирован американский лайнер! Или до тех пор, пока немецкая подводная лодка не совершит нападение на наше побережье!»

Напряжение росло. Обстановка тех дней, как впоследствии охарактеризовал ее один английский дипломат, «во многом напоминала состояние бутылки с шампанским, с которой уже снята проволока,

но ее пробка еще не выстрелила». 22 февраля 1917 г., понимая, что промедление в этом деле смерти подобно, англичане помогли пробке «выстрелить». С одобрения министерства иностранных дел Холл показал открытый текст шифртелеграммы Циммермана Эдварду Беллу, секретарю американского посольства в Лондоне. Белл прочитал поразительную историю немецкого заговора против своей страны:

«С 1 февраля мы намерены начать неограниченную подводную войну. Несмотря на это, мы должны приложить усилия к тому, чтобы Соединенные Штаты Америки оставались нейтральными. В случае, если добиться этого окажется невозможно, мы сделаем предложение Мексике о заключении союза на следующих условиях: совместное ведение войны, совместное заключение мира, щедрая финансовая поддержка и понимание с нашей стороны того, что Мексика должна получить обратно утраченные территории в Техасе, Нью-Мексико и Аризоне. Подробная разработка данного соглашения поручается вам.

Вы секретно информируете президента* о вышеизложенном, как только станет определенным начало войны с Соединенными Штатами Америки, и дополните эту информацию предложением о том, чтобы он, по собственной инициативе, пригласил Японию безотлагательно присоединиться к соглашению и в то же самое время выступил в качестве посредника между Японией и нами.

Обратите внимание президента на то, что решительное использование наших подводных лодок в течение нескольких месяцев вынудит Англию заключить мир.

Циммерман»

* Мексики

Белл отказался поверить прочитанному наотрез. Мысль о том, что кто-нибудь, будучи в здравом уме и твердой памяти, всерьез рассматривает возможность отторжения значительной части Соединенных Штатов, была слишком нелепа. Однако Холл сумел убедить Белла в достоверности предъявленного ему документа, после чего они оба направились к Пэйджу.

Когда Пэйдж увидел открытый текст шифртелеграммы Циммермана, он тотчас же понял, что вступление США в войну на стороне Англии теперь зависит исключительно от него. Пэйдж, Холл и Белл потратили целый день, пытаясь придумать, как лучше всего убедить президента Вильсона в подлинности открытого текста шифртелеграммы и усилить впечатление, которое этот текст на него произведет. Наконец было решено, что английское правительство официально передаст прочитанную немецкую шифртелеграмму Пэйджу. На следующий день министр иностранных дел Англии Артур Бальфур вручил ее в своем кабинете Пэйджу. Этот момент, как позже признался Бальфур, был самым драматичным в его жизни.

Над составлением сопроводительного письма, объясняющего, каким образом им был получен открытый текст шифртелеграммы Циммермана, Пэйдж проработал всю ночь. Наконец, 24 февраля 1917 г. в 2 часа ночи он телеграфировал в Вашингтон: «Приблизительно через 3 часа я направляю президенту и государственному секретарю телеграмму чрезвычайной важности».

«Телеграмма чрезвычайной важности» была передана Пэйджем лишь в час дня. В ней он доводил до сведения своего президента подборку полуправдивых фактов, которые ему сообщил Холл. Последний, естественно, скрыл от Пэйджа сведения о возможностях англичан в области криптоанализа, поскольку это могло вызвать у американцев горячее желание узнать, не читает ли Англия заодно и их шифрованные сообщения.

В телеграмме Пэйджа Вильсону, в частности, говорилось: «В начале войны английское правительство тайно приобрело экземпляр немецкого секретного кода и сочло своим долгом получать копии шифрованных телеграмм Бернсторффа вместе с другими немецкими шифртелеграммами, которые затем переправляются в Лондон и здесь дешифруются. Это служит объяснением способности англичан прочесть шифртелеграмму правительства Германии своему дипломатическому представителю в Мексике, а также двухмесячной задержки в получении ими информации. Вплоть до самого последнего момента времени они ревностно хранили все в тайне, и лишь сейчас английское правительство сообщает полученную информацию вам, учитывая чрезвычайные обстоятельства и свои дружеские чувства к Соединенным Штатам. Оно настоятельно просит вас не раскрывать ниточник этой информации и метод ее получения, но не накладывает никакою запрета на опубликование открытого текста самой шифртелеграммы Циммермана».

Первую телеграмму Пэйджа телеграфные аппараты отстучали в государственном департаменте США рано утром 24 февраля 1917 г. Обещанная в ней «телеграмма чрезвычайной важности» поступила только в 8.30 вечера. Фрэнк Поук, советник госдепартамента и исполняющий обязанности

государственного секретаря в отсутствие занимавшею этот пост Роберта Лансинга, позвонил президенту Вильсону с просьбой немедленно принять его. Через полчаса Поук доставил в Белый дом текст второй телеграммы Пэйджа. Прочитав его, Вильсон, выразил негодование вероломством немцев и хотел сразу же опубликовать этот текст в газетах. Но, немного поостыв, согласился с предложением Поука дождаться возвращения Лансинга.

27 февраля 1917 г. Лансинг вернулся в Вашингтон из поездки за границу. Поук незамедлительно проинформировал его о прочитанной англичанами шифртелеграмме Циммермана и показал очень большую шифрованную телеграмму, которую обнаружил в досье государственного департамента. Она пришла для Бернштorффа как часть американской телеграммы из Берлина от 17 января и являлась, по мнению Поука, оригиналом шифртелеграммы Циммермана.

В 11 часов утра Лансинг отправился в Белый дом для обсуждения сложившегося положения с президентом, который в ходе беседы с ним несколько раз воскликнул: «О Боже!» в связи с оскорбительным злоупотреблением предоставленными немцам «телеграфными привилегиями». Он согласился с планом Лансинга негласно передать телеграмму газетчикам, что, как считал Лансинг, «позволило бы избежать обвинения в неправильном использовании конфиденциального документа и привлекло бы больше внимания, чем ее официальное опубликование». На следующий день в 6 часов вечера представитель Ассошиэйтед Пресс был приглашен к Лансингу на дом. Ему дали прочесть телеграмму Пэйджа и ознакомили с некоторыми подробностями подоплеки этого дела, попросив дать честное благородное слово не разглашать величайшую сенсацию воины.

1 марта 1917 г. сообщение Ассошиэйтед Пресс было опубликовано на первых полосах утренних газет под огромными заголовками. Вся страна была шокирована. Палата представителей американского конгресса отреагировала на публикацию принятием законопроекта о вооружении торговых судов. Более осторожный сенат потребовал от правительства доказательств, что все это не являлось грубым заговором англичан с целью втянуть США в войну на стороне Антанты. Такая позиция сената не была неожиданной для Лансинга, который попросил Пэйджа «попытаться получить у г-на Бальфура копию немецкого кода». Бальфур отказал Пэйджу. заявив, что этот код «всегда использовался немцами не впрямую, а со значительными вариациями, известными лишь одному или двум экспертам, у которых нет времени на поездку в Америку». Это, конечно, опять было полуправдой.

Между тем Поук оказал сильное давление на президента американской телеграфной компании «Вестерн юнион», в результате чего ему удалось получить копию шифртелеграммы Бернштorффа к Эккардту вопреки федеральному закону США, защищавшему неприкосновенность переписки. Лансинг присовокупил ее текст к телеграмме, которую он направил Пэйджу 1 марта в 8 часов вечера. В ней говорилось: «Некоторые члены конгресса пытаются дискредитировать подлинность открытого текста шифртелеграммы Циммермана, выдвигая обвинения в том, что он был сфабрикован для нашего правительства одной из воюющих сторон. У американского правительства нет ни малейшего сомнения в ее достоверности, однако ему была бы оказана величайшая услуга, если бы правительство Англии разрешило вам или кому-либо еще из посольства лично прочесть шифртелеграмму, которую мы получили на телеграфе в Вашингтоне, а затем передать по телеграфу полученный открытый текст государственному департаменту. Убедите г-на Бальфура, что такой ход существенным образом упрочит положение государственного департамента и даст ему возможность заявить, что открытый текст шифртелеграммы Циммермана он получил от своих людей».

Телеграмма Лансинга была получена в Лондоне на следующий день. К 4 часам дня Пэйдж телеграфировал ответ: «Белл забрал в Адмиралтейство шифрованный текст, содержавшийся в вашей вчерашней телеграмме, и там лично дешифровал его с помощью немецкого кода, который имеется в их распоряжении». После этого Пэйдж передал в Вашингтон дешифрованный Беллом открытый текст, после ознакомления с которым Вильсон и Лансинг направили конгрессу официальное заявление о том, что у правительства есть неопровержимые доказательства его подлинности.

К этому времени почти у каждого американца уже была наготове своя собственная гипотеза относительно того, как Соединенные Штаты достали открытый текст шифртелеграммы Циммермана. Наибольшей популярностью пользовались шпионские версии. Согласно одной из них, четыре американских солдата обнаружили его у немецкого агента, пытавшегося перейти через границу в Мексику. По другой, он был найден среди личных вещей Бернштorффа, когда после отставки его личный багаж как следует проверили на американской таможне.

Тем временем в Берлине также недоумевали, где произошла утечка секретной информации. И хотя в открытом тексте шифртелеграммы Циммермана в том виде, в каком он был опубликован в американских газетах, не было изменений, внесенных в него Бернштorффом, в нем содержалась

важная дата — 19 января.

Министерство иностранных дел Германии написало Эккардту, который совсем уже было собрался публично обвинить Бернштorффа в предательстве: «Пожалуйста, телеграфируйте, кто расшифровывал телеграмму Циммермана и телеграфное сообщение, приказывающие Эккардту немедленно вступить в переговоры относительно союза с Мексикой, как хранились их шифрованные и открытые тексты и, в частности, находились ли все они в одном и том же месте».

Несколько дней спустя Эккардту пришла новая телеграмма из Берлина, из которой следовало, что немцы попали в сети, тщательно расставленные Холлом: «Различные признаки дают основания предположить. что предательство было совершено в Мексике. Требуется величайшая осмотрительность. Сожгите весь компрометирующий материал».

В свое оправдание Эккардт телеграфировал в Берлин: «Согласно моим специальным инструкциям, обе телеграммы были расшифрованы Артуром Магнусом, секретарем немецкой дипломатической миссии. Ни об одной из них, как и обо всем, касающемся секретов политического характера, не было известно другим сотрудникам миссии... Оригиналы в обоих случаях были сожжены Магнусом, а пепел развеян. Все сообщения хранились в абсолютно надежном стальном сейфе, специально приобретенном для этой цели и установленном в спальне Магнуса, вплоть до того времени, когда они были сожжены... Невозможно принять более строгие меры предосторожности, чем те, которые практикуются мной. Открытые тексты поступающих шифртелеграмм зачитываются мне Магнусом в моей квартире ночью тихим голосом. Мой слуга, который не владеет немецким языком, спит в отдельно стоящем флигеле».

Перед такими доводами министерство иностранных дел Германии не могло не капитулировать. Его последние сомнения были развеяны «тихим голосом», «стальным сейфом» и не говорящим по-немецки слугой. «После вашей телеграммы едва ли возможно, чтобы предательство было совершено в Мексике. Поэтому все признаки, которые свидетельствовали в этом направлении, теряют свою силу. Ни на вас, ни на Магнусе не лежит никакой вины за случившееся».

Между тем проблема достоверности опубликованного открытого текста шифртелеграммы Циммермана, которая так беспокоила англо-американских официальных лиц, была устранена самим Циммерманом. Совершенно неожиданно он признался: «Я не могу отрицать этого. Это правда». От осведомленности в существовании заговора упорно открещивались и мексиканцы, и японцы, и Эккардт. Поэтому по сей день неясно, почему Циммерман признался. Однако вне зависимости от мотивов, которыми он руководствовался, его признание похоронило последние сомнения в том, что сообщение о немецком заговоре против США могло быть обманом.

В результате у американцев, которых совершенно не волновал отдаленный грохот войны в Европе, вдруг пробудилось сознание того, что война стояла у их границ. Удивленно вздрогнули техасцы: оказывается, немцы хотели отдать их штат мексиканцам! Жители Среднего Запада живо представили себе, как мексиканские войска, ведомые немецкими офицерами, переходят через границу и захватывают их прерии. При упоминании о возможной японской агрессии, подобно фугасной мине, взорвалось Западное побережье США. В течение месяца общественное мнение стало единым. Его выразил Вильсон, который всего три месяца назад говорил, что было бы «преступлением против цивилизации» ввергнуть страну в войну. 2 апреля он заявил, что «справедливость дороже мира», и обратился к конгрессу с призывом любыми средствами добиться торжества справедливости. В своем выступлении перед конгрессом Вильсон сослался на шифртелеграмму Циммермана:

«О том, что немецкое правительство намерено натравить на нас врагов у самого нашею порога, красноречиво свидетельствует перехваченная телеграмма, адресованная немецкому посланнику в Мехико. Мы принимаем этот враждебный вызов... Я рекомендую конгрессу объявить, что проводившийся за последнее время курс имперского правительства Германии в действительности является не чем иным, как настоящей войной против правительства и народа Соединенных Штагов, и официально провозгласить статус воюющей стороны, который был нам навязан таким образом».

Конгресс удовлетворил просьбу президента Вильсона. Вскоре в Европу стали прибывать американские солдаты. Свежие силы молодой нации хлынули в окопы Западного фронта, чтобы спасти обессиленные войска Антанты.

Так прочтение дипломатической шифртелеграммы Германии помогло подтолкнуть Соединенные Штаты к вступлению в Первую мировую войну, что дало Англии и Франции возможность одержать победу над врагом и занять командные высоты в послевоенном мире. Никакая другая криптоаналитическая разработка не имела таких огромных последствий. Никогда, ни до этого, ни после, в результате дешифрования одного секретного сообщения не происходило так много важных

событий, влиявших на ход мировой истории.

СЕКРЕТНОСТЬ НА ПРОДАЖУ

Ранним декабрьским утром 1917 г. симпатичный молодой человек стремительно промчался между массивными колоннами вестибюля здания компании «Американ телефон энд телеграф» («AT&T»), расположенного в деловой части Нью-Йорка. Он вбежал в лифт и поднялся на нем на 17-й этаж, где находилось телеграфное отделение компании, входившее в состав ее научно-исследовательского отдела. Это отделение, в котором работали несколько самых талантливых инженеров, уже год занималось доведением до ума новейшего достижения в области телеграфии — буквопечатающего телеграфного аппарата, который в отделении нарекли телетайпом.

Молодого человека звали Гильберт Вернам, и он всегда немного опаздывал. Коллеги считали Вернама весьма толковым инженером и способным изобретателем. Среди них ходили слухи о том, что каждый вечер, растягиваясь на диване, он спрашивал сам себя вслух: «Что бы такое еще изобрести?» У Вернама был редкий склад ума, который позволял ему придумывать оригинальную электрическую цепь и затем переносить ее на чертежный холст, не воспроизводя все требуемые соединения с помощью проводов. Вернам очень хорошо зарекомендовал себя на работе, поэтому начальник телеграфного отделения компании «AT&T» Паркер без колебаний пригласил его принять участие в разработке особо секретного проекта. И хотя в это декабрьское утро Вернам опять опоздал, в его голове уже успела созреть прекрасная идея. Тихий и скромный по натуре, Вернам довольно несмело изложил свою идею коллегам, которые сразу же сочли ее заслуживающей особого внимания.

Работа над секретным проектом началась еще летом, несколько месяцев спустя после того, как Соединенные Штаты объявили войну Германии. Паркер поручил нескольким своим подчиненным исследовать вопрос о возможности сохранять в тайне сообщения, передаваемые по телетайпу. Оказалось, что колебания тока в линии связи могли быть записаны с помощью осциллографа и затем легко преобразованы в буквы передаваемого сообщения. Поэтому было решено внести изменения в соединения проводов печатающего механизма телетайпа. В результате текст сообщения шифровался методом одноалфавитной замены. В телеграфном отделении понимали, что такая защита являлась слишком слабой, однако ничего другого придумать не смогли и перестали заниматься этой проблемой до тех самых пор, пока Вернам не поведал им о своей идее.

Вернам предложил использовать особенности телетайпного кода, в котором кодируемый знак выражается в виде пяти элементов. Каждый из этих элементов символизирует наличие («плюс») или отсутствие («минус») электрического тока в линии связи. Таким образом, имеются 32 различных комбинации «плюсов» и «минусов». 26 из них ставятся в соответствие буквам, а оставшиеся 6 обозначают «служебные комбинации» (пробел между словами, переход с букв на цифры и знаки препинания, обратный переход с цифр и знаков препинания на буквы, возврат каретки печатающего устройства, переход на новую строку и холостой ход). Например, буква «А» выражается комбинацией «+ + - - -», букве «N» соответствует «- - + + -», а переход на цифры и знаки препинания задается через «+ + - + +». Закодированное сообщение набивается на перфоленте: «плюсы» представляются отверстиями, а «минусы» — их отсутствием. При считывании перфоленты металлические щупы проходят через отверстия, замыкают электрическую цепь и посылают импульсы тока по проводам. А там, где на перфоленте находится «минус», бумага не позволяет этим щупам замкнуть цепь, и в результате токовый импульс не передается.

Вернам предложил готовить перфоленту со случайными знаками (так называемую «гамму») заранее и затем электромеханически складывать ее импульсы с импульсами знаков открытого текста. Полученная сумма представляла собой шифртекст, предназначенный для передачи по линии связи. Вернам установил следующее правило суммирования: если сразу оба импульса являются «плюсами» или «минусами», то итоговый импульс будет «минусом», а если эти импульсы различны, то в результате получится «плюс».

Чтобы при шифровании суммировать импульсы электрически, Вернам сконструировал специальное устройство, состоящее из магнитов, реле и токо- съемных пластин. А поскольку процедура расшифрования была совершенно аналогична процедуре зашифрования, это же самое устройство могло быть использовано и при расшифровании. Импульсы поступали в устройство суммирования с двух считывателей: один считывал «гамму», а другой — открытый текст. Получающиеся на выходе «плюсы» и «минусы» можно было передавать подобно обычному телетайпному сообщению. На приемном конце устройство, изобретенное Вернамом, прибавляло импульсы, которые считывались с идентичной ленты с «гаммой», и восстанавливало исходные

импульсы открытого текста.

Вся прелесть изобретения Вернама заключалась в том, что больше не требовалось осуществлять зашифрование и расшифрование секретных сообщений в виде отдельных операций. Открытый текст входил в аппарат, находившийся у отправителя сообщения, и точно такой же открытый текст выходил из аппарата, принадлежавшего получателю этого сообщения. А если кто-либо перехватывал это сообщение по пути следования от отправителя к получателю, то в его распоряжении оказывалась ничего не значащая последовательность «плюсов» и «минусов». Теперь, чтобы зашифровать, передать, принять и расшифровать сообщение, требовалось приложить не намного больше усилий, чем при отправке сообщения открытым текстом. Основное преимущество изобретенного Вернамом метода засекречивания сообщений заключалось не в механическом шифровании открытого текста с последующей печатью результата на бумаге, что было осуществлено еще в начале 70-х годов XIX века французами Эмилем Винеем и Жозефом Госсеном. Вернам сумел слить воедино два процесса — шифрование и передачу сообщения. Он создал то, что впоследствии назвали линейным шифрованием, чтобы отличать его от ставшего традиционным предварительного шифрования. Вернам освободил процесс шифрования от оков времени и ошибок, исключив из этого процесса человека. Выдающийся вклад, внесенный Вернамом в практику шифрования, заключается именно в том, что он привнес в шифровальное дело автоматизацию, уже успевшую к тому времени сослужить людям огромную службу во многих областях их деятельности.

Вокруг идеи, высказанной Вернамом в кругу коллег, моментально развернулась кипучая деятельность. Сначала Вернама заставили изложить эту идею в краткой записке, датированной 17 декабря. Компания «AT&T» уведомила об изобретении Вернама американское военно-морское ведомство, с которым она поддерживала тесное сотрудничество. 18 февраля 1918 г. состоялось совещание, в котором приняли участие Паркер, Вернам и другие инженеры из телеграфного отделения компании «AT&T», с одной стороны, и военные моряки, с другой.

27 марта эти же инженеры встретились со своими коллегами из американской компании «Вестерн электрик», производственного филиала «AT&T», и договорились с ними об изготовлении первых двух линейных шифраторов с использованием как можно большего количества стандартных деталей. В лаборатории «Вестерн электрик» они подсоединили изготовленные шифраторы к телетайпам и осуществили первые испытания процесса, который назвали «автоматическим шифрованием». Все устройства, вовлеченные в него, работали превосходно. Компания «AT&T» проинформировала об этом факте майора Джозефа Моборна, который занимал тогда пост начальника отдела научно-исследовательских и конструкторских разработок войск связи США.

Нерешенным оставался всего один вопрос — откуда брать «гамму». В первые дни «гамма» для устройства Вернама представляла собой склеенные петлей короткие перфоленты, на которые были набиты знаки, извлеченные наугад из различных открытых текстов. Инженеры компании «AT&T» почти сразу обратили внимание на существенные изъяны такого процесса «автоматического шифрования», связанные с недостаточной длиной «гаммы». Поэтому, чтобы затруднить криптоанализ, они сделали перфоленты с «гаммой» более длинными. Но тогда с этими перфолентами стало слишком трудно обращаться.

Вернам предложил суммировать две короткие, имеющие различную длину «гаммы» таким образом, как будто бы одна «гамма» шифровала другую. Получающаяся в результате так называемая вторичная «гамма», имевшая значительно большую длину, чем две исходные, первичные «гаммы», которые были использованы для ее генерации, применялась для зашифрования открытого текста. Например, если одна закольцованная лента имела 1000 знаков, а другая 999, то данное различие в длинах всего в один знак давало 999000 комбинаций, прежде чем результирующая последовательность повторялась.

Однако Моборн понимал, что даже усовершенствованная система Вернама весьма уязвима для криптоанализа. В свои 36 лет будущий начальник войск связи США Моборн был незаурядным криптоаналитиком. Он основательно изучил криптоанализ в армейской школе связи и был хорошо знаком с последними достижениями в этой области. Более того, за несколько лет до описываемых событий Моборн сам принимал участие в одной научно-исследовательской работе, в ходе которой специалисты из армейской школы связи сделали вывод о том, что единственной стойкой «гаммой» является такая, которая сравнима по длине с самим шифруемым сообщением. Любое повторение в «гамме» подвергает огромному риску полученные с ее помощью криптограммы и, скорее всего, приведет к их вскрытию. Проведенный Моборном анализ системы «автоматического шифрования» еще более убедил его в этом. Он понял, что не имеет никакого значения, находятся ли повторения в пределах одной криптограммы или они распределены по нескольким, получаются ли они путем

комбинирования двух первичных «гамм» или в результате простого повторения в единой длинной «гамме». Важно то, что в «гамме» повторений не должно быть ни при каких условиях. Необходимо, чтобы она была совершенно уникальна и предельно хаотична.

Осознав это, Моборн объединил свойство хаотичности «гаммы», на которое опирался Вернам в своей системе «автоматического шифрования», со свойством уникальности «гаммы», выработанным криптографами армейской школы связи, в системе шифрования, которую ныне принято называть «одноразовым шифрблокнотом». Одноразовый шифрблокнот содержит случайную «гамму», которая используется один, и только один раз. При этом для каждого знака открытого текста, принадлежащего всей совокупности сообщений, которые уже были посланы данной группой шифркорреспондентов или еще только будут посланы ею в обозримом будущем, предусматривается использование абсолютно нового и не поддающегося предсказанию знака «гаммы».

Это абсолютно стойкая шифрсистема. Подавляющее большинство систем шифрования являются абсолютно стойкими лишь на практике, поскольку криптоаналитик может найти пути их вскрытия при наличии у него определенного количества шифртекста и достаточного времени для его исследования. Одноразовый же шифрблокнот является абсолютно стойким как в теории, так и на практике. Каким бы длинным ни был перехваченный шифртекст, сколько бы много времени ни отводилось на его исследование, криптоаналитик никогда не сможет вскрыть одноразовый шифрблокнот, использованный для получения этого шифртекста. И вот почему.

Вскрытие многоалфавитного шифра означает объединение всех букв, зашифрованных при помощи одного шифралфавита, в единую группу, которую можно изучать на предмет выявления ее лингвистических особенностей. Методы такого объединения могут быть различны в зависимости от вида «гаммы». Так, метод Казиского заключается в выделении идентично гаммированных букв открытого текста при повторяющейся «гамме». Связная «гамма» может быть вскрыта путем взаимного восстановления открытого текста и «гаммы». А «гамма», использованная для зашифрования двух или более сообщений, поддается вскрытию путем одновременного восстановления открытых текстов этих сообщений, причем правильность прочтения одного текста контролируется читаемостью другого. Почти для всех разновидностей многоалфавитиых шифров разработан свой метод вскрытия, который основан на их отличительных особенностях.

Совершенно иначе обстоит дело с одноразовым шифрблокногом. В этом случае криптоаналитик не имеет отправной точки для своих исследований, так как в одноразовой шифрсистеме «гамма» не содержит повторений, не используется более одного раза, не является связным текстом и не имеет внутренних структурных закономерностей. Поэтому все методы дешифрования, в той или иной мере основанные на этих характеристиках, не дают никаких результатов. Криптоаналитик заходит в тупик.

А как обстоит дело с методом тотального опробования? Ведь прямой перебор всех возможных ключей в конечном счете обязательно приведет криптоаналитика к открытому тексту. Однако успех, приобретенный этим путем, иллюзорен. Тотальное опробование действительно позволяет получить исходный открытый текст. Но оно также даст и каждый другой возможный текст той же длины, и сказать, какой из них является истинным, будет невозможно.

Предположим, что криптоаналитик пытается дешифровать четырехбуквенное военное сообщение, применяя все «гаммы», начиная с «AAAA». Используя «AABI» в качестве «гаммы», он получает открытый текст «kiss»*. Неподходящий вариант для данного контекста. Криптоаналитик не останавливается на достигнутом. С помощью «AAEL» получается открытый текст «kill»**. Уже лучше, но хочется удостовериться, нет ли чего более подходящего. Исследование продолжается, и при «гамме» «AAEM» выходит слово «kilt»***. «AAER» дает «kiln»****, «GZBM» — «fast»*****, «KHIA» — «slow»******, «HRIW» — «stop»*******, «PZVQ» — «hard»******** и «RZBU» — «easy»*********. Когда криптоаналитик доберется, наконец, до «гаммы» «ZZZZ», он обнаружит, что просто составил перечень всевозможных английских слов из четырех букв.

* «Поцелуй».
** «Убей».
*** «Килт».
**** «Обжигать».
***** «Быстро»
****** «Медленно»
******* «Остановиться».
******** «Трудно»
********* «Легко».

У криптоаналитика остается последняя надежда. Предположим, что он получил н свое распоряжение открытый текст какой-то отдельной криптограммы (например, в результате ошибки связиста). В состоянии ли криптоаналитик использовать «гамму», которую он сможет теперь вычислить, имея на руках открытый и соответствующий ему шифрованный тексты, для определения алгоритма, с помощью которого была выработана эта «гамма», чтобы потом предугадать все будущие «гаммы»? Нет, не в состоянии. Ведь если «гамма» действительно случайна, это значит, что она не подчиняемся никаким видимым закономерностям.

Правильный ответ опять ускользает от криптоаналитика. Одноразовая случайная «гамма» полностью подавляет его, растворяя все усилия криптоаналитика в хаосе, с одной стороны, и в бесконечности, с другой. Здесь он сталкивается с пропастью, непреодолимой для человека.

Почему же горда этот самый совершенный шифр не нашел всеобщего применения? Ответ прост, из-за огромного количества «гаммы», которая требуется при его использовании. Проблемы, возникающие при изготовлении, рассылке и уничтожении «гаммы», человеку непосвященному во все тонкости организации шифрсвязи могут показаться пустячными, однако в военное время объемы переписки зачастую удивляют даже самых бывалых связистов. В течение суток может понадобиться зашифровать сотни тысяч слов, а для этого требуется изготовить миллионы знаков «гаммы». И поскольку «гамма» для каждого сообщения должна быть единственной и неповторимой, то ее общий объем будет эквивалентен объему всей переписки за время воины.

В общем, практические проблемы не позволяют применять одноразовые шифрблокноты в быстро меняющихся ситуациях, например в ходе проведения военных операций. Этих проблем не существует в более стабильных условиях: в высших военных штабах, дипломатических представительствах или в агентурной переписке одноразовые шифрблокноты достаточно практичны и находят повсеместное применение. Однако и здесь возникают непреодолимые трудности, если объем переписки слишком велик.

Это как раз и произошло, когда Моборн, устроив первое крупное испытание шифрсистемы Вернама, установил его машины сразу в трех городах. Даже при сравнительно небольшом объеме переписки (до 135 коротких сообщений в день) оказалось невозможным изготовить достаточное количество качественной «гаммы». Поэтому, не найдя другого выхода из затруднительного положения, Моборн стал комбинировать две относительно короткие «гаммы», чтобы получать из них более длинную «гамму», как это первоначально предлагал делать сам Вернам.

В сентябре 1918 г. Вернам отправился в Вашингтон и подал там заявку на патент. Первая мировая война успела закончиться прежде, чем шифрсистема Вернама сумела хоть как-то проявить свои достоинства на практике. Тем не менее 22 июля 1919 г. на нее был выдан патент № 1310719, являющийся, по-видимому, самым важным в истории криптографии. Эксперты из вашингтонского патентного бюро признали возможную полезность этого изобретения и в мирное время.

Однако, хотя устройство, придуманное Вернамом, несомненно являлось ценным плодом творческой инженерной мысли талантливого изобретателя, в коммерческом плане оно потерпело полный провал. Телеграфные компании и коммерческие фирмы, которые, по мнению «AT&T», должны были в массовых количествах покупать запатентованные шифрприставки Вернама к своим телетайпам, отдавали предпочтение старомодным кодам, которые существенно снижали длину сообщений, тем самым уменьшая телеграфные расходы и одновременно обеспечивая хоть какую-то, пусть небольшую, безопасность переписки. После окончания Первой мировой войны бюджеты вооруженных сил всех стран были сокращены до минимума. Недостаток средств и нехватка материальных ресурсов вынудили армейских связистов снова вернуться к комбинированию двух относительно коротких лент с «гаммой», а продемонстрированная военными криптоаналитиками слабая стойкость такой системы генерации «гаммы» привела к тому, что шифрсистема Вернама на некоторое время была предана забвению.

Что же касается самого Вернама, то он продолжал заниматься научно-исследовательской работой в компании «AT&T». Он немного усовершенствовал свою шифрсистему, а также изобрел устройство для автоматического зашифрования написанного от руки текста во время его передачи фототелеграфом. В 1929 г. Вернама со значительным повышением перевели в один из филиалов компании «AT&T». Однако через четыре месяца в США разразился финансовый кризис, и, так как Вернам еще не успел заработать достаточный трудовой стаж на новом месте, его вскоре уволили. Он перешел на работу в другую крупную компанию, но резкая перемена в его личной судьбе, видимо, подействовала на него угнетающе. С каждым годом о Вернаме было слышно все меньше и меньше, пока, наконец, 7 февраля 1960 г. человек, автоматизировавший процесс шифрования, умер в полной

безвестности у себя дома.

История науки изобилует совпадениями. Например английский астроном Джон Адамс и его французский коллега Урбен Леверье почти одновременно сделали вывод о существовании планеты Нептун. Неудивительно, что подобные совпадения имели место и в криптографии. Случилось так, что в период между двумя мировыми войнами одно из таких совпадений затронуло сразу несколько человек. Как и Вернам, побуждаемые широким использованием секретной связи в военное время и вдохновляемые наступлением эпохи механизации, они независимо друг от друга изобрели машину, принцип действия которой на протяжении очень продолжительного времени находил наиболее широкое применение в криптографии. Этот принцип основывается на использовании колеса с перепайками — так называемого шифрдиска.

Шифрдиск представляет собой толстую круглую пластину, изготовленную из изоляционного материала (например, из твердой резины). С обеих сторон шифрдиска по окружности на равном расстоянии друг от друга закреплены по 26 электрических контактов (чаще всего они делались из латуни). Каждый контакт соединяется перепайкой с каким-либо другим контактом на противоположной поверхности шифрдиска. Таким образом, образуется электрическая цепь, которая начинается на одной стороне шифрдиска и заканчивается на другой.

Если условиться, что контакты на одной (входной) поверхности представляют буквы открытого текста, а контакты на другой (выходной) поверхности — буквы шифртекста, то проволочные перепайки между входной и выходной поверхностью обеспечивают преобразование открытого текста в криптограмму. Для зашифрования буквы открытого текста нужно только подать импульс тока на входной контакт, соответствующий этой букве. Ток пройдет по соединительному проводнику и появится на выходном контакте, представляющем букву шифртекста. Если записать все перепайки диска, зафиксировав соединения между входной и выходной поверхностью, то получится шифр одноалфавитной замены. Таким образом, шифрдиск воплощает процесс шифрования в форме, удобной для электромеханических манипуляций.

Для выполнения этих манипуляций шифрдиск устанавливается между двумя неподвижными круглыми пластинами, каждая из которых также изготовлена из изоляционного материала и снабжена 26 контактами, которые закреплены по кругу и соответствуют контактам, имеющимся на шифрдиске. Контакты входной пластины соединены с клавишами пишущей машинки, на которой набивается открытый текст. А каждый контакт выходной пластины связан с каким-либо устройством, предназначенным для вывода шифртекста (например, с сигнальной лампочкой). В результате, например, когда шифровальщик нажимает на клавишу «A» на пишущей машинке, он посылает токовый импульс от источника тока на контакт неподвижной входной пластины, закрепленный за буквой «A». Затем этот импульс попадает на входной контакт шифрдиска, соответствующий «A», и далее через перепайку проходит на выходной контакт, а с него — на лампочку, которая загорается над буквой шифртекста (пусть это будет буква «R»), которая ставится в соответствие букве «A».

Если бы все на этом и заканчивалось, то шифрдиск не был бы таким замечательным устройством. Тогда каждый раз при нажатии на клавишу «A» ток протекал бы по одной и той же электрической цепи и в итоге указывал бы на одну и ту же букву шифртекста.

Но все дело в том, что шифрдиск не остается неподвижным. Он вращается. Предположим, что он повернулся на одну позицию. Ток, который раньше, покидая контакт «A» входной пластины, попадал на контакт «R» выходной пластины, теперь преобразуется в совершенно другую букву, так как новый контакт шифрдиска с перепайкой, отличной от прежней, теперь встал против контакта «A» входной пластины. Подобным же образом всем другим буквам открытого текста ставятся в соответствие иные буквы шифртекста. Получается новый шифралфавит, причем каждый раз, когда шифрдиск поворачивается, используется другой шифралфавит. Можно выписать все эти шифралфавиты в виде таблицы из 26 строк и такого же количества столбцов. Если шифровальная машина сконструирована так, что шифрдиск поворачивается ровно на одну позицию каждый раз, когда зашифровывается какая-либо буква открытого текста, то итоговый результат будет таким же, как и при циклическом использовании этой таблицы строка за строкой сверху вниз. Получится не что иное, как шифр многоалфавитной замены с периодом 26.

Такая машина по-прежнему не оправдывает возлагаемых на нее надежд, поскольку реализуемый с ее помощью процесс шифрования слишком нестоек. Однако, если вместо неподвижной выходной пластины установить рядом с первым диском второй и заставить его перемешаться на одну позицию всякий раз, когда первый диск совершает полный оборот, то это позволит существенно усовершенствовать процесс шифрования. За счет поворота второго шифрдиска создается новый шифралфавит — 27-й по счету. И каждый новый вариант расположения этих двух шифрдисков

между неподвижными пластинами будет приводить к созданию нового шифралфавита. Следовательно, двухдисковая шифровальная машина реализует многоалфавитную замену со значительно большим периодом, чем однодисковая. Теперь он равняется 676.

Добавление третьего диска приводит к тому, что это число умножается на 26, так как все три диска возвращаются в свое исходное положение только через 17576 последовательных тактов зашифрования. При четырех и пяти дисках периоды равны 456976 и 11881376 соответственно.

Получается, что каждая буква открытого текста зашифровывается при помощи различных шифралфавитов. В этом и заключается сила дисковой системы: применение дополнительных дисков быстро доводит число шифралфавитов до таких астрономических величин, что количественные различия перерастают в качественные. Теперь можно создать свой шифралфавит для каждой буквы открытого текста, длина которого намного превосходит полное собрание сочинений Шекспира, «Войну и мир» Толстого, «Илиаду» Гомера, «Дон-Кихота» Сервантеса и «Кентерберийские рассказы» Чосера, вместе взятые.

Подобная длина сводит на нет всякую практическую возможность непосредственного вскрытия шифрсистемы на основе частоты встречаемости букв. Для такого вскрытия требуется примерно 50 букв на каждый шифралфавит, а это означает, что все пять дисков должны по 50 раз совершить свой полный оборот. Никакой криптоаналитик не может всерьез рассчитывать на то, чтобы стать обладателем такого трофея, даже если он сделает это делом всей своей жизни. Те же дипломаты, которые бывают не менее красноречивыми, чем политические деятели, редко поднимаются до подобных высот словоохотливости. Что уж тут говорить о военных и о шпионах, которые издавна славятся своей способностью держать язык за зубами и не тратят слов попусту.

Поэтому при вскрытии дисковых шифраторов криптоаналитик должен опираться на особые случаи, например, на получение открытого текста в полном объеме. Заполучить его криптоаналитик может несколькими путями. Случается, что для шифрования двух и более сообщении применяется одна и та же начальная установка шифрдисков или что эти установки очень близки одна к другой и последовательность шифралфавитов перекрывается на нескольких сообщениях. Иногда двум криптограммам соответствует один и тот же открытый текст (так бывает при рассылке идентичных приказов по нескольким подразделениям). Время от времени открытый текст становится известным в результате ошибок шифровальщика или опубликования дипломатических нот. На практике подобные ситуации встречаются довольно часто, что позволяет криптоаналитику использовать их с наибольшей выгодой для себя.

При вскрытии дисковых шифраторов криптоаналитики обычно применяют методы высшей математики, которые очень хорошо подходят для работы со многими неизвестными, связанными с шифрдисками. В основном этими неизвестными являются перепайки в каждом шифрдиске. Криптоаналитик математически разграничивает их, измеряя сдвиг между входными и выходными контактами. Например, перепайка со входного контакта 3 на выходной контакт 10 означает сдвиг, равный 7. Подобным же образом всем буквам придаются числовые значения, чаще всего «A» = 0, «B» = 1... «Z» = 25. Используя числовые значения известного или предполагаемого открытого текста, криптоаналитик составляет уравнения, в которых сдвиги в нескольких дисках являются неизвестными величинами, и затем решает эти уравнения.

Таковы основные принципы вскрытия дисковых шифраторов. Но их применение на практике обрекает криптоаналитика на самые жестокие испытания интеллекта среди известных человеку. Количество уравнений и неизвестных, кажется, превышает число песчинок в пустыне, а сами уравнения сложны и запутанны подобно гордиеву узлу. Отчасти эта сложность проистекает из необходимости указать все сдвиги по отношению к неподвижной входной и выходной пластине. С другой стороны, это связано с тем, что один сдвиг вычисляется через несколько других. Сдвиг на 3-м шифрдиске может быть известен только как сумма сдвигов на 1-ми 4-м шифрдисках, а сдвиг на 4-м шифрдиске может, в свою очередь, равняться сумме сдвигов на 2-м и 5-м шифрдисках. Таким образом, одно неизвестное может быть выражено через четыре или пять величин. Математическая теория групп очень подходит для решения уравнений такого типа, но она также очень подвержена ошибкам. В результате любое ложное предположение разрастается по древообразным ветвям этих уравнений, как злокачественная опухоль.

Характер сдвигов, восстановленных криптоаналитиком, может оказаться правильным только в относительном смысле, и потребуется дополнительно найти перестановку, с помощью которой можно будет получить абсолютно точные значения этих сдвигов. Кроме того, шифровальщики противника редко делают одолжение, устанавливая шифрдиски в одинаковые первоначальные положения при шифровании всех своих сообщений. Вскрытие также очень сильно затрудняется

использованием устройств, которые обеспечивают неравномерное движение шифрдисков. Сам шифровальщик может внести дополнительные поправки, просто переставив шифрдиски. Короче говоря, дисковая шифрсистема создает исключительно сложный и стойкий шифр, составленный из достаточно простых элементов. Кем же были изобретатели этого своеобразного криптографического лабиринта?

Американец Эдвард Хеберн посвятил дисковым шифраторам лучшие порывы своего таланта. Он родился 23 апреля 1869 г. в городе Стриторе в штате Иллинойс. В 19 лет Хеберн отправился на Запад и там долгое время плотничал, строил и продавал деревянные дома. Он был голубоглазым шатеном среднего роста и телосложения. Хеберн носил усы, слыл спокойным, добрым и уравновешенным человеком и очень много читал. Вскоре после того, как ему исполнилось 40 лет, Хеберн неожиданно проявил большой интерес к криптографии.

С 1912-го по 1915 г. Хеберн подал несколько патентных заявок на различные шифровальные устройства. Например, он создал шифрсистему, в которую входили две электрические пишущие машинки, соединенные между собой 26 проводами. Когда нажималась какая-либо клавиша на одной машинке, это приводило к тому, что на другой печаталась буква шифртекста. Так как провода оставались подсоединенными к одним и тем же контактам на протяжении всего периода времени, в течение которого набирался открытый текст, то шифрование осуществлялось методом одноалфавитной замены. Несмотря на слабость применяемого метода шифрования, изобретение Хеберна было весьма примечательно тем, что преобразование открытого текста в криптограмму выполнялось при помощи токовых импульсов, посылаемых по электрическим проводам. Взаимные соединения этих проводов представляли собой прообраз шифрдиска. К 1917 г. идея создания дискового шифратора окончательно созрела в голове американского изобретателя. В том же году Хеберн сумел воплотить эту идею в виде подробных чертежей, а еще через год — в виде реального аппарата.

В начале 1921 г. Хеберн прибыл в Вашингтон, связался с представителями службы связи американских ВМС и продемонстрировал им собственное изобретение, одновременно направив свою первую заявку на шифрдиск в вашингтонское патентное бюро. «У нас долгое время безуспешно пытались, — вспоминал позднее тогдашний начальник службы связи ВМС США, — внести радикальные изменения в систему обеспечения секретности военных коммуникаций. И вот появился г-н Хеберн с Западного побережья и принес нам свою машину. Мы были восхищены, когда он продемонстрировал, что она может делать, и сразу же пожелали заказать несколько таких машин для нужд всего нашего флота».

В 1921 г. Хеберн основал фирму «Хеберн электрик код», которая стала самым первым производителем дисковых шифраторов в США. Получив необходимую поддержку от ВМС, а также полагая (вполне справедливо), что его изобретение является шифрующим устройством будущего, он стал активно продавать акции своей фирмы, чтобы собрать необходимый капитал. Поскольку «Хеберн электрик код» владела десятками патентов по всему миру (среди них был не только патент на дисковый шифратор, но и патенты на многие другие передовые для своего времени устройства, такие, как электрические пишущие машинки и указатели направления движения для автомашин), Хеберн без труда продал акции своей фирмы на астрономическую по тем временам сумму примерно в 1 миллион долларов.

В 1922 г. на деньги, вырученные от продажи акций, Хеберн приобрел механические мастерские, чтобы наладить в них производство штампов, литейных форм и шаблонов для дисковых шифраторов. Выступая перед сотрудниками своей фирмы, Хеберн заявил: «Мы очень близки к большому финансовому успеху благодаря нашим изобретениям в области шифровальных машин, и поэтому необходимо подготовиться к тому, чтобы заняться этим бизнесом на постоянной основе». 21 сентября паровая землеройная машина, которой управлял сам Хеберн, начала земляные работы на участке, отведенном под трехэтажное здание в неоготическом стиле. Согласно планам Хеберна, под крышей этого здания должны были со временем разместиться полировочный, инструментальный и сборочный цехи, а также ряд других производств, необходимых, чтобы наладить массовый выпуск дисковых шифраторов.

Пока шло строительство, Хеберн продолжал бойко торговать акциями своей фирмы, убеждая потенциальных покупателей, что их капитал имеет такой же шанс на успех, как и первоначальный капитал, вложенный в телефон, радио и другие великие изобретения человечества. Он завалил держателей акций «Хеберн электрик код» радужными отчетами и держал двери своей канцелярии открытыми до 9 часов вечера каждый божий день, включая воскресенья, чтобы желающие могли воочию ознакомиться с его удивительным изобретением. Собственное творение вызвало у самого

Хеберна такой восторг, что он даже написал целую оду в честь дискового шифратора:

На Западе появилось удивительное изобретение.
Это триумф
многолетнего, неустанного, терпеливого труда
Решена многовековая, сложнейшая проблема.
Создан изумительный, совершенный шифр...
Его достоинства столь очевидны,
что ни одно государство в мире
Не может его игнорировать.
Он — результат глубоких исследований,
продиктованных необходимостью.
Теперь «Хеберн электрик код» властвует
над всеми шифрами.
Рыцарь радио, страж сокровищ,
Мозг нации, гарант полной безопасности,
Сердце корабля, хранитель жизней
В борьбе грубой силы против интеллекта...
Непостижимая, хитроумнейшая загадка для науки,
Настолько глубокая, что берегитесь, коварные предатели!
Вокруг вас расставлена невидимая гениальная западня.
Мировая война продемонстрировала
его крайнюю необходимость,
Ученые всех государств участвовали
в жестоком состязании.
Лучшие умы человечества стремились добиться успеха,
И сейчас в центре мирового внимания —
американское изобретение.

В ВМС США справедливо решили, что лучше полагаться не на результаты поэтических упражнений Хеберна, а на мнение своих квалифицированных экспертов-криптологов. Именно из них в 1923 г. была создана авторитетная комиссия для рассмотрения дискового шифратора Хеберна. После недолгих размышлений эта комиссия единогласно порекомендовала принять машину на вооружение, но только после ее усовершенствования.

К концу 1923 г. было, наконец, закончено строительство грандиозного предприятия по производству дисковых шифраторов. Его стоимость перевалила за отметку 380 тысяч долларов, что в полтора раза превысило первоначальную смету. Доходы «Хеберн электрик код» оказались значительно ниже расходов на строительство, и весной 1924 г. фирма не смогла рассчитаться по своим долговым обязательствам. В ходе последовавшей реорганизации Хеберн был снят с поста президента. 30 апреля состоялось собрание обозленных акционеров, которые потребовали привлечь Хеберна к уголовной ответственности за то, что он торговал акциями своей фирмы по 3-5 долларов за штуку вместо установленной американским законом цены в 1 доллар.

Расследование продолжалось с 1924-го по 1926 г. За это время ВМС США заказали в «Хеберн электрик код» два дисковых шифратора, заплатив за них по 600 долларов за каждый, а армия перечислила Хеберну 1000 долларов еще за два шифратора. Крупная судоходная компания «Пасифик стимшип» купила семь дисковых шифраторов Хеберна по цене 120 долларов за каждый (такие отличия в цене объяснялись разным количеством шифрдисков в машинах, выставленных на продажу) для использования на пароходах и в филиалах этой компании. Наконец, итальянское правительство приобрело для своих нужд еще один дисковый шифратор производства «Хеберн электрик код».

Тем временем давление со стороны держателей акций все нарастало. Они жаловались на недостаточные объемы продаж, регулярно проводили митинги протеста против неправильной, по их мнению, политики руководства фирмы. В конце концов 1 марта 1926 г. в суде высшей инстанции началось слушание дела Хеберна по обвинению в нарушении закона штата Калифорния о корпоративных ценных бумагах. После четырехдневного разбирательства суд удалился на совещание. Вернувшись через 12 минут, судьи признали Хеберна виновным. И хотя исполнение приговора было отложено, все эти события свели к нулю всякие шансы привлечь в «Хеберн электрик код» дополнительный капитал, чтобы расквитаться с долгами и продолжить производство дисковых

шифраторов. Через три месяца фирма обанкротилась.

Но Хеберн не желал сидеть сложа руки. Связывая свои надежды с ВМС, он учредил в штате Невада новую фирму под названием «Интернэшнл код машин». В 1928 г. ее дела пошли на лад, когда ей удалось продать американским ВМС четыре пятидисковых шифратора по 750 долларов за штуку и получить еще по 20 долларов за каждый шифрдиск к ним. Хеберн с несколькими своими сотрудниками сумел изготовить эти машины практически вручную и затем лично доставил их в штаб 12-го военно-морского округа в Сан-Франциско. Одна машина осталась там, а остальные были разосланы в военно-морское министерство и главнокомандующему флотом США. В ВМС в первую очередь хотели на практике убедиться именно в их механической надежности, а не в криптографической стойкости, которая тогда считалась вполне удовлетворительной. С 1929-го по 1930 г. эти машины обеспечивали секретность значительной части официальной переписки высшего командования американских ВМС. Дела Хеберна пошли еще успешнее в 1931 г.: ВМС купили у него 31 дисковый шифратор на общую сумму 54480 долларов для повседневного использования в качестве шифрсистемы командования высшего звена.

