

А. Ю. ЗУБОВ, А. В. ЗЯЗИН, Н. В. НИКОНОВ,
С. М. РАМОДАНОВ, А. А. ФРОЛОВ

ОЛИМПИАДЫ ПО КРИПТОГРАФИИ И МАТЕМАТИКЕ

	5		2		0		0	1		2		1
		5		3			3			5		
3		4							6			4
			5	3		3				5		
			2		3	3	3	2				1
2		2							0			
		0		3		5			3			0
						3			1			
		1	3									
0					9			7	8		2	
		6				6						
	3											
0					6		5					

	Ш								
И				Ф		Р	Р		
	Е				Ш				Е
			Т				К		
	А								
		