Однако, когда в 1934 г. Хеберн предложил ВМС приобрести новый, усовершенствованный вариант своей шифровальной машины, в ответ он совершенно неожиданно получил очень резкое письмо с категорическим отказом. Поскольку других заказчиков у Хеберна практически не было, этот отказ заставил Хеберна прекратить деятельность на поприще производства шифровальной техники. И хотя купленные у Хеберна дисковые шифраторы не были сняты с эксплуатации после разрыва отношений с ним, вскоре в результате интенсивной работы они износились и в 1936 г. были заменены на новые, произведенные другой американской фирмой. Интересно отметить, что эти машины были затем отремонтированы и установлены на береговых станциях, где продолжали использоваться вплоть до 1942 г. А две из них даже были захвачены японцами в качестве военных трофеев.

Последние годы своей жизни Хеберн прожил на доходы от собственности, оставленной сестрой его жены. Убежденный, что вооруженные силы воспользовались его основными идеями, не уплатив ему за это соответствующую компенсацию, в 1947 г. Хеберн предъявил всем трем видам вооруженных сил США иск на общую сумму 50 миллионов долларов. В течение последовавшего за этим шестилетнего периода бюрократической волокиты Хеберн умер. Ему было 82 года, когда 10 февраля 1952 г., пытаясь поднять слишком тяжелый ящик, он умер от сердечного приступа.

В начале 1953 г. армия, ВМС и ВВС США отвергли иск Хеберна. Через несколько месяцев его наследники вновь предъявили американскому правительству иск на сумму 50 миллионов долларов. Пользуясь мелкими юридическими зацепками, исковый суд США ограничил время возмещения ущерба периодом с 1947-го по 1953 г., а нарушение прав истца было сведено к очень узкому вопросу о незаконном использовании одного специального устройства для управления движением шифрдисков. Был проигнорирован основной вопрос о том, действительно ли вооруженные силы США позаимствовали у Хеберна основные принципы работы дискового шифратора и потом использовали эти принципы в сотнях тысяч стойких шифровальных машин во время Второй мировой войны без справедливой компенсации автору, который их изобрел.

Опираясь на букву закона, американское правительство изо всех сил стремилось не заплатить Хеберну и его наследникам ни цента. В 1958 г. оно, в конце концов, согласилось отдать им какие-то жалкие крохи — 30 тысяч долларов. И то отнюдь не из чувства справедливости, а поскольку опасалось, что, отстаивая свои права в суде, ему придется раскрыть некоторые свои секреты. А Хеберн явно заслуживал лучшего, и его история — трагическая, полная несправедливости — не делает чести его родной стране.

Днем рождения самого известного дискового шифратора в истории криптографии можно считать вторник 7 октября 1919 г., когда немецкий изобретатель Хуго Кох получил патент на свою «секретную пишущую машинку». Коху было тогда 49 лет. Он очень увлекался конструированием различных диковинных приспособлений и справедливо полагал, что его новое изобретение из области криптографии будет иметь коммерческий успех. Кох указал в своем патенте, что лучи света, воздух, вода или масло, протекающие по трубкам, могут переносить шифрующий импульс так же хорошо, как и электричество, передаваемое по проводам. Он также отметил, что этот импульс необязательно должен двигаться через диск, а может проходить, например, по трубкам, просверленным в болванках, скользящих между неподвижными пластинами. Кох отдавал предпочтение дисковому механизму, но не создал шифровальной машины в какой-либо из предложенных им в патенте форм. В 1922 г. Кох тяжело заболел и, предчувствуя скорую кончину, передал все права на свои патенты другому немецкому изобретателю. Через год Коха не стало.

Немецким изобретателем, унаследовавшим патентные права Коха, стал Артур Шербиус — толковый инженер, имевший степень доктора наук и ряд патентов, в том числе и в такой далекой от криптографии области, как керамика. Жил Шербиус в Вильмерсдорфе, пригороде Берлина. Первое придуманное им криптографическое устройство превращало цифровые кодовые обозначения в произносимые слова, поочередно заменяя цифры на соответствующие им гласные и согласные буквы с помощью специального устройства. Это устройство состояло из «нескольких коммутаторов, которые соединяют каждый входной проводник с одним из выходных проводников и которые устроены так, что можно легко изменять характер этих соединений». Именно оно стало прообразом дискового шифратора, позднее изобретенного Шербиусом и подробно описанного в его очередной патентной заявке. И хотя диски в этом шифраторе применялись только для преобразования цифровых последовательностей, в последующих подобных ему устройствах Шербиус увеличил количество контактов с 10 до 26, так что эти устройства вполне могли использоваться для шифрования букв.

Шербиус назвал свою машину «Энигма» («Загадка»). Первая ее модель была очень громоздкой. По своим размерам и форме она больше всего напоминала кассовый аппарат и вскоре была заменена другой моделью, представлявшей собой обычную пишущую машинку, дополненную шифрующим механизмом. Третья модель была портативной. Буквы в ней не печатались на бумаге, а подсвечивались лампочками.

«Энигма» имела два весьма существенных отличия от других дисковых шифраторов. Во-первых, ее последний шифрдиск на самом деле был полудиском: все его контакты располагались исключительно на одной стороне и были соединены только между собой (импульс, приходивший на этот шифрдиск, разворачивался на 180 градусов и вновь отправлялся через шифрдиски, через которые он только что прошел). А во-вторых, движение шифрдисков управлялось специальными зубчатыми колесами, чтобы сделать его неравномерным. Первоначально количество зубцов было слишком мало, чтобы существенно затруднить вскрытие шифратора, однако в более поздних моделях «Энигмы» этот недостаток был исправлен.

В июле 1923 г. была создана корпорация для производства и сбыта «Энигм». Она называлась «Корпорация шифрмашин» и даже в период жестокой послевоенной инфляции в Германии сумела собрать огромный капитал путем продажи своих акций. Шербиус вошел в совет директоров корпорации, состоявший из шести человек.

«Корпорация шифрмашин» развернула чрезвычайно энергичную деятельность по стимулированию спроса на свою продукцию. Она выставила «Энигму» на съезде Международного почтового союза в 1923 г., а на следующий год добилась, чтобы германское почтовое ведомство обменялось с участниками очередного съезда этого союза приветствиями, зашифрованными с помощью «Энигмы». «Энигма» стала широко рекламироваться на радио. О ней пространно рассказывалось в книге по шифрмашинам. написанной доктором Зигфридом Тюркелем, директором Криминологического института венской полиции. На немецком и английском языках были выпущены рекламные буклеты, в которых говорилось:

«Естественному любопытству ваших конкурентов сразу же будет положен конец, так как «Энигма» позволяет вам хранить содержание ваших документов или, по крайней мере, их самых важных частей в полной тайне от любопытных глаз без каких-либо существенных затрат. Один хорошо защищенный секрет может окупить всю стоимость этой машины».

Однако, несмотря на рекламу, дела у «Корпорации шифрмашин» шли из рук вон плохо. Несколько «Энигм» было приобретено армиями различных государств и компаниями, занимающимися связью, но массовых закупок так и не последовало. Производство постоянно сокращалось. Даже после 10 полных лет деятельности корпорация никак не могла приступить к выплате дивидендов своим акционерам. Поэтому 5 июля 1934 г. она была ликвидирована и передала свои активы новой фирме по производству шифраторов, организованной Рудольфом Хаймсетом и Элизабет Ринке, двумя директорами «Корпорации шифрмашин».

Вскоре Гитлер приступил к перевооружению Германии, и эксперты-криптографы Вермахта, решив, что «Энигма» обеспечивает достаточные гарантии в отношении безопасности связи, начали снабжать ею свои растущие вооруженные силы. Неизвестно, воспользовались ли Хаймсет и Ринке этими новыми возможностями. Скорее всего, их корпорация была национализирована или объединена с другими немецкими фирмами, занимавшимися выпуском дисковых шифраторов. На протяжении всей Второй мировой войны портативная, работавшая от батарей «Энигма» с загорающимися лампочками и в деревянном футляре, имевшая размеры и вес пишущей машинки, активно использовалась в армии, ВМС и ВВС Германии. Немецкие военные связисты считали ее очень надежной и полагали, что она обеспечивает необходимую безопасность связи. Ее

единственный видимый недостаток заключался в том, что она не могла печатать текст, и для быстрой работы с ней требовалось по крайней мере три человека — один читал вводимый текст и нажимал клавиши, второй произносил буквы громким голосом по мере того, как они загорались, а третий записывал текст на бумагу.

Примечательно, что самый сложный из дисковых шифраторов, изобретенных в начале XX века, был запатентован всего лишь через три дня после самого простого. Кох получил свой патент во вторник, а в пятницу на той же неделе в октябре 1919 г. шведу Арвиду Дамму был выдан в Стокгольме патент № 52279.

Шифровальное устройство, изобретенное Даммом, было двухдисковым: два шифрдиска вращались над и под горизонтальной неподвижной пластиной. Движением шифрдисков управляли зубчатые колеса, которые позволяли поворачивать их на различное количество шагов для каждой буквы открытого текста. Однако придуманный Даммом шифрующий механизм оказался настолько громоздким и сложным, что так никогда и не был построен. И хотя выдвинутая Даммом концепция построения дискового шифратора заставляет упомянуть его в почетном списке изобретателей шифрдиска, действительное влияние, оказанное им на криптографию, связано с тем, что он основал компанию по производству дисковых шифраторов, которая впоследствии стала единственной в мире, добившейся значительного коммерческого успеха.

Свою карьеру Дамм начал в качестве инженера в текстильной промышленности. Работая управляющим на фабрике в Финляндии, Дамм влюбился в цирковую наездницу-венгерку, нравственные устои которой были слишком твердыми, чтобы она могла позволить себе какие-либо отношения с мужчинами до брака. Тогда Дамм попросил своего товарища облачиться в одежду священника и «поженить» их на фиктивной церемонии в местной часовне, добившись тем самым желанной цели.

С юных лет Дамм очень увлекался механикой. На его вилле в пригороде Стокгольма были такие кресла, у которых нажатием кнопки можно было регулировать высоту подлокотников или упоров для ног. С помощью кнопок, расположенных на письменном столе, Дамм мог зажигать лампочки и открывать двери. Были у Дамма и другие трюки, которыми он любил забавлять своих гостей.

Интерес к шифровальному делу пробудился у Дамма под влиянием его брата Айвара, криптоаналитика-любителя, преподававшего математику в средней школе в шведском городе Евле. Дамм рассказал об изобретенной им шифрмашине одному своему знакомому, работавшему в шведском посольстве в Берлине. Этот знакомый организовал встречу Дамма со своим братом, капитаном 3-го ранга Олофом Гюльденом, начальником Королевского морского училища в Стокгольме. В 1916 г. Гюльден и Дамм основали фирму «Крипто АГ». Среди вкладчиков капитала фирмы оказались Эммануэль Нобель, племянник Альфреда Нобеля, изобретшего динамит и учредившего Нобелевские премии, и Цезарь Хагелин, близкий друг Эммануэля, работавший управляющим нефтедобывающей компанией братьев Нобель в России, а до этого занимавший пост генерального консула Швеции в Санкт-Петербурге. В 1921 г. фирма «Крипто АГ» снимала помещение из трех комнат в центре Стокгольма, и в ней работало больше управляющих, чем собственно рабочих: не считая самого Дамма, среди ее персонала числились исполнительный директор, технический директор, чертежник и бухгалтер.

Неудивительно, что успехи руководимой Даммом фирмы были практически нулевыми. Тем более, что Дамм не мог уделять достаточного внимания делам фирмы, поскольку личная жизнь поглотила его целиком. Началось все с того, что он влюбился в молоденькую девушку чуть старше 20 лет, которую он встретил в пригородном поезде. Дамм решил отделаться от своей фиктивной жены-венгерки путем бракоразводного процесса, который, как он считал, будет не более действительным с юридической точки зрения, чем и сама его женитьба. В качестве запасного варианта Дамм рассчитывал добиться высылки «жены» из страны, обвинив ее в шпионаже. Однако он оказался в очень трудном положении на суде, когда его партнер Гюльден рассказал о мошенничестве Дамма с женитьбой, а также о придуманной Даммом уловке с мнимым шпионажем. Дамм отомстил Гюльдену, передав пост исполнительного директора своей фирмы другому лицу, как только представилась такая возможность.

Однако к этому времени в фирме стало укреплять свои позиции новое лицо — Борис Хагелин, сын Цезаря Хагелина. Борис родился 2 июля 1892 г. на Кавказе, где некоторое время работал его отец. В течение трех или четырех лет он учился в Санкт-Петербурге, а затем вернулся в Швецию и в 1914 г. закончил Королевский технологический институт в Стокгольме, получив диплом инженера-механика. После шести лет работы в шведском филиале американской компании «Дженерал электрик» и года, проведенного в США на службе в компании «Стандард ойл», Цезарь Хагелин и

Эммануэль Нобель устроили Бориса в «Крипто АГ», чтобы он представлял их интересы, как основных вкладчиков капитала этой фирмы.

Три года спустя, когда Дамм был в командировке в Париже, молодой Хагелин узнал, что шведская армия рассматривает вопрос о закупке «Энигм». Он спешно внес ряд изменений в один из дисковых шифраторов, разработанных Даммом. Хагелин снабдил его клавиатурой и индикаторными лампочками наподобие тех, которые применялись в «Энигме», сделав более пригодным для использования в полевых условиях. Назвав переделанный им шифратор «Б-21», Хагелин предложил его шведской армии. Вернувшийся из Парижа Дамм в пух и прах раскритиковал «Б-21», но армия осталась им довольна и в 1926 г. сделала на него в «Крипто АГ» большой заказ.

В начале 1927 г. Дамм умер. Фирма «Крипто АГ», находившаяся в плачевном финансовом положении, была куплена семьей Хагелин. После реорганизации ее возглавил Борис Хагелин. Он прекрасно понимал, что печатающие шифраторы работают быстрее, точнее и более экономичны, чем индикаторные шифрмашины, подобные «Энигме». Вначале Хагелин подсоединил «Б-21» к электрической печатной машинке, но обнаружил, что получившееся в результате шифровальное устройство было слишком громоздким. Поэтому он объединил в одной машине и печатающий, и шифрующий механизмы, создав дисковый шифратор «Б-211». Этот шифратор весил около 17 килограммов, работал со скоростью 200 знаков в минуту и помещался в деревянном футляре размером с большой портфель.

В 1934 г. это был самый компактный печатающий дисковый шифратор. Но Хагелин пошел еще дальше, когда французский генеральный штаб обратился к нему с просьбой совершить, казалось бы, невозможное — создать карманный шифратор, который распечатывал бы текст и мог использоваться одним человеком. Чтобы иметь наглядное представление о размерах этого шифратора, Хагелин вначале выстрогал кусок дерева, который помещался в кармане. Пытаясь придумать шифрующий механизм, который имел бы такие размеры и, кроме того, был бы достаточно стойким, он вспомнил о конструкции, предложенной ему тремя годами ранее изобретателями автомата для штучной продажи товаров. Это было как раз то, что нужно. Тем более, что изобретатели уступили Хагелину все права на данное устройство, когда не смогли уплатить за прототип, изготовленный Хагелином по их просьбе.

Хагелин уменьшил это устройство до нужных размеров и назвал его «С-36». Весило оно примерно столько же, сколько весит обычная кодовая книга. При работе с «С-36» оператор сначала устанавливал ключ, а потом поворачивал ручку, расположенную слева от буквы открытого текста на клавиатуре, и вращал рукоятку, расположенную справа. При этом механизм делал один оборот, и маленькое колесико печатало выходной знак шифртекста на бумажной ленте. Хагелин даже добился, чтобы «С-36» распечатывал шифртекст с разбиением на пятизначные группы, а открытый текст — в виде обычных слов. Скорость работы «С-36» составляла в среднем 25 букв в минуту.

Когда французы увидели «С-36», они сразу же ухватились за него руками и ногами. Сделанный ими в 1935 г. заказ сразу на пять тысяч таких шифраторов оказался поворотным пунктом для процветания «Крипто АГ». Хеберн, Шербиус и Дамм потерпели неудачу не из-за внутренних недостатков изобретенных ими дисковых шифраторов, а просто потому, что в 20-х годах для этих машин еще не пришло время. До тех пор, пока не начался процесс перевооружения, пришедшийся на середину 30-х годов, рынок для подобных устройств просто еще не сложился, и найти им сбыт в количестве, достаточном для оправдания затрат на их производство, было просто невозможно.

В 1936 г. Ив Гюльден, сын одного из основателей «Крипто АГ», проанализировал стойкость шифратора «С-36» и порекомендовал внести в него некоторые важные изменения, которые были одобрены самим Хагелином. В этом же году Хагелин начал переписку с американцами относительно «С-36», а в 1937-м и 1939 гг. совершил длительные деловые поездки за океан.

Со своей стороны США выразили большую заинтересованность в закупке «С-36», однако при условии внесения в него определенных усовершенствований. Хагелин вернулся в Швецию, чтобы модифицировать «С-36» и подготовить его для массового производства, но уже через короткое время понял, что если хочет добиться успеха, то должен немедленно отправиться в США, поскольку начавшаяся Вторая мировая война, скорее всего, не позволит развернуть выпуск модифицированных дисковых шифраторов типа «С-36» в Европе.

«Обычную визу получить было невозможно, — вспоминал Хагелин, — поэтому я убедил шведское министерство иностранных дел послать меня в Америку в качестве дипломатического курьера. Мы с женой отправили наш багаж заранее и сели в поезд, следовавший в Стокгольм. Там мы узнали, что стокгольмские бюро путешествий отменили все поездки в США. Тогда мы решили попытаться отплыть из Италии. С чертежами в портфеле и двумя разобранными шифраторами в

сумке мы сели в экспресс Стокгольм — Берлин. Нам сопутствовала удача. Мы с грохотом промчались через самое сердце Германии и через три дня благополучно прибыли в Геную. В ту ночь стекла в окнах отеля, в котором мы остановились, были побиты — мы совершенно случайно решили расположиться в отеле «Лондон», а Италия уже находилась в состоянии войны с Англией. Но мы все же сумели отправиться в Нью-Йорк с последним рейсом парохода, отплывавшего из Генуи».

Этот лихой побег окупился с избытком. Усовершенствованный вариант «С-36» американцам очень понравился. После испытаний он был переименован в «М-209» и стал широко использоваться в американских военных подразделениях от дивизий до батальонов. Отчисления Хагелину, как владельцу патента, составили миллионы долларов. Он стал первым и единственным человеком, нажившим многомиллионное состояние благодаря криптографии.

В 1944 г. Хагелин, теперь уже мультимиллионер, вернулся в Швецию. Полагая, что с производством шифраторов покончено и на первый план выдвигаются проблемы мирного времени, Хагелин приобрел огромное имение и кирпичный завод, находившиеся в 50 километрах к югу от Стокгольма. Как же он ошибался!

Началась «холодная война». По мере того как две великие державы, испытывая огромное недоверие друг к другу, наращивали свою собственную военную мощь и вооруженные силы своих союзников, формировался новый, еще более емкий рынок для шифраторов. Затем стали разваливаться старые колониальные империи. Десятки новых государств, возникших на их руинах, в значительной степени увеличили потребность в шифраторах. За помощью в организации защиты каналов связи своих дипломатических представительств, которые они учредили по всему миру, эти страны обратились к Хагелину.

Вначале Хагелин сосредоточил все свои научно-исследовательские подразделения и производственные мощности в Стокгольме. Однако шведское законодательство позволяло правительству присваивать себе изобретения, в которых оно нуждалось для целей национальной обороны, и это вынудило Хагелина перенести в 1947 г. свою научно-исследовательскую работу в швейцарский город Цуг. Цуг оказался настолько привлекательным для предпринимательской деятельности Хагелина (в немалой степени из-за своих льгот по налогам), что в 1959 г. он перевел туда и остальные части своей фирмы.

Фирма «Крипто АГ» располагается на холме посреди жилого района в четырехэтажном здании фабричного типа, отделанном коричневатой штукатуркой. Из здания открывается вид на переливающееся искорками Цугское озеро и на расположенные вдалеке голубоватые Швейцарские Альпы. Вероятно, это самое красивое место, где когда-либо занимались криптографией. Изнутри доносятся гул и слабое жужжание — типичные звуки для промышленного предприятия. Более полутора сотен рабочих выполняют, главным образом, сборку шифраторов из комплектующих, которые Хагелин закупает у швейцарских и германских производителей. На верхнем этаже здания находятся помещения для конструкторов и чертежников. Большая часть третьего этажа выделена администрации. Там же у Хагелина отведено место и под собственный музей шифраторов, которые размещаются у него на двух огромных стеллажах.

Инструментальные цеха вместе с небольшим штамповочным производством занимают весь первый этаж. Сборка шифраторов происходит на втором этаже, где рядом с крохотными токарными станками, применяемыми в часовом производстве, располагаются груды отдельных частей и где рабочие производят пайку ультразвуком. В лаборатории инженеры создают и испытывают новые электронные устройства, которые моделируют механические операции для достижения очень высоких скоростей работы.

Хагелин не пытается заниматься криптоанализом своих собственных шифраторов. Он очень хорошо разбирается в методах их вскрытия и прекрасно осознает, что стойкость его шифрмашин зависит от их правильного использования. Поэтому Хагелин полагается на мнение тех, кто является потребителем его продукции, и это мнение служит ему в качестве неиссякаемого источника идей для внесения всевозможных усовершенствований.

Фирма «Крипто АГ» торгует тремя основными моделями. «С-52» является модифицированным вариантом «М-209» и стоит 600 долларов. «СД-55» представляет собой карманный шифратор, размером чуть больше транзисторного приемника. За него в «Крипто АГ» просят 200 долларов. «Т-55» относится к классу линейных шифраторов, предназначенных для шифрования телетайпных импульсов, а не букв открытого текста, и он гораздо больше по габаритам и тяжелее по весу, чем все другие шифраторы.

Кроме того, Хагелин предлагает своим клиентам целую серию весьма соблазнительных дополнительных приспособлений, оказывающих в своей области такое же воздействие на

покупателей, как те модные новинки, от приобретения которых так трудно удержаться любителям высококачественного воспроизведения звука или заядлым яхтсменам. «Крипто АГ» выпускает раму с клавиатурой и электромотором, на которую устанавливается шифратор «С-52». В результате работа на нем значительно ускоряется и уподобляется работе на обычной электрической пишущей машинке. Приставка «РЕ-61» производит набивку шифртекста, получаемого при помощи «С-52», на телетайпную ленту. Арабы, бирманцы, таиландцы и другие клиенты, использующие алфавиты, отличающиеся от латинского, могут покупать машины с буквами своих национальных алфавитов. Эти буквы обычно используются только для набора открытого текста, а в шифртексте применяются латинские буквы, которые более приемлемы для международной переписки. Можно также купить аппараты для изготовления одноразовых шифрблокнотов. Эти аппараты обычно вырабатывают «гамму» с помощью одного из самых известных случайных процессов — распада какого-либо радиоактивного элемента. Счетчик Гейгера заставляет такой аппарат пробивать отверстие в бумажной ленте всякий раз, когда распад превышает определенный уровень. Соответственно отверстие не пробивается, если интенсивность распада падает ниже этого уровня. Также используется тепловой шум, который в равной мере является случайным.

Покупателями почти всей продукции фирмы «Крипто АГ» являются правительственные ведомства различных стран. Лишь небольшая часть выпускаемого этой фирмой оборудования попадает в коммерческие компании, которые работают в таких отраслях с высокой степенью конкуренции, как добыча нефти и других полезных ископаемых, или в финансовой области. Полностью укомплектованные шифровальные установки обычно стоят от 30 до 50 тысяч долларов. Когда покупатели начинают возмущенно протестовать против слишком завышенной цены, Хагелин спрашивает их, посылают ли они сообщения, ценность которых ниже, чем та сумма, которую просят в «Крипто АГ» за оборудование для защиты этих сообщений. Такой вопрос, как правило, успокаивает разволновавшихся клиентов.

В «Крипто АГ» покупателям терпеливо разъясняют, что огромное количество изменяемых элементов в шифраторе — более 24 квинтильонов квинтильонов квинтильонов квинтильонов — позволяет каждому клиенту выбирать индивидуальный набор ключей к шифру. Им дают советы о том, какие процедуры работы с ключами являются хорошими, поскольку они не снижают стойкость шифратора, а какие — плохими. Но в «Крипто АГ» тщательно воздерживаются от того, чтобы рекомендовать конкретные ключи, так как не хотят, чтобы клиенты думали, что им даются однотипные инструкции, которые получают и все остальные покупатели. «Мы считаем плохой деловой практикой, когда продавец знает о том, как именно используется машина покупателя. Это должно действительно храниться в строгой тайне, — говорится в фирменной брошюре, — подобно тому, как изготовителю сейфов не следует быть осведомленным о конкретной ключевой комбинации сейфа своего клиента».

Хагелин, дом которого в Цуге расположен в нескольких десятках метров позади здания его фирмы, отошел от дел лишь частично. Он уже не проводит целые дни на своем уникальном предприятии, но все же продолжает лично руководить большей частью научно-исследовательских разработок фирмы. Хагелин говорит: «Я не знаю электроники, но я знаю, как много можно добиться с ее помощью». Он сам ведет дела со своими старыми клиентами, хотя и передал обслуживание новой клиентуры, а также рассмотрение многих административных деталей своему главному управляющему Стюру Нюбергу. Седовласый мужчина выше среднего роста и умеренной упитанности с волевыми, приятными чертами лица, Хагелин отличается спокойным юмором и добротой. Его карманы всегда набиты арахисом, которым он кормит птиц, слетающихся к нему на подоконник. Был случай, когда одна птичка села ему на голову, а другая — на руку, пока он вечером возвращался домой с работы. А по ночам птицы оставляют свои «визитные карточки» на светильнике в его спальне.

Круг интересов Хагелина очень широк. Как большой знаток, он разбирается в вопросах гастрономии, делает хорошие любительские фотографии, любит парусный спорт и со знанием дела беседует о цветах, растущих позади дома на клумбах, за которыми ухаживает его жена. Дважды в год Хагелин ездит в Швецию либо в свое поместье, находящееся неподалеку от Стокгольма, либо в бревенчатый коттедж на севере страны. Суфле, подаваемое на завтрак его кухаркой, такое же воздушное и приятное на вкус, как и в лучшем ресторане Нью-Йорка или Парижа. В белом «мерседесе», которым Хагелин правит сам, ощущается крепкий запах коричневатой кожи, которой отделаны сиденья. В его книге для гостей собраны подписи людей, приехавших в Цуг со всего света — из Германии, Египта, Ирана, США, Франции. Сам он — исключительно любезный и внимательный хозяин. Благодаря криптографии Хагелин получил наибольшие материальные выгоды

по сравнению с любым другим человеком во всем мире, и можно с уверенностью сказать, что для этой цели нельзя было бы подобрать личность более приятную.

«АМЕРИКАНСКИЙ ЧЕРНЫЙ КАБИНЕТ»

Один из самых знаменитых американских криптоаналитиков обязан своей славой в большей степени сенсационной манере собственных заявлений и в меньшей — достижениям в области дешифрования. И в этом нет ничего удивительного, поскольку Герберт Ярдли был, по-видимому, наиболее обаятельной, эрудированной и яркой личностью среди тех, кто когда-либо занимался криптоанализом.

Ярдли родился 13 апреля 1889 г. в Уортингтоне — маленьком городке на Среднем Западе США. Его детство и юность пришлись на спокойные и безоблачные годы, которые предшествовали Первой мировой войне. В школе Ярдли выделялся среди сверстников своей активностью: он был старостой класса, редактором школьной газеты и капитаном футбольной команды. Будучи посредственным учеником, Ярдли имел явную склонность к математическим дисциплинам. Начиная с 16-летнего возраста, его можно было часто застать в местных игорных салонах у покерных столиков за изучением карточной игры, которая позже стала главной страстью в жизни Ярдли. В детстве он хотел стать юристом по уголовным делам, но вместо этого в 23 года устроился работать шифровальщиком в государственном Департаменте.

Это было счастливым совпадением, поскольку работа шифровальщика идеально подходила для Ярдли. Его романтический ум приходил в трепет от соприкосновения с потоком мировой истории, который ежедневно проходил через его руки в виде посольских депеш. От своих коллег он слышал фантастические рассказы о криптоаналитиках, которые могли проникать в самые сокровенные государственные тайны. И когда однажды вечером президенту Вильсону было передано сообщение из 500 слов от его советника Хауза, Ярдли с присущей ему дерзостью решил попробовать вскрыть используемый для переписки код. Он был поражен, прочитав это сообщение всего за несколько часов.

Достигнутый успех еще более повысил интерес Ярдли к криптоанализу, и он написал 100-страничную записку по поводу вскрытия американских дипломатических кодов. Глубоко поглощенный проблемой возможного вскрытия очередного шифра, он первым поставил диагноз явлению, которое с тех пор известно среди американских криптоаналитиков как «симптом Ярдли»: «Просыпаясь, я сразу начинаю об этом думать. Засыпая, я все равно продолжаю думать об этом».

В апреле 1917 г., вскоре после вступления США в мировую войну, Ярдли сумел убедить военное министерство в необходимости создания дешифровальной спецслужбы. Он добился успеха не только потому, что американской армии были нужны криптоаналитики, но и благодаря исключительному дару убеждать людей в своей правоте. Уже в первые месяцы работы Ярдли на практике продемонстрировал свои выдающиеся криптоаналитические способности. Он настолько хорошо справлялся с порученными обязанностями, что почти сразу же добился для себя значительного повышения жалованья. Неудивительно, что вскоре 28-летний Ярдли получил звание лейтенанта и назначение на должность начальника криптоаналитического отдела разведуправления военного министерства — отдела МИ-8.

В то время отдел МИ-8 только начинал создаваться. Его учебное отделение по подготовке криптоаналитиков возглавил доктор Джон Мэнли. 52-летний филолог, бывший декан факультета английского языка в Чикагском университете, давний и страстный поклонник криптоанализа, Мэнли стал одним из лучших криптоаналитиков МИ-8. Из Чикагского университета Мэнли привел с собой в МИ-8 целую группу докторов философии, членов почетного общества студентов американских колледжей «Фи Бета Каппа». Руководимое им учебное отделение вело обучение криптоанализу в военном колледже армии США. В качестве одного из заданий слушателям учебного отделения предлагалось разработать общие принципы вскрытия кода с перешифровкой, когда кодовая книга известна и требуется определить систему перешифровки.

Отдел МИ-8 быстро разрастался. Одним из первых в нем появилось отделение стеганографии, которое могло читать письма, написанные с использованием более 30 различных систем. Вскоре эксперты-химики этого отделения сумели продемонстрировать свое искусство на практике, обнаружив шпионские послания, которые были написаны невидимыми чернилами, замаскированными под духи с настоящим ароматом.

Позже немцы заменили чернила, имевшие объем и весьма заметную форму жидкости, химическими веществами, которыми пропитывали шарфы, и другие предметы шпионской одежды.

После этого их нужно было только намочить в воде, чтобы получить жидкость для тайнописи, которая была настолько тщательно составлена, что вступала в реакцию только с одним определенным химическим веществом, создавая видимый текст.

В ответ американские химики создали реагент, который выявлял тайнопись с применением любого вида чернил, даже чистой воды. Осторожно нагретые кристаллы йода при возгонке превращались в пары фиолетового оттенка, которые более плотно оседали на волокнах бумаги, нарушенных при любом намокании, и тем самым выявляли, как двигалось перо. Тогда немцы стали писать письма симпатическими чернилами и затем смачивать ими весь лист. Американцы, в свою очередь, начали подвергать полоски бумаги химическим проверкам, которые показывали, была ли поверхность бумаги намочена. Это было почти такой же уликой, как и фактическое обнаружение письма, написанною симпатическими чернилами. Кто, кроме шпиона, станет смачивать письмо специальной жидкостью для тайнописи?

Шедшая с переменным успехом борьба между немецкими и американскими химиками зашла в тупик, когда обе стороны создали универсальный химический реагент, который выявлял симпатические чернила при любых условиях. К тому времени, когда появился этот реагент, отделение тайнописи МИ-8 подвергало проверке 20 тысяч писем в неделю с целью обнаружения невидимых текстов и сумело найти 50 очень важных шпионских посланий. Среди них оказались письма, которые привели к аресту некой Марии Викторики, очаровательной немецкой шпионки, замышлявшей ввезти предназначавшуюся для саботажа взрывчатку в пустотелых статуях Девы Марии и евангельских апостолов!

Отдел МИ-8 также дешифровывал большое количество криптограмм. Он читал дипломатическую шифрпереписку Аргентины, Бразилии, Германии, Испании, Коста-Рики, Кубы, Мексики, Панамы и Чили. Служба американской цензуры присылала в МИ-8 перехваченные шифрованные письма. Большинство из них на поверку оказывались любовными посланиями, в которых применялись очень простые шифры. Хотя многие из них были настолько компрометирующими, что Ярдли часто повторял: «Меня весьма раздражает тот факт, что мужья и жены доверяют свою тайную переписку таким слабым методам шифрования».

Самая важная из разработок МИ-8 привела к осуждению Лотара Витцке — единственного немецкого шпиона, приговоренного в США к смертной казни во время Первой мировой войны. 25 января 1918 г. при обыске в его багаже было обнаружено шифрованное письмо, датированное 15 января. Оно попало в МИ-8 только весной и пробыло там в течение еще нескольких месяцев, пока криптоаналитики безуспешно пытались его дешифровать. В конце концов это письмо удалось прочитать Мэнли, который в результате выяснил, что оно было послано Эккардтом немецкому консулу в Мексике. Открытый текст письма гласил:

«Предъявитель сего является подданным Германской империи, который путешествует под именем Павла Ваберского. Он является немецким секретным агентом. Если он обратится к вам с просьбой, пожалуйста, обеспечьте ему защиту и окажите помощь. Также выдайте ему до тысячи песо золотом и посылайте его шифрованные телеграммы в наше посольство в качестве официальных консульских депеш».

Когда Мэнли зачитал этот текст в зале суда на закрытом процессе по обвинению Витцке в шпионаже, сомнений в его виновности ни у кого не осталось. Шпион был приговорен к смерти через повешение. Однако Вильсон заменил смертный приговор пожизненным заключением. В 1923 г. Витцке был помилован и выпущен на свободу.

В августе 1918 г. Ярдли отплыл на пароходе в Европу, чтобы поучиться криптоанализу у союзников США в Первой мировой войне. Однако Европа встретила Ярдли крайне негостеприимно. Двери комнаты 40 так и остались для него наглухо закрыты, а во Франции его не пустили в криптоаналитическое бюро французского министерства иностранных дел. Только у Холла Ярдли удалось «разжиться» германским военно-морским кодом и дипломатическими кодами некоторых нейтральных государств.

По возвращении из Европы в США Ярдли в полной мере использовал свое уникальное умение убеждать других людей в собственной правоте. В мае 1919 г. он добился от Фрэнка Полка, исполнявшего обязанности государственного секретаря, и от начальника штаба военного министерства согласия на создание «постоянной организации для вскрытия шифров». Эта организация, которая позже стала известна как «Американский черный кабинет», должна была совместно финансироваться двумя министерствами на сумму приблизительно 100 тысяч долларов в год, но ее фактические расходы никогда не достигали этой суммы. По закону платежи госдепартамента, которые начали поступать в июне 1919 г., не могли быть на законных основаниях

израсходованы в пределах Вашингтона, и поэтому Ярдли вместе с подобранным из состава МИ-8 персоналом «Американского черного кабинета» вскоре переехал в Нью-Йорк. Вклад военного министерства в финансирование «Американского черного кабинета» был впервые выплачен лишь 30 июня 1921 г.

Одной из основных задач, поставленных перед «Американским черным кабинетом», было вскрытие кодов Японии, напряженность в отношениях с которой нарастала с каждым днем. В порыве энтузиазма Ярдли пообещал добиться их вскрытия в течение года или в противном случае уйти в отставку. Он пожалел о своей горячности сразу, как только приступил к этому делу, поскольку моментально запутался в открытых текстах на японском языке, не говоря уже о самом шифртексте.

После продолжительного предварительного анализа Ярдли выяснил, что для своих телеграфных сообщений, которые передавались буквами латинского алфавита, японцы использовали несколько видоизмененную форму иероглифической письменности, называемой «катакана». Но, несмотря на самое тщательное изучение перехваченных шифртелеграмм, прочесть их так и не удавалось. Много раз по ночам измученный и потерявший надежду Ярдли поднимался в свою квартиру по лестнице и валился на кровать только для того, чтобы через несколько часов возбужденно вскочить на ноги для проверки новой блестящей идеи, которая снова оказывалась бесплодной.

«К этому времени, — писал он, — я так долго работал с кодированными телеграммами, что каждая их строка, даже каждое кодовое обозначение неизгладимо отпечатались в моей голове. Я мог лежать на кровати с открытыми глазами и заниматься своими исследованиями в кромешной темноте... И вот однажды я проснулся в полночь, так как ушел с работы рано, и откуда-то из темноты пришло убеждение, что определенная последовательность двухбуквенных кодовых обозначений должна абсолютно точно соответствовать слову «Ирландия». Затем передо мной заплясали, быстро сменяясь, другие слова — «независимость», «Германия», «точка»... Великое открытие! Сердце мое замерло, я не смел двинуться с места. Было ли это со мной во сне или наяву? Не сошел ли я с ума? Решение? Наконец-то после всех этих месяцев! Я спрыгнул с кровати и в спешке (поскольку теперь я уже точно знал, что не сплю) почти скатился по лестнице. Дрожащими руками я открыл сейф, схватил папку с бумагами и торопливо начал делать заметки».

В течение часа Ярдли проверял пришедшие ему на ум гипотезы, а затем, убедившись, что начало успешному вскрытию положено, вернулся к себе домой и напился в стельку пьяным. Однако его радость была несколько преждевременной. Ярдли встретился с неожиданными трудностями, пытаясь подыскать переводчика с японского языка. В конце концов он нашел добродушного миссионера, который в феврале 1920 г. сделал для Ярдли первые переводы открытых текстов японских шифртелеграмм. Через 6 месяцев миссионер-переводчик уволился, осознав шпионский характер своей работы. Однако к тому времени один из подчиненных Ярдли совершил поистине неслыханный подвиг, выучив за полгода очень трудный японский язык.

Летом 1921 г. «Американский черный кабинет» прочел японскую шифртелеграмму от 5 июля, направленную в Токио послом Японии в Лондоне и содержавшую первые упоминания о конференции по разоружению, которая должна была состояться в ноябре в Вашингтоне. После этого чтение японской дипломатической шифрпереписки стало настолько регулярным, что за несколько месяцев до открытия конференции были введены ежедневные поездки курьеров между «Американским черным кабинетом» и государственным департаментом. Одно официальное лицо в правительстве США с улыбкой заметило, что руководители государственного департамента относились к работе криптоаналитиков из «Американского черного кабинета» с восхищением и каждое утро читали дешифрованные ими японские криптограммы, попивая при этом апельсиновый сок или кофе.

Вашингтонская конференция по разоружению должна была ограничить тоннаж крупных военных кораблей. По мере того как переговоры приближались к своему главному результату — договору пяти держав, который устанавливал определенное соотношение тоннажа для Англии, Италии, США, Франции и Японии, персонал Ярдли читал все большее количество секретных шифрованных инструкций, которые предназначались для сторон, участвовавших в переговорах. «Американский черный кабинет», глубоко спрятанный за надежными запорами, все видит и все слышит, — писал Ярдли. — Хотя ставни закрыты и окна тщательно зашторены, его зоркие глаза видят, что творится на секретных совещаниях в Вашингтоне, Женеве, Лондоне, Париже, Риме и Токио. Его чуткие уши слышат даже самые слабые шепоты в столицах иностранных государств».

Каждый участник переговорного процесса в Вашингтоне стремился добиться наиболее благоприятного для себя тоннажного соотношения. Самой агрессивной была Япония, которая вынашивала широкомасштабные экспансионистские замыслы в отношении Азии, но боялась вызвать

недовольство своими действиями со стороны США. В самый разгар конференции, когда Япония потребовала установить для себя соотношение 10 к 7 по сравнению с США, «Американский черный кабинет» прочитал японскую шифртелеграмму за 28 ноября, которую Ярдли позднее назвал самой важной из когда-либо дешифрованных им криптограмм.

«Вам надлежит удвоить усилия для достижения поставленных целей в соответствии с проводимой нами политикой, избегая при этом любых столкновений с Америкой по вопросу об ограничении вооружений, — телеграфировало японское министерство иностранных дел своему послу в Вашингтоне. — Вы должны добиться принятия предложения о соотношении тоннажа 10 к 6 с половиной. Если же, несмотря на все ваши усилия, ввиду сложившейся ситуации и в интересах нашей политики, возникнет потребность пойти на уступки, вам необходимо заручиться согласием всех сторон на ограничение права концентрации военно-морских сил и проведения маневров на Тихом океане в обмен на нашу гарантию сохранить там статус-кво. В принятом соглашении вам также следует сделать соответствующую оговорку, из которой было бы совершенно ясно, что именно в этом состоит наше намерение, когда мы принимаем соотношение 10 к 6».

Уменьшение тоннажа военно-морских сил Японии на 0,5 условных единиц, о котором шла речь в этой японской шифртелеграмме, примерно соответствовало двум крупным боевым кораблям. Поскольку представители США на переговорах своевременно получили из «Американского черного кабинета» информацию о том, что в случае нажима японцы согласятся на увеличение тоннажного соотношения между Америкой и Японией, оставалось только оказать этот нажим на практике. Что и сделал государственный секретарь Чарльз Хьюз.

10 декабря Япония капитулировала. В шифртелеграмме, прочитанной «Американским черным кабинетом», японская делегация на переговорах в Вашингтоне получила инструкцию из Токио о том, чтобы «принять соотношение, предложенное Соединенными Штатами». В результате договор, подписанный пятью державами, установил для США и Японии соотношение тоннажа крупных военных кораблей в размере 10 к 6. Японцы надеялись на большее, однако добиться желаемого им помешал «Американский черный кабинет».

За время проведения конференции в «Американском черном кабинете» было прочтено и переведено более 5 тысяч шифрсообщений. Вследствие перенапряжения несколько его сотрудников заболели на нервной почве: один начал что-то бессвязно бормотать, другой стал посвящать все свое свободное время ловле бродячей собаки, у которой на боку якобы был записан японский дипломатический код, а третий, терзаемый каким-то неизъяснимым кошмаром, постоянно носил при себе огромную сумку с камнями, собранными на морском берегу. Все трое были вынуждены уйти с работы. Сам Ярдли также оказался на грани нервного расстройства и в феврале 1922 г. получил четырехмесячный отпуск для поправки своего здоровья.

Кроме состояния здоровья сотрудников, предметом постоянной заботы стало также обеспечение безопасности функционирования «Американского черного кабинета». Его почта направлялась на подставной адрес. Фамилия Ярдли не значилась в телефонном справочнике города Нью-Йорка. Замки на дверях менялись как можно чаще. Тем не менее сведения о деятельности «Американскою черного кабинета», видимо, все же просочились за рубеж, так как была предпринята по крайней мере одна попытка подкупить Ярдли. Когда она провалилась, на служебное помещение «Американского черного кабинета» был совершен налет, после которого из столов пропали важные документы.

Чтобы не допустить новой пропажи, были приняты дополнительные меры безопасности. Теперь каждый листок бумаги запирался на ночь в сейф, чтобы ничего не оставалось в столах, хотя сотрудникам «Американского черного кабинета» все же разрешалось брать домой шифрматериалы, над вскрытием которых они трудились.

Через некоторое время Ярдли вместе со своими подчиненными переехал в другое служебное здание. В качестве надежного прикрытия для них была создана «Компания по составлению кодов». А чтобы «легенда» выглядела правдоподобно, Ярдли составил «Всеобщий торговый код», которым «Компания по составлению кодов» стала торговать вместе с другими распространенными коммерческими кодами.

В 1924 г. ассигнования «Американскому черному кабинету» были резко сокращены. В результате Ярдли пришлось уволить половину персонала, и штат сотрудников «Американского черного кабинета» сократился примерно до дюжины человек. Однако, несмотря на это, по словам Ярдли, «в 1917-1924 гг. «Американскому черному кабинету» удалось прочесть более 45 тысяч шифртелеграмм Англии, Аргентины, Бразилии, Германии, Доминиканской Республики, Испании, Китая, Коста-Рики, Кубы, Либерии, Мексики, Никарагуа, Панамы, Перу, Сальвадора, Советского Союза, Франции, Чили и Японии, а также проделать предварительный анализ многих других кодов, включая коды

Ватикана».

В 1929 г. плодотворной деятельности «Американского черного кабинета» неожиданно пришел конец. Дело в том, что Ярдли получал тексты иностранных шифртелеграмм от американских телеграфных компаний, которые передавали ему их с большой неохотой. Когда на пост президента США вступил Герберт Гувер, Ярдли решил урегулировать вопрос о шифрперехвате с новым правительством раз и навсегда. Он задумал составить «памятную записку для доклада прямо президенту с изложением характера деятельности «Американского черного кабинета», а также необходимых шагов, которые должны быть предприняты, если правительство США пожелает полностью использовать искусное мастерство своих криптоаналитиков». Прежде чем передать записку президенту, Ярдли выждал некоторое время, чтобы выяснить, в каком направлении дует ветер, и обнаружил, что этот ветер был отнюдь не попутным. По высокопарным морализаторским сентенциям первого публичного выступления Гувера в качестве президента Ярдли понял, что «Американский черный кабинет» обречен. И оказался прав.

После того как Генри Стимсон, государственный секретарь при Гувере, пробыл на своем посту несколько месяцев, что, как считал Ярдли, было необходимо для приобретения некоторого опыта практической дипломатии, «Американский черный кабинет» направил ему серию важных дешифрованных криптограмм. Однако, в отличие от прежних государственных секретарей, на которых эта тактика всегда оказывала должное воздействие, узнав о существовании «Американского черного кабинета», Стимсон пришел в негодование и сурово осудил его деятельность. Он обозвал ее подлой разновидностью шпионского ремесла и расценил как вероломное нарушение принципа взаимного доверия, которого неуклонно придерживался в своих личных делах и в своей внешней политике.

Все сказанное Стимсоном было совершенно справедливо, если отвергнуть точку зрения, в соответствии с которой любые средства оправданы, если служат интересам родины. Совершив акт морального мужества и прекратив всякую финансовую поддержку «Американского черного кабинета» со стороны государственного департамента, Стимсон тем самым утвердил главенство принципа над необходимостью*.

* Когда в 1940 г Стимсон стал военным министром он коренным образом пересмотрел свое мнение относительно чтения иностранной шифрпереписки. Оценивая этот факт, следует принять во внимание, что десятилетием ранее международная обстановка была совершенно иной. После окончания Второй мировой войны Стимсон, объясняя свой поступок, написал о себе в третьем лице: «В 1929 г. весь мир руководствовался доброй волей, стремлением к прочному миру, и в этом усилии все государства были партнерами. Стимсон, будучи государственным секретарем, вел себя как джентльмен с джентльменами, присланными дружественными государствами в качестве послов и посланников. А джентльмены не читают шифрпереписку друг друга... В 1940 г. Европа была объята войной, а США находились накануне вступления в войну»

Так как деньги, выделяемые госдепартаментом, составляли главный доход «Американского черного кабинета», это означало его неизбежное закрытие. Неистраченные 6666 долларов и 66 центов, а также все архивы «Американского черною кабинета» были переданы армейской службе связи. Его сотрудники быстро разбрелись кто куда (служить в армию никто из них не пошел), и 31 октября 1929 г. «Американский черный кабинет» перестал существовать. Десять лет его дешифровальной работы обошлись американской казне в 300 тысяч долларов, при этом государственный департамент предоставил две трети этой суммы, а военное министерство — одну треть.

Ярдли не смог подыскать себе подходящей работы и вернулся домой в родной Уортингтон. Наступившая депрессия лишила его последних сбережений: в августе 1930 г. Ярдли пришлось за бесценок продать все, что он имел. Несколько месяцев спустя Ярдли пришла в голову мысль написать книгу об «Американском черном кабинете» и заработать на этом немного денег, чтобы прокормить жену и сына. И когда в конце января 1931 г. его старый приятель по МИ-8 Мэнли, с которым он продолжал поддерживать дружеские отношения, отказался дать ему взаймы 3 тысячи долларов, Ярдли, отчаявшись изыскать другие средства к существованию, приступил к написанию книги. Весной 1931 г. он рассказал об этом в письме к Мэнли:

«Я так долго не занимался никакой настоящей работой, что попросил Бая* и Костэйна** помочь мне в создании книги. Я показал им несколько отрывков, и они оба посоветовали мне проделать всю работу самому. Целыми днями я беспомощно сидел за пишущей машинкой. Потом я кое-как

сдвинулся с места и постепенно, подбадриваемый Баем, уверовал в себя. Издательство «Боббс-Меррилл» выдало мне аванс в тысячу долларов. Затем последовала просьба ускорить написание книги. Я начал работать по сменам: несколько часов писал, несколько часов спал. Выходил я из своей комнаты только для того, чтобы купить немного яиц, хлеба, кофе и несколько банок с томатным соком. Боже, ну и писал же я! Иногда я успевал написать всего лишь тысячу слов, но чаще — до 10 тысяч в день. Новые главы я относил Баю, который читал их и излагал мне свои критические замечания. Как бы там ни было, я закончил книгу и подготовил ее отдельные части для публикации в качестве статей. Все это было сделано за 7 недель».

* Бай — литературный агент Ярдли.
** Костэйн — один из редакторов нью-йоркской газеты «Сатердей ивнинг пост».

1 июня 1931 г. американское издательство «Боббс-Меррилл компани» опубликовало книгу Ярдли «Американский черный кабинет» объемом в 375 страниц. К этому времени отрывки из нее уже успели появиться в виде трех статей, напечатанных с двухнедельными интервалами в «Сатердей ивнинг пост», ведущем печатном издании того времени.

Ярдли всегда был превосходным рассказчиком. Дар красноречия не изменил ему и при написании книги. Благодаря динамичному и интригующему стилю «Американский черный кабинет» сразу же завоевал успех и немедленно был признан классической книгой по истории криптоанализа. Оценки критиков были положительными. Один из них, выступая с хвалебным отзывом, так суммировал преобладающее мнение: «Я считаю, что эта книга является наиболее сенсационным вкладом, когда-либо внесенным американцем в секретную историю мировой войны и первых лет послевоенного периода. Содержащиеся в ней преднамеренно неосторожные высказывания превосходят все, что можно найти в недавних мемуарах европейских тайных агентов».

Газетчики поспешили забросать правительственные органы запросами о том, происходило ли описанное в книге Ярдли на самом деле. Государственный департамент, мастерски продемонстрировав искусство дипломатических уверток, ответил, что «не склонен верить» утверждениям Ярдли. А официальные лица военного министерства пошли на прямую ложь, заявив, что никакого «Американского черного кабинета» никогда не существовало.

Суждения бывших коллег Ярдли по поводу его книги сильно разнились. Мэнли, который сначала предупреждал Ярдли, что «вы можете подвергнуться очень серьезной критике, если раскроете тот факт, что вы читали официальные иностранные шифрсообщения», после появления статей в «Сатердей ивнинг пост» сказал ему: «Я одобряю эти статьи и думаю, что они хорошо написаны». Мэнли добавил, что сам не стал бы публично говорить о каких-либо дешифровальных успехах, связанных с дружественными государствами, но считает, что основным мотивом Ярдли было заставить правительство воссоздать полноценную криптоаналитическую спецслужбу.

Однако мнение Мэнли разделяли далеко не все американские криптоаналитики. Некоторые из них критически сравнивали поступок Ярдли с нарушением профессиональной этики адвокатом, раскрывшим конфиденциальные сведения о своем клиенте. Другие предупреждали, что колоссальный ущерб, который Ярдли причинил своей стране, станет полностью очевидным только по прошествии многих лет. Некоторый вред, нанесенный книгой Ярдли, стал ощущаться почти немедленно: один армейский криптоаналитик позже вспоминал, что ее опубликование сразу же доставило ему и его коллегам значительные дополнительные заботы.

Сам Ярдли был несколько ошеломлен той бурей, которую вызвала публикация его книги. Он откровенно признался Мэнли, что «если бы я несколько не драматизировал и книгу, и статьи, то читатель бы просто заснул», поскольку, «чтобы написать ходкую вещицу, неизбежно приходится драматизировать». Но когда Ярдли понял, что ему удалось добиться успеха у читателей, он занял несколько другую позицию, опасаясь вызвать снижение читательскою интереса к книге своими публичными признаниями в том, что изложенные в ней события сильно «драматизированы», то есть — вымышлены.

«Разве не очевидно, — спрашивал Ярдли риторически в своем письме редактору «Нью-Йорк ивнинг пост», — что если практика чтения шифрсообщений других государств должна быть исключена по соображениям дипломатии, то в качестве первого шага к такому исключению должно состояться публичное обсуждение сложившегося положения? Мне представляется, что моя книга сможет оказать действительную услугу обществу благодаря тому, что она, по крайней мере, указывает на существующие условия...»

Ярдли развернул контрнаступление на своих критиков в статье в американском журнале

«Либерти», озаглавленной «Выдаем ли мы наши государственные секреты?». В ней Ярдли обвинил государственный департамент в вопиющей халатности в шифровальном деле, поскольку там пользовались «кодами XVI века». Ярдли также заявил, что к его книге следует относиться не как к «какой-то фантастической истории», а как к публичному разоблачению отставания Соединенных Штатов в области шифрования.

В США «Американский черный кабинет» разошелся в количестве 18 тысяч экземпляров. Еще 5 тысяч были проданы в Англии. Но настоящий фурор книга Ярдли произвела в Японии. Тамошнему министерству иностранных дел пришлось признать, что чтение японских дипломатических шифртелеграмм, о котором говорилось в книге, «объяснялось тем, что правительство не произвело своевременную замену шифров». Министерство иностранных дел Японии также заявило, что еще в 1921 г., во время проведения Вашингтонской конференции, Ярдли «посетил наше посольство в Вашингтоне и сообщил, что все японские шифрованные телеграммы прочитаны, а затем предложил продать их переводы».

В свою очередь, военно-морское ведомство Японии выразило удивление, что подобная книга могла быть опубликована «даже в США», и заверило, что «делает все возможное для сохранения своих радиограмм в секрете». Воспользовавшись случаем, военные моряки покритиковали министерство иностранных дел за «серьезный промах», выразившийся в том, что дипломатические шифры не были сменены перед Вашингтонской конференцией, и пообещали оказывать ему помощь в виде консультаций.

Японские газеты одна за другой поведали о сенсации, которую откровения Ярдли произвели в правительственных кругах Японии. При этом сообщалось, что военное и военно-морское ведомства дали задание своим атташе в Вашингтоне купить по нескольку экземпляров книги Ярдли. От имени военных было распространено заявление о том, что они «полны решимости принять участие в приближающейся Женевской конференции по ограничению вооружений с соблюдением всех возможных предосторожностей»

Две японские газеты, выходившие на английском языке, в своих редакционных статьях выразили диаметрально противоположные мнения в отношении разоблачений, сделанных Ярдли. Одна написала в Духе Стимсона: «Это очень похоже на распечатывание писем других людей — вещь, которую не принято делать». Другая холодно заметила, что «попытки вскрыть код другого государства являются частью игры», и поэтому остается только «критиковать наше министерство иностранных дел, а не ругать американцев за то, что в этой игре они выиграли очко у японской команды».

Интерес к книге Ярдли не ослабевал еще очень долго. 5 ноября 1931 г., в ответ на просьбу государственного департамента как можно полнее проинформировать его о реакции на «Американский черный кабинет», посол США в Японии Камерон Форбес сообщил в Вашингтон: «Эта книга произвела в Японии огромное впечатление. Я часто слышу упоминания о ней в беседах с представителями различных кругов. По словам издателей, в Японии уже продано более 40 тысяч ее экземпляров. Она остается бестселлером и в настоящее время».

Поэтому, когда Стэнли Хорнбек, эксперт по дальневосточным делам в государственном департаменте, узнал о том, что Ярдли написал новую книгу, в которой цитировались открытые тексты японских дипломатических шифртелеграмм, посланных в ходе проведения Вашингтонской конференции по разоружению, он написал в своей докладной записке от 12 сентября 1932 г.: «Учитывая возбужденное состояние, в котором пребывает сейчас японское общественное мнение и которое характеризуется опасениями или враждебностью в отношении Соединенных Штатов, я решительно настаиваю, чтобы были предприняты все возможные усилия с целью не допустить появления этой книги. Ее публикация значительно увеличит силу взрыва, который назревает в Японии».

20 февраля 1933 г. судебные исполнители конфисковали рукопись новой книги Ярдли в издательстве «Макмиллан», куда Ярдли отдал ее после того, как издательская компания «Боббс-Меррилл» наотрез отказалась ее печатать. Однако никакого уголовного дела не было возбуждено ни против «Макмиллан», ни против Ярдли. Вместо этого правительство США попыталось добиться принятия закона, направленного против таких, как Ярдли.

«Любое лицо, находящееся на правительственной службе, — говорилось в законопроекте «Об обеспечении защиты правительственных документов», предложенном государственным департаментом для рассмотрения в конгрессе, — и получившее от другого лица, или имеющее в своем распоряжении, или имевшее в прошлом доступ к любому официальному дипломатическому коду или к любому документу, подготовленному по такому коду или якобы подготовленному по

такому коду, и без разрешения или полномочий полностью опубликовавшее или предоставившее другому лицу любой подобный код, или документ, или любой документ, который был получен в процессе пересылки между каким-либо иностранным правительством и его дипломатическим представительством в Соединенных Штатах Америки, должно подвергаться штрафу в размере не более 10 тысяч долларов, или тюремному заключению на срок не более 10 лет, или и тому и другому, вместе взятым».

10 мая 1933 г. в сенате прошли дебаты по этому законопроекту. В ходе дебатов сенатор Ки Питтмэн, выдвинувший его в сенате от имени правительства, в частности, заявил: «По моему мнению, неприлично, чтобы государственные служащие публиковали секретную корреспонденцию, доступ к которой они получают в силу своего служебного положения. Ничего более этой мерой не предусматривается». Однако демократ Гомер Боун ехидно спросил: «Мне очень бы хотелось узнать, как же это нам удавалось так долго обходиться без закона подобного рода, начиная с конгресса 1-го созыва и вплоть до нынешнего конгресса 73-го созыва?» На это Питтмэн ответил: «Должен заявить, что в прошлом нашему правительству, очевидно, очень повезло в том, что оно доверяло крайне конфиденциальные должности честным, порядочным людям. Однако недавно у него появились веские основания подозревать, что его доверием злоупотребили и могут злоупотребить снова».

Затем слово взял сенатор Джонсон, который выступил с нападками на законопроект, усматривая в нем угрозу свободе личности:

«Внешне он выглядит так же обычно, как свадьба, и так же респектабельно, как похороны... Но этот законопроект бьет мимо цели, которая перед ним была поставлена, когда его вносили на наше рассмотрение... Случилось так, что в один прекрасный день джентльмены из государственного департамента примчались сюда и заявили, что для того, чтобы у наших дверей не загрохотали пушки, необходимо тотчас же принять законопроект «Об обеспечении защиты правительственных документов»... Все это происходило полтора месяца тому назад. С тех самых пор законопроект все еще ожидает утверждения, но никто не слышал о том, чтобы случились те страшные и ужасные вещи, которые, как утверждали, должны были случиться, если этот законопроект не станет тотчас же законом. Таким образом, причин для принятия этого законопроекта, которого вначале так яростно добивались, сейчас не существует и, если спокойно проанализировать прошлое, их никогда не существовало».

Затем Джонсон упомянул о Ярдли и его книге, которую он прочитал и нашел «более или менее интересной». Джонсон покритиковал Ярдли за то, что тот нарушил «неписаные правила, регулирующие доверительные отношения», и сообщил, что Ярдли написал еще одну книгу, содержащую открытые тексты дипломатических шифрсообщений, связанных с Вашингтонской конференцией по разоружению. Далее Джонсон сказал:

«Вот тут-то и возникла та самая настоятельная «необходимость». Рукопись этой книги, насколько мне известно, была конфискована, и после ее конфискации в залы конгресса прибежали эти испуганные джентльмены из государственного департамента и заявили, что возникла настолько деликатная, опасная и неотложная ситуация, что нужен-де новый закон об уголовной ответственности... Так родился этот законопроект... Здесь мы имеем дело с законопроектом, который нацелен на одно конкретное дело. Он составлен крайне неудачно и никогда не будет применен в этом деле. Он будет оставаться в сводах законов до тех пор, пока в отдаленном будущем, когда все уже забудут о его первоначальной цели, он не будет использован для другой цели, для которой он никогда не предназначался, и причинит много зла. Так всегда случалось с законами подобного рода, принятыми для того, чтобы осудить какое-либо конкретное, уже совершенное нарушение».

Джонсону возразил еще один защитник интересов правительства при рассмотрении законопроекта «Об обеспечении зашиты правительственных документов» — сенатор Том Коннэли:

«Покажите мне сенатора, который одобрял бы хищение секретных сведений! Если есть таковой, пусть он встанет. Сенаторы, которые приходят в ярость, если человек украдет теленка, и стремятся надолго посадить его в тюрьму, по-видимому, допускают мысль, что другой человек может торговать секретными сведениями или документами, являющимися государственным достоянием, продавать их за деньги газетам и что это будет патриотическим актом и услугой государству. Я не разделяю такой точки зрения... Принимая законопроект, мы пресекаем безнаказанное воровство и безответственный обман доверия. Вот что мы пресекаем. Тем самым мы сможем положить конец цепи предательств, совершаемых в отношении правительства, вот и все».

Мнение Коннэли, подкрепленное политическим влиянием правительства, возобладало: поименным голосованием законопроект «Об обеспечении зашиты правительственных документов» был принят. 10 июня 1933 г., после подписания президентом Франклином Рузвельтом, он стал

государственным законом США.

А через четыре дня после этого «Боббс-Меррилл компани» направила в государственный департамент просьбу одобрить выполнение контракта, заключенного ею в 1931 г. с фирмой «Блю Риббон букс» о переиздании книги Ярдли «Американский черный кабинет» тиражом 15 тысяч экземпляров. В этой просьбе также сообщалось, что «Боббс-Меррилл компани» понесет большие финансовые убытки, если ей придется расторгнуть свой контракт с «Блю Риббон букс», не получив никаких доходов от продажи книги. Тем самым «Боббс-Меррилл компани» попыталась добиться от государственного департамента разрешения переиздать «Американский черный кабинет», которое позволило бы ей оградить себя от возможного юридического преследования со стороны министерства юстиции в связи с принятием нового закона.

14 июля Уильям Филлипс*, исполняющий обязанности государственного секретаря, дал следующий ответ на обращение «Боббс-Меррилл компани»: «Предоставление государственным департаментом разрешения на переиздание книги означало бы, что он не имеет возражений против ее публикации и распространения, и связало бы его с действиями автора и издателя, к которым государственный департамент никогда не относился с одобрением. Поэтому государственный департамент не может дать такого разрешения. Однако он не хочет усугублять финансовых убытков «Боббс-Меррилл компани» и поэтому не будет препятствовать продаже или распространению 4,5 тысячи экземпляров, уже напечатанных «Блю Риббон букс».

* По иронии судьбы именно Филлипс в 1917 г лично разрешил Ярдли уволиться из государственного департамента, чтобы организовать МИ-8.

Этот отказ государственного департамента разрешить переиздание «Американского черного кабинета» породил легенду о том, что книга Ярдли была запрещена. На самом же деле никаких действий в отношении огромного количества ее экземпляров, которые уже вышли из печати, предпринято не было.

Несмотря на всю эту суматоху, Ярдли оставался абсолютно спокойным. Он воспользовался возможностью, предоставленной ему сенатором из его родного штата, чтобы высказать свои доводы в отношении публикации «Американского черного кабинета»: «Я надеялся, что моя книга заставит государственный департамент пересмотреть свои собственные кодовые системы и поможет сделать американские дипломатические шифртелеграммы неуязвимыми для иностранных криптоаналитиков». Однако от дальнейшего участия в полемике вокруг книги Ярдли отказался, сказав, что слишком занят процессом создания новых невидимых суперчернил, чтобы интересоваться всякими законодательными мелочами. Вскоре суперчернила были созданы, но коммерческого успеха не принесли, а Ярдли потерял средний палец на правой руке из-за вызванного ими заражения.

Тогда Ярдли снова попробовал обратиться к писательскому ремеслу. Однако для работы его воображения требовались факты. Приключенческим романам «Красное солнце Японии» и «Белокурая графиня», написанным Ярдли, недоставало той интригующей увлекательности, которой отличался его основанный на фактическом материале «Американский черный кабинет». Тем не менее кинокомпания «Метро Голдвин Майер» сочла, что прелестная шпионка, секретные коды и проницательный криптоаналитик из «Белокурой графини» очень подходят для создания фильма. Трудность заключалась в том, что никакой храбрый киногерой не согласился бы на такую скучную канцелярскую работу, как вскрытие шифров. Кинокомпания справилась с этой трудностью, изменив сюжет романа Ярдли и сделав героем кабинетного ученого, который во что бы то ни стало желает отправиться воевать за океан. «Метро Голдвин Майер» заключила с Ярдли выгодный для него контракт, наняв в качестве технического советника. В результате был создан художественный фильм «Рандеву», премьера которого состоялась 25 октября 1935 г. в Нью-Йорке.

В 1938 г после неудачной попытки заняться торговлей недвижимостью Ярдли поступил на службу к китайскому диктатору Чан Кайши с окладом примерно 10 тысяч долларов в год, чтобы заниматься дешифрованием японских криптограмм. В 1940 г. Ярдли вернулся из Китая, чтобы отправиться в Канаду. Там он организовал дешифровальное бюро. Из Канады Ярдли вскоре выслали обратно в США, где в 1958 г. он умер от сердечного приступа.

В некрологах Ярдли присвоили титул «отца американского криптоанализа», что лишний раз продемонстрировало то глубокое впечатление, которое книга Ярдли произвела на сознание его сограждан. Несмотря на все ее недостатки, она прочно овладела воображением широкой публики и пробудила интерес к дешифрованию у многих талантливых людей. Их свежие идеи обогатили американский криптоанализ, и несомненная заслуга в этом принадлежит именно Ярдли.

ФРИДМАН

Хотя Ярдли является наиболее известным американским криптоаналитиком, самым великим, бесспорно, продолжает оставаться Уильям Фридман. Трудно вообразить себе двух более не похожих друг на друга специалистов в одной и той же области. В то время как Ярдли был человеком экспансивным, общительным, поверхностным, свободно обращающимся с деталями и готовым не упустить свой главный шанс, Фридман был склонен к сосредоточенности, глубине изучения, преданности, аккуратности и утонченности. Несмотря на относительную обыденность этих личных черт, а может быть, именно благодаря им теоретический вклад Фридмана и его практические достижения намного превосходят результаты работы любого другого американского криптоаналитика. Служебная биография Ярдли больше всего напоминает короткий полет удивительной ракеты, которая, взорвавшись, превращается в фантастические гирлянды, озаряющие небо. Карьеру же Фридмана скорее можно уподобить неторопливому движению солнца по небосклону.

Фридман родился 24 сентября 1891 г. в русском городе Кишиневе. При рождении ему было дано имя Вольф. Он был старшим сыном в семье Фредерика и Розы Фридман. Его отец, румын по национальности, говоривший на восьми языках и работавший переводчиком в почтовом ведомстве, эмигрировал в Америку в 1892 г. По прибытии на Американский континент Вольф был переименован в Уильяма. Семья Фридман поселилась в Питтсбурге, где в 1909 г. Уильям окончил среднюю школу и нашел работу в фирме, которая продавала паровые машины.

Осенью 1910 г. Фридман поступил в Мичиганский сельскохозяйственный колледж, главная привлекательная сторона которого заключалась в том, что обучение там было бесплатным. Однако довольно скоро Фридман обнаружил, что сельское хозяйство его мало интересует. В конце семестра он узнал, что бесплатное обучение ведется также на факультете генетики Корнельского университета в городе Итаке в штате Нью-Йорк. В феврале 1911 г. Фридман занял немного денег и переехал в Итаку. В феврале 1914 г. он окончил университет и поступил в аспирантуру.

Как раз во время пребывания Фридмана в Итаке богатый торговец текстильными товарами Джордж Фабиан, который содержал лаборатории по акустике, химии, генетике и криптоанализу (Фабиан пытался доказать, что это Фрэнсис Бэкон* написал пьесы Вильяма Шекспира, и искал в них криптограммы, свидетельствующие в пользу авторства Бэкона) в своем поместье Ривербэнк около г. Женева в штате Иллинойс, решил, что ему нужен специалист по генетике, чтобы улучшить сорта зерновых культур и породы скота на своей ферме. Фабиан обратился в Корнельский университет с просьбой порекомендовать ему творчески мыслящего специалиста. Оттуда Фабиану прислали Фридмана, который приступил к работе в Ривербэнкских лабораториях с 1 июня 1915 г.

* Бэкон Фрэнсис — английский философ XVI-XVII вв. Его теория познания, отводившая главную роль эксперименту, оказала большое влияние на развитие науки.

Фабиан был умным и энергичным человеком. Он страстно желал прославить свое имя в науке. Сам Фабиан читал мало, но от работавших на него образованных и талантливых людей он вобрал в себя достаточное количество различных сведений, чтобы его суждение почти по каждому вопросу производило впечатление на окружающих. Он был властолюбив и никогда не позволял своим подчиненным противоречить себе. Главный принцип, в который Фабиан глубоко верил, заключался в том, что с помощью хорошо организованной рекламной кампании можно добиться почти всего.

Фридман выполнял для Фабиана кое-какую исследовательскую работу в области генетики. Кроме того, поскольку Фридман был хорошим фотографом, он помогал криптоаналитикам, искавшим зашифрованные подписи Бэкона в работах Шекспира и делавшим увеличенные фотокопии с печатных текстов елизаветинских времен, которые использовались в этих поисках. Криптоаналитический отдел Ривербэнкских лабораторий Фабиана состоял из полутора десятка выпускников средних школ и колледжей. Они в основном занимались тем, что рассортировывали отдельные буквы шекспировских текстов времен английской королевы Елизаветы по типам типографских шрифтов. Фабиан содержал их на всем готовом и платил им жалованье в размере около 50 долларов в месяц.

Среди них была молодая сотрудница Элизабет Смит. Она родилась 26 августа 1892 г. в городе Хантингтоне в штате Инчиана и была самой младшей из девяти детей Джона Смита, торговца молочными продуктами, и его жены Сары. Закончив среднюю школу в Хантингтоне, а затем —

колледж, она поступила на работу в одну из чикагских библиотек, где в 1916 г. была нанята на службу Фабианом.

Ни она, ни Фридман до этого особенно не интересовались криптоанализом. Однако в ривербэнкских коттеджах они часто слышали красочные рассказы о здоровом образе жизни в елизаветинские времена, о не такой уж безгрешной английской королеве, об интригах придворных, а также разные байки, связанные с великими людьми в истории Англии. Фридман и Смит также узнали о «дешифровках» пьес Шекспира, которые якобы доказывали, что их написал Бэкон. Эти рассказы пробудили у Фридмана живой интерес. Понемногу он начал заниматься криптоанализом, всемогущие чары которого, подобно дурману, неодолимо завладели умом Фридмана. «Когда дело доходило до криптоанализа, — вспоминал он много лет спустя, — что-то во мне получало отдушину».

Сказано слишком мягко. Страстное увлечение криптоанализом не прошло незамеченным для босса, и вскоре Фабиан доверил Фридману руководство криптоаналитической лабораторией в Ривербэнке. Страсть к криптоанализу усиливалась влечением, которое он стал испытывать к одной из своих подчиненных — остроумной и веселой мисс Смит. В мае 1917 г. они поженились, став самой знаменитой супружеской парой в истории криптоанализа.

За месяц до этого Соединенные Штаты объявили войну Германии, и Ривербэнк, который имел единственную действующую криптоаналитическую организацию в стране, начал неофициально получать криптограммы для дешифрования от различных правительственных учреждений. Самой важной из них была шифрованная корреспонденция группы заговорщиков-индусов, которые не без помощи немцев попытались воспользоваться тем, что Англия была поглощена войной в Европе, и добиться независимости для Индии. Перехваченные шифртелеграммы индусов в Берлин передавались для дешифрования Фридману, который быстро вскрыл применяемый ими шифр.

Индусы были осуждены за попытку закупить в Соединенных Штатах оружие для организации восстания против Англии. В ходе массовых процессов в Чикаго и Сан-Франциско Фридман выступил с показаниями, которые по сути дела выглядели как изобличение заговорщиков из их же собственных уст. На процессе в Сан-Франциско произошла одна из самых драматичных сцен, которые когда-либо разыгрывались в американских судах: один из подсудимых индусов встал и двумя выстрелами из револьвера убил соотечественника, дававшего свидетельские показания против своих соратников, а затем был убит полицейским, выстрелившим поверх голов людей из публики. Суд признал большинство обвиняемых виновными.

Несколько месяцев спустя после прочтения шифрованной переписки индусов англичане направили в Ривербэнк 5 коротких криптограмм. Они были получены с помощью шифровального устройства, изобретенного сотрудником криптоаналитического бюро военного министерства Англии Дж. Плеттсом. Англичане настолько высоко оценивали эту машину, что один из аргументов, выдвигавшихся против ее использования, заключался в том, что если бы немцы захватили один ее экземпляр и стали бы использовать ее у себя, то союзники больше не смогли бы читать шифрсообщения противника! Однако Фридман моментально вскрыл ключ «CIPHER»* к одной из присланных из-за океана криптограмм. Но он никак не мог получить другой ключ и, зайдя в тупик, прибег к небольшому опыту в области «психологического криптоанализа». Уильям обратился к недавно нареченной г-же Фридман и попросил ее отвлечься от всяких мыслей. «Теперь, — продолжал он, — я хочу, чтобы ты произнесла первое попавшееся слово, которое придет тебе на ум, когда я назову тебе другое слово». Он выждал паузу. «Шифр», — сказал он. «Машина», — ответила она.

* «ШИФР»

Слово «MACHINE»* оказалось вторым искомым ключом. Через три часа после того, как Фридман получил криптограммы для криптоанализа, их открытые тексты были телеграфированы в Лондон. Первый из них содержал весьма лестную для гордого английского изобретателя фразу: «Этот шифр абсолютно невскрываем». Больше к рассмотрению вопроса об использовании устройства шифрования Плеттса союзники не возвращались.

* «МАШИНА»

Помимо криптоаналитической работы Фридман занимался преподавательской деятельностью в классе, который состоял из армейских офицеров, присланных осенью 1917 г. в Ривербэнк для изучения криптоанализа. Для преподавания на этих курсах Фридман подготовил серию монографий.

Известные как «Ривербэнкские публикации», они явились поворотным пунктом в истории криптоанализа. Почти во всех из них излагался новый материал, овладение которым до сих пор считается необходимым условием получения высшего криптоаналитического образования.

Фабиан попытался косвенно присвоить себе заслугу выхода в свет этих монографий, убрав фамилию Фридмана с их титульных листов и сохранив за собой авторское право на их издание. Вскоре полный комплект «Ривербэнкских публикаций» превратился в необходимый атрибут хорошей коллекции работ по криптоанализу, но, так как было напечатано всею лишь 400 экземпляров, они стали крайней редкостью. Один страстный любитель расценил их настолько высоко, что старательно перепечатал на машинке, а некоторые коллекционеры, отчаявшись заполучить оригиналы, покупали фотокопии этих брошюр.

Самой известной среди «Ривербэнкских публикаций» стала написанная в 1920 г. брошюра под названием «Индекс совпадения и его применение в криптоанализе». В ней описывался процесс вскрытия двух сложных шифров. Однако Фридман менее всего был заинтересован в доказательстве уязвимости этих шифров и использовал их в основном для разработки новых криптоаналитических методов.

Таких методов Фридман создал два. Один из них позволил восстанавливать шифралфавит, не строя никаких догадок в отношении хотя бы единственной буквы открытого текста. Другой его метод совершил настоящую революцию в криптоанализе. Фридман подошел к тексту на любом языке не просто как к совокупности отдельных символов, которые случайно стоят в определенном порядке, а как к единому целому — кривой, точки которой закономерно связаны. К этой кривой он применил статистические концепции. Полученные Фридманом результаты можно охарактеризовать как прометеевские. Его гениальная идея дала толчок к использованию многочисленных статистических инструментов, которые являются крайне необходимыми в современном криптоанализе.

До Фридмана криптоанализ существовал как чистая наука, ничего не заимствующая из других областей знания и ничем их не обогащающая. Подсчеты частот встречаемости букв, использование языковых характеристик, специфические методы вскрытия шифров — все это было характерным только для криптоанализа. Фридман вывел криптоанализ из этого состояния одинокого существования и соединил со статистикой. Когда Фридман отнес криптоанализ к категории статистических исследований, он широко распахнул дверь в арсенал средств, которыми криптоанализ никогда прежде не располагал. Они идеально подходили для изучения статистического поведения букв и слов. Криптоаналитики с готовностью воспользовались этими средствами и с тех пор с успехом применяют их на практике.

Вот почему, оглядываясь на пройденный жизненный путь, Фридман сказал, что «Индекс совпадения» является его самым важным творением. Даже одна эта работа принесла бы ему славу. Но фактически это было только началом его деятельности на поприще криптоанализа.

Фридман и его супруга покинули Ривербэнк в конце 1920 г. Обстановка там стала невыносимой. Фабиан увеличил Фридману жалованье, пообещав предоставить абсолютную свободу при доказательстве или опровержении существования шифров в произведениях Шекспира. Но на деле Фабиан безжалостно подавлял любую попытку ведения самостоятельных разработок в этом направлении и принудил Фридмана молчаливо согласиться с выводами, противоречившими взглядам Фридмана. 1 января 1921 г. Фридман заключил 6-месячный контракт с войсками связи на разработку шифрсистем. Когда этот контракт истек, он был взят на должность гражданского служащего в военное министерство.

Одним из первых служебных заданий Фридмана стало преподавание в школе войск связи. Для этой цели он написал учебник, в котором ликвидировал неразбериху, царившую в криптологической терминологии. Самым важным терминологическим вкладом Фридмана было понятие «криптоанализ», которое он ввел в 1920 г., чтобы устранить хронический источник путаницы в криптологии — двусмысленность глагола «расшифровать», означавшего тогда любое преобразование криптограммы в открытый текст. Фридман озаглавил свою книгу «Элементы криптоанализа», и этот термин настолько привился, что сегодня он применяется и в разговорной речи, и в научной литературе.

В начале 1922 г. Фридман стал главным криптографом войск связи, возглавив отделение кодов и шифров отдела научных исследований при штабе командующего войсками связи. Так как криптоаналитическую работу для военного министерства выполнял «Американский черный кабинет» Ярдли, номинально Фридман занимался исключительно криптографией. Однако, как это ни парадоксально, много внимания ему приходилось уделять и криптоанализу. Фридман постоянно испытывал новые системы шифрования, которые ревностные любители предлагали армии в качестве

«абсолютно невскрываемых».

Горизонты деятельности Фридмана постоянно расширялись. В 1924 г. он выступил в комиссии конгресса с показаниями в отношении прочтения им некоторых шифрованных сообщений, связанных с уголовным делом о махинациях с нефтеносными участками. Когда же через несколько месяцев планета Марс очень близко подошла к Земле, Фридмана захватило общее экзальтированное настроение шумных 20-х годов, и он всерьез начал готовиться к дешифрованию любых посланий, которые марсиане могли бы отправить землянам, пользуясь своей временной близостью к ним. Он вернулся к земным проблемам в 1927 г., когда написал статью о кодах и шифрах для «Британской энциклопедии».

Незадолго до того, как государственный департамент прекратил финансирование «Американского черного кабинета», военное министерство решило объединить шифровальную и дешифровальную службы в рамках войск связи. Приказом военного министра от 10 мая 1929 г. ответственность за криптографическую и криптоаналитическую деятельность в армии была возложена на начальника войск связи. Чтобы лучше выполнять эти новые обязанности, командование войск связи создало дешифровальную службу в составе штабного управления по военному планированию и подготовке. Фридман был назначен начальником этой службы.

Как было официально изложено, обязанности Фридмана заключались в составлении армейских кодов и шифров, а также в перехвате и дешифровании сообщений противника во время войны. В мирное время Фридман должен был заниматься обучением квалифицированных кадров и проведением научно-исследовательских работ, необходимых для того, чтобы немедленно приступить к оперативной работе в случае начала войны. Для выполнения этих обязанностей Фридман нанял трех криптоаналитиков, каждому из которых было немногим более 20 лет. Так было положено начало созданию солидной криптоаналитической организации, существующей в США сегодня.

Постепенно, несмотря на депрессию и изоляционизм, дешифровальная служба Фридмана расширялась. Вместе с ней рос и круг интересов Фридмана. В своих научных статьях он обсуждал криптоаналитические способности Эдгара По, вскрывал шифры, предлагавшиеся авторами более ранних работ по криптографии, исследовал различные исторические проблемы, связанные с шифртелеграммой Циммермана и первыми кодами американских экспедиционных войск. К несчастью, вынужденный хранить тайну и обуреваемый желанием добиться славы, в области криптоанализа Фридман стал вести себя подобно «собаке на сене» — если он не мог добиться славы, то она не должна была доставаться никому. Обычная тактика Фридмана сводилась к тому, чтобы чернить криптоаналитические разработки любителей, часто весьма достойные, как «непрофессиональные». Его жена, которая вскрывала коды торговцев спиртными напитками в период запрета на их продажу, продолжала заниматься криптоанализом в интересах министерства финансов.

Именно под руководством Фридмана персонал армейской дешифровальной службы добился выдающейся победы, проведя одну из самых трудных, кропотливых и триумфальных операций в истории криптоанализа — вскрытие японского «пурпурного» шифра. Это произошло в августе 1940 г., когда Фридману было 48 лет. Через несколько месяцев гениальный криптоаналитик не выдержал напряжения, связанного с этой разработкой. 4 января 1941 г. он был помещен в госпиталь в связи с нервным расстройством. Фридман выписался оттуда только 24 марта и был вынужден уйти в отставку по инвалидности.

По мере того как спадало напряжение, связанное с исполнением служебных обязанностей, Фридманы вернулись к той области криптоанализа, с которой они начинали, — бэконианским шифрам. Они подытожили опыт всей своей жизни в пространном и исчерпывающем докладе, отмеченном литературной премией.

В 1956 г. американский конгресс утвердил выплату Фридману 100 тысяч долларов в качестве компенсации за те доходы, которых он не смог получить ввиду того, что требования безопасности не позволили ему продать шифрмашины, изобретенные им для правительства. «Огромное напряжение и бремя ответственности, возложенное на него необходимостью постоянно соблюдать секретность, были основными факторами, подорвавшими здоровье г-на Фридмана, вследствие чего в настоящее время его шансы зарабатывать себе на существование становятся все более непрочными. Эти соображения побудили г-на Фридмана позволить нам обратить на данный вопрос внимание министерства обороны», — написали адвокаты Фридмана в прошении, поданном на имя министра обороны.

Теоретические исследования Фридмана, совершившие настоящую революцию в криптоанализе, сочетались с его вызывавшими изумление практическими работами по дешифрованию. Он положил конец путанице в терминологии. Введенные им терминологические определения занимают в

современных словарях не одну страницу. По его учебникам учились тысячи специалистов. Его статьи на исторические темы пролили свет на малоисследованные проблемы, а книга о Шекспире внесла большой вклад в ликвидацию многолетнего заблуждения в области литературы. И наконец, гигантская криптоаналитическая организация сегодняшнего дня, имеющая сотни тысяч служащих и разбросанные по всему миру станции перехвата, является прямым потомком маленького дешифровального отдела в военном министерстве, выпестованного Фридманом. Этот труд всей жизни увенчивает Уильяма Фридмана лаврами величайшего американского криптоаналитика.

НОВОЕ СРЕДСТВО БОРЬБЫ С КОНТРАБАНДОЙ

2 мая 1933 г. в Новом Орлеане в качестве главного свидетеля обвинения перед судом предстала выразительница нового направления в следственной практике: Элизабет Фридман, криптоаналитик службы береговой охраны США, выступила с показаниями по поводу прочитанных ею кодированных сообщений фирмы «Консолидейтед экспортерс», самой могущественной подпольной организации по контрабанде спиртных напитков во времена «сухого закона». Эти сообщения должны были доказать причастность руководителей фирмы к нелегальному ввозу спиртных напитков в Соединенные Штаты с моря. Элизабет Фридман не надо было незаметно красться за подозреваемыми по запутанным лабиринтам преступного подполья — она следила за их передвижениями только путем чтения зашифрованных сообщений. Не пришлось ей и снимать отпечатки пальцев на различных поверхностях при помощи специального порошка — она пользовалась лишь тонкими криптоаналитическими методами обнаружения признаков открытого текста в тайных посланиях. И, несмотря на это, ее показания были такими же убедительными, как и результаты обычной полицейской работы.

По мере роста числа подпольных баров в США нарушение «сухого закона» приняло устрашающие размеры. Спрос на спиртное вскормил криминальных гениев. Мелкие хулиганы стремительно превращались в заправил преступного бизнеса. Создавались целые бандитские синдикаты, которые по масштабам своей деятельности и денежному обороту могли соперничать с промышленными гигантами Америки. Принципы организации, разработанные торговцами запрещенным спиртным на суше, были заимствованы морскими контрабандистами-спиртовозами, ввозившими из-за границы запретную влагу, без которой алкогольные «реки» на материке давно бы пересохли. В то время как преступники на берегу имели дело с агентами отдела по борьбе с нелегальной торговлей спиртными напитками министерства юстиции, их коллеги на море сталкивались со службой береговой охраны, в обязанность которой входило пресечение контрабанды.

По мере того как спиртовозы становились более многочисленными и лучше организованными, они все чаще прибегали к радиосвязи для управления своими флотилиями. Послания, которыми обменивались суда спиртовозов и их радиостанции на берегу, своевременно предупреждали о действиях службы береговой охраны и сообщали плывшим из-за океана кораблям, где они должны были встретиться с быстроходными моторными лодками, доставлявшими напитки в уединенные бухты. Они же руководили отвлекающими действиями какого-либо судна, что позволяло другому кораблю незаметно проскользнуть мимо патрульных катеров.

Само собой разумеется, что все послания контрабандистов были закодированы. И несмотря на то, что в течение длительного времени радисты службы береговой охраны перехватывали эти сообщения, ни одно из американских ведомств по борьбе с преступностью не смогло их дешифровать. К апрелю 1927 г. в службе береговой охраны скопились сотни кодированных телеграмм преступников.

В связи с этим на работу в службу береговой охраны была приглашена Элизабет Фридман, эксперт в области криптоанализа. Начиная с 1916 г. ее услугами в разное время пользовались министерство обороны, министерство военно-морского флота, государственный департамент и министерство финансов.

Кроме того, были спешно смонтированы две станции радиоперехвата — во Флориде и в Сан-Франциско. Через два месяца Элизабет Фридман прочла основную часть накопленных сообщений контрабандистов, после чего занялась дешифрованием текущей переписки. Большая часть этой переписки исходила от двух конкурирующих флотилий по контрабандной перевозке спиртного — от упоминавшейся выше «Консолидейтед экспортерс» и от фирмы под названием «Хобс интерестс». Элизабет Фридман занималась дешифрованием в Вашингтоне, отправляя прочитанные сообщения на Тихоокеанское побережье (обычные — авиапочтой, а срочные — телеграфом).

Используя информацию, полученную благодаря криптоанализу, служба береговой охраны стала

чинить все более заметные препятствия действиям контрабандистов-спиртовозов. Но вскоре перевозчики нелегального спиртного обратили внимание на недостатки в своей системе радиосвязи, особенно в кодах и шифрах. В течение последующих лет их шифры постоянно развивались и совершенствовались. К середине 1930 г. практически каждое спиртовозное судно на Тихоокеанском побережье имело свой собственный шифр или код. «Ни одно правительство еще не прибегало к шифрам такой сложности для своей наиболее секретной переписки, — писала в 1930 г. в своем докладе Элизабет Фридман. — Во время мировой войны, когда методы секретной связи достигли наивысшего развития, такие усложненные системы, какие были обнаружены в переписке между судами-спиртовозами на Западном побережье, не применялись вообще».

Тем временем Элизабет Фридман дешифровала сообщения не только спиртовозов, но и других хорошо организованных банд контрабандистов, которые переняли их опыт. К примеру, в Сан-Франциско прочитанные Элизабет Фридман сообщения типа «Наш груз отправляем сегодня. Состоит из 520 коробок курительного опиума и 20 коробок опиума для инъекций...» заставили торговцев наркотиками Израэла и Джуда Эзра признать себя виновными. В результате их приговорили к 12 годам тюрьмы. По этому поводу один местный журналист написал: «Дюжина лет — это срок, за который они постараются придумать такой код, какой даже женщина не вскроет».

Самым крупным достижением Элизабет Фридман в борьбе с преступностью стало знаменитое дело фирмы «Консолидейтед экспортерс», которая сумела монополизировать всю нелегальную перевозку спиртных напитков на Тихом океане и в Мексиканском заливе. К началу 1932 г. в службе береговой охраны были накоплены сотни перехваченных шифрсообщений этой фирмы, а 11 апреля, когда полиция совершила налет на ее офис в Новом Орлеане, их было обнаружено еще больше. Все шифрсообщения были доставлены в Вашингтон, где под руководством Элизабет Фридман их вскоре успешно дешифровали.

Судебное разбирательство по обвинению руководства фирмы «Консолидейтед экспортерс» в контрабанде спиртного началось 1 мая 1933 г. На открытии процесса прокурор Амос Вудкок заявил, что братья Мерчант и Джозеф О'Нил, Натан Голдберг и Альберт Моррисон, возглавлявшие «Консолидейтед экспортерс», были «мозгом шайки, которая скупала виски в Канаде и других зарубежных странах на миллионы долларов, контрабандным путем доставляла его на побережье Мексиканского залива, откуда оно переправлялось в глубь страны».

Элизабет Фридман заняла место свидетеля 2 мая, сразу после показаний радиста службы береговой охраны Роя Келли, опознавшего 32 сообщения, которыми обменивались спиртовозные суда и береговые радиостанции в Новом Орлеане и Белизе. Все сообщения были перехвачены в период между 24 марта и 10 апреля 1931 г. Не останавливаясь подробно на примененных криптоаналитических методах, Элизабет Фридман дала показания относительно содержания дешифрованной ею переписки. Защита попыталась опротестовать эти показания на том основании, что они содержали «вывод и мнение» самого свидетеля. В ответ Элизабет Фридман выступила со следующим заявлением: «Хотя далеко не многие в Соединенных Штатах знакомы с принципами этой науки, любой эксперт после тщательного изучения представит текст, точно совпадающий с данным мною. Это отнюдь не вопрос личного мнения...»

Представитель защиты Уолтер Гекс подверг Элизабет Фридман перекрестному допросу, стремясь подорвать уверенность в правильности дешифровки.

«— Г-жа Фридман, как я понимаю, обозначения, направленные вам, были вам ранее неизвестны. Однако вы получили копию этих обозначений, которые вас попросили проанализировать и перевести, не так ли?

— Да.

— Для того чтобы вы соответствующим образом смогли перевести эти обозначения, не должен ли был кто-то вам сказать, что они относятся к перевозке спиртных напитков?

— О нет. Я могла бы получить обозначения, относящиеся к убийству или к наркотикам.

— Можно ли было использовать эти же обозначения в преступном сговоре с целью нарушения другого закона?

— Это возможно. Подобные обозначения могли бы быть использованы для таких целей, однако мне было бы невозможно определить, относятся ли они к торговле спиртным или к другому закону.

— Итак, какие же обозначения, как таковые, относятся к контрабанде спиртным?

— Это код. Я не смогу ответить вам, какое обозначение относится к контрабанде спиртным, если я не изучу весь материал в целом.

— Это нестандартный код. Могли ли эти джентльмены составить его сами?

— Да, могли.

— В таком случае, чтобы иметь четкую картину, вам пришлось бы сопоставить все слова и просмотреть всю переписку?

— Да. Анализ — это моя работа.

— Вы хотите сказать суду, что эти слова не могли быть использованы в заговоре с целью нарушить другой закон?

— Не с теми значениями, которые им придали здесь.

— Но ведь это вы придаете им значения?

— Нет, я не придаю им значений. Я получила их значения путем научного анализа. Они не придуманы.

— Предположим, я использую кодовое слово «CORA» для обозначения «виски», а вот Вудкок для виски использовал бы кодовое слово «AIM». Как бы вы это проанализировали?

— Вы мне дали только эти два слова, поэтому я не могу утверждать, что первое означает одно, а второе — другое или что оба означают одно и то же. Моя работа состоит в том, чтобы с помощью научных методов анализировать имеющийся в достаточном количестве материал. Я не скажу, что смогу дешифровать все, что угодно. Это зависит от количества материала и от типа применяемой системы кодирования.

— Утверждаете ли вы, что те же обозначения, использованные этими джентльменами, скажем, для слов «виски», «пиво», «координаты», могли быть применены для другой цели?

— Да, эти значения могли быть применены для другой цели».

После пятидневного слушания дела в суде Моррисон и оба О'Нила были осуждены, а Голдберг — оправдан. В обвинительном заключении, в частности, говорилось, что Моррисон и братья О'Нил виновны в том, что «намеренно подготовили и создали секретные коды для использования при передаче и приеме сообщений... судам и от судов, названных выше «спиртовозами», и в том, что «упомянутые сообщения... имели отношение к месту и времени прибытия упомянутых «спиртовозов», к контрабанде и выгрузке на территорию Соединенных Штатов больших количеств спиртного».

В июне 1933 г. Вудкок написал министру финансов: «Позволю себе обратить ваше внимание на необыкновенную услугу, которую оказала нам г-жа Фридман в судебном процессе по делу о контрабанде, самому крупному... в течение последних двух лет. Г-жа Фридман была вызвана в суд в качестве эксперта для дачи показаний относительно смысла некоторых перехваченных радиосообщений... Без раскрытия их содержания, как я полагаю, этот очень важный процесс не был бы выигран».

Признавая всю важность вклада Элизабет Фридман в пресечение контрабанды спиртным, следует все же отметить, что большинство случаев использования шифров в преступных целях относится к попыткам букмекеров скрыть свидетельства своей нелегальной деятельности. Их шифры в высшей степени специфичны и пригодны только для букмекерства. Обычно они сочетают шифрование цифр с сокращенными записями ставок и выплат. Вскрытие букмекерских шифров требует знания всевозможных форм нелегальных игр, каким обладает букмекер, — ведь «открытый текст» представляет собой всего лишь набор цифр!

Одной из наиболее распространенных азартных игр в США является «полиси». Играющий ставит деньги — порой не больше 10 центов — на трехзначную цифру. Если цифра выигрывает, он получает в 666 раз больше первоначальной ставки. У этой игры есть множество вариаций и комбинаций.

Самым знаменитым американским экспертом по вскрытию кодов «полиси» был Абрахам Чесс. Работая юрисконсультом в полицейском управлении Нью-Йорка, он, помимо основной работы, часто занимался криптоанализом, которым заинтересовался в возрасте 18 лет после того, как прочел «Золотого жука» Эдгара По. Однако применить на практике свои знания ему удалось совершенно случайно.

В 1940 г. один из нью-йоркских сыщиков целый день наблюдал, как букмекер собирает ставки и делает какие-то пометки. Арестовав букмекера, сыщик, к своему удивлению, обнаружил, что эти пометки были не обычными записями принятых ставок, а нотными листами. Без доказательств того, что букмекер занимался именно сбором ставок, а не какой-то странной, но вполне легальной деятельностью, его арест стал бы недействительным. Сыщик нутром чуял, что эти ноты представляли собой разновидность кода, однако в криминалистических лабораториях полицейского управления Нью-Йорка не было специалиста по дешифрованию. Вдруг один из детективов припомнил, что молодой сотрудник из юридического отдела интересуется криптоанализом, и вся эта «музыка» попала в руки 30-летнего Абрахама Чесса.

Чесс попробовал сыграть ноты на пианино: извлеченные из инструмента звуки явно не имели

совершенно никакого отношения к музыке. После семичасового исследования Чесс установил, что каждая нота заменяла цифру, которая определялась положением нотного знака на линейке. Такты указывали суммы ставок, а две точки в конце такта* обозначали комбинированную сделку. У Чесса набралось в общей сложности около 10 тысяч ставок. Благодаря показаниям Чесса суд смог установить вину букмекера.

* Две точки — нотный знак повторения.

После своего первого успеха Чесс стал выполнять эту работу регулярно и к 1951 г. вскрыл 56 шифров. Их разнообразие было удивительным. Для кодирования цифр игроки использовали буквы греческого, еврейского и даже древнего финикийского алфавита. Впоследствии Чесс ушел из управления полиции, но работа, начатая им, оказалась настолько ценной для органов правопорядка, что с тех пор над вскрытием букмекерских кодов постоянно трудятся десятки людей. Следственный отдел, полицейская академия, криминалистическая лаборатория и секретариат начальника полиции — все ввели в свои штаты специалистов по криптоанализу.

Полицейские управления, которым не выпало счастье иметь у себя эксперта вроде Абрахама Чесса, часто обращаются в ФБР с просьбой дешифровать букмекерские записи. Благодаря необычайно эффективной методике, искусно сочетающей чисто криптоаналитические методы с великолепным знанием букмекерского дела, только за 12 лет (с 1950-го по 1961 г.) в ФБР удалось прочесть несколько тысяч зашифрованных записей букмекеров. Чтобы понять их открытый текст, специалистам бюро предварительно пришлось не только попотеть на занятиях по криптоанализу, но и пройти ускоренный курс обучения в игорных домах Лас-Вегаса.

Например, в 1957 г. после налета бостонской полиции на одну из букмекерских контор были конфискованы бланки для заключения пари, журналы, посвященные скачкам, и спортивные выпуски газет, а также записная книжка, содержавшая написанные от руки символы, похожие на греческие буквы. Во время допроса владелец записной книжки упорно отрицал свою принадлежность к букмекерам и заявил полиции, что изучает греческий язык. Однако было достоверно известно, что задержанный неоднократно хвастался друзьям, будто полицейским никогда не удастся вскрыть его код, и он сможет продолжать беспрепятственно принимать ставки на лошадей. Полиция Бостона направила его записную книжку в ФБР, где вскоре было установлено, что буквами греческого алфавита в ней обозначены суммы ставок. При этом «α» заменяет «1», «φ» — «2», «κ» — «9», «β» — «11» и т. д. Записи оказались настолько сокращенными, что даже после того, как был установлен открытый текст, потребовалось провести дополнительное расследование, чтобы окончательно определить его смысл. Только тогда прокурор Бостона смог доказать вину обвиняемого в «использовании системы регистрации ставок на определенное животное, а именно лошадь, по результатам соревнования на скорость или выносливость» и выиграть судебный процесс.

ОДИН ДЕНЬ «МАГИИ»

В воскресенье 7 декабря 1941 г. в 1.28 ночи чуткое ухо военно-морской радиостанции США на острове Бейнбридж неподалеку от города Сиэтла уловило передачу в эфире. По линии Токио — Вашингтон передавалось сообщение, адресованное японскому посольству. Сообщение было коротким, его передача по радио заняла всего 9 минут.

На бейнбриджской радиостанции текст перехваченного японского сообщения набили на телетайпную ленту, потом набрали адрес телеграфной станции в американской столице и, когда связь была установлена, запустили ленту в механический передатчик, который считал ее со скоростью 60 слов в минуту. Через некоторое время сообщение появилось на буквопечатающем аппарате в комнате под номером 1649 в здании министерства ВМС США в Вашингтоне. Что происходило за ее стенами, было одним из самых тщательно охраняемых секретов американского правительства, так как именно там, а также в одной из комнат соседнего здания военного министерства Соединенные Штаты проникали в самые секретные планы и замыслы своих возможных противников, снимая кодовые покровы с их сообщений.

В комнате 1649 размещалась криптоаналитическая подсекция криптографической спецслужбы ВМС США. У стола дежурного офицера этой подсекции, младшего лейтенанта Фрэнсиса Бразерхуда, стоял буквопечатающий аппарат. По условным обозначениям, которые ставились для сведения японских шифровальщиков, Бразерхуд сразу же определил, что перехваченное сообщение, присланное с острова Бейнбридж, было зашифровано с использованием самой секретной

шифрсистемы Японии. Это был чрезвычайно сложный машинный шифр, который американские криптоаналитики окрестили «пурпурным».

Группа военных дешифровальщиков, возглавляемая главным криптоаналитиком войск связи армии США Уильямом Фридманом, сумела вскрыть «пурпурный» шифр и создала аппарат, который дублировал шифровальную часть японской машины. Затем войска связи построили несколько «пурпурных» машин, одна из которых была предоставлена в распоряжение ВМС и стояла на столе в комнате 1649. К ней и отправился Бразерхуд.

Установив на машине ключ от 7 декабря, Бразерхуд набрал на ее клавиатуре текст перехваченной японской шифртелеграммы. Электрические импульсы побежали по проводам, в обратном порядке проделывая сложный процесс зашифрования, и через несколько минут перед Бразерхудом лежал открытый текст этой шифртелеграммы.

Текст был на японском языке. Хотя Бразерхуд окончил краткосрочные курсы по изучению японского языка, которые ВМС организовали для своих криптоаналитиков, он не рискнул перевести телеграмму самостоятельно. В соседней комнате, где размешалась подсекция перевода, никого не оказалось. Поэтому Бразерхуд поставил на дешифрованном сообщении красный штемпель, свидетельствовавший о его срочности, и лично вручил представителю армейской дешифровальной службы. Там, как было известно Бразерхуду, переводчики с японского дежурили круглые сутки. Оставив им сообщение, он вернулся обратно.

Было уже 5 часов утра по вашингтонскому времени когда сотрудник армейской дешифровальной службы перевел с японского: «Послу следует вручить наш ответ правительству США (если возможно, государственному секретарю) в 1.00 дня 7 декабря по вашему времени». «Ответ», о котором говорилось в этой телеграмме, был японской дипломатической нотой, передававшейся из Токио в течение последних 18 часов. Бразерхуд только недавно закончил дешифрование ее последней, 14-й части на «пурпурной» машине. Нота была составлена в Токио на английском языке и заканчивалась словами: «Японское правительство с сожалением должно уведомить американское правительство, что ввиду позиции, занятой последним, правительство Японии не может не считать, что никакой возможности достигнуть соглашения путем продолжения переговоров не имеется».

Когда Бразерхуд сменился в 7 часов утра, перевод открытого текста японского шифрсообщения, в котором указывалось время вручения дипломатической ноты, все еще не был получен из армейской дешифровальной службы. Бразерхуд предупредил об этом своего сменщика, младшего лейтенанта Альфреда Перинга. Спустя полчаса прибыл специалист в области японского языка капитан-лейтенант Элвин Крамер, возглавлявший подсекцию перевода и отправлявший адресатам открытые тексты прочитанных японских шифрсообщений.

Крамер сразу же увидел, что получено самое важное — окончание длинной японской дипломатической ноты, 13 предыдущих частей которой он уже доставил адресатам этой ночью. Крамер отредактировал ее последнюю часть и приказал своему помощнику отпечатать, как обычно, 14 экземпляров. Двенадцать из них рассылались президенту, государственному секретарю, военному и военно-морскому министрам, а также другим высокопоставленным офицерам. Два последних экземпляра подшивались в дело. Прочитанное шифрсообщение было одним из целой серии перехваченных японских шифровок, которым еще давно, частично в целях обеспечения безопасности, частично для облегчения ссылок, было дано общее название — «Магия».

В 9.30 Крамер выехал с 14-й частью японской дипломатической ноты к адмиралу Гарольду Старку, главнокомандующему ВМС, и Фрэнку Ноксу, военно-морскому министру. У Нокса на 10 часов этого воскресного утра была назначена встреча в государственном департаменте с госсекретарем Корделлом Хэллом и военным министром Генри Стимсоном. Они должны были обсудить критический характер американо-японских переговоров, которые, как стало ясно из предыдущих 13 частей ноты, фактически зашли в тупик.

Крамер вернулся в комнату 1649 только в 10.20. Пока он отсутствовал, был уже получен перевод японского сообщения относительно вручения ноты в час дня.

Время, назначенное японским послом для вручения извещения о прекращении переговоров с американцами, было весьма необычным. Крамер быстро удостоверился, что час дня по вашингтонскому времени означает 7.30 утра на Гавайях и два часа до рассвета в неспокойном дальневосточном районе вокруг Малайи, куда угрожающе нацелились японские корабли с войсками. Крамер немедленно вложил сообщение о вручении дипломатической ноты в час дня в портфель, застегнул «молнию» и щелкнул замками. Через десять минут он опять был в пути.

Этот момент, когда Крамер, неся в портфеле важнейшую перехваченную телеграмму, бежал по пустынным улицам Вашингтона за час до того, как сонные шифровальщики в посольстве Японии

принялись за ее расшифрование, и за час до того, как японские самолеты с ужасным ревом поднялись с взлетных палуб авианосцев, чтобы выполнить свою вероломную миссию, — этот момент, бесспорно, является великим часом в истории американского криптоанализа. Крамер бежал, в то время как его сограждане безмятежно нежились в своих постелях, совершенно не думая об агрессии, надеясь, что она минует их, и отказываясь допустить, пусть даже в шутку, возможность того, что какие-то желтолицые коротышки японцы осмелятся напасть на могущественные Соединенные Штаты. В этот день национального унижения американский криптоанализ сумел достичь таких вершин бдительности и совершенства, какие оказались не по плечу ни одному из ведомств США. Налицо огромное достижение криптоанализа. Его слава. И Крамер, бегущий по пустынным улицам, как нельзя лучше ее символизирует.

Но почему же тогда не был предотвращен позор Перл-Харбора?! Да потому, что японцы никогда не посылали сообщения, в котором говорилось бы что-либо похожее на: «Мы атакуем Перл-Харбор». Было перехвачено и прочтено большое количество шифртелеграмм, проливавших свет на огромный интерес японцев к передвижениям военных судов США в направлении к Перл-Харбору и от него. Но эти дешифровки подвергались изучению и оценке наравне с большим количеством сообщений относительно движения боевых кораблей США в окрестностях других портов и по Панамскому каналу. Причин разгрома Перл-Харбора много, но никто и никогда не возлагал ответственности за случившееся на американских криптоаналитиков. Наоборот, комиссия конгресса США, расследовавшая обстоятельства нападения на Перл-Харбор, выразила им благодарность и отметила, что выполнение ими своего долга «заслуживает наивысшей похвалы».

7 декабря 1941 г. клерки посольства Японии в США один за другим приступили к работе около 10 часов утра. Сперва они начали расшифровывать длинные сообщения, так как их опыт подсказывал, что обычно именно эти сообщения были наиболее важными. Примерно в 11.30 японский шифровальщик установил на «пурпурной» машине нужный ключ и отпечатал короткое сообщение. К ужасу всего посольства, в расшифрованной телеграмме содержались инструкции о вручении ноты из 14 частей государственному секретарю Хэллу в час дня по вашингтонскому времени. А 14-я часть этой ноты еще не была даже выбрана из пачки входящих шифртелеграмм!

Тем временем на расстоянии нескольких зданий от японского посольства начальник генштаба вооруженных сил США генерал Джордж Маршалл только что прибыл в военное министерство. На его столе лежала подшивка телеграмм «Магии». Самой верхней была телеграмма с японской дипломатической нотой из 14 частей, а под ней лежала телеграмма, в которой сообщалось о вручении этой ноты в час дня. Маршалл начал внимательно изучать ноту, перечитывая некоторые ее части по нескольку раз. Затем он прочитал телеграмму о времени вручения ноты. Она поразила Маршалла точно так же, как и Крамера. Маршалл схватил телефонную трубку, позвонил Старку и предложил ему составить совместное предупреждение американским сухопутным и военно-морским силам на Тихом океане. Приблизительно в это же самое время посол Японии в США Номура связался с Хэллом и попросил у него приема в час дня. А в 600 километрах к северу от Гавайских островов первая волна японских самолетов с ревом взлетела с палуб авианосцев.

В ответ на предложение Маршалла Старк сказал, что уже было послано достаточно предупреждений и еще одно только запутает командующих. После этого Маршалл в одиночку составил текст предупреждения, которое он хотел бы послать: «Сегодня в час дня японцы вручают нам что-то похожее на ультиматум... Точно неизвестно, что нас ожидает в ближайшее время, но мы должны быть в состоянии готовности, соответствующей сложившейся обстановке».

На столе Маршалла стоял телефон, по которому он мог позвонить на Гавайи. Но Маршаллу было известно, что эта аппаратура обеспечивает защиту только от случайного подслушивания и не дает никаких гарантий при использовании специального оборудования. Поэтому Маршалл не очень доверял телефону и полагался на медленный, но зато более надежный способ — на шифрование письменных сообщений.

Когда Маршалл уже заканчивал писать свое сообщение, позвонил Старк. Он передумал и просил Маршалла добавить в это сообщение указание о том, чтобы оно было показано также командующим военно-морскими силами США. Поэтому Маршалл добавил в него фразу: «Информируйте командующих военно-морскими силами».

Маршалл приказал отнести подготовленное им сообщение в центр связи военного министерства для передачи командующим американскими войсками на Филиппинах, Гавайях, в Карибском море и на Западном побережье США. Маршаллу было обещано, что сообщение будет зашифровано через 3 минуты, на его передачу уйдет еще 8 минут, а через 20 минут оно будет в руках адресатов. Но было уже слишком поздно: японские самолеты находились менее чем в 60 километрах от своих целей.

Лихорадочное возбуждение продолжало царить в японском посольстве. Его шифровальщики в поте лица трудились над расшифрованием и перепечаткой набело дипломатической ноты, которую необходимо было вручить в час дня. Во втором часу, когда стало ясно, что сделать это вовремя никак не удастся, Номура позвонил Хэллу и попросил отложить встречу с ним на 1.45 дня, так как документ, который он хотел вручить, еще не был готов. Хэлл согласился.

Только в 1.50 дня по вашингтонскому времени, через 20 минут после начала нападения Японии на США, японская нота была подготовлена для вручения. Номура сразу же отправился с ней в госдепартамент.

Хэлл вспоминает:

«Японский посол прибыл в госдепартамент в 2 05 и прошел в комнату ожидания для дипломатов. Почти в это же время из Белого дома мне позвонил президент. Его голос был спокойным и ровным.

Он сказал: «Пришло сообщение, что японцы атаковали Перл-Харбор» Я спросил: «Подтверждено ли это сообщение?» Он ответил: «Нет»

Мы оба выразили уверенность, что сообщение было, по всей вероятности, правильным. Я проявил желание получить подтверждение сообщения, имея в виду предстоящую встречу с японскими послами.

Номура явился ко мне в 2 20. Я принял его холодно и не пригласил сесть.

Номура робко заявил, что он получил инструкции от своего правительства вручить мне в час дня документ, но что трудности, встретившиеся при его расшифровании, задержали это вручение. Затем он передал мне ноту своего правительства.

Я спросил его, почему в своем первом обращении ко мне он попросил принять его в час дня.

Он ответил, что он не знает, но таковы были его инструкции. Я сделал вид, что просматриваю ноту. Я уже знал ее содержание, но, естественно, не должен был раскрывать этого. Прочитав две или три страницы, я спросил Номуру, вручил ли он документ в соответствии с инструкциями своего правительства.

Он ответил утвердительно.

Когда я закончил просмотр страниц документа, я повернулся к Номуре и, глядя на него, сказал:

«Я должен заявить, что во время моих переговоров с вами в течение последних 9 месяцев я не произнес ни одного слова неправды. Это абсолютно точно подтверждается протоколами. За все 50 лет моей государственной службы я никогда не видел документа в такой степени насыщенного позорными инсинуациями и ложными утверждениями, настолько чудовищными, что до сегодняшнего дня я не мог и представить себе, что какое-либо правительство на этой планете в состоянии измыслить их».

Номура, казалось, хотел что-то ответить. Лицо его было бесстрастным. Но я чувствовал, что он испытывал огромное эмоциональное напряжение. Я остановил его знаком руки и указал ему на дверь. Посол повернулся и, не говоря ни слова, вышел, понурив голову».

Надежды японских военных сократить время предупреждения до минимума не оправдались, и Япония начала военные действия против США без всякого предварительного уведомления. Впоследствии нападение без объявления войны стало одним из основных обвинений, предъявленных японским военным преступникам. За это они были осуждены, а некоторые поплатились своей жизнью.

В Вашингтоне на другой день после нападения на Перл-Харбор, вскоре после полудня, президент Соединенных Штатов Америки под бурные аплодисменты вышел на трибуну конгресса. Когда наступила тишина, зазвучал его взволнованный голос: «Вчерашний день, 7 декабря 1941 г., навечно станет днем позора — Соединенные Штаты Америки были внезапно и неспровоцированно атакованы военно-морскими и военно-воздушными силами Японской империи...»

Война началась. Свершилось одно из самых вероломных нападений в мировой истории. Но если у американских криптоаналитиков не было шансов предупредить о нем заранее, с тем чтобы военные успели принять все необходимые меры, они с успехом воспользовались возможностью применить свое искусство во время войны. С их помощью Америка превратила тактическую перл-харборскую победу японцев в их стратегическое поражение. Американские криптоаналитики, как впоследствии было отмечено конгрессом США, «внесли огромный вклад в дело победы над Японией, значительно сократили сроки войны и спасли многие тысячи жизней». Но это уже тема для отдельного разговора.

ПРОМАХИ АЗИАТОВ

Вскоре после нападения Японии на США в 1941 г. ее военные планы в основном были

выполнены. Она не собиралась вторгаться в пределы Соединенных Штатов, а скорее стремилась создать кольцо неприступных оборонительных укреплений вокруг захваченных территорий. Однако высшее японское командование, ослепленное достигнутыми успехами и страстно жаждавшее новых, решило продолжать наступление. Потери японских ВМС, которые по предварительным подсчетам должны были составить четверть личного состава и боевой техники, оказались ничтожно малыми. Сил для нового наступления оставалось более чем достаточно. Кроме того, японские военные стратеги утверждали, что защита захваченных территорий будет обеспечена лучше, если периметр обороны будет больше.

Поэтому японцы приступили к выполнению двух честолюбивых планов. Один из них предусматривал наступление десантных войск в южном направлении для создания угрозы Австралии. Второй был нацелен на Мидуэй, крошечный атолл в центре Тихого океана, который, как часовой, стоял на пути к Гавайским островам. Этот план состоял из Двух частей. Первая включала захват атолла, имевшего стратегическое значение. Целью второй, более важной части было завлечь в ловушку и уничтожить оставшийся после разгрома Тихоокеанский флот США, который, несомненно, попытался бы защитить атолл Мидуэй.

Но японское командование не знало, что у американцев было секретное оружие, которое могло изменить положение на Тихом океане. Это оружие находилось в длинном, узком подвальном помещении административного здания на территории военно-морской базы на Перл-Харборе. Там размещалось подразделение радиотехнической разведки, обслуживавшее Тихоокеанский флот США. К началу войны оно состояло из тридцати офицеров и рядовых. В их задачу входило вскрытие японской военно-морской шифрсистемы, сокращенно именовавшейся «ЯВ-25А». Название было присвоено ей американскими криптоаналитиками, занимавшимися вскрытием этой самой распространенной системы шифрования японских ВМС, с помощью которой передавалась примерно половина всех сообщений.

Тем временем японцы, которые и не подозревали обо всей этой бурной деятельности, начали проявлять смутное беспокойство по поводу слишком большого срока действия кода «ЯВ-25А». Его новое издание, которое американцы стали потом называть кодом «ЯВ-25Б», планировалось ввести 1 апреля 1942 г. Однако трудности доставки кодовых книг кораблям, находившимся в движении, вынудили отложить замену кода до 1 мая.

Благодаря этой отсрочке к 17 апреля из перехваченной американцами военно-морской шифрпереписки Японии остались непрочитанными лишь отдельные части. Полученные большие участки открытого текста давали возможность проникнуть в суть японских военных планов наступления в направлении Австралии. Своевременно принятые командующим Тихоокеанским флотом США Нимитцем меры сорвали эти планы. Но остановка японцев на южном направлении не изменила их грандиозных планов достичь победы в войне против Америки.

Наступило 1 мая, а смены кода «ЯВ-25А» на «ЯВ-25Б» так и не произошло: в силу тех же причин, что и раньше, японцы вновь отложили ее на месяц — до 1 июня. По-видимому, они полагали, что их шифры не вскрыты и замена не обязательна. Если бы замена произошла 1 мая, как планировалось, то она бы лишила американских дешифровальщиков возможности чтения японской военно-морской шифрпереписки по крайней мере на несколько недель, которым суждено было стать решающими.

20 мая 1942 г. главнокомандующий японским объединенным флотом адмирал Ямамото издал и разослал своим подчиненным оперативный приказ с подробным изложением тактических приемов, которые необходимо использовать в ходе нападения на атолл Мидуэй. Приказ Ямамото перехватили посты подслушивания американцев. Очень большая длина криптограммы указывала на ее важность. Более недели американские дешифровальщики бились над десятой частью ее текста, никак не поддававшейся прочтению. Именно она содержала самые важные данные приказа — даты, время начала и место проведения военных операций. О них американские дешифровальщики могли только догадываться, опираясь в своих предположениях на косвенные данные.

Из-за предположительного характера полученной информации беспокойство высшего военного руководства страны все возрастало: от точности дешифрования приказа Ямамото зависели как будущий ход военной кампании на Тихом океане, так и само существование американского флота. Поэтому проверка догадок относительно самой важной части приказа Ямамото была поручена другим разведывательным службам ВМС США, а основное внимание дешифровальщиков подразделения радиотехнической разведки было обращено на прочтение остальных девяти десятых шифрованного текста этого приказа.

Начальник подразделения радиотехнической разведки капитан Джозеф Рошфор решил

хитростью заставить японцев подтвердить правильность догадок относительно содержания той части шифртелеграммы с приказом главнокомандующего, которую дешифровальщики никак не могли прочесть. Рошфор составил донесение, в котором гарнизон Мидуэя сообщал, что его установка по опреснению воды якобы вышла из строя. Донесение было передано открытым текстом. Два дня спустя среди вороха перехваченных японских сообщений появилось одно, в котором говорилось, что «AF» испытывает нехватку пресной воды. Таким образом было раскрыто кодовое слово, применявшееся японцами для обозначения атолла Мидуэй.

Оказавшаяся в распоряжении американцев информация о планировавшемся нападении на Мидуэй была во всех отношениях достоверной — она поступила от самих японцев и даже была перепроверена. Оставалось только выяснить, когда это произойдет. 27 мая 1942 г. штаб главнокомандующего Тихоокеанским флотом США Нимитца выдвинул предположение, что операция начнется 3 июня. Аргументация в пользу этой даты была убедительной, но она не была подтверждена выводами криптоаналитиков.

И вот — очередной успех подразделения радиотехнической разведки: взломан шифр, с помощью которого были засекречены даты и время в тексте приказа Ямамото. Предположения Нимитца полностью подтвердились. Последовавшая смена японского кода в июне 1942 г. не повлияла на ход событий у атолла Мидуэй, поскольку все планы были уже составлены и японская военная операция начала разворачиваться. Впоследствии в своих воспоминаниях Нимитц написал: «Мидуэй был в основном победой криптоанализа. Пытаясь нанести удар внезапно, японцы сами попали под внезапный удар». Маршалл был более конкретен: «Благодаря криптоанализу мы могли сконцентрировать наши ограниченные силы для отражения нападения японских военно-морских сил на Мидуэй, в противном случае мы были бы за тысячи и тысячи километров от нужного места».

Справедливости ради надо сказать, что работу американских дешифровальщиков часто облегчали сами японцы. Безопасность связи последних была на таком низком уровне, что иногда казалось, что им все равно. Например, ВМС Японии пытались найти для печатания своих кодовых книг растворявшуюся в морской воде типографскую краску, с тем чтобы при выбрасывании их за борт или потоплении судна печатный текст исчезал. Однако, когда научно-техническая лаборатория сообщила, что она не может изготовить такую краску, которая полностью растворялась бы при попадании в морскую воду и тем не менее была бы стойкой против дождя, морских брызг и испарений, от этой разумной идеи отказались. А зря.

Ночью 29 января 1943 г. японская подводная лодка с грузом имела несчастье всплыть вблизи новозеландского противолодочного корабля «Киви». Заметив лодку, капитан «Киви» дал команду «полный вперед» для ее тарана, хотя та была в полтора раза больше «Киви» и обладала значительно большей огневой мощью. После четырех таранов лодка обратилась в бегство и через несколько часов, потеряв управление, села на мель на северо-западном выступе острова Гуадалканал. Среди прочего груза японская подводная лодка везла двести кодовых книг. Ее экипаж закопал часть из них на побережье, занятом противником. Когда об этом стало известно японскому штабу, был отдан приказ о том, чтобы бомбардировкой с воздуха и торпедированием с подводных лодок попытаться уничтожить документы, которые перевозила севшая на мель подлодка. Однако американцы подоспели раньше и успели захватить кодовые книги, в числе которых были как действующие, так и резервные. А через несколько месяцев японцы поплатились за эту неудачу жизнью своего командующего флотом.

Удивительно, но факт остается фактом: в том, что касалось безопасности связи, японцы возлагали основные надежды не на подготовку персонала или стойкость своих шифров, а больше следили, чтобы своевременно были «вознесены молитвы во имя славных успехов в выполнении священного долга в великой войне в Восточной Азии». К тому же они слишком полагались на малопонятность своего языка, придерживаясь того взгляда, что иностранец не в состоянии выучить многочисленные значения отдельных иероглифов достаточно твердо, чтобы знать японский язык хорошо.

В 1943 г., благодаря стараниям криптоаналитической службы Тихоокеанского флота США, случилось одно из самых драматических событий, которое когда-либо происходило в результате получения доступа одной воюющей стороны к секретным данным другой.

Весной этого памятного в истории криптоанализа года адмирал Ямамото решил совершить инспекционную поездку по военно-морским базам Японии в северной части Соломоновых островов. 59-летний Ямамото был выдающейся фигурой в японских ВМС. Именно он задумал удар по Перл-Харбору и хвастал, что будет диктовать условия мира американцам в Белом доме. Американские спецслужбы характеризовали его как исключительно способного, энергичного и сообразительного

человека и сделали вывод, что любой его преемник был бы ниже Ямамото и по личным, и по деловым качествам. Смерть командующего, являвшегося самым одаренным стратегом военной машины противника, несомненно, деморализовала бы его подчиненных, которые в силу японской традиции чтили своих командиров гораздо больше, чем американцы.

Обычно японские базы заранее предупреждались о визите командующего, чтобы там могли как следует подготовиться к инспекции. Поэтому 13 апреля 1943 г. маршрут поездки Ямамото, намеченной на 18 апреля, был передан частям и соединениям, которые тот намеревался посетить. Слишком большое разнообразие адресов, а также необходимость обеспечить безопасность главы ВМС Японии побудили японского связиста выбрать действовавшее издание кода «ЯВ-25», наиболее распространенного и стойкого, чтобы закрыть эту информацию «броней» шифра.

К несчастью для японцев, «броневое покрытие» их линий связи оказалось «растворено» едкой «кислотой» американского криптоанализа. Объединенными усилиями военных криптоаналитиков США и с помощью документов, добытых с севшей на мель у острова Гуадалканал японской подводной лодки, удалось прочитать шифртелеграмму, содержавшую данные о маршруте Ямамото.

Смертный приговор Ямамото был вынесен Нимитцем 17 апреля, запечатан и доставлен по назначению будущим палачам японского главнокомандующего — летчикам-истребителям военно-воздушных сил США. Выгоды от успешной операции по устранению Ямамото перевесили опасения вызвать у японцев подозрения, что американцы вскрывают их шифры, и тем самым лишить последних возможности продолжать получать разведывательную информацию из японских каналов связи в будущем. 18 апреля приговор был приведен в исполнение. В воздушном пространстве над островом Бугенвиль в Тихом океане самолет с Ямамого на борту сбили американцы.

Как и предполагал Нимитц, смерть Ямамото потрясла всю страну. С большой помпой его обугливщееся тело было предано земле в одном из токийских парков. Смерть героя, который пользовался огромной популярностью, привела в уныние японских солдат, моряков и гражданское население.

Представители вооруженных сил США, следуя совету Нимитца, решительно отрицали, что им известны какие-либо подробности случившегося. Ходили слухи, что то ли произошла банальная авиакатастрофа, то ли Ямамото в порыве отчаяния сделал себе харакири. Однако правдивые сведения о произошедшем просачивались во все более и более широкие круги американской общественности.

Третий из четырех параграфов, напечатанных на всех обложках секретных сводок «Магии», неизменно гласил: «Нельзя предпринимать никаких действий на основании сообщенной здесь информации, несмотря на временную выгоду, если такие действия могут привести к тому, что противник узнает о существовании источника».

Еще 7 июня 1942 г., когда битва у атолла Мидуэй была в полном разгаре, американская газета «Чикаго трибюн» поместила на своих страницах статью, в которой прямо говорилось о наличии в руках военно-морского министерства США информации об оперативных планах японского командования ВМС. Более того, в газетной статье подробно описывался состав и характеристики японских морских соединений, участвовавших в этой битве. В ходе последовавшего разбирательства ВМС США отказались от предъявления газете обвинения в разглашении государственной тайны только для того, чтобы не привлекать внимания японцев. Надежды оправдались: японцы так и не догадались, что их шифрованные сообщения читались противником.

Не заметили японцы и выступления в конгрессе члена палаты представителей от штата Пенсильвания Холланда. Тот начал с критики «Чикаго трибюн» за злоупотребление свободой прессы. «Американские парни будут продолжать умирать из-за услуги, которая была оказана врагам этой газетой», — сказал Холланд. А затем пояснил для непонятливых, в чем именно состояла услуга: «Чикаго трибюн», мол, проболталась о том, что «каким-то образом ВМС США добыли секретный военно-морской код Японии».

Осенью 1944 г. в котле американской национальной политики создалась взрывоопасная ситуация. Республиканская партия готовилась выставить кандидатуру Дьюи на пост президента. Одним из главных аргументов республиканцев в предвыборной кампании было обвинение правительства США в том, что его непростительная инертность позволила японцам осуществить успешное нападение на Перл-Харбор. Делались даже намеки на то, что президент Рузвельт, учитывая сильные настроения в американском обществе в пользу изоляционизма, умышленно вызвал нападение, чтобы втянуть Америку в войну. Для подтверждения обвинений распространялись сведения, что американцы вскрыли японские шифры еще до Перл-Харбора. Из этого республиканцы делали вывод, что дешифрованные криптограммы Японии предупреждали Рузвельта о грядущем нападении, но тот с преступной небрежностью ничего не предпринял, чтобы дать японцам достойный

отпор. По мере того как предвыборная кампания набирала ход, в речах американских политиков равного ранга стали появляться прозрачные намеки на «Магию».

Обеспокоенный сложившейся ситуацией начальник генштаба вооруженных сил США Маршалл написал Дьюи письмо на трех страницах, указав в нем на чрезвычайную опасность разглашения «магической» информации. Во втором абзаце этого письма говорилось: «То, что я должен сообщить вам ниже, представляет собой такой большой секрет, что я считаю себя обязанным попросить вас либо приняв письмо с условием, что вы никому не сообщите его содержание и вернете его, либо прекратить дальнейшее чтение».

При чтении третьего абзаца в поле зрения Дьюи попало слово «криптография» Он тут же прекратил чтение, вернул письмо доставившему его офицеру армейской дешифровальной службы Картеру Кларку и сказал, что «не может давать неблагоразумных обязательств».

Обсудив отказ Дьюи, Маршалл и Кларк решили попытать счастья еще раз. Они частично переделали письмо и позвонили кандидату в президенты. Тот согласился прочитать письмо только в присутствии своего советника. Дьюи хотел иметь подтверждение факта прочтения письма в случае, если что-то произошло бы с Маршаллом. По этой же причине он настаивал, чтобы письмо оставили ему на хранение. Второе письмо оказалось более убедительным для Дьюи. В нем Маршалл изложил поистине трагические последствия, которые могли бы иметь место, если бы из политических дебатов противник догадался о важнейших источниках информации, находившихся в распоряжении американцев. Дьюи тщательно взвесил аргументы Маршалла, к которому был лично расположен, как к весьма справедливому и уважаемому человеку. С одной стороны, на карту было поставлено руководство могущественной страной, с другой — вероятность продолжения войны, в которой ежедневно гибли сотни американцев. После двух дней размышлений Дьюи решил пожертвовать карьерой и не упоминать в своих публичных выступлениях о вскрытии японских шифров.

Дьюи потерпел на президентских выборах полное поражение. После этого Маршалл и Дьюи долго обменивались любезностями в византийском стиле, работая явно на публику. Маршалл направил Дьюи подборку копий телеграмм «Магии», чтобы тот мог воочию убедиться, как содержавшаяся в них информация помогала проведению операций на Тихом океане. Дьюи заявил Маршаллу, что слышал, будто в конгрессе пройдут дебаты по поводу Перл-Харбора, и предложил свои услуги, чтобы помешать их проведению. Маршалл ответил, что он уже однажды поставил Дьюи в затруднительное положение своими просьбами, которые повлияли на ход избирательной кампании. На что Дьюи отреагировал заявлением, что это было не его личным делом, а делалось ради достижения победы в войне. Так перестала существовать самая серьезная угроза безопасности «Магии», которая, как это ни парадоксально звучит, исходила не от японцев, а изнутри, от собственных политиканов.

В ДЕБРЯХ ТОТАЛИТАРНЫХ ДЖУНГЛЕЙ

Как и в любой другой стране с диктаторским режимом, высокопоставленные лица гитлеровской Германии укрепляли свои позиции, создавая атрибуты личной власти. Эту власть можно было упрочить еще больше, располагая сведениями, полученными с помощью криптоанализа.

Еще в начале 1919 г. в немецком министерстве иностранных дел была создана собственная криптоаналитическая спецслужба — так называемое отделение «Z». Ее возглавил 32-летний капитан армейской службы радиоперехвата Курт Зелхов. Первоначально отделение «Z» было укомплектовано в основном специалистами, с которыми Зелхов свел знакомство еще во время Первой мировой войны. Однако после прихода Гитлера к власти в 1933 г. оно начало неуклонно расширяться. К 1939 г. криптоаналитиков в отделении «Z» было уже столько, что они разделились на две группы в соответствии со специализацией. Первая занималась шифрами, причем по составу и профессиональным склонностям у этой группы обнаружился математический уклон. Вторая дала лингвистический крен и взяла под свою «опеку» вскрытие кодов. Эти группы возглавили три старших криптоаналитика отделения «Z»: Шауффлер, преподававший до Первой мировой войны в школе, и Пашке, уроженец Санкт-Петербурга, совместно руководили лингвистической группой, так как она была очень велика, а Кунце, прослуживший всю войну кавалеристом, верховодил математиками.

Все трое были профессионалами высокого класса. Шауффлер — специалист по восточным языкам с хорошей математической подготовкой, криптоаналитик с уклоном в теоретические исследования. Пашке — прирожденный лингвист, целиком посвятивший себя криптоанализу. Кунце — доктор математики Гейдельбергского университета. Все они начали профессионально заниматься

криптоанализом еще до создания отделения «Z», но послужной список Кунце был самым впечатляющим. На его счету — вскрытие нескольких английских шифров и французского дипломатического кода в 20-х годах, а также двух японских машинных шифров, известных американским криптоаналитикам под условным названием «оранжевый» и «красный».

С началом Второй мировой войны набор в отделение «Z» осуществлялся в «пожарном» порядке. Там позарез были нужны специалисты-криптоаналитики, и поэтому приходилось делать исключения для людей «неарийского» происхождения. К примеру, Людвиг Дойбнер читал для немцев русские военные шифртелеграммы во время Первой мировой, а при нацистах за свои успехи в дешифровании был отмечен званием «почетного арийца». Его сына Оттфрида, наполовину еврея, в память о заслугах отца взяли на работу в отделение «Z» — читать итальянскую шифрованную переписку.

Значительную помощь немецким криптоаналитикам из отделения «Z» оказывала информационная группа, которую возглавлял пастор Цигенрюкер. Эта группа собирала данные из радиопередач, меморандумов министерств иностранных дел, зарубежных газет и материалов отделения «Z». Она могла дать криптоаналитикам точный ответ на такой сложный вопрос: «Кто, начинающийся на А, беседовал с кем-то оканчивающимся на Б, в пункте с названием, похожим на В, в последний четверг?», что оказывало им неоценимую помощь в работе по вскрытию шифров.

Большую стимулирующую роль в отделении «Z» играли денежные вознаграждения за знание иностранных языков. Их величина зависела от трудности языка. Ничего не платили там только за английский и французский, так как считалось, что в любом случае квалифицированный криптоаналитик без их знания обойтись не мог. Дешифровальщикам приходилось каждые четыре года сдавать экзамен по языку, чтобы подтвердить свое владение им. Перед каждой сдачей они освежали свои знания в берлинской школе иностранных языков. В отделении «Z» были специалисты по языку каждой страны, достаточно большой, чтобы содержать за границей свой дипломатический корпус.

Вскрытие шифров в общей сложности 34 стран мира, включая Англию, США и Францию, говорило о том, что криптоаналитики отделения «Z» работали не впустую. Дешифрованные в отделении «Z» и отпечатанные на машинке материалы поступали к Зелхову, который затем отправлял их дальше наверх — министру иностранных дел Риббентропу. А тот выбирал информацию для ознакомления с ней Гитлера. Однако последний не всегда оценивал ее по достоинству. Например, это произошло с текстом одного пространного сообщения, содержавшего важную информацию о положении в сельском хозяйстве СССР, состояние дел в котором не могло не сказаться на военном потенциале Советского государства. Гитлер начертал на нем резолюцию: «Этого не может быть». Он предпочитал свои собственные выдумки и пропаганду нелицеприятной правде.

Отделение «Z» отличилось и тем, что внесло посильный вклад в развязывание Германией Второй мировой войны. В последний день мирной жизни шведский бизнесмен Далерус встретился с Риббентропом в Берлине. Далерус давно и безуспешно пытался предотвратить надвигавшуюся войну, совершая перелеты между Англией и Германией в качестве неофициального посредника. Когда Далерус и Риббентроп обсуждали сложившуюся обстановку, в кабинет Риббентропа вошел его адъютант и вручил ему красный конверт, применявшийся в особо срочных случаях государственной важности. Прочитав содержание переданного ему сообщения, Риббентроп заявил, что располагает доказательствами саботажа со стороны поляков любого шага в направлении мирного урегулирования. В руках у него был открытый текст шифртелеграммы польского правительства своему послу в Берлине. Криптоаналитики из отделения «Z», вскрывшие польский дипломатический код, прочли шифртелеграмму и сделали перевод прочитанного с польского на немецкий язык. Весь процесс от перехвата шифртелеграммы до вручения перевода ее открытого текста Риббентропу потребовал меньше часа.

В конце шифртелеграммы стояло специальное предписание польскому послу: «Ни при каких обстоятельствах не вступайте в настоящие переговоры». Риббентроп собственноручно снял копию с перевода и вручил Далерусу для передачи английскому послу. Он добавил, что Англия должна узнать от Германии, насколько вероломны поляки, хотя бы и ценою риска лишиться полезного источника информации. Конечно, не вероломство поляков, мнимое или действительное, было настоящей причиной для начатой на следующий день мировой войны. Оно послужило лишь предлогом для нее. Дешифрованная польская телеграмма просто продемонстрировала точность и эффективность одного из главных орудий шпионажа Германии в момент развязывания ею очередной мировой войны.

Отделение «Z» успешно читало шифрпереписку не только противников Германии, но и ее союзников. В начале 1941 г. сложилась весьма деликатная ситуация. 4 февраля немецкий посол в Турции сообщил, что через иракского посланника в Анкаре ему стало известно о знании англичанами

намерений итальянцев, так как в Англии вскрыли итальянский шифр. Начальник одного из отделов МИД Германии Верманн дал отделению «Z» задание разобраться. В конце марта Зелхов доложил, что итальянцы пользуются тремя группами шифров: первая вскрывалась криптоаналитиками отделения «Z» легко, а вторая и третья — труднее. Англичане вскрыли шифр, относившийся ко второй группе. Им как раз и закрывалась итальянская дипломатическая линия связи Багдад-Рим.

Верманн предложил несколько способов уведомить итальянцев. Например, сказать, что информация из Анкары побудила немцев попытаться дешифровать шифртелеграмму из линии связи Багдад-Рим, и их усилия не пропали даром. К своему удивлению, немцы обнаружили, что даже после деликатного уведомления итальянцев о слабости их шифра те даже не удосужились его сменить. Однако дело было не в чрезмерной деликатности немецкого уведомления и уж отнюдь не в тупости или безответственности итальянцев. Министр иностранных дел Италии граф Чиано после того, как узнал, что немцы читают шифртелеграммы вверенного его заботам министерства, записал в своем дневнике: «Хорошо, что стало известно об этом. В будущем они будут читать то, о чем захочу, чтобы они знали».

Отделение «Z» было не единственным криптоаналитическим подразделением в гитлеровской Германии. В 1933 г., через несколько недель после того, как Гитлер назначил Геринга министром авиации, бывший самолетный ас создал в министерстве авиации специальный отдел из восьми человек для осуществления как можно более широкого перехвата. Геринг назвал его Исследовательским отделом, но исследования этот отдел вел весьма своеобразные. Он подслушивал телефонные разговоры, перлюстрировал письма и дешифровывал криптограммы. В 1934 г. Исследовательский отдел сделал как раз то, что Геринг ожидал от него: снабдил информацией, которая помогла завоевать доверие Гитлера в битве за власть между его ближайшими соратниками — гомосексуалистом Ремом, с одной стороны, и Герингом с Гиммлером, с другой. Рем был убит, и вскоре его участь разделил глава Исследовательского отдела за то, что делал свою работу слишком хорошо и знал в результате чрезмерно много.

В 1939 г. все партийные и правительственные полицейские организации Германии, за исключением Исследовательского отдела, были слиты в одну — Главное управление имперской безопасности. Его VI управление имело своей задачей поставлять секретную информацию о других странах. Первоначально оно сконцентрировало внимание на более традиционных методах их сбора. Но вот после аншлюса* один молодой сотрудник VI управления обнаружил в архивах австрийской секретной службы интереснейшие документы по криптоанализу. Эта находка напомнила Вильгельму Хеттлю, другому молодому сотруднику этого управления, о славных делах австро-венгерских криптоаналитиков в Первую мировую войну. Узнав, что генерал Фигль, бывший глава австрийской дешифровальной службы, в 1938 г. был арестован и содержится в тюрьме, Хеттль добился от начальника VI управления освобождения Фигля и назначения его преподавателем криптоанализа на специально оборудованную для занятий виллу в Берлине. Здесь Фигль передавал свой опыт новому поколению немецких криптоаналитиков.

* Аншлюс — аннексия Австрии Германией в 1938 г.

Однако подготовка криптоаналитических кадров требовала времени, а пока информация, полученная путем дешифрования, поступала в VI управление из других источников. Однажды его сотрудникам каким-то образом удалось достать испанский код, который потом использовался для чтения шифрперехвата. Кое-что само плыло в руки. Во время хирургической операции в одном из берлинских госпиталей пациент под наркозом вдруг заговорил о необходимости сменить шифр и несколько раз выкрикнул: «Почему Москва не отвечает?» Врач-хирург поспешил в компетентные органы и сообщил о случившемся. Обнаруженная в результате вражеская агентура насчитывала в общей сложности шестнадцать человек, включая и свежепрооперированного радиста. Вскоре после этого пришла еще одна удача: глава японской шпионской сети в Европе предложил продать оптом действующие коды югославского генерального штаба, а также дипломатических служб Бразилии, Ватикана, Португалии и Турции. Предложение было немедленно принято.

С необходимостью применять в своей деятельности криптоаналитические методы Шелленберг, которому в начале 40-х годов было суждено возглавить VI управление, впервые столкнулся еще в 1938 г., когда во время аншлюса ему пришлось выполнять задание по аресту начальника разведывательного отдела австрийского генерального штаба полковника Ронге. При просмотре документов, захваченных во время ареста Ронге, по свидетельству самого Шелленберга, «для получения интересных результатов пришлось прибегнуть к помощи дешифровщиков»

В июле 1940 г. в Мадриде Шелленберг имел возможность ознакомиться с работой военного сектора посольства Германии, который включал сотни служащих, образуя одно из самых крупных немецких шпионских подразделений за границей. Они размещались в посольском здании и активно занимались дешифрованием перехваченных сообщений, пользуясь исключительно благоприятным географическим положением Испании для осуществления перехвата с ее территории. В результате Шелленберг пришел к однозначному выводу о том, что для повышения эффективности операций VI управления требуется, во-первых, установление контроля над всей системой почтово-телеграфной связи Германии с заграницей, а во-вторых, превращение криптоанализа в одно из главных орудий шпионажа и контршпионажа.

Но это предстояло воплотить в жизнь в будущем. А пока в том, что касалось данных, получаемых с помощью криптоанализа, VI управление продолжало зависеть от Абвера* и Исследовательского отдела Геринга. Например, осенью 1941 г. Шелленберг, ставший к тому времени заместителем начальника VI управления, вынужден был обратиться с просьбой к Гейдриху, возглавлявшему тогда Главное управление имперской безопасности, войти в контакт как с Абвером, так и с Исследовательским отделом, чтобы те нацелили свои средства перехвата на переписку вишистской Франции с Белградом для получения необходимой Шелленбергу информации.

* Абвер — военная шпионская организация гитлеровской Германии.

Гиммлеру давно не нравилась такая зависимость. В марте 1942 г. он послал Шелленберга в загородный дом Геринга, чтобы убедить последнего включить Исследовательский отдел в состав VI управления. Геринг встретил Шелленберга в римской тоге, сандалиях и с маршальским жезлом в руке. Выслушав посланника Гиммлера, он сказал неопределенно: «Хорошо, я поговорю с Гиммлером». После этого разговора ничего не изменилось. Только в 1944 г. Геринг наконец согласился передать свой Исследовательский отдел в подчинение Гиммлеру, включив его в систему Главного управления имперской безопасности. Соответствующие проекты распоряжений и указов о переводе уже были ими оговорены в совместных беседах. Не за горами был момент, когда Гиммлер и Геринг должны были поставить свои окончательные подписи под этими документами. Но так как речь в них шла о реорганизации сложного и обширного аппарата, насчитывавшего несколько тысяч человек, Шелленберг не стал настаивать па скором принятии окончательного решения. «Тысячелетний рейх» уже агонизировал, у его заправил были другие неотложные дела, и практического воплощения план включения Исследовательского отдела в состав VI управления так и не получил.

Став начальником VI управления, Шелленберг тут же создал хорошо финансируемый отдел для проведения исследований в области средств секретной связи. Однако новый отдел не оправдал возлагавшихся на него надежд. Количество информации, добываемой им с помощью криптоанализа было небольшим, и Шелленберг продолжал получать ее преимущественно извне.

Начиная с 1942 г. через каждые три недели глава VI управления регулярно давал у себя дома званые обеды. На них руководители дешифровальных спецслужб — из министерства обороны, из министерства почт, которое вело дешифрование трансатлантических телефонных разговоров, и из Исследовательского отдела — обсуждали последние достижения в области криптоанализа и помогали друг другу советом в решении стоявших перед ними проблем. Представителя отделения «Z» на этих совещаниях у Шелленберга не было, что отражало личную неприязнь и борьбу за власть между Гиммлером с Герингом, с одной стороны, и Риббентропом, с другой.

Шелленбергу принадлежат слова беспримерного выражения благодарности криптоаналитикам от «рыцаря плаща и кинжала»: «Именно сотрудничество и интерес, проявляемые со стороны этих людей ко мне лично, сделали возможным достижение большей части моих успехов в операциях секретной службы».

Шелленберг оплатил часть этой щедрой помощи результатами одной из самых крупных шпионских операций Второй мировой войны, которая получила название «Цицерон». Камердинер английского посла в Анкаре снял восковые отпечатки с ключей к сейфу, где посол хранил секретные документы, которые любил просматривать до поздней ночи. Документы представляли собой, главным образом, открытые тексты шифртелеграмм с пометками о месте и времени зашифрования. Вместо отделения «Z», которое по логике вещей должно было получить их в первую очередь, Шелленберг передал эти тексты своим друзьям из военных дешифровальных подразделений с просьбой незамедлительно заняться вскрытием английского шифра на основе документов, приобретенных у «Цицерона». Лучшие криптоаналитики несколько недель подряд бились над этим

шифром, пока им не удалось разгадать его часть, что позволило узнать лишь малозначительные технические подробности передачи шифртелеграмм из Лондона в английское посольство в Анкаре. Лишь после того, как военные специалисты по криптоанализу потерпели неудачу, с английскими телеграммами ознакомили Кунце и Пашке, но задача вскрытия дипломатического шифра Англии на линии связи Анкара — Лондон не вызвала большого энтузиазма и у них. Дело в том, что англичане перешифровывали свои наиболее важные телеграммы при помощи одноразовых блокнотов, а это делало их чтение маловероятным событием. Операция «Цицерон», явившаяся полным успехом в области агентурного шпионажа Германии, стала не менее полным провалом немецких криптоаналитиков.

В Германии, еще задолго до создания Главного управления имперской безопасности, вопросами шпионажа занимался Абвер. До Второй мировой войны у Абвера не было своей собственной дешифровальной службы. Являясь частью Вермахта, он зависел от военных дешифровальных органов. Органов было четыре: один в верховном главнокомандовании для всех вооруженных сил в целом и по одному в каждом из главнокомандований армии, ВМС и ВВС.

С ростом военной активности росли не только вооруженные силы, но и их дешифровальные органы. По размерам, но не обязательно по эффективности. Сказывалось отсутствие достаточного числа квалифицированных специалистов в этой трудной области, чтобы удовлетворить все потребности. Одних военных дешифровальщиков перебросили для укрепления Исследовательского отдела Геринга, других — в так называемую «Озерную службу» министерства пропаганды, которая занималась перехватом зарубежных передач новостей и поставляла материал для борьбы с пропагандой противника. К середине 1938 г. в немецких дешифровальных службах сотрудников было в восемнадцать раз больше, чем за семь лет до этого, но эффективность их работы явно не соответствовала количественному росту.

Немецкий дешифровальный орган, оказавший наибольшее влияние на ход войны, был самым малочисленным и наименее известным среди аналогичных ему спецслужб. Он подчинялся главному командованию ВМС Германии. Командующий немецким военным флотом адмирал Дениц называл его «Службой наблюдения».

«Служба наблюдения» поддерживала слабый контакт с другими дешифровальными спецслужбами. Тем не менее ее успехи зачастую оказывались более значительными.

Созданная в начале 20-х годов, «Служба наблюдения» через два десятилетия сумела раскрыть некоторые из наиболее секретных шифров английского Адмиралтейства. Это давало возможность немецким подводным лодкам уклоняться от опасных столкновений с флотом Англии, а тяжелым немецким кораблям — избегать случайных встреч с более сильным противником. Только за три месяца 1940 г. благодаря использованию информации от «Службы наблюдения» были потоплены сразу шесть английских подводных лодок.

Данные, полученные «Службой наблюдения», оказали неоценимую и решающую помощь в осуществлении плана оккупации Норвегии. Самая существенная трудность в его реализации состояла в обеспечении безопасного передвижения слабо вооруженных военных транспортов из Германии в Норвегию без помех со стороны мощного английского флота. Узнав от «Службы наблюдения» о военной операции англичан по блокированию поставок железной руды в Германию, немецкий флот нанес отвлекающий удар по участвовавшим в ней английским кораблям. Для их защиты Англия выслала туда остальную часть своих военных кораблей, что позволило немецким транспортам спокойно достичь берегов Норвегии, не боясь крупных морских атак противника.

«Служба наблюдения» продолжала читать шифрованную переписку английского Адмиралтейства и в критическое лето 1940 г., когда Гитлер готовился к операции «Морской лев» — вторжению в Англию. Шпионские данные, полученные в результате криптоанализа, с самого начала Второй мировой войны использовались немцами для оперативного планирования, и главное командование ВМС Германии стало в значительной мере зависеть от них. Но 20 августа, когда Англия уже напрягала все силы, ее Адмиралтейство, догадавшись, наконец, о дешифровании немцами своих шифртелеграмм, сменило шифры.

Главное командование ВМС Германии сразу «оглохло». Один шпионаж с воздуха не мог дать немцам достаточных сведений. Немецкие суда больше не могли по своему усмотрению наносить удары по более крупным английским силам или избегать встречи с ними. Английская военно-морская мощь быстро достигла своего нормального уровня. Главное командование ВМС Германии, никогда не питавшее особо теплых чувств к операции «Морской лев», охладело к ней еще больше. В последующем Гитлер отложил операцию по высадке немецких войск в Англии на неопределенный срок, а значит, навсегда.

Не раз «Служба наблюдения» давала в руки командиров немецких подводных лодок такие сведения, которые ставили их на грань победы. В 1941 г. она читала шифртелеграммы командующего английскими ВМС на западных подходах к Британским островам, адресованные караванам судов, в которых давались указания, как им миновать опасные зоны на подходе к родным берегам. Располагая такой информацией, командование немецкими подводными лодками дислоцировало их с максимальным эффектом.

В январе и феврале 1943 г. «Служба наблюдения» овладела навыками вскрытия английских военно-морских шифрсистем настолько хорошо, что читала даже английский «Доклад о местонахождении немецких подводных лодок», который регулярно передавался в зашифрованном виде по радио командирам караванов, находившихся в море, и в котором сообщались известное и предполагаемое нахождение немецких субмарин. Дениц писал в своем дневнике, что эти «Доклады о местонахождении» имели огромное значение для успешного определения, какими возможностями обладал противник в отношении обнаружения немецких подводных лодок и с какой степенью точности он делал это.

Следующий месяц — март 1943 г. — стал кульминацией битвы за Атлантику. Этот один из самых напряженных моментов Второй мировой войны, когда жизненно важный для Англии морской путь между Старым и Новым Светом был почти полностью перерезан немецким подводным флотом, явился прямым следствием ряда успехов в криптоаналитической работе «Службы наблюдения». Позже штаб английских ВМС констатировал, что «немцы никогда не подходили так близко к полному нарушению коммуникаций между Старым и Новым Светом, как в эти первые 20 дней марта 1943 г.».

Однако ожесточенные сражения Второй мировой войны разворачивались не только в Атлантике или в Европе, но и на далеком африканском континенте.

Американский военный атташе в Каире имел гораздо больше возможностей наблюдать за военными действиями, чем его коллеги в Москве. Полковник Боннер Феллерс, кадровый военный, был назначен на эту должность в октябре 1940 г. Он без устали разъезжал по местным боевым фронтам, изучал тактику и проблемы ведения войны в пустыне. Англичане доверяли ему некоторые из своих не слишком важных секретов, надеясь, что это приведет к улучшению американского снаряжения, поставлявшегося им по ленд-лизу. Феллерс переваривал эту информацию и отправлял ее в Вашингтон в виде объемистых и подробных сообщений. Он писал об английских войсках, их задачах, возможностях и эффективности. Говорил об ожидавшихся подкреплениях и о кораблях со снабжением, которые уже прибыли. Анализировал различные тактические шаги, которые обсуждали с ним англичане, и даже сообщал о планах местных военных операций. И когда его материалы передавались на родину по радио, у них всегда был еще один верный слушатель — Германия. Перехваченные ею шифртелеграммы Феллерса после дешифрования шли прямиком на стол генералу Роммелю, командующему немецким корпусом в Северной Африке. Тот мог оценить их по достоинству.

Полученная через Феллерса информация давала Роммелю гораздо более широкую и четкую картину намерений противника, чем та, которую имел перед собой любой другой немецкий военачальник в течение всей войны. Телеграммы Феллерса представляли собой наиболее заметные кубики той богатой подробностями информационной мозаики, которая была в распоряжении Роммеля и которая помогла ему заслужить прозвище «лис пустыни».

Предупрежденные Феллерсом о планируемой операции английских диверсионных частей по нападению на девять немецких аэродромов, немцы устроили напавшим на них отрядам английских коммандос кровавую резню. Тщательно подготовленная операция провалилась. А на следующий день немецкие самолеты, счастливо избежавшие уничтожения, провели мощные атаки против английского конвоя, шедшего из Александрии на Мальту, потопив три эсминца и два торговых судна. Конвой повернул обратно. Как следствие, подходы с востока к Мальте, служившей базой для английских кораблей, подводных лодок и самолетов, которые наносили удары по конвоям Германии, подвозившим снабжение Роммелю, оказались закрытыми, и ни один англо-американский конвой больше не пытался пройти этим путем. А линии снабжения Роммеля продолжали беспрепятственно действовать.

Стратегическую информацию из телеграмм Феллерса дополняли тактические шпионские данные, которые добывала для Роммеля рота под командованием капитана Зеебома. Она записывала все переговоры, при помощи пеленгации определяла концентрацию войск и танков противника, узнавала дислокацию и наименование частей, изучала английские шифртелеграммы с целью дешифрования. Однако 10 июня 1942 г. рота Зеебома оказалась на пути танкового удара англичан, сам Зеебом был

убит, большая часть его роты уничтожена или взята в плен, многие ее архивы попали в руки англичан. Таким образом, Роммель потерял «микроскоп», дававший ему возможность тщательно изучать позиции противника.

Примерно в это же время Роммель лишился и своего «телескопа». Помимо немцев, шифрпереписку Феллерса начали читать англичане. После недели изучения пространных и полных пессимизма посланий американского атташе они уведомили американцев о возможном попадании информации Феллерса в руки противника и о его позиции, несовместимой с должностью. Самому Феллерсу ничего сказано не было, но его вскоре отозвали в Вашингтон. Позднее, в том же году, Феллерс был награжден медалью «За выдающиеся заслуги» за свою работу в качестве атташе. В представлении к награде говоритесь: «Его сообщения военному министерству были образцом точности и честности». Лучше не скажешь. Под этим мог бы подписаться и Роммель.

Новый американский военный атташе в Каире сменил шифр, который выдержал все попытки немцев его раскрыть. Роммель оказался отрезанным от стратегической информации, которой так долго пользовался. Осенью 1942 г. его корпус был разгромлен.

РАЗВЕДЧИКИ И ЦЕНЗУРА

Шифр — это язык разведчиков, а они обычно вынуждены вести свои тайные разговоры шепотом. Успех разведчика, да и сама его жизнь, зависят от умения оставаться незамеченным. Шифрованные сообщения, посылаемые им в явной форме, немедленно привлекут внимание контрразведки. И все же связь разведчику совершенно необходима, иначе его работа будет бесполезной. Поэтому, вместо обычных способов секретной связи, он выбирает наиболее изощренные. Разведчик использует коды, имеющие вид обычных открытых текстов, невидимые чернила, послания микроскопически малых размеров, то есть стеганографические методы, которые скрывают сам факт отправки какого-то сообщения.

Чтобы лишить иностранных разведчиков возможности пользоваться этими методами, при отделениях почтовой и телеграфной связи создаются мощные фильтрующие организации, в задачу которых входит обнаружение и пресечение тайной переписки. Эти фильтры, беспрепятственно пропускающие все безвредные сообщения, представляют собой органы цензуры.

Цензура ведет свою родословную от «черных кабинетов» XVIII века и в демократических странах является порождением войны, а в диктаторских — тирании. В широких масштабах цензура была впервые введена англичанами во время Первой мировой воины и уроки, которые усвоила тогда Англия, она с успехом применила 20 лет спустя, когда вновь принялась фильтровать всю переписку.

В декабре 1940 г. один из сотрудников органа цензуры, который англичане создали на Бермудских островах в просторном отеле «Принцесса», обратил внимание на письмо, отправленное из Нью-Йорка в Берлин. Это письмо вызвало подозрение, так как в нем подробно говорилось о морских перевозках англичан и использовались некоторые выражения (например, при описании вооружения кораблей употреблялось слово «cannon»* вместо «gun»**), которые наводили на мысль, что автором письма был немец. В конце письма стояла подпись: *«Джо К.»*. В результате наблюдения, установленного с целью выявления других писем, написанных этим же почерком, был обнаружен целый ряд посланий, направленных, главным образом, в Испанию и Португалию. Их язык показался цензорам несколько неестественным. Поэтому они попытались установить, не является ли это признаком тайнописи, и по возможности определить подлинное содержание писем.

* «Пушка»
** «Орудие»

Среди этих цензоров была Надя Гарднер, молодая женщина с упорным характером, которая пришла к выводу, что в письмах использовались невидимые чернила. Традиционные проверки с помощью химикалиев, которые выявляют обычные симпатические чернила, дали отрицательные результаты. Но Надя не отступила. По ее просьбе химики произвели проверку с помощью паров йода (этот метод был изобретен еще в Первую мировую войну), и, к их удивлению, на оборотной стороне листов писем действительно проступила тайнопись: «Англичане имеют в Исландии около 70 тысяч солдат. Пароход «Билль де Пьеж» потоплен приблизительно 14 апреля. Спасибо... 20 ноября 1940 г. 20 самолетов «Б-17» были переданы Англии армией США...» Эти послания были написаны раствором пирамидона, который часто применяется как лекарство от головной боли и продается почти в любой аптеке.

Однако личность их отправителя установить не удалось. На письмах не было обратного адреса, да и вряд ли подпись *«Джо К.»* содержала подлинное имя и инициал разведчика. Наконец, в одном из писем Джо К. английская цензура прочитала, что 18 марта какой-то «Фил» был смертельно ранен в автомобильной катастрофе в Нью-Йорке и скончался в больнице. Сотрудники ФБР быстро выяснили, что пострадавший был более известен под именем Хулио Лидо и что, по показаниям свидетелей, после катастрофы сопровождавший Лидо человек схватил принадлежавший ему портфель и скрылся. В ФБР вскоре обнаружили, что Хулио Лидо по-настоящему звали Ульрихом Остеном и что автором писем Джо К. был некий Курт Людвиг, который родился в Огайо, но воспитывался в Германии и приехал в США в марте 1940 г. для создания разведывательной организации. При аресте у Людвига было обнаружено несколько бутылок пирамидона.

Другой немецкий разведчик, выловленный английской цензурой на Бермудах, получил смертный приговор. В ноябре 1941 г. у бдительного цензора вызвал подозрение почерк письма, написанного по-испански и отправленного из Гаваны в Лиссабон. Он подверг это письмо обычной проверке с целью обнаружения симпатических чернил. Предположение цензора подтвердилось: было найдено длинное сообщение, в котором перечислялись суда, грузившиеся в порту Гаваны, и затрагивался вопрос о строительстве на Кубе военного аэродрома. Всем цензорам было дано задание разыскивать письма с таким почерком. Вскоре был выявлен подлинный адрес их отправителя в Гаване, написанный симпатическими чернилами. 5 сентября 1942 г., накопив достаточное количество улик, американская полиция арестовала некого Гейнца Лунинга. Он был послан в Гавану из Германии в сентябре 1941 г. Из отправленных им в Европу 48 писем английские цензоры перехватили все, кроме пяти. 9 ноября 1942 г. Лунинг был расстрелян за шпионаж.

После нападения Японии Соединенные Штаты создали собственный орган цензуры. Вскоре его штат насчитывал около 15 тысяч сотрудников, которые размещались в 90 зданиях по всей стране, проверяли ежедневно около миллиона писем, подслушивали бесчисленное множество телефонных разговоров, просматривали кинофильмы, газеты, журналы и знакомились со сценариями радиопередач. Миллионы американцев получали письма в конвертах со следами ножниц цензора и штампом «Вскрыто цензурой».

Чтобы перекрыть максимальное число стеганографических каналов связи, американская цензура категорически запретила отправление по почте целого ряда сообщений. Были отменены шахматные матчи по переписке. Из писем вымарывались кроссворды, так как у цензоров не хватало времени решать их, чтобы проверить, не содержат ли они тайные послания. Из почтовых отправлений изымались газетные вырезки, потому что они могли содержать секретный текст. Не разрешалось пересылать по почте табели успеваемости учащихся. Одно письмо с инструкциями по вязанию было задержано до тех пор, пока цензор не связал по ним свитер, чтобы проверить, не содержат ли они какой-либо скрытой информации. В каждом цензурном отделении имелся запас марок: цензоры снимали подозрительные марки и заменяли их другими того же достоинства, но с иным номером и рисунком. Чистая бумага, которую жители США часто посылали своим родственникам, проживавшим в странах, где не хватало бумаги, также заменялась из соответствующих запасов, чтобы исключить применение симпатических чернил. Конфисковывались даже детские рисунки, которые родители слали дедушкам и бабушкам, так как среди этих рисунков могли попасться закодированные карты или схемы.

Согласно правилам, установленным американской цензурой для телеграфа, запрещалось посылать любой текст, который был непонятен цензору. Иногда цензоры специально перефразировали сообщения. Эта практика вызвала к жизни классический анекдот, родившийся еще в годы Первой мировой войны. К цензору на стол попала телеграмма следующего содержания: «Отец умер». Цензор немного подумал, вычеркнул «умер», написал «скончался» и отправил телеграмму по адрес) Вскоре после этого на стол к цензору поступила ответная телеграмма с вопросом: «Отец умер или скончался?»

Телеграммы с заказами на цветы («Вручите субботу моей жене три белые орхидеи») предоставляли настолько удобную возможность для передачи секретной информации, что цензоры запретили указывать в них названия цветов и день вручения. Ни одна американская фирма не могла пользоваться собственным телеграфным кодом без разрешения цензуры. Под давлением англо-американских союзников Аргентина, которая не порвала дипломатических отношений с Германией, наложила запрет на передачу кодированных сообщений. Примеру Аргентины и США последовала нейтральная Швеция, которая требовала предоставления копий используемых кодов и не разрешала применять шифрование. Лишь в Швейцарии отсутствовали любые ограничения в отношении пользования кодами или шифрами.

Меры предосторожности принимались также в отношении средств массовой информации. Газеты должны были проявлять осторожность при публикации различных объявлений. Были взяты под контроль коммерческие радиостанции, поскольку с их помощью можно было быстро и без труда передавать условные сигналы для подводных лодок или агентов противника, что весьма наглядно продемонстрировал один офицер военной разведки за год до Перл-Харбора. Он ухитрился передать условным языком следующее тайное сообщение: «Подводной лодке «S-112»: лайнер «Куин Элизабет» отправляется сегодня в Галифакс, имея на борту несколько сот самолетов». Ни диктор, прочитавший текст на условном языке, ни директор радиостанции, ни тысячи радиослушателей даже и не подозревали, что за сообщение было услышано ими по радио.

Служба цензуры отменила телефонные и телеграфные заказы на исполнение по радио тех или иных музыкальных произведений, а выполнение заявок, присланных по почте, велела задерживать на неопределенное время. Эти меры должны были исключить возможность передачи сообщения для подводных лодок противника с помощью модной песенки. Аналогичные меры были приняты в отношении передачи радиостанциями объявлений личного характера.

Первичная проверка писем происходила в местных отделениях цензуры. Самое крупное из них занимало огромное здание в Нью-Йорке. Около 4,5 тысячи его сотрудников просматривали лавины почты, которые ежедневно поступали на их столы. Они изымали все, что могло нанести ущерб военным усилиям США и их союзников, тщательно разыскивая какие-либо признаки наличия секретных посланий. Подозрительный финансовый отчет давали на просмотр сотруднику, знающему бухгалтерию. Садовод-любитель мог точно сказать, насколько соответствовало действительности письмо об устройстве грядок для тюльпанов.

Один из сотрудников нью-йоркского отделения цензуры обратил внимание на письмо из Германии, в котором говорилось, что Гертруда добилась выдающихся успехов в плавании, и перечислялись ее победные результаты. Сотрудник проконсультировался со знакомым любителем плавания, и тот ответил, что подобных результатов человек достичь не в состоянии. В ходе дальнейшего расследования было установлено, что в действительности речь шла о скорости нового американского истребителя и что его характеристики разболтал хвастливый работник военного министерства.

В политическом отделении цензоры отфильтровывали данные о местонахождении запасов стратегических материалов военного назначения, чтобы предотвратить их приобретение Германией и ее союзниками. Экономическое отделение перехватывало информацию о нехватках продовольствия и других товаров. Письма на неизвестных языках направлялись в лингвистическое отделение, которое располагало переводчиками с редких языков.

После первичного просмотра все письма со странными формулировками, пометками или с другими подозрительными особенностями направлялись в отдел безопасности. В нем имелось два отделения: лингвистические стеганограммы попадали в отделение кодов и шифров, а технологические — в лабораторное отделение.

Лингвистические стеганограммы подразделяются на две основные категории: условное письмо и семаграммы. Существуют три вида условного письма: жаргонный код, пустышечный шифр и геометрическая система.. В жаргонном коде внешне безобидное слово имеет совершенно другое реальное значение, а текст составляется так, чтобы выглядеть как можно более невинно и правдоподобно. Сначала он может содержать лишь упоминание об обоюдно известных событиях и лицах: «Я посетил человека, с которым вы обедали на прошлой неделе». А далее может идти отрезок текста, понятный только адресату, как, например, когда один преступник сообщает об аресте другого: «Этот человек попал в больницу», вместо слова «тюрьма» используя слово «больница».

Цензура противопоставляет этим уловкам повышенное внимание к искусственным оборотам и тяжелым фразам, а также здоровый скептицизм по отношению к существу вопроса. Вот один известный случай со вскрытием жаргонного кода времен Первой мировой войны. У одного английского цензора вызвали подозрения слишком крупные ежедневные телеграфные заказы на сигары (главным образом — из портовых городов Англии) от «двух голландских дельцов». Однажды из Портсмута они заказали 10 тысяч сигар «Корона». На следующий день из Плимута они потребовали крупную партию более дешевых сигар. Затем в течение одной ночи в заядлых курильщиков превратились все жители Ньюкасла. Казалось, все население прибрежных районов Англии внезапно почувствовало непреодолимую тягу к курению — так чудовищно возрос спрос на сигары. По предложению цензора была предпринята проверка. «Двое голландских дельцов» оказались немецкими разведчиками, а их заказы — условным письмом, в котором заказ на 5 тысяч сигар для Ньюкасла означал, что в этом порту находятся пять крейсеров. 30 июля 1915 г. оба

немецких разведчика были расстреляны.

До тех пор, пока жаргонный код не привлекает к себе внимания, он вполне надежен. Однако его почти всегда удается вскрыть вскоре после обнаружения. Как ни парадоксально, но чем менее подозрительно внешнее содержание жаргонного кода, тем легче он поддается вскрытию. Ибо чем больше жаргонный код перегружен всякими правдоподобными подробностями, тем больше он содержит данных, которые могут быть использованы для раскрытия его подлинного смысла.

Так, во время Второй мировой войны от внимания американской цензуры не ускользнула целая серия писем, в которых проявлялся вполне законный, хотя и несколько нездоровый интерес к куклам. Эти письма возбудили подозрение после того, когда одно из них вернулось из Буэнос-Айреса с пометкой «адресат не обнаружен» и было возвращено женщине, проживавшей в городе Портленде в штате Орегон и значившейся как отправитель. Не имея никакого отношения к этому письму, она передала его в ФБР. В письме говорилось: «Я только что приобрела чудесную сиамскую танцовщицу. Она была повреждена — порвана посередине. Но сейчас ее починили, и я просто обожаю ее. Я не могла найти пару этой танцовщице и поэтому переодеваю обыкновенную маленькую куклу — она изображает другую сиамскую куклу». После этого цензоры перехватили еще несколько писем о куклах, написанных в том же легкомысленном женском стиле с большим количеством ошибок: «Сломанная кукла в юбке из гавайской травы будет полностью починена к первой неделе февраля» и «Сломанные английские куклы будут полностью починены в мастерской лишь через несколько месяцев. Мастерская работает круглосуточно».

Криптоаналитики отделения кодов и шифров установили, что на жаргонном коде «куклы» означали «военные корабли», причем каждый вид кукол соответствовал определенному классу кораблей. Подлинное значение невинной болтовни оказалось довольно серьезным: «Я только что получила информацию о первоклассном авианосце. Он был торпедирован в средней части. Но теперь его отремонтировали. Другого авианосца пока в наличии нет, и поэтому еще один корабль переоборудуют в авианосец», «Повреждения легкого крейсера «Гонолулу» будут полностью ликвидированы к первой неделе февраля» и «Поврежденные английские военные корабли будут полностью отремонтированы на судоверфи лишь через несколько месяцев. Судоверфь работает круглосуточно». Отправительницей этих писем оказалась некая Элизабет Дикинсон, которая содержала дорогой кукольный магазин в Нью-Йорке. Она любила все японское и поддерживала знакомство с некоторыми известными японскими дипломатами. Элизабет Дикинсон предъявили обвинение в шпионаже, грозившее смертным приговором. Однако дело кончилось тем, что ей разрешили признать себя виновной в менее серьезном преступлении — в нарушении правил цензуры военного времени путем незаконного использования кодов в международной переписке. Элизабет Дикинсон была приговорена к 10 годам тюремного заключения и к штрафу в 10 тысяч долларов.

Самое знаменитое из сообщений с использованием жаргонного кода содержало сведения о дне высадки англо-американских союзников в Нормандии. Немцы перехватили его, поняли смысл и... проигнорировали.

Другим видом условного письма является пустышечный шифр. При его применении в тексте имеют значение лишь некоторые определенные буквы или слова. Например, читаются каждое пятое слово или первая буква каждого слова, в то время как все остальные буквы или слова служат в качестве «пустышек» для сокрытия значимого текста. Пустышечные шифры обычно выглядят еще более искусственно, чем жаргонный код. Даже если взять для примера два самых удачных сообщения, отправленных немцами во время Первой мировой войны, то оба они имеют «странный» вид, столь характерный для подобных посланий.

Первое из них выглядело так: «President's embargo ruling should have immediate notice. Grave situation affecting international law. Statement foreshadows turn of many neutrals. Yellow journals unifying national excitement immensely»*. Читая только первые буквы слов, получаем: «Pershing sails from N.Y. June I»**.

* «Следует обратить внимание на решение президента относительно эмбарго. Создается серьезное положение, затрагивающее международное право. Это заявление предвещает разорение многих нейтралов. Желтая пресса чрезвычайно подогревает всеобщее возбуждение».

** «Першинг отправляется из Нью-Йорка 1 июня»

Другое сообщение, посланное для подтверждения первого, имело то же самое содержание, но читать его надо было по вторым буквам слов: «Apparently neutrals' protest is thouroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on byproducts, excluding suets and

vegetable oils»*.

* «Очевидно, протест нейтралов совершенно не принимается во внимание и игнорируется. Исмэн сильно пострадал. Проблема блокады создает предлог для эмбарго на побочные продукты, исключая нутряное сало и растительное масло»

Кто бы ни был отправителем этих сообщений, он зря потратил свою изобретательность, поскольку Першинг* фактически отбыл из Нью-Йорка 28 мая.

* Першинг Джон — американский генерал, командующий армиями США и союзников в Первой мировой войне.

Во время Второй мировой войны пустышечные шифры в большинстве случаев применяли не шпионы, а вполне лояльные американцы, которые не могли устоять перед искушением «надуть» цензора. Особенно часто этим занимались военнослужащие, которые пытались сообщить о своем местонахождении семьям, которые ничего не знали о том, где находится их родственник.

Одна такая система, несмотря на свою примитивность, привела получателей сообщения в состояние полного недоумения. Молодой американский солдат, пользуясь заранее условленной системой переписки со своими родителями, пытался довести до их сведения, что находится в Тунисе. Для этого в пяти письмах домой в качестве второго инициала своего отца он использовал сначала «Т», затем «У», «Н», «И» и «С». К несчастью, эти письма были получены в другом порядке, а беспечный солдат забыл проставить на письмах даты. Обезумевшие родители написали ему, что они перерыли весь свой атлас, но нигде не смогли найти «Нутси»! В 1943 г. подобные попытки настолько участились, что руководству ВМС США пришлось предупредить моряков о том, что пользование «семейными кодами» может привести к суровому наказанию.

Третьим видом условного письма является геометрическая форма. При ее применении имеющие значение слова располагаются на странице в определенных местах или в точках пересечения геометрической фигуры заданного размера. В XVII веке Джон Тревэнион*, ожидавший неминуемой казни от рук сторонников Кромвеля**, получил письмо, которое было тщательно изучено его тюремщиками, прежде чем было передано ему в руки. Прочитав в этом письме каждую третью букву после каждого знака препинания, он узнал, что «в восточной стене часовни открывается одна панель». Во время вечерни Тревэнион сбежал.

* Тревэнион Джон — сторонник английского короля Карла I, свергнутого в 1649 г.

** Кромвель Оливер — английский политический и военный деятель времен буржуазной революции XVII в.

Другой пример. В период Второй мировой войны пленные немецкие офицеры-подводники в своих письмах домой посылали тайные сообщения, делая небольшие пробелы после каждой значимой буквы. Один бдительный английский цензор заметил, что эти маленькие пробелы попадаются в самых неестественных местах, даже в середине слогов. Оказалось, что в своих скрытых посланиях немцы сообщали о тактике, применявшейся англо-американскими союзниками в борьбе с немецкими подводными лодками, а также об их технических недостатках.

Вторую категорию лингвистических стеганограмм составляют семаграммы — тайные сообщения, в которых шифробозначениями являются любые символы, кроме букв и цифр. Эти сообщения могут быть переданы, например, в рисунке, содержащем точки и тире для чтения по коду Морзе. Однажды в нью-йоркском цензорном отделении перевели все стрелки в предназначенной для отправки партии часов, опасаясь, что их положение может заключать в себе какое-то сообщение.

Исследование сообщений, скрытых лингвистическими средствами, или, точнее, подозрительных в этом отношении, является весьма мучительным процессом. Часто криптоаналитик не может даже сказать, скрывается ли какое-либо содержательное сообщение за неуклюже составленным или просто безграмотным текстом. И даже если он совершенно уверен, что такое сообщение там спрятано, найти его зачастую просто невозможно. Обычно в распоряжении цензора имеется всего одно сообщение, а вероятные слова, на которые можно опереться при криптоанализе, отсутствуют начисто. В начале Второй мировой войны американской цензуре даже рекомендовалось не работать над предполагаемой криптограммой свыше получаса, исходя из того, что, если за это время криптоаналитик не вскрыл ее, он вообще никогда ее не прочтет. Эти непрочитанные сообщения

представляли собой трудную проблему для цензоров. В них могла содержаться важная секретная информация, и тогда их не следовало отправлять дальше по адресу. Но пока подозрительное послание не было дешифровано, вина его отправителя оставалась недоказанной. Тем не менее иногда письма специально задерживали или видоизменяли, чтобы предполагаемая тайная информация не дошла до адресата.

Технологическая стеганография сводится почти исключительно к применению невидимых чернил. Это воистину древнее изобретение. Плиний Старший* в своей «Естественной истории», написанной им в I веке до нашей эры, рассказывает, каким образом можно использовать сок растений из семейства молочаев в качестве симпатических чернил. Овидий** упоминает о них в книге «Искусство любви». Несколько видов симпатических чернил описывает Калкашанди. Упоминает о них и Альберта. Порта посвятил вопросу о невидимом письме отдельную книгу.

* Плинии Старший — римский ученый, погиб, наблюдая извержение вулкана Везувия.
** Овидий — римский поэт, живший и творивший в 1 в до нашей эры.

Невидимые чернила бывают двух видов — органические жидкости и симпатические химикалии. Первые, к которым относятся моча, молоко, уксус и фруктовые соки, становятся зримыми в результате незначительного нагревания. Несмотря на давнюю известность и слабую стойкость, они настолько удобны, что применялись даже во время Второй мировой войны. Граф Вильгельм Рауттер, американец немецкого происхождения, занимавшийся шпионажем в пользу родной Германии, был вынужден использовать мочу, когда у него кончился запас невидимых чернил.

Симпатические чернила представляют собой химические растворы, бесцветные после высыхания, но реагирующие на обработку другим химикалием (реагентом) и образующие видимое соединение. Например, если разведчик пишет железным купоросом, то текст невидим, пока его не обработают раствором цианата калия, после чего образуется «берлинская лазурь» — вещество, обладающее очень красивым цветом. Искусство изготовления хороших чернил для тайнописи состоит в том, чтобы найти вещество, которое реагировало бы с минимальным количеством химикалиев (лучше всего — лишь с одним).

Во время Второй мировой войны американские цензоры «полосовали» письма, чтобы выявить наличие в них невидимых чернил. Лаборант водил по письму несколькими щетками, закрепленными в одном держателе и смоченными в растворах различных проявителей. Эти проявители обладали различными свойствами и реагировали даже на выделения человека, так что после обработки на бумаге появлялись отпечатки пальцев и капли пота.

Письма также проходили проверку в инфракрасных и ультрафиолетовых лучах. Текст, написанный крахмалом и невидимый при дневном или электрическом свете, начинал светиться под воздействием ультрафиолета. Инфракрасные лучи помогали различать цвета, неотличимые при обычном освещении. Например, зеленые надписи на зеленой почтовой марке.

Местные отделения американской цензуры подвергали проверке все подозрительные письма, а также проверяли наугад некоторую часть обычной почты. Иногда в течение недели они профильтровывали всю исходящую и входящую переписку какого-либо города. За время войны в ФБР было передано более 4,5 тысячи подозрительных писем. 400 из них представляли определенную оперативную ценность.

Проблемы, в которых местные отделения не могли разобраться своими силами, передавались в лабораторию отдела безопасности. Одна из таких проблем заключалась в том, что немецкие агенты расслаивали лист бумаги пополам, писали текст невидимыми чернилами на внутренней поверхности, а половинки затем вновь соединяли между собой. Поскольку чернила оказывались внутри листа, никакой реагент, нанесенный на его внешнюю поверхность, не мог их проявить. Эта уловка была обнаружена лишь после того, как один немецкий агент использовал для своего письма слишком много чернил и их избыток просочился сквозь бумагу.

Основная трудность при применении симпатических чернил была связана с невозможностью обеспечить быструю обработку огромного количества информации, которую приходилось передавать разведчикам. Один из способов стеганографирования информации большого объема состоял в том, что специальным раствором отмечались необходимые буквы в какой-либо газете. В обычных условиях эти отметки были невидимы, но при обработке ультрафиолетовыми лучами они начинали фосфоресцировать. Однако поскольку газеты пересылались со скоростью обычной почты, подобный способ едва ли обеспечивал быструю доставку информации к месту назначения.

Тогда немцы применили способ тайнописи, который директор ФБР Гувер назвал «шедевром

немецкой разведки». Это так называемая микроточка — крошечная фотография, на которой с достаточной ясностью воспроизводился текст письма. Известие, полученное в феврале 1940 г. от агента-двойника («Ищите точки, множество маленьких точек»), привело сотрудников ФБР в состояние паники. Они начали лихорадочно разыскивать повсюду признаки появления «маленьких точек». Лишь в августе 1941 г. один лаборант внезапно заметил слабое свечение на поверхности конверта, найденного у человека, которого подозревали в связях с немецкой разведкой. В результате была обнаружена первая микроточка, замаскированная под знак препинания машинописного шрифта.

Микроточки позволили немцам решить проблему передачи большого количества информации. Вскоре в Германию хлынул поток разведывательных данных, замаскированных под сотни точек в телеграммах, любовных письмах, деловых сообщениях, семейных посланиях, а иногда в виде кусочков тонкой фотопленки, наклеенных под марками. Самая первая из обнаруженных микроточек содержала распоряжение немецкому агенту выяснить, «где в США производятся урановые испытания». В Мехико свила гнездо немецкая разведгруппа, которая делала микрофотоснимки американских изданий в области торговли и техники, которые запрещалось вывозить за границу, и отправляла их целыми партиями по тайным адресам в Европе, причем иногда в одном письме было до 20 микроточек. Таким же образом через океан переправлялись украденные технические чертежи и схемы.

Поскольку почтовая и телеграфная связь США находилась под тщательным наблюдением цензоров и имели место непредвиденные задержки отправлений, можно было предположить, что немецкие агенты, в целях более быстрой и скрытной передачи добытой ими информации, будут пытаться выходить в эфир. И здесь США были готовы к отпору. В мирное время отдел радиоразведки федеральной комиссии по связи пристально следил за тем, чтобы на волнах, являющихся государственной собственностью, не допускалось нарушений существующих правил пользования радио. Во время войны его 12 главных и 60 вспомогательных контрольных постов, а также около 90 подвижных станций контролировали весь спектр радиочастот с целью обнаружения радиостанций вражеской агентуры. Эти посты и станции были связаны друг с другом с помощью телетайпов и составляли единую пеленгаторную систему, которая управлялась из Вашингтона. Отдел радиоразведки располагал новейшим радиооборудованием, включая приемник, который всякий раз подавал сигнал тревоги при нахождении нелегального сигнала на любой частоте из огромного диапазона, и «ищейку» — радиопеленгаторный прибор, который умещался в одной руке и предназначался для точного обнаружения места в здании, откуда посылался радиосигнал.

Отдел радиоразведки вполне оправдывал свое назначение, действуя и за пределами США. Его сверхчувствительные антенны принимали тайные переговоры по коду Морзе между другими континентами. Еще до Перл-Харбора операторы контрольного поста в Майами перехватили неясные сигналы радиостанции, работавшей в Лиссабоне, и засекли ее корреспондентов в Западной Африке. Двое криптоаналитиков из отдела радиоразведки, Альберт Макинтош и Абрахам Чекоуэй, сумели вскрыть шифр перестановки, с помощью которого засекречивались передаваемые из Лиссабона сообщения. Их дешифрование показало, что в африканских странах работают немецкие агенты, которые сообщают в Германию буквально обо всем — о судоходстве, о передвижении войск, о политической обстановке и т. д. Когда Макинтош и Чекоуэй прочли шифрованное сообщение из Лиссабона, в котором содержалось неосторожное распоряжение агенту в Западной Африке по кличке Армандо «лично вручить письма» по указанному адресу, судьба большой группы немецких агентов была решена. Несколько недель спустя она была ликвидирована усилиями контрразведки англо-американских союзников.

В начале 1942 г. сотрудники отдела радиоразведки получили от своих английских коллег предложение о сотрудничестве в области слежения за работой немецких дипломатических и разведывательных радиостанций. В ходе совместной работы они установили, что многие подпольные немецкие передатчики ежедневно меняли свои позывные в течение месяца. С наступлением нового месяца этот график смены позывных повторялся вновь. Были заведены каталоги особенностей работы отдельных немецких передатчиков и операторов, чтобы опознавать их в различных сетях связи. Контрразведывательные спецслужбы США и Англии сообщили, как обучаются в разведшколе вблизи Гамбурга немецкие радисты, как записывается их «почерк», чтобы затруднить возможность имитации, как устанавливают они свои рации для обеспечения максимально сильного сигнала и сведения рассеивания к минимуму. В кульминационный момент войны в Европе отдел радиоразведки контролировал более 200 частот, на которых работали вражеские радиостанции, и вскрывал большую часть шифров, которыми пользовались в своих радиопередачах немецкие агенты. Наиболее значительные результаты были достигнуты в Латинской Америке, где ФБР сумело оказать

существенную помощь местным властям в ликвидации шпионских очагов. Отдел радиоразведки отслеживал передачи основных агентурных сетей Германии в Бразилии. Благодаря дешифрованию их криптограмм он помог ФБР выявить там почти всех немецких агентов.

Но эти достижения американцев были лишь невинными забавами по сравнению с величайшим «радиообманом», который удалось осуществить немцам. Они нарекли его «funkspiel» («функшпиль»), и лучшего названия придумать было невозможно. Слово «funk» по-немецки означает «радио», а «spiel» — «игра» или «спектакль», но может иметь и такие оттенки значения, как «забава», «спорт» и «матч».

Руководителем радиоигры, которая принесла самые потрясающие результаты за всю Вторую мировую войну, был 46-летний майор Герман Гискес, родившийся на Рейне и прослуживший большую часть своей жизни в немецкой армии. Гискес возглавлял нидерландский отдел контрразведывательной секции Абвера. И хотя Абвер располагал собственными эффективными подразделениями радиоразведки, Гискес предпочел использовать для своего «функшпиля» радиоконтрразведывательную секцию оккупационной полицейской службы — функабвер.

Немцы сделали первые ходы в большой радиоигре, когда завербовали обрюзгшего, хромого и вечно потного голландца по имени Георг Риддерхоф, который стал их агентом. Такие агенты, притворяясь патриотами, внедрялись в голландское подполье и добывали для немцев необходимую информацию. В течение нескольких месяцев Риддерхоф безуспешно старался втереться в доверие к голландским бойцам Сопротивления, работавшим в Гааге.

Тем временем в функабвере регулярно перехватывали и дешифровывали сообщения, посылавшиеся 5 раз в неделю подпольным радиопередатчиком с позывными «UBX». Радиопеленгаторы постепенно нащупывали этот передатчик, и вскоре были захвачены радист и его помощник, а вместе с ними — передатчик и материалы разведывательного характера.

Это был первый крупный успех Абвера в Голландии, и Гискес тотчас же стал думать над тем, каким образом можно было бы «реанимировать» «UBX» для ведения радиоигры, которая сулила весьма значительные выгоды. Если бы немцы взяли на себя руководство работой радиостанции, которую англичане все еще считали передающей сообщения от имени голландских подпольщиков, Абвер заполучил бы множество сведений о намерениях противника из инструкций, присылаемых из Лондона. Он смог бы использовать эту информацию для противодействия военным усилиям англичан, а также для ликвидации других групп Сопротивления. Абвер снабжал бы английскую разведку дезинформацией, надеясь, что в результате провала планов, построенных на этой дезинформации, английское командование утратит доверие к своей разведке. Со своей стороны голландские подпольщики хорошо знали об опасностях радиоигры и, чтобы воспрепятствовать немцам, устанавливали мины-ловушки в передающей аппаратуре и у дверей в помещения, откуда вели свои радиопередачи, а также оставляли на столах «недопитые» бутылки с отравленным вином.

Но «UBX» оказалось не так-то просто «реанимировать». Отсутствовали некоторые важные детали, необходимые для того, чтобы сделать «реанимацию» правдоподобной, а радист отказался сообщить их на допросе. Были захвачены еще две нелегальные радиостанции, однако попытки «реанимировать» их также были безуспешными. Эти неудачи только разожгли стремление Гискеса добиться успеха.

В январе 1942 г. у Гискеса появились некоторые надежды. Риддерхоф сообщил, что подпольная группа, в которую он внедрился, должна получить из Англии оборудование, которое будет сброшено на парашюте, и что об этом была достигнута договоренность по радио. На донесении Риддерхофа Гискес с раздражением написал: «Идите вы с вашими сказками на Северный полюс. Между Голландией и Англией никакой радиосвязи нет». Однако несколько дней спустя функабвер засек обмен сообщениями между радиостанцией с позывными «RLS» на юге Голландии и другой радиостанцией с позывными «PTX» севернее Лондона, откуда осуществлялась связь со многими подпольными радиостанциями в Европе. Риддерхоф подтвердил, что «RLS» входит в его подпольную группу. Связной Риддерхофа, докладывая об этом Гискесу, лукаво упомянул о его реплике про «Северный полюс». Гискес рассмеялся и предложил назвать предстоящую радиоигру «Северный полюс».

Радиостанция «RLS» была немедленно взята под тщательное наблюдение. Вскоре функабвер установил порядок ее работы в эфире, а радиопеленгаторы засекли передатчик, работавший в одном из домов на улице Фаренгейт в Гааге. Риддерхоф поставлял для этой радиостанции как ложные, так и достоверные данные. Например, информацию о том, что немецкий крейсер «Принц Евгений» находится в порту города Шейдама. В результате в течение месяца Гискес собрал достаточное количество материала по «RLS», чтобы приступить к долгожданному «функшпилю».

6 марта 1942 г. в 6 часов вечера 4 замаскированных полицейских автомобиля блокировали дом на улице Фаренгейт. Гискес рассчитывал накрыть передатчик, прежде чем он выйдет на связь, чтобы помешать радисту сообщить в Лондон о провале. Но радист, предупрежденный домовладельцем о том, что около дома появились несколько автомашин с людьми, прервал передачу и, прихватив с собой 3 неотправленные шифровки, попытался скрыться. Он был схвачен в нескольких метрах от дома. Ворвавшись в его квартиру, полиция обнаружила чемоданчик с рацией и документами около черного хода, куда их отнесла жена домовладельца.

Началась игра в кошки-мышки. При обучении в английской разведшколе радиста Хьюберта Лоуэрса инструктировали, что немцы попытаются (сначала уговорами, а затем и пытками) добиться от него сотрудничества, чтобы в Англии не смогли догадаться о провале по внезапной смене его почерка. И поскольку было желательно, чтобы Лоуэрс избежал пыток и не выдал действительно важных сведений, ему было приказано притвориться, что он согласен сотрудничать, предупредив при этом Лондон об аресте и компрометации рации. Лоуэрс должен был послать предупреждение путем изъятия из своих радиопередач специального контрольного сигнала. Этот сигнал должен был включаться в каждое сообщение для удостоверения его подлинности. Если в принятом сообщении контрольный сигнал отсутствовал или был передан неправильно (можно было ожидать, что немцы не хуже своих противников знают о необходимости присутствия такого сигнала в радиопередаче), это должно было насторожить Лондон.

Тогда англичане могли бы начать двойную радиоигру. Немцы считали бы, что они дурачат англичан, снабжая их ложными данными и выкачивая из них достоверную информацию, а англичане били бы немцев их собственным оружием и поставляли бы им дезинформацию, а сами бы делали выводы об истинных планах немцев, изучая те ложные данные, которые немцы посылали в Лондон. Этот колоссальный «обман обманщиков», эта радиоигра против радиоигры, эти честолюбивые мечты первоклассных разведчиков могли бы стать реальностью, если бы в радиопередачах Лоуэрса своевременно было замечено отсутствие контрольного сигнала.

Немцы начали склонять Лоуэрса к сотрудничеству даже еще до того, как они увезли его с улицы Фаренгейт. Начальник подразделения функабвера лейтенант Хейнрикс заявил, что может прочитать все три шифровки, найденные у Лоуэрса. Лоуэрс впоследствии вспоминал: «Он* хотел дать мне возможность спасти свою жизнь путем добровольного раскрытия подробных деталей моего шифра и добавил, что, сделав это, я избавлю его от лишних хлопот. Я счел благоразумным согласиться на это предложение и обещал, что я исполню его желание, если ему удастся дешифровать хотя бы одно из 3 сообщений, найденных у меня. К моему удивлению, он тотчас же согласился, сел за стол, глубоко задумался и минут через 20 торжествующе воскликнул: «Все ясно! «Крейсер «Принц Евгений» стоит в Шейдаме» — ведь так?» Это была информация, исходившая от Риддерхофа. Хейнрикс использовал ее как подсобный материал для вскрытия шифра.

* Лейтенант Хейнрикс.

Удивленный этой демонстрацией всезнания Лоуэрс сдержал свое обещание относительно передачи подробных сведений об используемом шифре, однако «забыл» упомянуть о своем контрольном сигнале. В конце допроса Гискес неожиданно спросил Лоуэрса: «А какую ошибку вы должны сделать?» Контрольный сигнал Лоуэрса состоял в том, что он должен был преднамеренно сделать ошибку в 16-м знаке открытого текста. Эта ошибка должна была быть такой, что ее ни при каких обстоятельствах нельзя было совершить в результате случайного добавления или пропуска одной точки или одного тире по международному коду Морзе. То есть вместо «s» («...») нельзя было поставить «i» («..») или «h» («....»), а надо было передать, например, «t» («-»).

Однако случилось так, что в двух из трех захваченных сообщений 16-й буквой была «о» в слове «stop»*. Лоуэрс вместо «о» («- - -») в одном случае поставил «i» («..»), а в другом — «е» («.»). Это удачное совпадение дало ему возможность придумать ложный контрольный сигнал, который не противоречил тому, что было известно Гискесу. Лоуэрс сказал, что в соответствии с этим сигналом в каждом сообщении следует слово «stop» один раз заменить словом «step» или «slip».

* «Стоп»

Немцы приняли слова Лоуэрса за чистую монету. Они так и не заметили, что ни третье из захваченных сообщений, ни перехваченные ранее сообщения не удовлетворяли этому условию. А может, они посчитали, что Лоуэрс просто допустил ошибки.

Лоуэрс дал согласие работать на передатчике «RLS», причем он сам должен был зашифровывать сообщения, чтобы вставлять в них контрольный сигнал. Лоуэрс был уверен, что голландское отделение Управления специальных операций* (УСО) обратит внимание на отсутствие контрольного сигнала и примет соответствующие меры.

* Управление специальных операций — английская спецслужба, в годы Второй мировой воины руководившая работой подполья в Европе.

Первый радиосеанс с участием Лоуэрса состоялся 12 марта в 2 часа дня. Лоуэрс отправил шифровки, которые он не успел радировать в Лондон 6 марта. Контрольный сигнал в этих сообщениях был, разумеется, подлинным, поскольку в них содержалась правдивая информация, которую Лоуэрс так или иначе должен был передать. В следующем сообщении «RLS» по указанию Гискеса попросила, чтобы подготовленный ранее выброс снаряжения с парашютом был произведен в другом районе, чем это было оговорено ранее. 25 марта УСО сообщило о своем согласии, а еще два дня спустя передало предупреждение о выбросе. Это был критический момент. Контрольный сигнал УСО был подлинным, способ зашифрования также не вызывал никаких сомнений. Может быть, англичане придумали какую-то ловушку? Вместо обещанного снаряжения самолет доставит бомбы, и на воздух взлетят не только надежды Абвера на радиоигру, но и несколько самих абверовцев. Лоуэрс, рассчитывавший, что в УСО обнаружат его ложный контрольный сигнал, надеялся, что так оно и произойдет.

27 марта Гискес и группа абверовцев укрылись в кустах можжевельника на болоте. Вскоре после полуночи послышался шум самолета, направлявшегося к треугольнику, образованному красными и белыми световыми сигналами. За его хвостом показались 5 больших темных предметов, устремившихся к земле. Сброшенные на парашютах большие черные ящики приземлились с глухим стуком. Самолет мигнул полетными огнями, повернул на запад и исчез в тумане. Немцы радостно пожали друг другу руки. Первый успех был достигнут.

А как же контрольный сигнал? Почему же он не сработал? Из-за глупости и нерадивости сотрудников УСО, у которых было единственное оправдание — слабость агентурных передатчиков и низкая квалификация подпольных радистов. Вследствие этого сообщения подпольщиков очень редко принимались без искажений и помех. В некоторых случаях шифровальщики голландского отделения УСО вообще не могли установить, сделана ли данная ошибка преднамеренно, чтобы подтвердить контрольный сигнал, или же это обычное искажение. От 5 до 15% получаемых сообщений были настолько исковерканы, что читавшие их шифровальщики были рады, если им вообще удавалось прочитать открытый текст. В этих случаях ни о каких опознавательных сигналах не могло быть и речи. Но даже если сделать скидку на тяжелые обстоятельства, все равно небрежность сотрудников УСО была преступной. В огромном большинстве случаев, когда не было никаких сомнений в отсутствии контрольного сигнала, сообщения все равно принимались как достоверные. Некоторые из них были даже специально помечены: «Опознавательный сигнал отсутствует», однако УСО почему-то их не браковало. Таким образом, в результате пренебрежения к мерам предосторожности, которые оно само же и ввело, УСО попало в ловушку, расставленную противником.

За первым успехом немцев в радиоигре «Северный полюс» последовали другие. Несколько раз сбрасывались на парашюте предметы снаряжения, и с каждым разом росла уверенность Гискеса. В начале мая 1942 г. немцы, ловко использовав ряд промахов движения Сопротивления, получили в свои руки контроль над всеми подпольными сетями радиосвязи в Голландии. В итоге Гискес вел радиоигру с УСО по 14 линиям. Сам Гитлер регулярно читал отчеты об этой радиоигре.

Во многих радиопередачах по-прежнему отсутствовал контрольный сигнал: один только Лоуэрс в течение целых 7 месяцев передавал свои сообщения без этого сигнала. В УСО несколько раз задумывались над тем, не удалось ли противнику внедриться в голландское подполье, и не следует ли оборвать с ним связь. Однако каждый раз принималось решение продолжать контакты на том основании, что контрольные сигналы считались «недостаточно надежным средством проверки».

Яркой иллюстрацией неразберихи, царившей в голландском отделении УСО, может служить, например, тот факт, что на 14 передатчиках, участвовавших в радиоигре, работало всего лишь 6 радистов, которые были настолько перегружены, что Гискес хотел вывести из радиоигры некоторые рации, послав сообщения о том, что они ликвидированы немцами. УСО или вообще не записывало почерк своих агентов перед их отправкой, или же не желало утруждать себя сверкой принимаемых передач с этими записями. С другой стороны, во многих сообщениях содержался правильный контрольный сигнал. Заслуга в том, что они выглядели правдоподобно, принадлежала немецкому

криптоаналитику Эрнсту Маю, полному, коротко подстриженному пруссаку лет под сорок, который тщательно изучал шифры движения Сопротивления и содержавшиеся в них «ошибки».

Для успешного ведения игры «Северный полюс» требовалось гораздо больше, чем просто изобретать ложные сообщения и передавать их в эфир. Необходимо было регулярно выполнять распоряжения, поступавшие из Лондона. Как мог Абвер поддерживать уверенность УСО в том, что его подпольные группы действительно работают нормально? Гискесу приходилось изощряться в придумывании различных уловок и отговорок, а иногда даже предпринимать реальные меры для оказания содействия англичанам. В большинстве случаев эти меры сводились к тому, что сбитым английским летчикам помогали бежать в Испанию. Когда эти летчики добирались до Англии, они на все лады превозносили помощь, которую им оказали голландские подпольщики. УСО, имея в качестве доказательства своей эффективной работы живых летчиков, ни о чем таком не подозревало. А когда УСО приказало подпольной группе в Голландии взорвать антенны немецкой радиостанции, Гискес ответил сообщением о том, что попытка не удалась из-за минного поля вокруг антенн.

Однажды в Голландию был сброшен на парашюте новый английский агент, который сразу же попал в руки Абвера. Он рассказал, что до 11 часов утра следующего дня должен послать в Лондон условное сообщение «Экспресс отправился вовремя», а иначе в УСО будут считать, что он захвачен немцами. Гискес, быстро найдя выход из положения, сообщил через другую радиостанцию, участвовавшую в «функшпиле», что английский агент приземлился неудачно и находится в бессознательном состоянии. А 4 дня спустя УСО получило сообщение о том, что этот агент умер, так и не придя в сознание.

Гискес дошел даже до того, что организовал взрыв баржи в гавани Роттердама на глазах у нескольких тысяч голландцев, которые кричали от восторга, а затем, приписав эту акцию движению Сопротивления, поместил статьи о ней в контролируемых немцами газетах в надежде на то, что они попадут в Англию, и эго подтвердит правдоподобность сообщений, составляемых в ходе «функшпиля».

Что же касается Лоуэрса, то он был просто вне себя. Сначала он считал, что Лондон ведет свою радиоигру с Абвером, но потом понял, что произошла серьезная ошибка, и стал искать другие способы дать знать УСО об истинном положении вещей. Лоуэрс обманным путем радировал в Лондон слово «caught»*: вместо сигнала «QRU» («- -.-.-.-…-»), который означает «У меня ничего для вас нет», он передал сигнал «CAU» («.-..-..-») и далее свой позывной по коду Морзе, который он выбрал сам как «GHT». И хотя Лоуэрсу удалось сделать это незаметно для немцев, в Лондоне его намек не поняли. Затем Лоуэрс попытался снова передать слово «caught», несколько изменив какую-нибудь похожую 5-значную группу шифртекста и добавив к ней тире для обозначения «t». В конце концов он передал слово «caught» под видом ошибки, повторив ее несколько раз как бы в приступе раздражения. Но ответа так и не дождался.

* «Пойман».

В результате Гискесу удалось эффективно вести радиоигру «Северный полюс» в течение 20 месяцев. Она завершилась лишь после того, как два английских агента сбежали из тюрьмы и, пробравшись в Швейцарию, связались с УСО. Но Гискес нашел выход и здесь: он попытался скомпрометировать этих агентов, послав через одну из радиостанций «Северного полюса» сообщение о том, что их побег был организован немцами специально для внедрения в УСО. Но когда 23 ноября 1943 г. убежали еще три английских агента, «функшпиль» подошел к концу. Гискес осознал это после того, как из Англии стали поступать сообщения, содержавшие одну лишь дезинформацию.

Тем не менее радиоигра «Северный полюс» продолжалась еще несколько месяцев, так как обе стороны пытались извлечь хоть какие-то преимущества из передачи ложных сообщений, не имеющих никакого реального значения. Абвер первым решил прекратить это бесполезное занятие. Гискес составил и отправил открытым текстом последнее сообщение, которое адресовал руководителям голландского отделения УСО:

«Господам Бланту, Бингхэму и К°, Лондон.

Нам стало известно, что в течение некоторого времени вы пытались вести свои дела в Голландии без нашей помощи. Мы в курсе этого, поскольку давно и к нашему взаимному удовлетворению мы действуем там в качестве ваших единственных представителей. Тем не менее мы можем заверить, что, если у вас появится намерение нанести нам достаточно представительный визит, мы, как и прежде, окажем вашим эмиссарам достойное внимание и столь же теплый прием.

Надеемся вскоре увидеться с вами».

Гискес приказал, чтобы это издевательское сообщение было передано 1 апреля 1944 г. Его отправили все 10 радиопередатчиков, участвовавших в радиоигре. 4 английские станции подтвердили его прием, а 6 просто не ответили на вызовы. Радиоигра «Северный полюс» была окончена.

В ходе этой радиоигры немцы получили от англичан более 13 тонн взрывчатых веществ, 3 тысячи автоматов, 5 тысяч пистолетов, 2 тысячи ручных гранат, 75 радиопередатчиков, 500 тысяч патронов и полмиллиона голландских гульденов наличными. Были захвачены 54 английских агента, 47 из которых были расстреляны без суда и следствия. Радиоигра «Северный полюс» предрешила крушение всех надежд англо-американских союзников на организацию жизнеспособного движения Сопротивления на территории Голландии. Благодаря ей немецкие оборонительные сооружения в этом районе остались целыми и невредимыми: диверсанты даже не пытались их уничтожить. Она ввела англичан и американцев в заблуждение относительно возможностей немецких войск в Голландии. Ко всеобщему удивлению, Гаага была освобождена лишь через 7 месяцев после высадки союзных войск в Нормандии.

Это было самым тяжелым поражением англо-американских союзников в тайной войне разведок в годы Второй мировой войны.

АГЕНТСТВО НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Современные сверхдержавы в значительной степени обязаны своей мощью чрезвычайно разветвленным и работающим с огромной нагрузкой сетям связи, которые повсеместно используются для передачи информации. Эти сети предоставляют криптоаналитикам небывалые возможности для демонстрации умения взламывать шифры, а непрекращающееся соперничество между различными государствами повсеместно стимулирует максимальное использование этих возможностей. Поэтому Соединенные Штаты Америки принимают все необходимые меры, чтобы обезопасить свои каналы связи от посягательств других стран. В то же время они осуществляют широкомасштабный перехват и дешифрование сообщений, передаваемых по зарубежным линиям связи. Важность этой задачи породила величайшую в истории человечества криптоаналитическую организацию — Агентство национальной безопасности (АНБ).

Датой своего рождения АНБ обязано Перл-Харбору. После расследования обстоятельств внезапного нападения Японии на США конгресс порекомендовал американскому правительству создать централизованную криптоаналитическую спецслужбу. Рекомендация была принята во внимание, и 4 ноября 1952 г. президент Трумэн издал директиву, в соответствии с которой было создано АНБ.

Эта директива изначально была строго засекречена. В течение нескольких последующих лет после ее подписания Трумэном ни в одном правительственном документе не допускалось публичного упоминания о существовании АНБ. Лишь в 1957 г. в «Справочник по правительственным учреждениям США» впервые было включено краткое описание Агентства в очень расплывчатой формулировке. Через несколько лет это описание было слегка изменено и приобрело стереотипную форму из трех предложений.

В первых двух в сжатом виде сообщается о создании АНБ и его административном положении: «Агентство национальной безопасности было создано в 1952 г. согласно директиве президента. Оно входит в состав министерства обороны, его деятельность направляется и контролируется министром обороны». В третьем, самом главном предложении говорится: «Агентство национальной безопасности осуществляет в высшей степени специализированные технические и координационные функции, связанные с национальной безопасностью».

Несмотря на расплывчатость, это описание абсолютно точно. «Технические» функции АНБ состоят в перехвате и криптоанализе шифрованных сообщений всех государств, как дружественных, так и враждебных Соединенным Штатам Америки. «Координационные» функции включают в себя обеспечение безопасности связи, то есть организацию, контроль и объединение усилий всех заинтересованных ведомств (министерства обороны, госдепартамента, ЦРУ, ФБР и других) в области разработки, производства и эксплуатации средств криптографической защиты.

Директива президента, в соответствии с которой было создано АНБ, все еще продолжает расцениваться как секретная информация. Покров таинственности, которым Агентство было окутано с момента своего появления на свет, существует и в наши дни. АНБ — даже еще более молчаливая, секретная и мрачная организация, чем ЦРУ. Официальные представители ЦРУ время от времени делают заявления для печати, передают представителям прессы благоприятную для себя информацию. Официальные лица из Агентства не занимались этим никогда. Таким образом, АНБ

остается наиболее скрытной и таинственной организацией среди американских секретных служб.

В первые годы после своего создания АНБ размещалось в различных зданиях, разбросанных по всему Вашингтону. В 1954 г. министерство обороны США заключило контракт на строительство для АНБ единого большого здания в Форт-Миде (штат Мэриленд) приблизительно на полпути между Вашингтоном и Балтимором. Строительство было в основном закончено осенью 1957 г., но только в начале 1958 г. новоселье справили последние служащие АНБ.

И хотя этот храм криптоанализа несомненно стал самым грандиозным из когда-либо построенных для его жрецов*, он оказался слишком мал уже через 5 лет. Поэтому в конце 1965 г. к нему был пристроен еще один 9-этажный корпус. Расширение было вызвано невиданно быстрым ростом численности сотрудников АНБ.

* Здание АНБ стало третьим по величине в окрестностях Вашингтона после зданий Пентагона и госдепартамента.

В отношении рекрутов в АНБ действуют строжайшие критерии отбора. Будущий сотрудник должен пройти всеобъемлющую проверку, включающую тест на детекторе лжи. Затем его могут принять для участия в программе обучения, но окончательное оформление на работу произойдет только после скрупулезного изучения его личного дела. Будут проверены время и место рождения, образование и послужной список. Друзьям, соседям, бывшим сослуживцам и работодателям будут заданы вопросы относительно того, заслуживает ли он доверия и насколько зрелым является его поведение. Будет проведен анализ его кредитоспособности. Посланы запросы о причастности к подрывным организациям. Но даже после прохождения всех этих проверок и окончательного оформления на работу все сотрудники АНБ регулярно подвергаются новым проверкам каждые 4 года. Это требуется для подтверждения разрешения на их доступ к секретным документам.

АНБ упорно внушает своим сотрудникам мысль о том, что нужно все время быть бдительным. Причем делается это с беспощадной настойчивостью до тех пор, пока бдительность не станет для них более чем привычкой, более чем второй натурой, пока она не станет настоящим основным инстинктом. Сотрудники АНБ никогда не рассказывают своим женам и детям, что представляет собой их работа. Однако, несмотря на все меры предосторожности, АНБ оказалось причастным к самым скандальным провалам в истории американских спецслужб, исключая один только атомный шпионаж со стороны русских.

Первый провал связан с Джозефом Петерсеном. 9 октября 1954 г. на первые полосы двух крупнейших ежедневных газет попало сообщение о его аресте за кражу секретных документов из АНБ. 39-летний Петерсен, бывший преподаватель физики, изучал криптоанализ на заочных военных курсах в 1940-1941 гг., а затем был взят в армейскую дешифровальную службу. После войны по собственной инициативе Петерсен занялся преподаванием криптоанализа на курсах повышения квалификации министерства обороны. В 1953 г. разработанная им программа обучения стала базовой в АНБ. После поимки Петерсен сказал в свое оправдание, что взял всего два секретных документа для подготовки к проведению занятий.

В ходе начавшегося следствия выяснилось, что во время Второй мировой войны Петерсен подружился с полковником Феркуилом, одним из лучших голландских криптоаналитиков. Вместе с Феркуилом Петерсен занимался вскрытием японского дипломатического кода. В этой области у Феркуила был значительный опыт, приобретенный им еще до войны. Через Феркуила Петерсен познакомился с Джакомо Стуитом, офицером связи голландского посольства.

После войны, когда Феркуил возвратился из США в Голландию, в своих письмах Петерсен рассказывал ему о методах преподавания криптоанализа и других деталях, которые, по мнению Петерсена, полезно было знать при создании в Голландии собственной криптоаналитической спецслужбы. Стуит оставался в Америке, и Петерсен продолжал поддерживать с ним дружеские отношения.

В то время для зашиты своей дипломатической переписки голландцы применяли шифрмашины швейцарской фирмы «Хагелин». В 1948 г. Петерсен снял копии с двух секретных документов, в которых говорилось об успехах американцев во вскрытии голландских шифрмашин, присовокупил к этим копиям оригинал еще одного документа под названием «Криптоанализ шифрмашины «В-211» фирмы «Хагелин» и показал их Стуиту. Феркуил считает, что Петерсен не имел ни малейшего намерения нанести ущерб Соединенным Штатам, а просто руководствовался желанием помочь своим друзьям защитить родину от шпионажа других государств.

Осенью 1954 г. во время обыска квартиры Петерсена сотрудники ФБР обнаружили обе копии и

оригинал. Это был первый серьезный случай нарушения закона сотрудником АНБ. Вероятно, именно поэтому министерство юстиции и министерство обороны приняли решение передать дело в суд, вместо того чтобы решить вопрос в административном порядке внутри АНБ. Возможно, они хотели сделать дело Петерсена показательным. Но, как сказал его адвокат, «приняв такое решение, они попали впросак», так как арест получил слишком широкую огласку в американской печати.

Обвинение посоветовало Петерсену признать себя виновным, чтобы избежать свидетельских показаний, которые потребовались бы в суде. Петерсен, испытывавший угрызения совести, готовый возместить ущерб, который он нанес своей стране, и надеявшийся на смягчение приговора, согласился. И действительно, судья Альберт Брайэн отклонил два из трех пунктов обвинительного акта. Но, заявив, что «сущность этого преступления не в том, какие документы обвиняемый унес, а в том, что он унес документы из Агентства национальной безопасности», он ошарашил Петерсена 7-летним сроком тюремного заключения.

Петерсен отсидел целых 4 года, прежде чем был отпущен на поруки. Таким образом АНБ удалось преподать урок другим потенциальным правонарушителям, избежав необходимости рассказывать о характере своей деятельности в ходе судебного разбирательства. Остается открытым вопрос о том, насколько это было справедливо по отношению к Петерсену. Но эффективность принятых мер не вызывает сомнения: после дела Петерсена судебных преследований за разглашение информации, имевшей отношение к криптоанализу, не было в течение очень долгого времени.

Правда, в одном из случаев единственной причиной отсутствия судебного разбирательства явилось бегство потенциальных обвиняемых за пределы действия юрисдикции федеральных властей США: они перебрались в Советский Союз. Это были криптоаналитики из АНБ Уильям Мартин и Бернон Митчелл. В 1960 г. в ходе 90-минутной пресс-конференции в Москве они рассказали огромной аудитории об усилиях американской нации в области криптоанализа больше, чем это сделали какие-либо другие известные перебежчики.

Хотя о Мартине и Митчелле многое известно, фактически никто не знает достоверно о том, почему они предали свою страну. Оба были способными молодыми людьми и выросли в типичной американской среде. И тот и другой прошли строгую проверку при устройстве на работу в АНБ.

В июне 1960 г. Мартин и Митчелл, подружившиеся между собой еще во время службы в армии, обратились с просьбой о предоставлении им очередного отпуска, чтобы навестить своих родителей. Просьба была удовлетворена, однако у родителей они так и не появились. Вместо этого Мартин и Митчелл улетели в Мехико, а оттуда — в Гавану. Из кубинской столицы они, по-видимому, отплыли на советском траулере в Россию.

В течение примерно месяца ничего не произошло. Когда 26 июля шеф Мартина и Митчелла не смог связаться с ними в домах их родителей, было начато расследование, в результате которого было установлено, что Мартин и Митчелл вылетели в Мехико. Через 4 дня министерство обороны признало, что «вероятно, они сбежали за «железный занавес».

6 сентября Мартин и Митчелл появились на сцене ярко освещенного зала Дома журналистов в Москве. Во время с размахом организованной пресс-конференции они зачитали длинное заявление, в котором говорилось, что они отказываются от своего американского гражданства и становятся гражданами СССР. В заявлении были изложены причины их дезертирства:

«Основная причина нашего недовольства заключается в некоторых методах, которые Соединенные Штаты используют для сбора разведывательной информации. Мы крайне озабочены проводимой Соединенными Штатами политикой преднамеренного нарушения воздушного пространства других стран и практикой правительства США выступать с лживыми заявлениями относительно таких нарушений в расчете на обман общественного мнения. Кроме того, нас возмущает осуществляемая правительством Соединенных Штатов практика перехвата и дешифрования секретных сообщений своих собственных союзников. Наконец, мы не согласны с тем, что правительство США зашло настолько далеко, что стало вербовать агентов из числа служащих своих союзников».

Мартин и Митчелл пояснили, почему в качестве своей новой родины они выбрали именно Советский Союз: «Там наши основные взгляды и интересы разделяются большинством людей. Поэтому мы считаем, что в социальном отношении мы будем лучше себя чувствовать и сможем плодотворнее работать в соответствии со своей профессией. Другим мотивом является то, что в Советском Союзе таланты женщин поощряются и используются в гораздо большей степени, чем в Соединенных Штатах. Мы считаем, что это обогащает советское общество и делает советских женщин более привлекательными».

Затем Мартин и Митчелл перешли к рассказу об американских достижениях в области

криптоанализа. Их откровения заставили многие государства сменить свои шифры вместе с ключами к ним. Результатом стали временные трудности в деятельности АНБ. Криптоаналитикам АНБ пришлось работать по нескольку смен подряд, чтобы заново вскрыть сложные коммутации дисков в иностранных шифрмашинах.

Пентагон объявил о Мартине и Митчелле, что один из них «душевнобольной» (не уточнив, кто именно), что оба они «явно запутались», а затем назвал сделанные ими признания «ложью». Комиссия палаты представителей США по расследованию антиамериканской деятельности и Пентагон начали тщательное расследование обстоятельств случившегося.

Никто из них не смог внятно объяснить, почему сбежали Митчелл и Мартин. Возможно, что они были гомосексуалистами. Но в таком случае зачем обязательно нужно ехать в СССР, чтобы без помех предаваться любовным утехам с себе подобными?

Некоторые высказывали предположение о том, что у Мартина и Митчелла могла вызвать протест противоречащая морали деятельность АНБ по вскрытию шифров. Но почему этот факт должен был столь серьезно обеспокоить только их, а не остальных сотрудников АНБ?

Ответ на вопрос об истинных причинах дезертирства Мартина и Митчелла, по-видимому, не будет найден никогда.

В ходе проведенной проверки комиссия по расследованию антиамериканской деятельности обнаружила многочисленные нарушения режима секретности в АНБ. В результате были уволены 26 сотрудников, признанных сексуальными извращенцами, а также нечистый на руку заместитель директора по кадрам Морис Клейн. Последний признал, что в своей анкете указал об окончании Гарвардской юридической школы, в то время как в действительности он закончил юридическую школу в штате Нью-Джерси. Клейн также рассказал, что пытался скрыть это и несколько других прегрешений, перепечатав свое личное дело и поставив в нем другие даты.

Через год после опубликования отчета комиссии бывший сотрудник АНБ раскрыл еще ряд секретов АНБ в письме, опубликованном в газете «Известия». Им был Виктор Гамильтон, сириец, получивший американское гражданство после приезда в США с американкой, которую он встретил в Ливии и на которой женился. 13 июня 1957 г. Гамильтон поступил на работу в АНБ в качестве криптоаналитика. Там он занимался вскрытием шифрсистем арабских стран.

3 июня 1959 г. Гамильтон был вынужден уйти в отставку. По его словам, руководители проявили подозрительность, когда он захотел возобновить контакты с родственниками, проживавшими в Сирии. По мнению же руководства, Гамильтон пребывал «на грани параноидальной шизофрении» и не мог продолжать службу в АНБ. Какова бы ни была настоящая причина ухода Гамильтона в отставку, он попросил Советский Союз предоставить ему политическое убежище и, по-видимому, рассказал советскому правительству о своей работе, прежде чем написать письмо в «Известия» с разоблачением американской шпионской деятельности.

Письмо Гамильтона появилось в «Известиях» 23 июля 1963 г. В тот же самый день курьер АНБ покончил жизнь самоубийством, задохнувшись угарным газом в своей автомашине. Это был сержант Джек Данлэп, отмеченный наградами ветеран войны с безупречным личным делом. Сначала он водил машину помощника директора АНБ генерал-майора Гаррисона Кловердэйла. Позже Данлэпа перевели на должность курьера.

Мотивы, побудившие Данлэпа к предательству, никогда официально объявлены не были. Но цена за измену родине была выяснена довольно точно: 60 тысяч долларов. Он истратил их на покупку моторной яхты, глиссера с воздушным винтом, спортивной машины марки «Ягуар», двух «кадиллаков» последней модели, а также на многочисленные выпивки на дорогих курортах по всему Атлантическому побережью США и на пышнотелую любовницу-блондинку. Вероятно, он начал передавать секретные данные русским примерно в середине 1960 г., так как в июне этого года он купил моторную яхту, заплатив наличными сразу 3400 долларов.

Данлэп проносил секретные документы под рубашкой и передавал их русским сначала раз в неделю, позднее — раз в месяц. Его любовница знала только, что Данлэп регулярно посещает «бухгалтера» и возвращается с большими пачками банкнотов. Он рассказывал знакомым различные истории, чтобы объяснить свое новое богатство: что у него есть земля, в которой обнаружен ценный минерал, что он получил небольшое наследство, что его отец (в действительности — смотритель мостов) имеет огромную плантацию. Что именно Данлэп успел рассказать и передать русским, узнать так и не удалось.

Данлэп оказался в безвыходном положении не из-за бдительности, проявленной в АНБ. Он пал жертвой собственной жадности. Боясь, что по окончании срока военной службы его могут перевести из АНБ в другое место, в марте 1963 г. Данлэп обратился с просьбой уволить его из армии, но

попросил разрешения продолжить работу в АНБ в качестве гражданского служащего. В результате его впервые проверили на детекторе лжи. Военный персонал, приписанный к АНБ, не подвергается проверке на этом детекторе, однако будущие гражданские служащие подлежат ей в обязательном порядке. В ходе двух проверок Данлэпа были обнаружены признаки мелкого воровства и аморального образа жизни.

В течение двух месяцев все оставалось по-прежнему. Данлэп продолжал исполнять обязанности курьера и воровать секретные документы. Дополнительные проверки показали, что он жил не по средствам, и тогда Данлэпа перевели на работу без доступа к секретам. После самоубийства Данлэпа расследование шло неспешным чередом до тех пор, пока его вдова не нашла среди вещей своего мужа пачку служебных документов. Пришлось обратиться в ФБР, но смерть Данлэпа похоронила все надежды до конца разобраться в масштабах его предательства. «Чтобы чувствовать себя в безопасности, — заметил один из руководителей АНБ, — мы должны действовать, исходя из предположения о том, что все, проходившее через руки Данлэпа, покоится в сейфах на Лубянке в Москве».

Таким образом, как явствует из откровений предателей и перебежчиков, наиболее ценную информацию АНБ получает в результате вскрытия иностранных шифров. Как сказали Мартин и Митчелл, «успехами, достигнутыми в чтении шифрпереписки других государств, Агентство национальной безопасности обязано прежде всего искусству криптоаналитиков, которым помогают компьютеры».

Сколько криптоаналитиков работает в АНБ? Трудно дать точный ответ, так как современный криптоанализ весьма специализирован и раздроблен в административном плане. Многие сотрудники АНБ заняты элементарным криптоанализом или же выполняют почти механическую работу после того, как криптоаналитики проникли в шифр и в основном вскрыли его.

Несмотря на большую секретность, которая окружает работу криптоаналитиков, она напоминает действия служащих любого другого учреждения. Криптоаналитики сидят за компьютерами, перелистывают страницы документов, советуются с коллегами и делают перерывы, чтобы выпить кофе. Они имеют по крайней мере одно преимущество перед обычными служащими: нельзя брать работу домой на ночь. Однако они все равно не могут от нее отделаться, так как криптоаналитическая задача полностью захватывает ум и, кажется, никогда не оставляет в покое. Если идея приходит ему в голову дома, криптоаналитик делает необходимые записи или, если живет достаточно близко, он приезжает в свое служебное здание, чтобы поработать над ней.

Как и служащие других крупных учреждений США, американские криптоаналитики работают в больших, просторных, светлых комнатах. Туда в сыром виде поступают перехваченные сообщения. Самые срочные послания приходят по радио. Если в Форт-Миде получают несколько экземпляров одного и того же сообщения, перехваченных разными радиостанциями, редакторы пытаются устранить в нем все имеющиеся искажения. Затем сотрудники АНБ сравнивают и сопоставляют местонахождение отправителей и получателей сообщений, маршруты их прохождения и служебные пометки, присутствующие в этих сообщениях для сведения шифровальщиков и операторов связи. Это позволяет отсортировать перехваченные сообщения по принципу принадлежности к одинаковым шифрсистемам. А изучая картину переписки во всей ее полноте, можно выявить общую структуру сети связи и получить другую полезную информацию.

Криптоаналитики работают группами. Сложные современные шифры превратили работу одиночки в дело прошлого. Руководитель группы распределяет задания между подчиненными, проводит совещания, решает, является ли данный метод более продуктивным, чем другие.

Работа отдельно взятого криптоаналитика в составе группы заключается в отыскании закономерностей, которые дают значительные отклонения от случайного текста. Эти закономерности очень тонки, и отдельные буквы, в которых они проявляются, повторяются через очень большие интервалы. Только огромное количество текста может сделать неясные закономерности заметными. И только самые мощные суперкомпьютеры могут поглотить реки букв и проверить немыслимое количество возможностей, чтобы найти открытый текст криптограммы в реально допустимый промежуток времени, то есть до того, как она потеряет свое значение.

АНБ обладает гораздо большим парком компьютерного оборудования, чем любое другое подобное учреждение в мире. Однако одержать полную победу в бесконечной борьбе с шифрами с помощью компьютера американским криптоаналитикам так и не удалось, поскольку теория шифровального дела идет в ногу с достижениями криптоанализа. Также не получается полностью автоматизировать труд криптоаналитика. Компьютер смог только освободить его от утомительной монотонной работы.

В криптоанализе все еще имеются богатые возможности для чутья, интуиции, опыта и индивидуальной одаренности. В АНБ компьютеры являются, как и повсюду, орудиями труда криптоаналитиков, а не их заменой. Вычислительные машины служат криптоаналитиками-роботами, причем в весьма ограниченной степени. Во второй половине XX века, в пору расцвета компьютеров, американские криптоаналитики часто сталкиваются с теми же проблемами, которые четыре столетия назад решал Джованни Соро: заменяет знак «X» криптограммы букву «а» или букву «о» открытого текста?

Стойкость шифров, с которыми имеет дело АНБ, весьма различна. Компетентность в криптографии, как, впрочем, и в других областях человеческих знаний, изменяется прямо пропорционально техническим возможностям и экономическому богатству страны. Соединенные Штаты Америки, по-видимому, имеют наиболее надежные шифрсистемы и самую информативную разведку средствами связи в мире. Из государств, чьи шифрсообщения АНБ пытается дешифровать, безусловно, наиболее сложными должны быть шифры Советского Союза, Англии и Франции. Именно в таком порядке.

АНБ пытается вскрыть все шифры всех стран — по крайней мере, в идеале. Но ограничения в людях и средствах стесняют АНБ, как и любые другие американские спецслужбы. Эти ограничения вместе с непрерывно возникающими чрезвычайными обстоятельствами, которые отрывают американских криптоаналитиков от их обычной работы, делают идеал недостижимым. И хотя АНБ, возможно, хочет заняться военными шифрами Ливии, ему приходится сконцентрировать усилия своих криптоаналитиков на советской шифрсистеме, вскрытие которой, скорее всего, позволит получить доступ к гораздо более ценной информации.

Как долго в АНБ будут работать над конкретной шифрсистемой, зависит от данных, которые там рассчитывают получить с помощью ее успешного вскрытия. Агентство может заниматься этой шифрсистемой в течение двух или трех лет в надежде на то, что шифровальщик может в один прекрасный день ошибиться и открыть путь к ее вскрытию*. И если некоторые иностранные государства будут продолжать платить своим шифровальщикам всего 500 долларов в месяц, как в 60-х годах это делала Италия в Вашингтоне, ждать таких ошибок — отнюдь не бессмысленное занятие.

* В современных шифрсистемах, при условии их правильного использования и частой смены ключей, ошибка шифровальщика является единственной надеждой криптоаналитика.

Диапазон успеха и полноты во вскрытии иностранных шифрсистем криптоаналитиками АНБ довольно широк — от полного чтения всех сообщений для данной шифрсистемы до абсолютной нечитаемости. Между этими двумя крайностями бывает и достаточно полное вскрытие с немногими сомнительными местами, и частичные вскрытия с многими пустотами.

Прочитанная шифрпереписка направляется тем правительственным организациям США, которым действительно нужно с ней ознакомиться: военные сведения — министерству обороны, дипломатические — государственному департаменту и т. д. Вместе с ЦРУ именно эти ведомства являются главными клиентами АНБ.

Насколько успешна деятельность АНБ и насколько ценны ее результаты?

АНБ читает лишь незначительную часть общего объема перехваченного шифрматериала — менее 10%. В мирное время шифровальщики могут работать медленнее и аккуратнее, чем в военное. Однако даже в условиях войны при наличии огромного количества шифрованных сообщений и гораздо большего количества ошибок немецкая группа армий «Север» читала менее 30% русских военных шифровок. Более того, станции перехвата АНБ концентрируют свое внимание на иностранных сообщениях высшей степени секретности, а они должны быть наилучшим образом защищены, снижая таким образом средний процент достижений АНБ.

Тем не менее АНБ все-таки читает достаточное количество шифрсообщений, чтобы получать из них информацию, имеющую для страны огромную ценность. Мартин и Митчелл обрисовали масштабы успехов АНБ. Они заявили, что АНБ вскрыло шифры более сорока стран (что составляло почти половину всех стран мира, существовавших на тот момент, когда Мартин и Митчелл делали свое заявление). На вопрос: «Шифры каких стран вскрываются в АНБ?» Мартин ответил: «Италии, Турции, Франции, Югославии, Индонезии, Уругвая. Я полагаю, этого достаточно, чтобы составить общее представление».

Гамильтон дополнил этот ответ Мартина некоторыми занимательными подробностями:

«Я был зачислен экспертом в сектор стран Ближнего Востока... Этот сектор занимался Сирией, Ираком, Ливаном, Иорданией, Саудовской Аравией, Йеменом, Ливией, Марокко, Тунисом, Турцией,

Ираном, Грецией и Эфиопией. В обязанности моих коллег входило изучение и вскрытие военных шифров этих стран, а также дешифрование всей корреспонденции, поступающей в их, дипломатические представительства в любой части мира... АНБ вскрывает шифры всех этих стран с помощью криптоанализа...

Особенно важно отметить, что американские власти пользуются расположением штаб-квартиры ООН на американской земле. Их произвол достиг такой степени, что дешифрованные инструкции правительств Ирака, Иордании, Ливана, Турции и Греции их представительствам в ООН попадали в руки государственного департамента до того, как они доходили до своих законных адресатов».

А что можно сказать о других государствах? Ни одно из них не может соперничать с США в области криптоанализа. Как всегда, вопрос сводится к экономике. Эти государства не в состоянии разместить свои станции перехвата по всему миру. Они не могут содержать крупные криптоаналитические организации, подобные АНБ, которое обладает материальными ресурсами, необходимыми для вскрытия современных стойких шифров. В этих государствах криптоаналитики являются скорее одаренными любителями, чем профессионалами.

ШИФРЫ И ИСТОРИЯ

Не все криптоаналитики служили исключительно богу войны Марсу. Некоторые из них полностью посвятили свою жизнь музе истории Клио. Эти малоизвестные труженики, чьи успехи принесли пользу всему человечеству, в большинстве своем плодотворно работали в XIX веке. Ведь именно тогда, в поисках неисследованных документов из дипломатической переписки прошлых веков, историки устремились в архивы, двери которых открыли перед ними буржуазно-демократические революции.

К своему огорчению ученые обнаружили, что многие архивные документы были полностью или частично зашифрованы. Причем неизменно оказывалось, что шифрованной была самая интересная их часть. Например, в середине XVI столетия посол Венеции писал домой о своей беседе с королем Франции Генрихом II: «Его величество вдруг повернулся ко мне и, заметно волнуясь, сказал...» Далее шел шифрованный текст.

Некоторые историки, незнакомые с криптоанализом, были склонны считать эти криптограммы непреодолимым препятствием, и относились к ним как к навсегда пропавшим частям архивных документов. Другие рассматривали криптограммы в качестве средства для испытания своих интеллектуальных способностей. К последней категории ученых-историков принадлежал немец Густав Бергенрот.

Бергенрог родился 26 февраля 1813 г. в небольшом городке в Восточной Пруссии. Закончив Кенигсбергский университет и поработав некоторое время на литературном поприще, Бергенрот увлекся историей Англии. Увидев, что имеющихся материалов недостаточно, в возрасте 40 лет Бергенрот отправился в город Симанкас, расположенный в северо-западной части Испании, где находилось громадное хранилище архивных документов. Предварительно от хранителя архива Англии Бергенрот сумел добиться выделения ему стипендии для того, чтобы отыскать, скопировать и оформить в виде отдельного тома документы, хранившиеся в Симанкасе и имевшие отношение к английской истории.

В сентябре 1860 г. Бергенрот приехал в Симанкас и поселился там в гостинице. Один англичанин, посетивший Симанкас, так описал этот город: «Симанкас — это скопление жалких лачуг, наполовину засыпанных песком и пылью. В городе нет ни одного приличного дома. Дом, в котором живет г-н Бергенрот, имеет два этажа, все стены оштукатурены, а полы выложены кирпичом. Ни в одной комнате не камина, а поскольку зима здесь очень суровая и стены полны дыр, то ничто, кроме очень сильного желания послужить истории, не смогло бы примирить человека с такими большими лишениями».

Более того, Бергенроту пришлось столкнуться с довольно необычными явлениями, которые вряд ли когда-либо еще сопутствовали дешифрованию. Его комната выходила на площадь, всегда заполненную крикливыми извозчиками. На эту площадь часто приходила одна женщина, чей «резкий голос, постоянно исполнявший одну и ту же арию из «Травиаты» и одну испанскую мелодию, и ничего больше», по признанию самого Бергенрота, доводил его «почти до сумасшествия». Более того, служанка Бергенрота регулярно вешала сушить белье на его балконе, а затем «с похвальной решимостью» гладила это белье прямо на письменном столе немецкого ученого.

Но с еще большими затруднениями Бергенрот столкнулся в архиве. Этот архив размещался в старинном замке с зубчатыми стенами, окруженными глубокими рвами с перекинутыми через них

подъемными мостами. В 46 комнатах замка хранилось более 100 тысяч мешков, в каждом из которых содержалось от 10 до 100 тысяч документов, а всего их насчитывалось несколько миллионов. Из этого громадного собрания бумаг Бергенроту предстояло отобрать лишь имевшие отношение к теме его исследования. Сначала ему пришлось затратить много сил и времени на то, чтобы научиться разбирать шрифт эпохи Возрождения, поскольку даже хранитель архива иногда не мог его правильно прочесть. Затем из чувства зависти хранитель архива начал умышленно мешать работе Бергенрота, отказывая ему в доступе к имевшимся шифровальным ключам. В таких случаях Бергенроту приходилось искать эти ключи самому.

Картину кропотливого труда Бергенрота по дешифрованию архивных документов можно восстановить на основании его собственных заметок:

«Прежде чем поехать в Испанию, я тщательно подготовился к моей работе. Я потратил много времени на дешифрование старых испанских документов, обнаруженных в библиотеках Лондона и Парижа...

В Симанкасе... я счел необходимым самым доскональным образом изучить не только испанскую орфографию того периода, но и особенности почерка каждого государственного деятеля, который мог предположительно написать какое-либо из писем. Даже этого было недостаточно. Я должен был изучить склад мышления, любимые слова и выражении каждого государственного деятеля...

Занимаясь переписыванием, я постоянно рассчитывал натолкнуться на слабое место, будучи убежденным в том, что ни один человек не может в течение какого-то длительного времени столь полно скрывать свои мысли и что он каким-либо образом должен выдать себя внимательному наблюдателю... Сотни раз мои усилия были тщетны, но, наконец, я восторжествовал...

Брешь была пробита, и до 3 часов утра следующего дня я вскрыл 83 знака, представлявшие буквы алфавита, и 33 отдельных слога, означавшие слова. Ключ был далеко не полный, но больше не существовало непреодолимых трудностей... Этот шифр является самым трудным и в то же самое время самым важным из всех, так как большая часть непрочитанных сообщений зашифрована этим шифром, а не каким-либо другим...

Могут спросить, заслуживают ли доверия дешифрованные мной сообщения? Я отвечу с полной уверенностью утвердительно. У меня больше, чем у кого-либо другого, имеется оснований утверждать так. После того как я дешифровал эти сообщения, я обнаружил в некоторых случаях, что они являются зашифрованными копиями проектов, написанных открытым текстом. Так у меня появилась возможность сравнить мои дешифровки с подлинниками, и я нашел, что по всем существенным пунктам они идентичны...»

За 10 месяцев Бергенрот превзошел в искусстве дешифрования многих профессиональных криптоаналитиков, вскрыв 19 номенклаторов — в среднем по одному в каждые две недели. К тому же он еще и сам переписывал часть своих бумаг, контролировал работу переписчика, искал документы в архиве и вел отчаянную борьбу с бюрократией. Заниматься дешифрованием Бергенроту не нравилось. В одном из писем домой он написал: «Ничто, кроме абсолютной необходимости, не заставило бы меня взяться за решение такой задачи, которая, я думаю, является одной из самых трудных, когда-либо взятых на себя человеком». Однако 23 июля 1861 г. Бергенрот смог гордо рапортовать домой: «Все шифрованные сообщения переписаны и дешифрованы, за исключением двух небольших писем, которые я намерен дешифровать в Барселоне или Лондоне. Сейчас я слишком устал для работы, требующей столь большого умственного напряжения, как вскрытие ключей к неизвестному шифру».

В Симанкасе Бергенроту оказывал помощь один странствующий архивариус по имени Поль Фридманн, который собирал для Французской национальной библиотеки коллекцию шифров, применявшихся различными французскими политическими деятелями XVI века. В 1868 г. Фридманн заинтересовался шифрованными сообщениями Джованни Микеля, венецианского посла при дворе английской королевы Марии, сестры и предшественницы Елизаветы I. Никто из архивных работников в Венеции не мог прочесть эти сообщения. Фридманн исследовал переписку Микеля и «вскоре пришел к убеждению, что этот шифр не относится к категории чрезвычайно трудных шифров, что им не всегда пользовались с достаточной осторожностью и что если приложить небольшие усилия, то можно раскрыть смысл переписки».

Фридманн писал, что «переписка Микеля представляет значительную ценность. Она исправит многие ошибки и заполнит многие пробелы в изложении фактов...». Например, до этого историки считали, что будущая королева Англии Елизавета была освобождена из тюрьмы и переведена в Хэмптон-Корт* в июне 1554 г., когда у католички Марии пропала всякая надежда родить ребенка и ей уже не нужно было больше содержать под стражей предполагаемую наследницу-протестантку.

Однако письма Микеля, дешифрованные Фридманном, свидетельствуют как раз об обратном. Переезд состоялся не в июне, а в апреле, и это было отнюдь не освобождение. Просто в Хэмптон-Корт в отношении Елизаветы можно было принять более строгие меры безопасности, учитывая рост народного недовольства по поводу намерений посадить на английский трон отпрыска короля Испании Филиппа и Марии. Так криптоанализ помог уточнить трактовку важного эпизода в биографии Елизаветы.

* Хэмптон-Корт — бывшая королевская резиденция в предместьях Лондона.

В XIX веке вскрытием венецианских дипломатических шифров 300-летней давности занимался также итальянский архивариус Луиджи Пазини. Он пришел на работу в государственный архив в Венеции в 1855 г. в возрасте 20 лет. Благодаря незаурядным криптоаналитическим способностям Пазини достоянием исторической науки стали сообщения шести венецианских послов, написанные под впечатлением таких значительных событий, как первые религиозные войны в Европе.

Другой итальянский архивариус — аббат Доменико Габбриелли — был поистине неиссякаем в своем усердном труде на ниве криптоанализа. Габбриелли вскрыл или восстановил в общей сложности 1755 номенклаторов, относящихся к периоду 1414-1742 гг. Их описание, выполненное аббатом, насчитывает 16 томов.

Однако, несмотря то что во славу богини Клио трудились многие талантливые криптоаналитики, самая известная историческая криптограмма остается до сих пор недешифрованной. Она представляет собой громадную безымянную книгу, называемую самой таинственной рукописью в мире. В 1962 г. торговец книжными раритетами из Нью-Йорка Ганс Краус привлек к ней внимание всего мира, купив за огромную по тем временам сумму.

Сама книга не производит большого впечатления. Ее украшают десятки крошечных женских обнаженных фигурок, астрологических диаграмм и около 400 рисунков растений причудливой формы, раскрашенных в разные цвета. При беглом изучении страниц рукописи глаз улавливает повторение букв и даже слов, иногда с несколько измененными окончаниями.

На первый взгляд кажется, что прочтение текста рукописи, которая по своему виду больше всего напоминает травник*, не представляет никакой проблемы. Знаки в ней сохраняют общую форму букв средневековья. Почерк — ровный, знаки выписаны слитно, словно переписчик копировал понятный ему текст. При этом все выглядит так, будто текст написан если не на известном языке, скрытом от современного глаза незнакомым почерком, то на каком-то ином диалекте, который можно легко установить. Однако знатоки самых трудных языков заявили, что они не могут понять его, а палеографы признали, что данный рукописный шрифт им неизвестен.

* Травник — книга, в которой перечисляются растения с целебными свойствами и даются рецепты приготовления из них лекарств.

Криптоаналитики установили, что частота повторяемости знаков в рукописи примерно соответствует шифру обычной одноалфавитной замены. Но они торжествовали недолго, считая, что прочесть рукопись проще, чем найти решение для любой из помещаемых в газетах криптоаналитических головоломок. Все их отчаянные попытки перевести текст рукописи на любой человеческий язык полностью провалились.

Тайна окутывает рукопись с самого первого упоминания о ней в истории. Оно датируется 19 августа 1666 г., когда ректор Пражского университета Иоганнес Марчи послал рукопись своему бывшему учителю Атанасиусу Кирчеру, самому известному в то время иезуитскому ученому, за три года до этого издавшему книгу по криптографии. В сопроводительном письме, приложенном к рукописи, Марчи напомнил, что ее бывший владелец когда-то посылал Кирчеру часть текста рукописи для возможного прочтения. Этому занятию ее владелец «посвятил неослабевающие усилия... и только с его смертью работа прекратилась. Его усилия были тщетны... Примите эту рукопись в том виде, как она есть, как выражение, возможно и запоздалое, моей любви к вам; сокрушите все преграды, если они встретятся на вашем неизменно успешном пути...». Преграды, несомненно, встретились, но Кирчер, который никогда не упускал случая похвастаться своими успехами, скорее всего, так и не преодолел их, ибо его молчание говорит само за себя.

Марчи написал Кирчеру, что рукопись была куплена императором Священной Римской империи Рудольфом II. Тот факт, что она хранилась при его дворе в Праге, был позднее подтвержден, когда на полях одной страницы обнаружили автограф одного известного богемского ученого, который был

любимцем Рудольфа. Марчи также выразил уверенность, что автором рукописи был английский францисканский монах Роджер Бэкон*, который жил приблизительно с 1214-го по 1294 г.

* Не путать с английским философом Фрэнсисом Бэконом.

Следующее упоминание о таинственной рукописи относится к 1912 г., когда американский торговец редкими книгами Уилфред Войнич купил ее в Италии у монахов одной иезуитской школы. Горя желанием прочитать рукопись, Войнич щедро снабжал фотокопиями каждого, кто брался ее дешифровать. А пытались очень многие.

Ботаники считали, что надо лишь установить, что за растения нарисованы на полях страниц, и допустить, что их названия фигурируют в тексте. Однако большая часть флоры оказалась воображаемой. Астрономы опознали в астрологических диаграммах некоторые звезды, но все равно не смогли добиться успеха. Филологи опробовали методы, применявшиеся для восстановления забытых языков. Безуспешно. Криптоаналитики (в их числе был Джон Мэнли) нашли, что рукопись стойко противостоит всем испытанным способам дешифрования.

В 1919 г. некоторые из репродукций рукописи Войнича попали к профессору философии Пенсильванского университета Ромэну Ньюбоулду. Ньюбоулд, которому недавно исполнилось 54 года, имел широкие интересы, многим из которых был свойствен элемент таинственности. В иероглифах текста рукописи Ньюбоулд углядел микроскопические значки стенографического письма и приступил к дешифрованию, переводя их в буквы латинского алфавита. В результате получился вторичный текст с использованием 17 различных букв. Затем Ньюбоулд удвоил все буквы в словах, кроме первой и последней, и подверг специальной замене слова, содержавшие одну из букв «a», «c», «m», «n», «o», «q», «t», «u». В полученном в результате тексте Ньюбоулд заменил пары букв одной буквой по правилу, которое он так никогда и не обнародовал. При этом, ввиду фонетического сходства, Ньюбоулд рассматривал некоторые буквы текста как эквивалентные. Наконец, Ньюбоулд произвел анаграммирование* букв, чтобы выписать окончательный открытый текст на латинском языке.

* При анаграммировании осуществляется перестановка букв одного слова, с тем чтобы получить из них другое.

В апреле 1921 г. Ньюбоулд огласил предварительные результаты своей работы перед ученой аудиторией. Эти результаты характеризовали Роджера Бэкона как самого великого ученого всех времен и народов. Согласно Ньюбоулду, в большой туманности в созвездии Андромеды Бэкон опознал галактику, имеющую форму спирали, а также установил строение биологических клеток и их ядер. По Ньюбоулду, Бэкон фактически создал микроскоп с телескопом и с их помощью сделал многие открытия, предвосхитившие находки ученых в XX веке. Ньюбоулд утверждал, что его решение не может быть субъективным, так как он «не знал тогда*, что какая-либо туманность будет обнаружена в определенном таким образом районе».

* Во время вскрытия шифра.

Доклад Ньюбоулда произвел сенсацию в мире науки. Многие ученые, хотя и отказались высказать мнение об обоснованности примененных Ньюбоулдом методов преобразования текста рукописи, считая себя некомпетентными в криптоанализе, с готовностью согласились с полученными результатами. Один знаменитый физиолог даже заявил, что некоторые из рисунков рукописи, вероятно, изображают эпителиальные клетки, увеличенные в 75 раз. Широкая публика была очарована. Этому событию посвящались целые воскресные приложения к солидным газетам. Одна бедная женщина прошла сотни километров, чтобы попросить Ньюбоулда с помощью формул Бэкона выгнать злых духов-искусителей, которые овладели ею.

Через некоторое время всеобщее возбуждение спало. Ньюбоулд продолжил свою работу над рукописью. В 1926 г. он умер. Рабочие записки и главы для книги, которую Ньюбоулд собирался издать, были тщательно отредактированы и подготовлены к печати его другом Роланом Кентом. В 1928 г. они были изданы под названием «Шифр Роджера Бэкона». Американские и английские историки, занимавшиеся изучением средних веков, отнеслись к этой работе более чем сдержанно.

В 1931 г. Мэнли, подробно изучивший метод Ньюбоулда, пришел к выводу, что этот метод «вызывает возражения такого серьезного характера, что нельзя согласиться с его результатами». В

статье объемом в 47 страниц Мэнли указал, что бездоказательная система Ньюбоулда допускает слишком много различных трактовок. Поэтому шифровальщик никогда не сможет быть уверен, что его сообщение будет расшифровано правильно. Главная причина этой неопределенности кроется в процессе анаграммирования, поскольку с увеличением числа букв количество возможных анаграмм возрастает в геометрической прогрессии.

Мэнли также показал, что микроскопические значки стенографического письма являются не чем иным, как густыми чернилами, расползшимися на грубой поверхности пергаментной бумаги. Наконец, он раскритиковал отрывки открытого текста, полученные Ньюбоулдом, заявив, что они «содержат предположения и утверждения, которые не могли исходить от Бэкона или какого-либо другого ученого XIII столетия».

Никто не сомневался в честности Ньюбоулда. По словам Мэнли, Ньюбоулд просто пал жертвой «своего собственного энтузиазма и своего научного и изобретательного подсознания». Сенсационный крах теории Ньюбоулда не отпугнул других ученых от попыток дешифровать рукопись, хотя он и заставил их быть более осторожными при публикации своих открытий. Но не всех.

В 1943 г. адвокат одной нью-йоркской фирмы Джеймс Филине обнародовал отрывок открытого текста рукописи, который он якобы сумел получить. В переводе с латинского этот отрывок звучит так: «Превращенные в женщин, после того как они были сделаны женщинами, нажимают вперед; те, кто нажимает, увлажнены; у них раздуты вены; они лопнут; они уменьшились». Комментарии излишни.

Два года спустя авторитетный специалист по раковым заболеваниям доктор Леонелл Стронг пришел к выводу, что рукопись Войнича принадлежит перу Энтони Эскэма, английского ученого XVI века, автора известного травника. Стронг предал гласности текст формулы противозачаточного средства, якобы извлеченный им из рукописи посредством «двойной обратной системы арифметических прогрессий множественного алфавита», под которой он, по-видимому, подразумевал некую форму многоалфавитной замены. Противозачаточное средство действует на самом деле, и всякий, кто хочет испытать его, может это сделать, так как Стронг опубликовал его формулу. Однако он счел нецелесообразным поступить точно так же со своим методом криптоанализа, и поэтому истинность этого метода проверить невозможно. Что касается самого опубликованного Стронгом текста, против него были выдвинуты убедительные аргументы лингвистического характера, а появление формулы противозачаточного средства было объяснено подсознательной осведомленностью ученого.

С тех пор предпринималось еще много попыток дешифрования рукописи, результаты которых не публиковались, так как в конце концов все авторы честно признались в своей неудаче. Рукопись стала еще более таинственной, поскольку было обнаружено, что ее слова и группы слов повторяются чаще, чем в обычном языке. Уже один этот факт отличает рукопись от любых других криптограмм, поскольку все известные шифры стремятся избавиться от повторений, а не учащать их.

Одна из правдоподобных гипотез была выдвинута в 1944 г. и состоит в том, что рукопись представляет собой текст на каком-то искусственном, условном языке, в котором все сущее в природе разделено на категории, каждой категории придан ее основной знак, а подклассы определяются дополнительными значками, присоединяющимися к первому. Вполне очевидно, что в любом тексте на таком языке должны неоднократно повторяться корни слов, в то время как суффиксы видоизменяются — это явление очень характерно для рукописи Войнича.

Другим объяснением обилия повторений может служить предположение о том, что оно отражает многочисленные повторы фармацевтических формул, которые, несомненно, должны встречаться в любом травнике или медицинском трактате.

Однако люди раскрыли куда более глубокие тайны. Почему же никто не разгадал эту? По мнению Мэнли, причина заключается в том, что «попытки дешифрования до сих пор предпринимались на основе ложных предположений. Мы фактически не знаем, когда и где была написана рукопись, какой язык лежит в основе зашифрования. Когда будут выработаны правильные гипотезы, шифр, возможно, предстанет таким же простым и легким...».

Ну а может быть, это просто чудовищная фальсификация, подобно «кардиффскому гиганту»* или «пилтдаунскому человеку»**? Никто из изучавших рукопись Войнича так не думает. И для подобного вывода у них были серьезные основания.

* «Кардиффский гигант» — грубо выполненная статуя человека из гипса высотой более 3 м, тайно закопанная недалеко от города Кардиффа в штате Нью-Йорк и «найденная» в 1869 г.

** «Пилтдаунский человек» — доисторический человек, предположение о существовании

которого было сделано на основе фрагментов скелетов, найденных в Англии в селении Пилтдаун в 1911 г.; в 1953 г. установлено, что находка являлась фальсификацией.

Войнич умер в 1930 г. Его жена Этель* хранила рукопись в течение 30 лет вплоть до своей смерти в 1960 г. Душеприказчик Этель Войнич продал рукопись книготорговцу Краусу. Мнения по поводу ее ценности в наше время расходятся. Некоторые считают, что эта рукопись содержит информацию, которая могла бы дать новые сведения об истории человечества. «Когда кто-нибудь сможет ее прочитать, — заявил Краус после оформления сделки, — эта книга будет стоить миллион долларов». Другие думают иначе. Они оспаривают ее принадлежность перу Бэкона, отмечая, что рукопись больше похожа на работу XVI века, а также считают, что она не содержит ничего нового, что это, в конце концов, всего лишь разновидность причудливого травника.

* Войнич Этель — английская писательница, автор романа «Овод» (1897 г).

С тех пор книга мирно лежит в своем ящике в темном подвале Крауса, являясь, возможно, бомбой замедленного действия для истории науки и ожидая человека, который сможет объяснить эту самую загадочную рукопись в мире.

ПАТОЛОГИЧЕСКИЙ КРИПТОАНАЛИЗ

В криптоанализе болезненное состояние человеческого разума чаще всего проявляется в форме гипертрофированной криптоаналитической активности. Жертвы этого недуга занимаются чересчур тщательным криптоанализом совершенно невинных документов, исходя из предпосылки, что под внешне безобидной формой любой текст несет в себе тайную информацию. Одним из самых известных проявлений этой мании стал криптоанализ драматургических произведений Уильяма Шекспира, чтобы доказать, что истинным их автором был не кто иной, как Фрэнсис Бэкон.

Первым человеком, который начал публично утверждать, что дело обстоит именно так, был Игнатиус Доннелли, одна из самых колоритных политических фигур в истории Соединенных Штатов Америки. Это был круглолицый мужчина, обладавший большим умом и выдающимися ораторскими способностями, благодаря которым он завоевал себе широкую популярность. В возрасте 28 лет Доннелли стал помощником губернатора штата, а четыре года спустя, в 1863 г., был избран в конгресс. Политическая карьера Доннелли в конгрессе оборвалась в 1878 г. после того, как на перевыборах избиратели отклонили его кандидатуру.

В том же году, случайно услыхав о новой теории, которая приписывала авторство шекспировских пьес Бэкону, Доннелли преисполнился решимости осуществить план, о котором он написал в своем дневнике буквально следующее: «Зимой 1878/79 г. я собираюсь заново прочитать драматургические произведения Шекспира, но не так, как раньше, ради удовольствия, которое они неизменно доставляют мне, а сосредоточив все свое внимание на том, чтобы выявить, есть ли в них какие-либо признаки шифра. Объектами поисков во время моего чтения будут слова Фрэнсис, Бэкон, Николас* и сочетания «Шек» и «спир» или «Шекс» и «пир», которые могли бы вместе составить слово — Шекспир».

* Николас Бэкон — отец Фрэнсиса Бэкона.

Этими поисками Доннелли занимался на фоне другой, более серьезной литературной работы, которую он выполнял для того, чтобы содержать свою семью. В 1882 г. появилась его книга «Атлантида». В ней, проявив большую и разностороннюю эрудицию, Доннелли впервые связно изложил легенду древнегреческого философа Платона об исчезнувшем континенте, который в описании Доннелли превратился в настоящий райский сад.

Книга Доннелли имела огромный успех. В течение 8 лет она выдержала 23 переиздания в Соединенных Штатах и 27 — в Англии. Книга принесла ее автору гарантированный доход и сделала его одним из самых популярных писателей. В следующем году Доннелли опубликовал новую книгу под названием «Рагнарек*: век огня и гравия», которая также очень быстро разошлась. В ней была предпринята попытка доказать, что на ранней стадии развития Земля столкнулась с гигантской кометой. Библейская легенда о Содоме и Гоморре, евангельский рассказ о том, что по повелению Иисуса Христа Солнце приостановило свое движение, а также другие предания об аналогичных явлениях — все это, по словам Доннелли, подтверждало факт катастрофы.

* В переводе с древнескандинавского языка это слово означает «приговор богов».

Но даже в разгар усердной работы над «Рагнареком» Доннелли записал в своем дневнике: «Сейчас я подхожу, как я полагаю, к самому крупному открытию, которое я сделал, а именно — ко вскрытию шифра в драматургических произведениях Шекспира... Я доказываю, что автором этих пьес был Фрэнсис Бэкон... Я уверен, что в них спрятан шифр, и я думаю, что ключ к нему в моих руках. Все это не может быть случайностью». Год спустя идея вскрытия бэконовского шифра завладела им целиком. «Я думаю о нем в течение всего дня, я грежу о нем всю ночь напролет, это поразительно сложный и головоломный шифр». В мае 1884 г. утомленный до предела Доннелли с облегчением смог, наконец, приступить к написанию своего самого крупного литературного труда, который он озаглавил «Великая криптограмма».

В сентябре 1884 г., когда Доннелли снова повел избирательную борьбу за место в конгрессе, один из его знакомых пустил слух о том, что Доннелли обнаружил шифр в пьесах Шекспира. Известие об этом возбудило некоторый интерес, но победу на выборах Доннелли все равно одержать не смог. Тем не менее он продолжил свои занятия криптоанализом наряду с политической деятельностью.

1887 г. стал вдвойне знаменателен для Доннелли: он одержал победу на выборах в законодательный орган штата Миннесота, а также принял у себя дома профессора математики, который приехал с целью изучения предложенного Доннелли метода вскрытия шифра Бэкона. 28 августа нью-йоркские газеты на своих первых страницах опубликовали благоприятный отзыв профессора. Всю следующую зиму Доннелли работал по 14 часов в сутки, стремясь как можно скорее завершить книгу, написание которой он назвал «ужасной задачей». Весной он закончил ее последнюю страницу с «безмерным чувством облегчения».

Что же открыл Доннелли? По его словам, под видом драматургических произведений, авторство которых до сих пор приписывалось Шекспиру, он обнаружил повествование о том, что «Шекспир не написал в них ни единого слова» и что на самом деле «пишет их ваш кузен из Сент-Олбанса»*. Каким же образом Доннелли сделал свое открытие?

* Фрэнсис Бэкон носил дворянский титул виконта Сент-Олбанского.

Он приступил к исследованию исходя из допущения о том, что в текстах пьес Шекспира присутствует шифр Бэкона. Основываясь на этом предположении, Доннелли попытался найти последовательность чисел, которые помогли бы ему определить местонахождение слов тайного сообщения в открытом тексте шекспировских пьес. Например, по определенному правилу получить последовательность чисел 17, 18, 19, 20, чтобы затем показать, что 17-е, 18-е, 19-е и 20-е слова на 17-й, 18-й, 19-й и 20-й страницах какой-то пьесы составляют фразу: «Я, Бэкон, написал это». Начав с бесплодных поисков такой взаимосвязи в современном издании драматургических произведений Шекспира (как будто Бэкон предвидел точную нумерацию страниц «своих» пьес, которой будут пользоваться 200 лет спустя после его смерти!), Доннелли вскоре опомнился и перешел к. работе над первым сборником шекспировских пьес, опубликованном в 1623 г., за три года до смерти Бэкона.

В конце концов Доннелли стал получать результаты. Они не были такими же простыми и логичными, как приведенный выше пример. По какому-то косвенному умозаключению, суть которого Доннелли так никогда внятно и не изложил, он выбрал числа 505, 506, 513, 516 и 523 в качестве «корневых». Из этих чисел он вычитал иногда «константы», иногда «множители». От остатков Донелли отнимал количество слов, выделенных на странице курсивом. При этом ремарки иногда учитывались, а иногда нет. Полученные результаты затем изменялись путем прибавления или вычитания количества слов, написанных через дефис, и слов, заключенных в скобки (хотя Доннелли сам признает, что «иногда мы включали слова, заключенные в скобки, и дополнительные слова, написанные через дефис, а иногда мы их пропускали»).

Окончательная цифра указывала на позицию слова открытого текста на странице. Затем видоизменялась и сама страница: иногда на ней выбиралась первая колонка, иногда — вторая. Нередко подсчет начинался с начала сцены, а не с начала страницы, а кое-где — с ее конца. Доннелли ничуть не заботился о том, чтобы объяснить, почему он предпочел одну альтернативу другой, хотя излагал свои математические выкладки в таких мельчайших подробностях, что они производили на читателя поистине глубокое впечатление.

В целом «Великая криптограмма» Доннелли была составлена из «дешифрованных» отрывков

пьес Шекспира, которые сопровождались соответствующими вычислениями, а также доводами в защиту версии о существовании скрытого шифра и примененного Доннелли метода его вскрытия. Владелец издательской компании «Пил энд компани» выпустил первое издание книги тиражом всего 12 тысяч экземпляров. Однако, несмотря на солидную репутацию автора, она потерпела фиаско. Враждебно настроенные рецензенты подвергли ее суровой критике. Читатели сочли демонстрацию вскрытия шифра слишком запутанной. Но хуже всего было то, что по самому шифру были нанесены уничтожающие удары.

Житель штата Миннесота Джозеф Пайл спародировал не только название книги Доннелли, но и изложенный в ней метод вскрытия, написав свою собственную книгу «Крошечная криптограмма», в которой с помощью аналогичного метода вывел из «Гамлета» «открытый» текст следующего содержания: «Доннелли, писатель, политик и шарлатан, откроет тайну этой пьесы. Мудрец из Найнинджера* — выдающаяся личность».

* Найнинджер — город в штаге Миннесота, где родился Доннелли.

В столь уничтожающей критике Пайла поддержал преподобный А. Николсон, который в своем блестящем опровержении использовал одно из «корневых» чисел Доннелли, причем на тех самых страницах, на которых работал Доннелли, но с результатами «дешифрования», диаметрально противоположными выводам Доннелли. Открытый текст, прочитанный Николсоном, гласил: «Г-н Уильям Шекспир написал эту пьесу и работал у занавеса».

Не добившись признания на родине, Доннелли отправился в Европу для чтения лекций о своем методе дешифрования. В университетском студенческом клубе в Оксфорде, где он принял участие в дискуссии с одним известным шекспироведом, в результате голосования, проведенного среди присутствовавшей публики, Доннелли потерпел сокрушительное поражение при соотношении голосов 167 к 27. Критика приобретала все более и более резкий характер, и, когда Доннелли после 5-месячной поездки вернулся на родину, Пил сообщил ему, что его книга убыточна. Доннелли не поверил своему издателю и договорился с сыскной конторой «Пинкертон» об оказании услуг по проверке отчетной документации «Пил энд компани».

В отместку издательская компания возбудила против Доннелли иск о взыскании 4 тысяч долларов, выплаченных ему авансом в качестве авторского гонорара. Чтобы уладить дело, Доннелли передал «Пил энд компани» принадлежавшие ему участки земли в обмен на печатные формы, изготовленные для книги. «Я сложу их в своем саду и построю небольшой домик, чтобы укрыть их от зноя и дождя, — трогательно написал он в своем дневнике 22 декабря 1892 г. — Маленькое строеньице станет памятником моему колоссальному краху. Каждый раз, когда я посмотрю на него, я буду вспоминать о рухнувших надеждах и несбывшихся мечтах».

Доннелли оказался в чрезвычайно подавленном состоянии по той причине, что незадолго до того потерпел поражение на выборах губернатора. Тем не менее вскоре он воспрянул духом и возобновил борьбу, в которой его постоянно преследовали неудачи. Интересно отметить, что в своих дешифровках Доннелли старался изобразить Бэкона таким, каким он мысленно видел самого себя — мужественным и честным политическим деятелем, ставшим жертвой продажных честолюбцев и невежд. Доннелли никогда не терял веры в свои бэконовские открытия и продолжал заниматься вскрытием шифров. В 1899 г. на собственные средства он опубликовал книгу «Шифры в пьесах и на надгробиях». Едва она вышла в свет, как тут же была предана забвению. А 1 января 1901 г., в первый день XX века, Доннелли умер.

Говоря о «системе» Доннелли, можно отметить, что ничего подобного в криптоанализе не появлялось ни до него, ни после. Его «система» не имеет себе равных, поскольку лишена системы вообще. В выборе исходных чисел, на основе которых делались дальнейшие выводы, отсутствовала какая-либо схема или разумное начало. Хотя Доннелли работал всего лишь над несколькими страницами из двух частей пьесы Шекспира «Генрих IV», он заранее исходил из того, что грандиозные творения великого английского драматурга были лишь производным продуктом работы шифра. Неужели Фальстаф, удивительный Фальстаф с его бьющей через край энергией, существовал лишь для того, чтобы дать возможность озвучить полученный Бэконом шифртекст?! С мыслью об этом примириться очень и очень трудно.

Расправа Доннелли над логикой в криптоанализе привела к возникновению целой вереницы «призраков». В среде бэконианцев эти «призраки» почему-то считаются шифрами. Однако в действительности в них нет ничего от настоящих шифров. И методика их вскрытия на деле не имеет никакого отношения к криптоанализу, а результаты работы — к дешифрованным текстам подлинных

криптограмм. Они являются продуктом патологического криптоанализа. Предложение именовать все это «энигматологией», исходящее от одного бэконианца, подходит здесь как нельзя кстати, поскольку оно дает возможность не употреблять термин «криптоанализ» для манипуляций, не имеющих с ним ничего общего, и не называть «шифром» то, что заведомо шифром не является. Поэтому при дальнейшем изложении бэконовский «шифр» будет именоваться «энигмапланом», для определения процесса его вскрытия будет употребляться глагол «энигмализировать», а результат этой работы будет называться «энигмадукцией».

Наиболее известные энигмапланы стали предметом изучения Уильяма и Элизабет Фридман в их совместной книге «Исследование шекспировских шифров». Уже на одной из ее первых страниц Фридманы отметили, что в отличие, скажем, от какого-нибудь профессора английской филологии, у них не было «никакой профессиональной или эмоциональной предубежденности относительно любого конкретного утверждения об авторстве шекспировских пьес» и что «любые заявления, основанные на криптоанализе, могут быть научно исследованы и одобрены или опровергнуты». Они указали, что примут за настоящий любой из шифров, которые удовлетворяют двум условиям: первоначальный открытый текст, подвергнутый их действию, имеет смысл, а также является недвусмысленным и единственным в своем роде, то есть он не должен представлять собой один из нескольких возможных результатов дешифрования. Отметив это, Фридманы поставили перед собой задачу выяснить, обнаружил ли кто-либо в произведениях Шекспира настоящий шифр, вскрытие которого дало бы доказательство того, что они написаны другим лицом.

И хотя такого доказательства Фридманы не нашли, они сумели предложить читателю своего «Исследования шекспировских шифров» увлекательное путешествие по сюрреалистическому ландшафту, где супергении от литературы творят, превосходя самых плодовитых писателей по величию своих творений и наиболее даровитых философов по глубине мысли, просиживают дни и ночи, зашифровывая секретные сообщения, в которых они рассказывают о своих достижениях, и где неистовые энигматологи сколачивают наспех свои дикие и шаткие построения на зыбучих песках догадок. И хотя иногда Фридманы чувствуют себя оскорбленными поведением аборигенов этого ландшафта, они никогда не теряют самообладания. Как гиды, они мудры, учтивы и занимательны.

Фридманы знакомят своих читателей с Орвиллом Оуэном, врачом из американского города Детройта. Его основным инструментом было «шифровальное колесо». Оно состояло из тысячи страниц писаний елизаветинской эпохи, наклеенных на холст, который был намотан на две гигантские катушки. С помощью своего «шифровального колеса» Оуэн энигмализировал упомянутые выше страницы и в качестве энигмадукции получил автобиографию, в которой Фрэнсис Бэкон рассказывает о том, что он является внебрачным сыном английской королевы Елизаветы и графа Роберта Дадли и что он написал не только произведения Шекспира, но и многие другие известные сочинения.

Энигмаплан Оуэна имел в своей основе четыре ключевых слова «FORTUNE», «HONOR», «NATURE», «REPUTATION»*. Фридманы изложили правила энигмализации, произведенной Оуэном, так: «Сначала вы находите одно из ваших ключевых слов (или одно из его многочисленных производных). Затем вы отыскиваете подходящий текст где-либо неподалеку от того места, где оно встречается. Если вам удается его найти и он согласуется с желательной для вас версией, ваша цель достигнута».

* «УДАЧА», ЧЕСТЬ», «НАТУРА», «РЕПУТАЦИЯ»

Среди прочего Оуэн получил текст, согласно которому Бэкон зарыл оригинальные рукописи своих пьес в нескольких железных ящиках на территории замка Чепстоу в Англии. Оуэн отправился туда и занялся раскопками, несколько раз переходя от одного места к другому, поскольку энигмадукция указывала на разные части замка. Никаких рукописей найдено не было.

Некоторые бэконианцы утверждают, что они выявили «зашифрованные подписи» своего героя в шекспировских пьесах. Уолтер Аренсберг, состоятельный филадельфиец, попытался показать, что в течение сотен лет многочисленные читатели проявляли слепоту и не видели в этих пьесах очевидных признаков авторства Бэкона. Аренсберг нашел такую подпись в нравоучении Полония своему сыну Лаэрту из «Гамлета»:

Costly thy habit as thy purse can buy;
But not exprest in fancie; rich, not gawdie;
For the Apparell oft proclaimes the man.

And they in France of the best ranck and station*.

* Рядись, во что позволит кошелек,
Но не франти — богато, но без вычур.
По платью познается человек,
Во Франции ж на этот счет средь знати
Особенно хороший глаз.

«Обратите внимание, — писал Аренсберг, в этих строках буквы акростиха
Co
B
F
An
читаются как F Bacon*».

* Ф Бэкон.

Фридманы опровергли утверждение Аренсберга, старательно промаркировав первые буквы 20 тысяч строк первого сборника шекспировских пьес. Они вычислили, что вероятность группирования букв «B», «A», «C», «O» и «N» в слово «BACON» составляет лишь 0,0244 приблизительно на 100 тысяч строк. Именно поэтому Аренсберг не обнаружил ни одного такого акростиха. Ему пришлось расширить область поиска и включить в него также вторые буквы, что сразу же увеличило эту вероятность. В этом и состоит суть «открытия» Аренсберга. Если игральная кость выпадает вверх двойкой тысячу раз из 6 тысяч метаний, это доказывает только то, что случившееся, вероятно, могло произойти.

Фридманы также продемонстрировали, как энигматологи допускают натяжки, игнорируют или ломают свои собственные правила, если они стоят на пути успешной энигмализации. Например, скептически смотрят на множество анаграмм, получаемых из самого длинного шекспировского слова «honorificabilitudmitatibus» из реплики шута в пьесе «Бесплодные усилия любви».

Бэконианец Эдвин Дэрнинг-Лоуренс энигмализировал это слово как латинскую фразу следующего содержания: «Hi lu-di P Ba-co-nis na-ti tui-ti or-bi»*. В ответ Фридманы привели целый ряд других, в равной степени обоснованных анаграмм этого слова, одна из которых своим содержанием намекает на то, что именно Данте, умерший за 200 лет до рождения Шекспира, вполне мог являться фактическим автором пьес великого английского барда: «Ubi Italicus ibi Danti honor fit»**.

* «Эти пьесы, детище Ф Бэкона, сохраняются для всего мира».
** «Там, где есть итальянец, почести оказываются Данте».

В стихотворении «К читателю», помещенном под известным портретом Шекспира в первом издании сборника его пьес, некий Эдвард Джонсон узрел симметричную схему из 22 букв, которые после перестановки неожиданно дали фразу из 25 букв: «Fr Bacon author, author, author»*. Троекратный повтор слова «author» настолько подкрепил уверенность Джонсона в правильности произведенной энигмализации, что он бросил вызов скептически настроенным читателям:

* «Фр Бэкон автор, автор, автор»

«Если после проверки подписи под портретом... читатель все еще придерживается того мнения, что повторения являются чисто случайными, пишущий данные строки хотел бы попросить его проделать небольшой эксперимент. Пусть он возьмет из любой книги, древней или современной, 20 последовательно идущих одна за другой строк прозы или поэзии, расположит их буквы в таблице и затем попробует убедиться в том, сможет ли он составить из этих букв какое-либо слово, которое встречалось бы в тексте через одинаковые промежутки в виде цепочки».

Фридманы нашли затруднительным воспротивиться такой учтивой просьбе Джонсона:

«Мы решили использовать для этой цели текст, который брал в качестве примера сам Джонсон. Из стихотворения «К читателю» мы получили следующее сообщение: «Без обмана, Фрэнсис Бэкон: именно я написал эти пьесы! *Шекспир».* Наше сообщение почти в два раза длиннее фразы Джонсона.

Это законченное предложение, и в нем каждая буква схемы используется только один раз. Но слабость этого «метода» проявляется здесь весьма четко. Поскольку выбранные нами буквы не обязательно должны «появляться» в своем правильном «порядке» (то есть мы можем расставить их любым путем, каким нам только заблагорассудится), здесь может быть несколько альтернативных «сообщений» для выбора, причем одно из них, придающее совершенно другой смысл тексту, гласит: «Без обмана! Я, Фрэнсис Бэкон, написал эти шекспировские пьесы». Уже этого достаточно для того, чтобы показать, что метод Джонсона абсолютно ничего не стоит с точки зрения криптоанализа».

Почти все бэконовские энигмапланы имеют один серьезный недостаток: они допускают множество ответов, как это весьма убедительно продемонстрировали Фридманы. Такой недостаток сразу же делает несостоятельным любой метод секретной связи на основе этих энигмапланов. Кому нужен шифр, пользуясь которым отправитель никогда не может быть уверен в том, что сообщение, которое он зашифровывал, будет именно тем сообщением, которое его предполагаемый получатель расшифрует?

Практические соображения такого характера редко волнуют бэконианцев. Не часто они отвечают и на критику в свой адрес, а их защита чаще всего повторяет замечание, высказанное однажды Аренсбергом. Для того чтобы показать несостоятельность его системы, Фридманы воспользовались энигмапланом Аренсберга и энигмализировали из его книги фразу: «Автором был Уильям Фридман». С величайшей невозмутимостью Аренсберг ответил на это: «Проделанное вами не опровергает присутствия в шекспировской «Буре» фразы, которую я там нашел».

Но такой фразы как раз и нет в «Буре». Аренсберг извлек ее из тысяч букв, которые составляют пьесу. Это все равно что посмотреть на согни звезд в ночном небе и мысленно создать из них образ мифического героя или животного. Орион и Пегас существуют лишь в воображении наблюдателя, так же как и фраза Аренсберга. Энигмагология очень напоминает испытания, проводимые психологами, во время которых обследуемый человек должен рассказывать о том, что он видит в чернильной кляксе. Клякса конечно же не имеет определенной формы, и поэтому все, что рассказывает о ней обследуемый, исходит только от него самого. Думать, что воображаемые картины, навеяны ли они звездами, или чернильными кляксами, или литературными произведениями, существуют на самом деле, значит полностью оторваться от действительности. Однако есть один шифр, который для бэконианиев имеет особую привлекательность, поскольку был изобретен самим Фрэнсисом Бэконом.

Бэкон начал с того, что заменил 24 буквы английского алфавита* различными пятизначными перестановками букв «А» и «В»:

* Бэкон использовал буквы «i» и «j», а также «u» и «v» как равнозначные величины

a AAAAA e AABAA i ABAAA n ABBAA r BAAAA w BABA.A
b AAAAB f AABAB k ABAAB o ABBAB s BAAAB x BABAB
c AAABA g AABBA 1 ABABA p ABBBA t ВДАВА y BABBA
d AAABB h AABBB m ABABB q ABBBB v BAABB z BABBB

В этой кодировке, которую Бэкон назвал двухбуквенной, английское слово «but» будет иметь следующий вид:

«AAAAB BAABB BAABA».

Бэкон писал: «Эти шифрзнаки важны не только сами по себе, ибо открывают для человека путь, благодаря которому он может на любом расстоянии выражать и передавать свои мысли при помощи предметов, доступных зрению и слуху, лишь бы только они были способны на два различия. К таким предметам можно отнести, например, колокола, трубы, фонари и факелы, мушкетные выстрелы и иные средства подобного характера».

К предметам, которые «способны на два различия», относятся, в частности, типографские шрифты. Использование шифра Бэкона можно весьма четко проиллюстрировать, используя стандартную и полужирную формы любого шрифта. Буква «А» тайного послания будет передаваться стандартными литерами, а буква «В» — полужирными. Таким образом, вполне невинный текст «Do not go till I come»* будет содержать в себе предупреждение «Fly»**, если набрать этот текст как «Do **n**ot g**o** t**ill** I come».

* «Не уходите до моего прихода»
* «Бегите».

Приведенный пример не отличается особой утонченностью ввиду явного различия между стандартным и полужирным начертанием шрифтового рисунка. Однако первоначальная мысль Бэкона заключалась в том, чтобы использовать не две резко контрастирующие формы одного и того же шрифта, а два отдельных шрифта, имеющие лишь незначительные различия между собой. Если они будут иметь достаточно близкое сходство, обычный читатель так никогда и не заподозрит наличие в сообщении двух разных шрифтов. Получателю, расшифровывающему это сообщение, придется всего лишь заметить некоторые весьма тонкие расхождения в конфигурации, кривизне и размерах, скажем, строчных литер «r» в двух шрифтах, чтобы он был в состоянии отличить «r», передающую букву «A», от «r», соответствующей «B».

Естественно, что бэконианцы не замедлили обратиться к шифру, изобретенному их героем, для того, чтобы доказать свою правоту. Для начала ими была исследована эпитафия на первом надгробии могилы Шекспира:

Good Frend for Jesus SAKE forbeare
To diGG TE Dust EncloAsed HERE
Blese be TE Man thy spares TEs Stones
And curst be He thy moves my Bones*.

* Молю тебя, друг добрый, ради Бога,
Сей прах, что здесь зарыт, не трогай,
Благословен, кто камню дань возложит,
Будь проклят тот, кто кости потревожит.

В 1887 г. Хью Блэк, приняв строчные буквы за формы «A», а прописные буквы — за формы «B», отнеся две буквы «G» в слове «diGG» к строчным буквам и использовав сочетание «TE» в качестве одной прописной буквы, получил текст «saehrbayeeprftaxarawar».

«Для обыкновенного человека, — писали Фридманы в своей книге «Исследование шекспировских шифров», — этого текста было бы вполне достаточно, чтобы доказать, что никакой шифр здесь не используется. Бэконианец же отличается от обыкновенного человека, и разница между ними заключается, по нашему мнению, в степени упорства и изобретательности».

Блэк расположил буквы своего текста в особом порядке, провел линию, разделившую текст на две части, затем путем анаграммирования получил из первой части слово «Shaxpeare», а из второй -— «Fra Ba wrt ear ay», уверенно истолковав последнее как означающее «Фрэнсис Бэкон написал шекспировские пьесы».

Труд Блэка был подкорректирован и расширен неким Эдгаром Кларком. Из надгробной надписи он энигмализировал две фразы: «Fra Ba wryt ear. AA! Shaxpere» и «Fra B a wrt ear. HzQ AyA Shaxpere». Для него эти фразы означали следующее: «Фрэнсис Бэкон писал здесь. Да, да! *Шекспир»* и «Фрэнсис Бэкон писал здесь. Его реплика. Да, да! *Шекспир».* Среди многих энигматологов эпитафии на могиле Шекспира были и другие «первооткрыватели» — ничем не лучше Блэка и Кларка.

В 1899 г. был опубликован первый отчет об обнаружении послания, зашифрованного бэконовским шифром в том виде, в котором он был рекомендован к использованию самим Бэконом. Речь идет о творении под длинным названием: «Двухбуквенный шифр сэра Фрэнсиса Бэкона, обнаруженный в его трудах и расшифрованный г-жой Элизабет Гэллап».

50-летняя директриса мичиганской средней школы Элизабет Гэллап была честной, доброй и весьма религиозной женщиной, получившей образование в Сорбоннском и Марбургском университетах. Ее заинтересовали работы доктора Орвилла Оуэна, и она занялась своими собственными поисками тайных сообщений, основанных на двухбуквенном шифре.

Пораженная вариациями шрифта, использованного для набора первого издания пьес Шекспира, Элизабет Гэллап стала изучать печатный текст с помощью увеличительного стекла, чтобы выяснить, не говорили ли эти вариации о применении Бэконом двухбуквенного шифра. Поскольку различия наиболее резко проявились в курсивных буквах, для начала она попыталась расшифровать пролог к пьесе «Троил и Крессида», который почти целиком был набран курсивом. Медленно, но не ослабляя своего усердия, Элизабет Гэллап собирала по крупицам то с одних, то с других страниц сенсационную историю жизни Бэкона, аналогичную его автобиографии, энигмализированной Оуэном.

Вскоре Элизабет Гэллап обнаружила, что автобиографию Бэкона, засекреченную двухбуквенным шифром, можно найти не только у Шекспира, но и у других известных писателей. Автобиографическое повествование было непоследовательным, фразы прерывались в одной книге и продолжались в следующей, но их содержание повторялось все снова и снова, как будто Бэкон старался сделать так, чтобы по крайней мере одно из его сообщении было обязательно найдено.

Суть всех этих сообщений Элизабет Гэллап нашла в оглавлении первого издания пьес Шекспира:

«Королева Елизавета — моя настоящая мать, и я законный наследник трона. Найдите зашифрованную повесть, содержащуюся в моих книгах. Она рассказывает о великих тайнах, каждая из которых, будь она передана открыто, стоила бы мне жизни.

Ф. Бэкон».

Элизабет Гэллап открыла, что отцом Бэкона был граф Роберт Дадли, и в своей книге поведала историю, от которой у любого здравомыслящего человека волосы становятся дыбом. Якобы английская королева Елизавета, «не желая объявить себя женщиной неповенчанной и беременной на седьмом месяце», родила мальчика, которого она позднее отдала Николасу Бэкону на воспитание: «Та, что родила меня, даже в час моего нежеланного появления, неистово подавляя все естественные инстинкты женщины-матери, испытывая родовые муки и страдания, лелеяла одно сокровенное желание. «Убейте, убейте, — кричала эта обезумевшая женщина, — убейте!»

В 1907 г. Элизабет Гэллап отправилась в Англию на поиски рукописей, которые, согласно ее дешифровкам, находились либо в лондонском замке, где одно время жил Бэкон, либо в его сельском поместье в пригороде. Однако в замке к тому времени была произведена перестройка, а от поместья остались только развалины, и Элизабет Гэллап, так же как и доктору Оуэну, не удалось найти никаких рукописей Бэкона.

Спустя несколько лет после возвращения Элизабет Гэллап в Соединенные Штаты ее нанял американский миллионер Джордж Фабиан для работы в своих Ривербэнкских лабораториях. Он финансировал раскопки Оуэна и узнал от него об исследованиях Элизабет Гэллап. В Ривербэнке она должна была продолжить «дешифрование» рукописей, для чего ей в помощь был выделен штат сотрудников и предоставлено специальное фотооборудование. Богач Фабиан надеялся завоевать славу литературного первооткрывателя. Чтобы создать рекламу работе Элизабет Гэллап, Фабиан регулярно приглашал в Ривербэнк видных ученых, за свой счет кормил их, обеспечивал жильем и развлекал, в первый же день потчуя их прекрасно организованной лекцией о двухбуквенном шифре с показом диапозитивов и призывая без предубеждений побеседовать с Элизабет Гэллап.

Элизабет Гэллап покинула Ривербэнк лишь за несколько лет до своей смерти. Она скончалась в 1934 г. в возрасте 87 лет, не издав больше никаких работ по «дешифрованию».

Среди ассистентов Элизабет Гэллап были Уильям Фридман и Элизабет Смит, будущая г-жа Фридман Мисс Смит, поначалу восхищавшаяся той легкостью, с которой Элизабет Гэллап извлекала информацию там, где сама мисс Смит видела лишь тарабарскую грамоту, обнаружила, что ее восхищение постепенно переросло «сначала в неловкое недоумение, потом в мучительное сомнение и в конце концов в откровенное недоверие». «Я могу категорически засвидетельствовать, — написала она, — что ни мне, ни какому-либо другому добросовестному научному сотруднику в Ривербэнке никогда не удавалось извлечь ни одной сколько-нибудь длинной фразы скрытого сообщения. Ни один из нас не смог самостоятельно воспроизвести хотя бы одно полное предложение из тех, которые г-жа Гэллап уже дешифровала и опубликовала».

Это свидетельство никоим образом не опровергает возможного существования двухбуквенного шифра в первом издании шекспировских пьес. Ведь вполне можно предположить, что Элизабет Гэллап просто неправильно вскрыла его. Поэтому Фридманы собрали заявления других экспертов, указывавшие на то, что никакого шифра не существовало.

Оказалось, что печатники того времени часто изменяли написание фамилий авторов для того, чтобы облегчить себе набор текста. Из-за плохого качества краски буквы, отпечатанные одной и той же формой шрифта, оказывались разными. Перед печатанием бумага смачивалась и, поскольку высыхала неровно, давала усадку. В результате идентичные буквы получались разных размеров. Нередко «закрытые» буквы «а», «е», «о» заполнялись изнутри краской, что смазывало различия между ними. Поэтому отдельные экземпляры издания в целом сильно разнились между собой. А следовательно, ни одно сообщение, зашифрованное двухбуквенным шифром, не могло быть передано в них с абсолютной точностью.

Окончательные доказательства отсутствия двухбуквенного шифра в произведениях Шекспира были получены от двух экспертов. Прежде всего, они поступили от Фредерика Гауди, одного из самых известных и авторитетных типографов Америки. В 1920 г. Фабиан поручил ему выяснить

присутствие двухбуквенного шифра в первом издании пьес Шекспира, а потом скрыл полученный доклад, ибо Гауди подверг тщательным измерениям, анализу и сопоставлениям буквы этого издания, нарисовал их эскизы и в конечном итоге пришел к выводу, что в нем использовалось множество шрифтовых рисунков, а не два рисунка, которые требовались для двухбуквенного шифра. Такой же вывод сделал и Фред Миллер, занимавшийся в ФБР экспертизой документов. В своем заключении после исследования текста первого издания пьес Шекспира он написал: «Не было обнаружено никаких характеристик, которые подтвердили бы разделение исследованного текста ни два комплекта шрифтов».

Казалось бы, сказано ясно и недвусмысленно. Однако защитники версий об авторстве Бэкона, хотя и именуют себя учеными, не удосуживаются заново пересмотреть свои выводы, произвести новые испытания, подвергнуть собственные суждения проверке в свете новых данных. Вместо этого они поносят своих критиков, прибегают к различным увертками и изыскивают всяческие оправдания. Не было случая, чтобы они когда-нибудь признались, что, возможно, ошибаются. Когда Элизабет Гэллап, чтобы добиться желаемого результата, была вынуждена выдать белое за черное, она призвала на помощь такое «липовое» объяснение: ошибка была-де умышленно включена автором для введения в заблуждение, потому что «шифры делаются для того, чтобы скрывать смысл послания, а не раскрывать его».

Когда Фридманы полностью и окончательно развенчали энигмапланы, бэконианцы неожиданно выдвинули новые доводы, которые они никогда ранее не приводили: «Хотя этот шифр может считаться недействительным по современным стандартам строгой криптографии, он предоставляет своим создателям вполне надежный метод записи исторических фактов или личных мнений, которые они были не в состоянии выразить открыто без серьезного риска». Ни йоты доказательства этому не существует, если, конечно, не считать самих голословных утверждений бэконианцев. Более того, на каждое «предположение» в пользу Бэкона можно при желании вывести эквивалентное предположение в пользу Шекспира. Но этим заниматься столь же бесполезно, как бесполезно возражать телевизору, ибо бэконианцы не стремятся к познанию. Они не ученые, а проповедники.

Перед лицом каких свидетельств бэконианцы могли бы отказаться от своих утверждений? Перед лицом найденной авторской рукописи «Гамлета»? Если судить по опыту, они непременно заявят, что Шекспир переписал ее по распоряжению Бэкона. Или перед лицом обнаруженной записки Бэкона о том, что он ненавидел пьесы Шекспира и не имел ничего общего с этой дешевой стряпней? Бэконианцы и здесь найдутся: это-де, несомненно, умный прием, специально придуманный Бэконом для того, чтобы сбить с толку своих современников.

А так ли важно, кто написал шекспировские пьесы? В конце концов, имеет значение содержание самих пьес, а не их авторство.

Да, важно, так как в любом вопросе важна правда. По своему характеру ошибка бэконианцев выходит далеко за рамки вопроса об авторстве Бэкона и Шекспира. Если можно доказать, что свидетельства в пользу Шекспира не означают того, о чем они говорят, что они были фальсифицированы, чтобы подкрепить гигантскую мистификацию, которая остается нераскрытой в течение многих столетий, тогда с таким же успехом можно доказать, что другим историческим свидетельствам тоже нельзя доверять и что история — это пустая болтовня.

Справедливости ради надо сказать, что бэконианцы не являются единственными энигматологами. Габриэль Россетти, итальянский националист XIX века, «нашел» в «Божественной комедии» Данте секретный язык, которым некое тайное общество, выступавшее против политической и церковной тирании, формулировало свои цели и уведомляло о своей деятельности. Другие энигмадукции были извлечены из Библии, трактатов Аристотеля, а также из прочих, менее великих литературных творений человечества.

Энигматологов так же бессмысленно пытаться разубедить в их взглядах на разумной основе, как и демонстрировать пациенту психиатрической больницы фотоснимки похорон Эйнштейна, чтобы доказать этому пациенту, что он не Эйнштейн. Дело в том, что ни психически больные, ни энигматологи не выражают своих взглядов разумно. Они делают это эмоционально. Проблема энигматологии является по своей природе не логической, а психологической: энигматологи живут в мире иллюзий. Энигмадукции являются классическими результатами игры воображения. Они также подобны раковым опухолям на теле криптоанализа. Они представляют собой патологический криптоанализ.

ГОЛОСА ПРЕДКОВ

В конце каждого года редакция американского научного журнала «Очерки из истории греческой литературы» выпускает итоговый номер. В его статьях подробно рассматриваются узкие исторические вопросы греческой филологии, представляющие интерес для специалистов. Стиль этих статей ровный, повествование бесстрастное, заголовки сдержанные.

В одном из таких номеров можно найти статью, мало чем отличающуюся от других. В ней разбираются дебри глагольных окончаний и других грамматических форм греческого языка. Сугубо академичный заголовок этой статьи также ничем не примечателен: «Свидетельства о греческом диалекте в микенских архивах». Тем не менее после ее прочтения в воображении читателей возникают наполненные криками равнины вокруг обдуваемой ветрами Трои и развевающиеся султаны из конских хвостов на блестящих шлемах воспетых Гомером героев, толпящихся под стенами и башнями этого древнего города.

Дело в том, что в статье сообщается о дешифровании древнегреческого письма, оставленного на глиняных табличках в те времена, когда по земле ходили Ахиллес и Агамемнон, Елена и Менелай. В ней описывается одна из многих дешифровок, благодаря которым приглушенные голоса наших предков, молчавших несколько тысячелетий, через бездны времени и пространства дошли до ныне живущих людей. Некоторые из этих дешифровок следует причислить к величайшим достижениям человеческого ума, ибо они отвечают на вопросы о том, как прочитать неизвестную письменность давно умерших и как звучат слова тех, чьи голоса сегодня могут почудиться только в завываниях ветра.

При решении задачи дешифрования древней письменности используются некоторые методы криптоанализа. С одной стороны, для криптоаналитика такая задача легче, чем классическая проблема вскрытия шифра, так как здесь не надо иметь дело с сознательным стремлением скрыть информацию. С другой стороны, она является более трудной, поскольку иногда для ее решения бывает необходимо восстановить весь язык. Возможны четыре варианта.

В нулевом варианте известны и письменность, и язык. Поэтому никаких трудностей не возникает: англичанин может читать на английском, пользуясь знакомым ему алфавитом.

В варианте I язык известен, а письменность неизвестна. Эта задача равнозначна вскрытию шифра замены. Если письменность основана на алфавите, то ее дешифрование проводится методами, применяемыми при вскрытии однозначной буквенной замены. Если это слоговое письмо, например «катакана», то оно дешифруется способами, используемыми при криптоанализе номенклаторов. Если письмо идеограммное, как в китайском языке, то решение задачи напоминает вскрытие кода.

В варианте II письменность известна, а язык неизвестен. Американец, не знающий итальянского языка, может прочитать вслух статью из итальянской газеты на языке, близком к итальянскому, но он ничего не поймет в том, что произнесет. Задача, с которой сталкивается дешифровальщик в варианте II, подобна той, которую пришлось бы решать американцу, пожелавшему выучить итальянский язык без грамматических справочников и словарей, имея лишь некоторые картинки к текстам и их английский перевод, а также зная родственные языки, например испанский и латинский.

В варианте III ни письменность, ни язык не известны. В условиях культурной изоляции задача дешифрования никогда не будет решена. Но часто случается так, что, хотя в начале изучения и письменность, и язык неизвестны, позднее с помощью дополнительной информации, доступной благодаря другим источникам, удается установить значение звуков письма. Их перевод и привлечение родственных языков дают возможность восстановить и сам язык. Таким образом, в варианте III задача дешифрования сводится к последовательному решению задач в вариантах I и II.

Дешифрование для варианта I зачастую выглядит как пример из учебника по элементарному криптоанализу. Осенью 1946 г. известный французский востоковед Эдуард Дорм взялся за изучение надписей, найденных во время раскопок в сирийском городе Библе. Письмо имело сходство с иероглифическим, но не обретало смысла при попытках его прочитать. Учитывая место, где были обнаружены надписи, а также их возраст, Дорм уверенно предположил, что имевшиеся у него примерно 100 письменных знаков относятся к финикийскому языку. Их количество наводило на мысль о слоговом характере письменности, при котором каждый знак соответствует слогу. Но обычное финикийское письмо в соответствии с нормами, присущими семитским языкам, передает все слова лишь костяком входящих в них согласных букв. Поэтому у финикийцев слова «мистер» и «мастер» выглядели бы как «мстр».

Поскольку звучание слов найденного в Библе письма было никому не известно, Дорм не мог восстановить гласные звуки древнего слогового языка, на котором оно было написано. Но это не обескуражило 65-летнего ученого, награжденного орденом за успешные криптоаналитические разработки во время Первой мировой войны, и он энергично принялся за дешифрование найденных в

Библе псевдоиероглифов, предположив с самого начала, что семь знаков в нижнем левом углу глиняной таблички означают дату вступления очередного финикийского царя на престол.

«Без колебаний я придал знакам, предшествующим дате, значение «в годы» или «в год». Это предположение позволило мне пренебречь внешним видом знака при определении его звукового значения. Вся моя работа теперь состояла в том, чтобы разносить эти четыре буквы по соответствующим позициям, и в том, чтобы заполнять пустые места результатами перекрестной проверки, пользуясь моим знанием финикийского языка.

В первой строке таблички я нашел группу «n?s», а поскольку табличка была медной, я восстановил слово «nhs» («медь» или «бронза»). Звук «h», отождествленный со знаком, изображающим птицу, дал мне окончание «??bh», по которому я узнал слово «mzbh» («алтарь»). Получив таким образом «m» и поставив его на место предпоследнего знака в 14-й строке, я обнаружил сочетание «btm?», которое могло обозначать лишь «в месяц Таммуз». Теперь я уже располагал вторым «z», которое я обозначил как «zl».

Но названию месяца должно предшествовать упоминание о дне. Так как в 14-й строке чисел не было, в группе «s?s» я узнал название числа и сначала принял эту группу за «sls», что означает «три». После некоторых безуспешных попыток пристроить куда-нибудь согласный звук «l» я понял, что в действительности это было не «sls» («три»), а «sds» («шесть»). К отождествленным знакам добавилось «d»...

Всякий занимавшийся такого рода дешифрованием, в котором беспрестанно приходится пускать в ход то карандаш, то резинку, когда разносишь сначала одни предполагаемые значения, потом вместо них другие, уступающие место окончательным решениям, — поймет, ценою каких усилий мне удалось составить слоговый алфавит и прочесть финикийские слова, скрывавшиеся в этом непрочитанном письме, которое, по мнению специалистов, не поддавалось дешифрованию...»

Дорм считал, что поскольку латинский алфавит произошел от греческого, греческий — от финикийского, а финикийский — от египетских иероглифов, то проведенная им дешифровка является новым связующим звеном «между иероглифами и латинским алфавитом». Некоторые ученые оспаривают это толкование, но мало кто сомневается в том, что благодаря работе Дорма в распоряжении историков появились доселе неизвестные документы.

Что же касается задач для варианта II, то их решение к дешифрованию никакого отношения не имеет. В действительности это восстановление языка. Таких задач было решено много, особенно в пору бурного развития лингвистических наук в XIX веке.

Одной из самых известных задач, относящихся к варианту III, является загадка иероглифов майя. Ее удалось разгадать при помощи современного всепобеждающего оружия криптоаналитиков — компьютера. Три советских математика Е.В. Евреинов, Ю.Г. Косарев и В.А. Устинов первыми применили компьютерную технику для дешифрования древней письменности. Они предположили, что наиболее часто высеченные на камнях знаки представляют запись самых частых звуков языка майя. А этот язык и его звуки были известны, во-первых, из двух майя-испанских словарей, составленных в период завоевания земель майя европейцами, во-вторых, из переродившегося языка майя, на котором все еще говорят на Юкатане, и в-третьих, из текстов, записанных жрецами племени майя с помощью алфавита конкистадоров.

Советские математики записали 60 тысяч слов, взятых из этих текстов, в память компьютера. В результате произведенных вычислений они установили, что в исследованных словах имеются 70 пар букв, которые приходятся на половину начал этих слов. Они также нашли 73 иероглифа, которые присутствуют в половине начал слов, высеченных на камнях, и отождествили обе группы. После этого в ходе 40-часовой электронной «блицдешифровки» ученые из СССР установили аналогичные соотношения для средних и конечных групп в словах. На основании найденных соотношений они пришли к окончательному выводу о том, что им удалось успешно дешифровать письменность майя. Вот образцы прочитанных ими прекрасных древних афоризмов на языке племени майя: «Молодой бог маиса обжигает сосуды из белой глины» и «Бремя, возложенное на женщину, — это бог войны».

АНАТОМИЯ КРИПТОАНАЛИЗА

Криптографию и криптоанализ иногда называют науками-двойниками. И действительно, на практике они взаимно дополняют друг друга: то, что одна наука создает, другая разрушает, и наоборот. Однако но своей природе криптография и криптоанализ различаются весьма существенно. Шифровальное дело абстрактно и до предела теоретизировано. Взлом же шифров эмпиричен и конкретен.

Голландский криптограф Моуриц Фрис так написал о теории шифрования: «Вообще криптографические преобразования имеют чисто математический характер. Например, перестановки набора первичных элементов (букв алфавита), преобразования координат узлов решеток, сложение и вычитание в конечных кольцах, линейные алгебраические преобразования. Простым примером таких математических преобразований, используемых для засекречивания, служит равенство: $y = ax+b$, где x — буква сообщения, y — буква шифртекста, полученная в результате операции шифрования, a и b являются постоянными величинами, определяющими данное преобразование. Таким образом, вычисления над буквами легко выполняются после определения для них соответствующего алгебраического закона».

Операции шифрования и их результаты настолько же универсальны и справедливы, насколько это свойственно законам математики. Отрицать, что при применении классического шифра Виженера* буква «d» открытого текста дает знак «F» шифрованного, невозможно точно так же, как и заявлять, что 4 + 2□ 6. Эта истина была справедлива в XIV веке во Франции, когда Виженер изобретал свой шифр. Будет она верна и десять веков спустя на Марсе. Различные шифры, как и разные геометрии, дают отличные друг от друга, но одинаково действительные результаты.

* Для засекречивания сообщений в этом шифре используется математическое преобразование вида $y = x + 2$, в котором, как и у Фриса, x — это буква открытого текста сообщения, а y — соответствующий ей знак шифртекста.

В криптоанализе положение несколько иное. Эта наука пользуется методологией других наук, изучающих материальный мир. Ее методы основаны не на неизменных законах математической логики, а на подмеченных фактах реального мира. Криптоаналитик получает эти факты с помощью экспериментов и измерений. В противоположность криптографу, который может вывести уравнение шифрования для классического шифра Виженера, не прибегая к дополнительным опытам, криптоаналитик, имея любое число высказываний об английском языке, априори не может сказать, какая буква встречается в нем наиболее часто. Он должен сперва подсчитать частоту встречаемости всех букв. В криптоанализе факты могут быть постоянными в каждом конкретном случае, но они логически не обусловлены и зависят от обстоятельств, от реальной действительности.

Эмпирический характер криптоанализа наиболее отчетливо проявляется в его операциях. Последние проделываются в четыре этапа, которые можно найти в других науках, занимающихся материальным миром. Эти этапы включают. 1) анализ (подсчет букв); 2) выдвижение гипотезы (знак x в шифртексте, возможно, заменяет букву «е» открытого текста); 3) предсказание (если x означает «е», то появляются некоторые возможности для нахождения открытого текста); 4) проверку (такие возможности существуют) или опровержение (таких возможностей нет, так что x вовсе не означает «е»). Данный научный метод, общий для криптоанализа и для других естественных наук, оправдывает употребление метафор вроде: «Он пытался дешифровать историю Земли, изучая отложения пород».

В криптоанализе применяются два метода — дедуктивный и индуктивный. Дедуктивные решения основываются на анализе частот встречаемости и используются при вскрытии любого шифра. Индуктивные решения основываются на вероятных словах или на благоприятном стечении обстоятельств, например наличии двух шифртелеграмм с одним и тем же открытым текстом.

Типичный силлогизм при анализе частот встречаемости букв в телеграмме на английском языке, засекреченной шифром простой однобуквенной замены, имеет в качестве универсальной посылки утверждение о том, что самым частым знаком в шифртелеграмме, вероятно, является замена для буквы «е», а в качестве частной — заявление о том, что знак x встречается в шифртелеграмме наиболее часто. Вывод: знак x шифртекста, вероятно, заменяет букву «е» открытого текста. Поскольку всем языкам присущи строго определенные характеристики частот встречаемости букв, этот дедуктивный метод, как известно, применим к любой шифрованной телеграмме еще до ее изучения.

По своему характеру такой подход к дешифрованию является априорным. При наличии достаточного объема шифртекста он всегда дает правильный ответ и поэтому представляет собой общее решение.

С другой стороны, вскрытие шифра индуктивными методами может быть успешным лишь при выполнении определенных условий. Поскольку криптоаналитик не может сказать, действительно ли выполнены определенные условия, пока он не получит шифртелеграмму и не познакомится с ее особенностями, индуктивные методы вскрытия шифров по своему характеру являются

апостериорными.

Если противник посылает шифрованное сообщение сразу же после того, как он был подвергнут массированному артиллерийскому обстрелу, за которым последовала танковая атака, криптоаналитик вполне может предположить, что в открытом тексте посланной шифровки содержатся слова: «артиллерийский обстрел» или «атака». Он может использовать эти вероятные слова для того, чтобы прочесть шифровку*. Рассуждения криптоаналитика основываются на множестве конкретных фактов, связанных с перехваченным шифрованным сообщением, и кристаллизуются всего в один вывод относительно открытого текста этого шифрсообщения. Такие рассуждения чисто индуктивны.

* Распространенные слова «что», «и» и определенный артикль, которые очень часто можно найти во всех текстах на английском языке, в этом смысле но являются вероятными.

То же можно сказать и о криптоаналитических рассуждениях, используемых при вскрытии шифров в других особых случаях.

Так как наличие вероятных слов и особые случаи позволяют криптоаналитику добыть дополнительную информацию, такое вскрытие шифров является весьма эффективным и плодотворным. Поэтому криптоанализ новых шифрсистем чаще всего начинают именно с них. К сожалению, этот подход ограничен конкретными ситуациями, и от него криптоаналитики, как правило, затем переходят к поиску общего дедуктивного решения, основанного на частоте встречаемости букв.

Представление о криптографии как о математической науке, которое впервые сформулировали в своих работах Бэббидж* и Фрис, позволило глубоко изучить ее. Осознание этого факта породило также новые способы аналитического вскрытия шифров.

* Бэббидж Ч. — английский математик, в XIX в. разработавший идею вычислительной машины, осуществленную лишь в середине XX в.

Применение принципа частот встречаемости букв в криптоанализе постепенно ширилось. В результате были вскрыты шифры, которые вначале казались ему неподвластными. Затем этот принцип столкнулся с явлением, на котором основывается современный криптоанализ, — с постоянством частотных характеристик текстов. Только после Первой мировой войны в криптоанализе возникла новая замечательная теория, которая дала объяснение этому явлению и всему процессу самого криптоанализа. Она позволила, наконец, ясно и четко понять, почему вообще возможно аналитическое вскрытие шифров.

Часто не учитывают поразительной стабильности и универсальности частот букв. Кроме криптоанализа есть и другие виды человеческой деятельности, в которых постоянство частот букв всегда принимается во внимание, поскольку пренебрежение этим явлением может причинить большие материальные убытки. Для иллюстрации этого положения обратимся к некоторым забавным фактам, прямо не связанным с криптоанализом.

В 1939 г. в США был напечатан 267-страничныи роман со скромными литературными достоинствами, но настолько оригинальный, что в своем роде у него нет равных во всей многовековой истории английского языка.

Само название романа указывает на его уникальность: «Гэдсби — роман, содержащий более 50 тысяч слов без буквы «е». Это — поразительное творение. Пусть скептически настроенный читатель убедится сам, как долго приходится подбирать хотя бы одно предложение на английском языке без использования буквы «е». Автор «Гэдсби», Эрнст Райт, перечислил некоторые трудности, с которыми он столкнулся при написании «Гэдсби». Ему приходилось избегать употребления большинства правильных глаголов в прошедшем времени, так как они оканчиваются на «ed». Он не мог использовать определенный артикль «the» или местоимения «he», «she», «they», «we», «me» и «them»*. В «Гэдсби» надо было отказаться от просто незаменимых глаголов «are», «have», «were» и «be»** и крайне необходимых слов, как «there», «these», «those», «when», «then», «more», «after» и «very»***.

* «Он», «она», «они», «мы», «мне» и «им».

** «Являются», «иметь», «являлись» и «быть».

*** «Там», «эти», «те», «когда», «затем», «больше», «после» и «очень».

Строго придерживаясь избранного им принципа, Райт отказался от использования числительных между 6 и 30 даже в цифровом написании, так как буква «e» используется при их написании прописью. Райт жаловался: «Почти непреодолимая трудность возникла при введении в повествование молодых женщин: ведь про них не напишешь, что им за тридцать». Были изъяты также сокращения «Mr.»* и «Mrs.»** из-за присутствия «e» в полном написании этих слов. Сложную задачу приходилось решать в конце почти каждого длинного абзаца: будучи не в состоянии найти слово, не содержащее «e», которым можно было бы закончить мысль, автор возвращался назад и переписывал весь абзац.

* «Г-н».
** «Г-жа».

Райт так часто испытывал искушение использовать запрещенное слово, что ему пришлось заклинить рычаг буквы «e» на пишущей машинке, чтобы исключить ее попадание в текст. В предисловии к своей книге автор сообщает: «Часто буква «e» пыталась-таки проскользнуть незамеченной. Когда я писал, первоначально от руки, вокруг моего стола столпилась целая армия крохотных «e», нетерпеливо ожидавших, когда их позовут. Но постепенно, наблюдая, как я пишу, не замечая их, они забеспокоились и, возбужденно перешептываясь, стали вскакивать верхом на мое перо, постоянно посматривая вниз в надежде улучить момент и прыгнуть в какое-нибудь слово. Они вели себя, как морские птицы, удобно рассевшиеся для охоты за проплывающей рыбой. Но когда они увидели, что я уже отмахал 138 страниц на бумаге машинописного формата, они соскользнули на пол и, взявшись за руки, удалились с поникшими головами, а потом, обернувшись, прокричали: «Представляем, какую тарабарщину ты там нацарапал без нас. Вот уж, право, человек! В любом рассказе нас всегда пишут сотни тысяч раз! А сейчас нас гонят прочь! Впервые за всю нашу жизнь!»

Райт говорил, что для написания романа ему потребовалось «пять с половиной месяцев упорного труда, причем в тексте пришлось сделать столько подчисток и поправок, что при воспоминании о них меня до сих пор бросает в дрожь». Эти эмоции Райта наглядно свидетельствуют о всепроникающей распространенности одной только буквы английского языка. Остальные буквы тоже держатся цепко.

Не только Райт, но и другие авторы написали, в качестве литературных курьезов, липограммы, то есть сочинения, из которых намеренно исключается одна или несколько букв. Древнегреческий писатель Трифиодор сочинил «Одиссею», в первой книге которой не встречалась буква «α», во второй «β» и т. д.

Несмотря на постоянство частот встречаемости букв и на большое различие частот отдельных букв во всех языках, они не настолько заметны, чтобы об их существовании знали все. Одним из людей, которые, очевидно, и не подозревали об этом, был Латам Шоулс, изобретатель пишущей машинки, увековечивший ее ужасную клавиатуру.

Такая клавиатура с неудобным размещением букв впервые появилась в опытном образце, изготовленном в 1872 г. Остатки алфавитного порядка сохранились в расположении букв «d», «f», «g», «h», «j», «k», «1» во втором ряду, а в верхний ряд были включены буквы слова «typewriter»*, чтобы торговцы могли их легко найти при демонстрации работы.

* «Пишмашинка».

Клавиатура с неудачным подбором букв первого ряда «q», «w», «e», «r», «t», «y», «u», «i», «o», «p» оборачивается для предпринимателей потерями времени и денег. Несмотря на то, что основная рабочая нагрузка у большинства людей приходится на правую руку, при такой клавиатуре левая рука делает более половины всех ударов. Получается, что для печатания слов вроде «federated»* и «addressed»** левая рука лихорадочно мечется по клавишам, а правая тем временем пребывает в абсолютном покое. Кроме того, получается, что два самых «работящих» пальца правой руки приходятся на клавиши с наиболее редкими буквами английского алфавита — «j» и «k».

* «Объединенный в федерацию».
** «Адресованный».

Ввиду этих вопиющих недостатков было разработано множество других, более удачных клавиатур. Однако все нововведения были отвергнуты машинистками, не захотевшими переучиваться для работы на новой клавиатуре, и фирмами, не желающими платить за переделку

печатающих машинок, имеющих стандартную клавиатуру Шоулса.

В тех случаях, когда изобретатели и предприниматели учитывают явления, связанные с частотами встречаемости букв, они могут получить значительную дополнительную прибыль. Наиболее ярким примером является Ф. Морзе. В 1838 г. он решил использовать алфавитную систему сигналов для своего только что изобретенного электромагнитного телеграфа. Морзе сосчитал буквы в наборной кассе типографии одной филадельфийской газеты и присвоил наиболее короткие сочетания из точек и тире самым частым буквам.

За небольшими исключениями Морзе придерживался этого правила и при создании своего знаменитого кода, поставив в соответствие самый короткий знак (точку) самой распространенной букве («e»), другой короткий знак (тире) — следующей часто встречающейся букве («t») и т. д. При использовании современного кода Морзе, слегка отличающегося от его первоначального варианта, на передачу телеграммы из 100 букв на английском языке требуется около 940 знаков. Если бы код Морзе был составлен произвольным образом, то на такую же телеграмму потребовалось бы около 1160 знаков, или примерно на 23% больше. Благодаря проницательности изобретателя, принесшей, кстати, значительные денежные выгоды его потомкам, стало возможно передавать за один сеанс почти на 25% больше телеграмм, чем в случае, если бы Морзе составлял свой код наугад.

Из этих примеров видно, что частоты букв действительно довольно постоянны. Неоднократно проведенные опыты по их подсчету подтверждают этот факт. Например, восемь немецких криптоаналитиков независимо друг от друга подсчитали частоту буквы «e» в различных текстах на родном языке объемом примерно в тысячу букв. Полученные ими результаты колеблются от 16 до 19,2%. Эти цифры можно сравнить с подсчетом частот встречаемости букв, проведенным в лингвистических целях немецким филологом Ф. Кёдингом в 1898 г. Его подсчет можно принять за эталон: Кёдинг обработал 59298274 буквы, извлеченные из 20 миллионов слогов немецкого языка. Среди них он насчитал 10598015 букв «e», или 17,9%. Интересно, что средняя цифра от восьми результатов аналогичных подсчетов на текстах меньшего объема составляет 18%, то есть отклонение от нормы, полученной Кёдингом, составляет лишь одно «e» на тысячу букв. Получается, что любой человеческий язык укладывается в строгие статистические нормы!

В чем причина этого поразительного явления? Ответ можно найти с помощью разработанной после Второй мировой войны теории, которая называется «теория информации». Предметом ее изучения являются математические законы, которым подчиняются системы передачи данных. Созданная для решения проблем телефонии и телеграфии, она оказалась применима практически ко всем устройствам, передающим информацию, включая компьютеры и нервную систему животных. Ее идеи оказались настолько плодотворными, что были взяты на вооружение другими науками — психологией, лингвистикой, молекулярной генетикой, историей, статистикой и нейрофизиологией. Создатель этой теории стал также родоначальником ее применения в криптографии.

Клод Шеннон родился в городе Петоски в штате Мичиган 30 апреля 1916 г. Поступив в Мичиганский университет, Шеннон занялся серьезным изучением электротехники и математики. Именно там у него впервые проявился интерес к теории связи и криптографии.

В Массачусетском технологическом институте Шеннон написал диссертацию, в которой содержалось множество новаторских идей, связанных с разработкой телефонных систем. Получив степень доктора математических наук, Шеннон поступил на службу в лабораторию компании «Белл», которая была заинтересована в реализаций этих идей на практике.

«Во время Второй мировой войны, — рассказывал Шеннон, — компания «Белл» работала над засекречиванием информации. Я тогда занимался системами связи и был назначен в несколько комиссий, изучавших криптоаналитические методы. Начиная примерно с 1941 г., исследования в области математической теории связи и теории шифров велись мной одновременно. Я трудился в обеих областях сразу, и кое-какие идеи в одной из них возникали у меня, когда я работал в другой. Я не хочу сказать, что одна из этих областей доминирует над другой. Просто они настолько тесно связаны, что их невозможно разделить». Хотя разработка обеих теорий была в основном завершена примерно к 1944 г., Шеннон продолжал уточнять полученные результаты до 1948-1949 гг., когда они были опубликованы в виде двух отдельных статей в солидном теоретическом журнале «Белл систем текникал джорнэл».

В обеих статьях Шеннона — «Математическая теория связи» и «Теория связи в секретных системах» — идеи излагаются в краткой, математической форме. Обе они изобилуют выражениями вроде «должно существовать единственное обратное преобразование» и формулами вида «$T_iR_i(T_kR_l)^{-1}T_mR_n$». Тем не менее точный и выразительный стиль изложения Шеннона вдохнул в них жизнь. В результате его первая статья породила теорию информации, а вторая — теорию шифров.

Главной в работах Шеннона является концепция избыточной информации. В его интерпретации слово «избыточность» сохраняет свое основное значение ненужного избытка, но оно уточняется и расширяется. Избыточность, по Шеннону, означает, что в сообщении содержится больше символов, чем в действительности требуется для передачи информации. В простом примере, который привел сам Шеннон, входящая в сочетание «qu» буква «u» — лишняя, поскольку в английских словах «u» всегда стоит после «q». По его мнению, также не обязателен и определенный артикль, употребляемый перед существительными во множественном числе. Ведь, посылая телеграммы, англичане прекрасно обходятся без него.

Насколько велика избыточность английского языка, наглядно демонстрируют некоторые из военных сообщений, которые спрессовываются в «черную магию» сокращенных слов и выражений вроде: «off pres on AD for an indef per». Человек посвященный без особых затруднений прочтет: «officer present on active duty for an indefinite period»*. Эта избыточность связана с излишком правил, обременяющих все языки.

*«Офицер, находящийся на действительной службе без ограничения срока».

Одни правила, приводящие к избыточности, можно найти в грамматике («I am», а не «I is»), другие — в фонетике (ни одно из английских слов не может начинаться на «ng»), третьи — в идиомах (после глагола «believe» не может стоять глагол в инфинитиве). Четвертые основаны на различного рода ограничениях, налагаемых на словарь. Пользуясь языком, гораздо более избыточным и ограниченным, чем речь взрослых, подросток говорит «swell»* для выражения одобрительного отношения, передать которое старший по возрасту может с помощью доброго десятка других слов. Как писал Шеннон: «Две крайности избыточности в английском языке представлены словарным запасом «бэйсик инглиш»** и книгой Джеймса Джойса*** «Поминки по Финнегану». Словарь первого ограничен 850 словами, его избыточность очень велика. Это отражается в расширении, происходящем при переводе какого-нибудь отрывка из «Поминок по Финнегану» на «бэйсик инглиш». Со своей стороны, Джойс увеличивает словарь и этим самым, как утверждают, достигает сжатости семантического содержания».

* «Замечательный, превосходный».
** Упрощенный английский язык.
*** Джойс Джеймс — английский писатель-модернист, ирландец.

Еще два источника избыточности имеют особое значение, учитывая их влияние на таблицу частот встречаемости букв. Один из них берет свое начало от различных связей, к которым так часто обращаются люди и которые, естественно, отражаются в языке. Это связи одного лица или предмета с другим («the son of John»* или «the book on the table»**) и какого-то предмета с действием («put it down»***). Английский язык выражает такие связи отдельными словарными единицами, называемыми «словами-функциями». Местоимения, предлоги, артикли и союзы — все это слова-функции. Некоторые из них служат для задания чисто грамматических связей, являясь своего рода лингвистической стенографией: говорят «я» вместо того, чтобы все время повторять свое имя. Слова-функции самостоятельного значения не имеют. Но они входят в число наиболее распространенных слов английского языка, так как передаваемые ими связи встречаются чаще других. Всего лишь десяток английских слов («the», «of», «and», «to», «a», «in», «that», «it», «is» и «I») занимает более $'/_4$ любого текста. Преобладание этих слов неизбежно влияет на таблицу частот встречаемости. Например, своим появлением в ней буква «h» в большинстве случаев бывает обязана только определенному артиклю «the».

* «Сын Джона».
** «Книга на столе».
*** «Положи это».

Второй источник языковой избыточности проистекает из человеческой лености, которая заставляет людей выбирать легко выговариваемые и узнаваемые звуки. На произнесение глухих согласных «p», «t», «k» тратится меньше энергии, чем на соответствующие звонкие согласные «b», «d», «g». Поэтому частота первых в среднем вдвое превосходит частоту вторых в 16 различных языках. Равным образом и краткие гласные звуки используются заметно чаще, чем долгие гласные

или дифтонги*.

* Дифтонги — гласные, состоящие из двух элементов, произносимых в пределах одного слога.

Всякий, кто желает овладеть каким-то языком, предварительно должен узнать лингвистические правила, которые, собственно, и порождают присущую вожделенному языку избыточность. Знание этих правил позволяет находить и исправлять ошибки, появляющиеся при передаче сообщений. Если, например, в телеграмме на английском языке будет пропущена одна точка и буква «i» («..») в слове «individual»* превратится в «e» («.»), получатель телеграммы сообразит, что сделана ошибка, так как в английском языке слова «endividual» нет. Когда в языке нет избыточности, как в случае с телефонными номерами, где одна неправильно набранная цифра приводит к вызову другого абонента, люди сами привносят ее. Они повторяют номер, сообщая его кому-либо, а при передаче фамилий они обычно говорят: «б — Борис, о — Ольга...» Объясняется это просто: чем больше избыточность, тем легче обнаружить ошибки. Если в деловом письме получатель встретится с последовательностью «rhe company», он выделит «rhe» как несуществующее слово, вспомнит, что правила английского языка позволяют поставить перед словом «company»** определенный артикль, учтет, что на клавиатуре пишущей машинки «г» соседствует с «t», и придет к выводу, что вместо «rhe» должно стоять «the».

* «Индивидуальный».
** «Компания».

Этот процесс корректорской правки сродни криптоанализу, ибо при вскрытии шифров криптоаналитики также используют свое знание правил фонетики, грамматики, идиом, слов-функций и фонетических склонностей, которые в совокупности и придают языку избыточность. Способы, применяемые людьми в обыденной жизни для обнаружения опечаток, криптоаналитики употребляют для отыскания деформаций открытого текста. Разумеется, криптограмма несравненно более сложна и запутанна, но в ней заложена скрытая закономерность, какой нет в изолированной, случайной описке. Именно такое построение криптограммы помогает во многих ее «исправлениях», составляющих сущность криптоанализа, и подтверждает их правильность.

С чего начинается криптоанализ? При исправлении ошибки все избыточные элементы, используемые для правки, лежат в готовом виде на поверхности. В криптограмме все наоборот — они незаметны. Криптоаналитик начинает с того, что дробит эти элементы до тех пор, пока не получит их простейшей формы — буквенной. Затем он сравнивает буквы с избыточными элементами языка, приведенными к общему знаменателю. Иными словами, криптоаналитик производит подсчет частот букв криптограммы и соотносит полученные результаты с известными частотами букв предполагаемого языка, на котором записан открытый текст. Методику подсчета иногда приходится менять в зависимости от построения шифра. Для многоалфавитного шифра подсчет необходимо сделать для каждого алфавита, а если перехвачено кодированное сообщение, то простейшей формой избыточных элементов являются слова, и считать надо их.

Откуда у криптоаналитика уверенность в том, что частоты букв открытого текста данной криптограммы примерно совпадают с частотами эталонного открытого текста? Разве не может это соответствие нарушиться из-за различий в словарном запасе корреспондентов и в темах их переписки? Нет, не может, ибо избыточные элементы языка превалируют над остальными: 75-процентная избыточность английского языка подавляет влияние его «свободной» части, хотя не настолько, чтобы она не могла воспрепятствовать точному совпадению частот встречаемости букв в различных текстах.

Именно избыточные элементы в совокупности обеспечивают стабильность таблицы частот встречаемости для любого текста. Действительно, из-за постоянного употребления артикля «the» нередко случается, что буква «h» оказывается среди часто встречающихся букв английского языка. Склонность англичан к использованию альвеолярных согласных приводит к тому, что буквы «n», «t», «r», «s», «d», «l» имеют высокую или среднюю частоту встречаемости. А поскольку в Англии не жалуют буквы «p» и «k», они незаслуженно попали в разряд редко встречающихся. Однако такие избыточные элементы постоянны, заранее известны и поэтому дают стабильные данные для таблиц частот встречаемости. В немецком языке доминирующее влияние избыточности наглядно проявилось в весьма близких пропорциях буквы «e» при подсчетах частот встречаемости букв, произведенных Кёдингом и К°. И конечно же оно проявляется в повседневных успехах криптоаналитиков.

Сила ума Шеннона, его огромный вклад в теорию шифровального дела выразились в открытии избыточности как основы криптоанализа: «Вскрытие большинства шифров становится возможным только благодаря существованию избыточности в открытых текстах». Шеннон первым сумел объяснить постоянство частот встречаемости букв, а тем самым и такое зависящее от него явление, как криптоанализ, дав возможность глубоко понять процесс аналитического вскрытия шифров.

Понимание этого процесса позволяет сделать ряд выводов. Получается, что чем меньше избыточность, тем труднее аналитическим путем прочесть криптограмму. Это видно из двух примеров, иллюстрирующих две крайности в избыточности и приведенных самим Шенноном. Книга «Поминки по Финнегану» заканчивается словами:

«End here. Us then, Finn, again! Take. Bussoftlee, mememor mee! Till thousends thee. Lps. The keys to. Given! A way a lone a last a loved a long the».

Криптоаналитику прочтение такого открытого текста доставит значительно больше хлопот, чем получение отрывка из Нового Завета на «бэйсик инглиш»:

«And the disciples were full of wonder at his words. But Jesus said to them again: Children, how hard it is for those who put faith in wealth to come into the kingdom of God!»*

* «И изумились ученики словам Его. Но Иисус сказал им: Как трудно, дети мои, войти в царство Божье верующим в богатство!»

Криптограммы, помещаемые для занимательности в журналах для широкой публики, достигают поставленной цели — в максимальной степени затруднить их отгадывание — за счет того, что для них подбирают архаические и редкие слова, соединяемые в почти бессмысленные тексты. Избыточность в таких криптограммах сравнительно низкая. Вот образец открытого текста одной такой криптограммы: «Tough cryptos contain traps snaring unwary solvers abnormal frequencies, consonantal combinations unthinkable, terminals freakish, quaint twisters like «myrrth»*.

* «В стойких криптограммах есть ловушки, в которые попадаются неосторожные люди, пытающиеся раскрыть их ненормальные частоты, немыслимые сочетания согласных, странные окончания, необычные головоломки вроде «мирра».

Но даже в этом случае избыточные элементы берут верх. Хотя от некоторых из них отделываются, другие все-таки остаются. Они-то и дают искомое решение задачи. Правда, никогда не проверялся интересный вопрос о том, создают ли отмечаемые среди естественных языков различия в избыточности дополнительные трудности при вскрытии криптограмм аналитическими способами.

Проблема низкой избыточности особенно актуальна, когда криптоаналитик работает над вскрытием кода с перешифровкой. Для того чтобы снять перешифровку и выделить кодированный текст, требуется прочесть криптограмму, открытый текст которой состоит из кодовых обозначений и может выглядеть как бессмысленный набор букв «I X K D Y W U K J T P L K J E...». Здесь избыточность очень низка из-за более равномерного использования букв, большей свободы их сочетания, нивелировки частот путем употребления омофонов и т. д. Но при неизбежном наличии в переписке повторяющихся фраз давление избыточности языка, внутренне присущей коду, а также необходимость подбора структуры кодовых обозначений с учетом возможности их исправления в случае искажения при передаче — все это превращает скрытый кодированный текст в достаточно прочный материал, из которого криптоаналитик делает опору для всего здания успешного вскрытия кода с перешифровкой.

Из сказанного выше следует, что сокращение избыточности значительно затрудняет криптоанализ. Перед зашифрованием Шеннон рекомендует обязательно проделывать над открытым текстом операцию, «которая убирает все излишества... То обстоятельство, что из текста можно без особого вреда убрать гласные буквы, дает простейший способ существенного усовершенствования почти любой шифрсистемы. Сначала уберите все гласные буквы или ту максимально большую часть сообщения, без которой не будет риска разночтения при восстановлении его слов, а затем зашифровывайте то, что осталось». Криптоаналитики, пытавшиеся прочесть шифртелеграммы, из открытых текстов которых изымалась одна только буква «е», подтвердили, что трудность решения задачи вскрытия после этого заметно возрастала. Понижение избыточности действует весьма эффективно, так как оно притупляет одно из главных орудий криптоаналитика. К этому приему прибегали еще итальянские составители шифров эпохи Возрождения, приказывавшие шифровальщикам опускать вторую букву в удвоениях, например «1» в слове «sigillo»*. Прием этот

основан на знании криптографами своего языка, которое позволяет им без всякого ущерба убирать из него элементы избыточности.

* «Тайна».

Низкую избыточность могут иметь и сокращения: для их прочтения иногда требуется настолько большое приращение информации (например, как в случае с сокращением «bn» для слова «battalion»*), что они не только затрудняют получение открытого текста при аналитическом вскрытии шифра, но и сами пригодны для использования в быту в качестве простейшего средства шифрования. Например, две болтающие кумушки могут упомянуть в разговоре между собой о третьей, назвав лишь ее инициалы, чтобы никто из лиц, находящихся рядом, не понял, о ком, собственно, идет речь.

* «Батальон».

Следующий вывод состоит в том, что для прочтения криптограммы, открытый текст которой обладает низкой избыточностью, требуется, чтобы она была более длинной, чем в случае криптограммы с высокой избыточностью. Шеннону удалось определить количество шифртекста, необходимого для получения единственного правильного решения задачи вскрытия шифра при условии, что соответствующий открытый текст имеет известную степень избыточности. Необходимое для этого количество букв он назвал «расстоянием единственности» и описал, как вычислить его с помощью довольно сложной формулы. Эта формула, естественно, видоизменяется для различных шифров, но непременным ее членом всегда остается избыточность.

В одной из своих ранних работ, в которой Шеннон исходил из 50-процентной избыточности английского языка, он установил, что расстояние единственности для шифра однобуквенной замены составляет 27 букв, для многоалфавитных шифров с известными алфавитами — двойную длину периода, а с неизвестными алфавитами — 53 длины периода. Наиболее интересное применение шенноновской формулы расчета расстояния единственности связано с определением правильности решения задачи аналитического вскрытия шифра. Шеннон писал: «Вообще можно утверждать, что если ключ и предложенный метод позволяют прочитать криптограмму при наличии шифртекста, длина которого значительно превосходит расстояние единственности, то решение надежно. Если же длина шифртекста имеет тот же порядок, что и расстояние единственности, или короче его, значит, решение весьма сомнительно».

Вскоре появилась возможность проверить это утверждение Шеннона на практике. Иб Мельхиор, сын известной оперной звезды Лорис Мельхиор, решил, что дешифрование эпитафии, найденной им на надгробии Шекспира, может помочь найти первое издание «Гамлета». Мельхиор преобразовал эпитафию в цифровой шифртекст, прочитал его и отредактировал полученный в результате открытый текст, убрав служебные символы и модернизировав написание слов, принятое в эпоху английской королевы Елизаветы. В конечном итоге Мельхиор стал обладателем загадочной фразы: «Elsinore laid wedge first Hamlet edition». Эти слова, по мнению Мельхиора, означали, что первое издание «Гамлета» было замуровано в клинообразной нише в толще стен замка Эльсинор. О своей находке Мельхиор сообщил в интервью журналу «Лайф».

Один из читателей журнала в своем письме в редакцию обратил внимание Мельхиора на то, что даже при заведомо заниженной 50-процентной оценке избыточности английского языка основная часть этой зашифрованной надписи совершенно не укладывается в найденную Шенноном формулу расстояния единственности. Несмотря на это математическое предсказание неудачи, Мельхиор все-таки отправился в Эльсинор в составе поисковой экспедиции, снаряженной «Лайфом». Вскоре ее участники возвратились из Эльсинора с отличным фоторепортажем для журнала, но без первого издания «Гамлета».

Таким образом, шенноновская концепция избыточности вновь и вновь демонстрирует свою силу, объясняя многие явления криптоанализа, каждое из которых прежде приходилось толковать в отдельности. Почему занимательные криптограммы из газет и журналов труднее поддаются дешифрованию, чем обычные шифртелеграммы? Раньше криптоаналитики могли лишь сказать, что это происходит потому, что для «газетно-журнальных» криптограмм подбираются более редкие и необычные слова. Теперь они могут опереться на принцип избыточности Шеннона и указать, что такие криптограммы обладают более низкой избыточностью.

Почему криптоаналитиков так часто выручают стандартные выражения вроде: «В ответ на вашу

телеграмму от...»? Да потому, что они повышают избыточность до весьма значительных величин. Чтобы ее понизить, можно разделить текст пополам и переместить его первую половину в конец, а вторую — в начало. При этом стандартное начало телеграммы оказывается упрятанным в середину, что значительно затрудняет криптоанализ.

Шеннон также рассмотрел криптоанализ с двух других точек зрения, которые существенно расширили горизонты возможного в этой области. Первая из них является следствием преломления криптоанализа через призму теории связи.

Шеннон писал: «С криптографической точки зрения секретная система почти тождественна системе связи при наличии шума». В теории связи термин «шум» имеет особое значение. Под шумом подразумевается любая помеха, создающая ошибки при передаче по каналу связи. В качестве примеров шума можно указать плохое соединение по телефону и иностранный акцент собеседника. Шеннон исходит из того, что шум схож с шифрованием. Он утверждает: «Основное различие между ними заключается, во-первых, в том, что преобразование при помощи шифра имеет обычно более сложный характер, чем возникающее за счет шума в канале; во-вторых, в том, что ключ в секретной системе выбирается из конечного множества, тогда как шум обычно вносится в канал постоянно и выбирается из бесконечного множества».

Когда автора статистической теории детектирования сигнала Карла Хелстрома спросили, имеет ли техника отделения полезных сигналов от помех какое-либо сходство с криптоанализом, он ответил: «Я полагаю, что аналогия между правилом шифрования по ключу и беспорядочной помехой вряд ли полезна. Со значительно большим основанием можно рассматривать зашифрование как «фильтрацию» открытого текста для получения его в преобразованном виде. Здесь «фильтр» представляет собой определенное правило преобразования, но оно неизвестно криптоаналитику. Поэтому его задача состоит в отыскании характера «фильтра», когда известны статистические данные текста, вводимого в «фильтр», и текста уже «профильтрованного». Это вроде нахождения структуры электрического фильтра путем пропускания через него произвольной помехи и замера статистических распределений на входе и напряжений на выходе».

Другая точка зрения, с которой Шеннон рассмотрел криптоанализ, касается соревнования между криптографом и криптоаналитиком. Он первым предложил отождествить это соревнование с конфликтом — понятием из математической теории игр. Шеннон отмечает: «Действия составителя шифра и криптоаналитика можно представить как игру с очень простой структурой ходов... Ход криптографа состоит в выборе им шифра. Криптоаналитик, осведомленный об этом выборе, разрабатывает метод вскрытия. «Ценой» в игре является средний объем работы, требуемый для прочтения криптограммы, засекреченной выбранным шифром, при помощи разработанного метода».

Как и в любой игре, взаимодействие криптографа и криптоаналитика всегда связано со временем, ибо любые практические дела человека в конце концов неотделимы от этого неотвратимого, необратимого и невозместимого фактора.

У криптографа отношение к фактору времени сложное. Один из самых общих принципов его работы основан на соблюдении баланса между скоростью и секретностью. Когда необходимость в ускоренной связи возрастает, соответственно уменьшается потребность в секретности. На ранних стадиях разработки крупной военной операции нужна повышенная секретность связи, так как, если противник сможет прочитать шифрпереписку, он успеет выработать эффективные контрмеры. В разгар же самого сражения командиры могут обмениваться и открытыми сообщениями, поскольку, даже если противник их перехватит, времени для осуществления полноценных ответных действий у него все равно не будет.

В отличие от криптографа, криптоаналитик постоянно испытывает гнет времени и стремится как можно быстрее довести до конца свои разработки. Вероятно, справедлива истина, что содержание любой шифртелеграммы будет представлять какую-то ценность всегда (хотя бы для историков). Но это слабое утешение для командующего, который мог бы заранее узнать из нее о сроках наступления противника, но так и не узнал, поскольку криптоаналитики не прочли ее вовремя. В числе факторов, определяющих время, необходимое для дешифрования, помимо таких внешних факторов, как скорость доставки криптографу перехваченных шифрсообщений, следует назвать стойкость шифра, разумность правил его использования, точность их соблюдения шифровальщиками, объем перехвата, а также количество и качество вспомогательной информации.

Если говорить о профессиональном уровне криптоаналитика, то встает вопрос: является криптоанализ наукой или искусством? С одной стороны, как было продемонстрировано выше, криптоанализ — это стройная наука. А с другой — успехи во вскрытии шифров явно зависят от личных способностей. Одни криптоаналитики работают лучше других. В этом смысле криптоанализ

— искусство. Как сказал Ярдли, выдающиеся криптоаналитики наделены «шифрмозгом», то есть особыми способностями, однако при рассмотрении вопроса о том, кто и почему обладает «шифрмозгом», приходится сталкиваться с загадками.

Никому не ведомы побудительные мотивы к занятию криптоанализом. Фрейд* считает, что ребенок стремится к учебе, к приобретению знаний, поскольку прежде всего желает увидеть скрытые от него половые органы взрослых и детей. Тогда криптоанализ можно рассматривать как одно из проявлений вуайеризма**.

* Фрейд Зигмунд — австрийский врач, разработавший психоанализ — метод исследования подсознательных процессов человека.

** Вуайеризм — половое извращение, характеризующееся тем, что источником сексуального наслаждения является тайное подглядывание за действиями, совершаемыми другими лицами.

Эта гипотеза получила поддержку у некоторых известных специалистов. Например, Теодор Райк, авторитетный психоаналитик, так ответил на вопрос о взаимосвязи криптоанализа и вуайеризма: «Я склонен считать, что в основе стремления вскрыть шифр аналитическим путем заложено продолжение детского желания узнать, в чем заключается секрет сексуальности, который родители или взрослые скрывают от мальчика». Высказывание Райка созвучно с точкой зрения Фрейда, который считает, что ученые и вообще все специалисты, труд которых связан с математическим или умозрительным видением мира, руководствуются в своей работе именно такими побудительными мотивами. Знаменитый психолог Эрих Фромм особо подчеркивал, что вуайеристическое толкование склонности к криптоанализу «иногда оказывается правильным, но ни в коем случае не настолько универсальным, как думают фрейдисты».

Попытался внести ясность в гипотезу о вуайеристическом происхождении криптоанализа и английский писатель Олдос Хаксли. В его книге «Опавшие листья» есть такие строки: «Любила ли она меня? Во всяком случае, она часто говорила и даже писала, что любит. У меня сохранились все ее письма — два десятка наспех набросанных записок, передававшихся с рассыльным из одного крыла отеля «Сесиль» в другое, и несколько писем, присланных ею, когда она уезжала от меня на праздники или одна проводила где-нибудь уик-энд. Эти листки передо мной. Почерк грамотного, интеллигентного человека. Перо, едва отрываясь от бумаги, торопится от буквы к букве, от слова к слову. Письмо быстрое, но аккуратное, четкое и понятное. Лишь кое-где, обычно в концовках ее записок, четкость почерка нарушается и появляются слова-каракули, составленные из бесформенных букв. Я склоняюсь над ними, пытаясь разобрать. «Я обожаю тебя, любимый мой... тысячу раз целую тебя... тоскую в ожидании вечера... люблю тебя безумно». В ее каракулях мне удается прочитать лишь эти слова. Мы пишем о таких вещах неразборчиво по той же причине, по какой мы прикрываем наготу наших тел. Стыд не позволяет нам ходить обнаженными, и, даже если мы сделаем над собой усилие, доверив мысли бумаге, мы не можем допустить, чтобы наши самые сокровенные думы, страстные желания и тайные воспоминания слишком легко читались и понимались. Записывая наиболее скабрезные детали своих любовных похождений, Пипс не довольствовался их зашифрованием; он прятался еще и за плохой французский. И, вспоминая о Пипсе, я думаю о том, что и сам я проделывал такие фокусы в моих письмах к Барбаре, которые я заканчивал фразами вроде: «Bellissima, ti voglio un bene enorme» или «Je t'embrasse en peu partout»*.

* Обе фразы содержат ошибки. Видимо, герои хотел сказать по-итальянски: «Красавица, люблю тебя безумно» и по-французски: «Целую тебя тысячу раз».

У вуайеристической гипотезы нашлись оппоненты. Психиатр-фрейдист Джепта Макфарлейн считает, что криптоанализ выражает только стремление к власти: «Криптоаналитик не интересуется содержанием шифртелеграмм. Для него имеет значение лишь аналитическое вскрытие шифра. Его обуревает не подленькое любопытство и не желание прочесть чужую шифрованную переписку, а гордость за победу над шифром. Криптоаналитик не подсматривает сквозь замочную скважину. Он сокрушает саму дверь».

Гипотеза Макфарлейна подкрепляется и высказываниями самих криптоаналитиков. Вернер Кюнзе из отделения «Z», объясняя недостаточное знание им конечных результатов своей работы, говорил, что не обращает особого внимания на содержание телеграмм и что у него пропадает всякий интерес к шифру, как только он этот шифр вскрывает. С Кюнзе солидарны и любители отгадывать занимательные криптограммы в газетах и журналах: ответ их совершенно не интересует, они просто

хотят разгадать саму криптограмму.

Хотя факты скорее подтверждают гипотезу о стремлении криптоаналитика к власти, ни эта гипотеза, ни вуайеристическая не были научно проверены. Частичное объяснение этому дает третья гипотеза, согласно которой вуайеристические побуждения вызывают у человека общий интерес к криптоанализу, а стремление к власти обеспечивает ему успех при работе над вскрытием конкретных шифров.

Какое отношение указанные гипотезы имеют к людям, избравшим своей профессией разработку стойких шифров? Райк полагает, что в основе такого профессионального интереса, «возможно, лежит подозрительность и опасение, что посторонние могут подсмотреть за нами и узнать что-то не только о нашей половой жизни, но и о нашей враждебности, агрессивности и т. д., а также желание не допустить этого». В отличие от Райка, Фромм считает, что «интерес к дешифрованию и составлению секретных кодов в большой мере связан с отношением человека к окружающему миру, а конкретнее говоря, с чувством одиночества и с надеждой, что он отыщет родственную душу, с которой мог бы связаться... Мир закрыт для него, и поэтому он вынужден дешифровывать то, что пишется не для него». Психолог Гарольд Гринвальд, интересовавшийся одно время криптологией, пишет: «Лечившиеся у меня пациенты, которые работали в данной области, имели побудительный мотив, отличный от вуайеризма. Преимущественно это были люди стремившиеся испытывать превосходство в силе, скрывая свои действия и мысли (путем их зашифрования) или разгадывая то, что другие хотят держать в секрете (занимаясь криптоанализом)».

Это объяснение проливает некоторый свет на исследуемый вопрос, но и оно ненамного убедительнее других гипотез. Однако, если психологические корни криптографии и криптоанализа не разгаданы, их биологические корни ясны. Эти корми уходят в глубь геологических эпох, к простейшим одноклеточным организмам, боровшимся за жизнь в теплых морях первобытной Земли.

Шифры — это защита. Для современного человека это то же, что панцирь для черепахи, чернильный мешок для осьминога, маскировка для хамелеона. А криптоанализ собирает информацию о внешнем мире наподобие уха летучей мыши, чувствительности амебы к химическим раздражителям, глаза орла. Защита нужна для самосохранения. Это закон жизни, одинаково непреложный и для государства, и для отдельного организма. В условиях соперничества знания существуют в двух формах — у меня и у моего врага. Все организмы пытаются первую форму довести до максимума, а вторую — до минимума. Криптография и криптоанализ являют собой примеры этих двух форм. Составители шифров стремятся сохранить в тайне запас знаний своей страны, а криптоаналитики — увеличить этот запас за счет окружающих.

Но знания сами по себе — это еще не сила. Для придания им веса их нужно соединить с физической силой. Оба направления криптологии, подобно службам снабжения и транспорта, помогают вооруженным силам, составляющим главный элемент мощи страны. Правительство использует эту мощь для достижения своих политических, социальных и военных целей. И криптология в целом — одно из средств их достижения.

Но даже если цели, достижению которых служит криптология, являются чисто оборонительными по отношению к другим государствам, между криптоанализом и вооруженными силами существует огромное различие морального порядка. Последние представляют собой честные, открытые средства устрашения агрессора. Криптоанализ же агрессивен сам по себе. И хотя эта агрессия часто носит превентивный характер, она все-таки остается агрессией, правонарушением. Криптоаналитики действуют исподтишка, подглядывают за чужими делами, норовят стащить то, что им не принадлежит.

В таком случае существует ли моральное оправдание для криптоанализа? Конечно же существует. Один и тот же поступок, в зависимости от обстоятельств, может быть моральным или аморальным. При самообороне убийство допустимо. Так и с криптоанализом. Во время войны он определенно выглядит как благо, особенно если сохраняет людям жизнь. Но и в мирное время криптоанализ может выступать в качестве формы самозащиты. Криптоаналитик способен предупредить о враждебных намерениях и предоставить правительству возможность сохранить своим гражданам жизнь и свободу. Если же государству никто не угрожает, то оно будет не право, если станет попирать достоинство другой страны, тайно подсматривая за ее перепиской.

Человечество доказало, что оно вполне способно познать высшую истину. Вся история развития человечества со времен варварства неопровержимо подтверждает это. Накопление мудрости и моральных ценностей, управляемое в наше время таким императивом, как реальная угроза полного уничтожения, может когда-нибудь привести человечество к тому, что оно перекует мечи на орала, а после этого откажется от услуг криптоаналитиков. И да будет таким венец их славных дел!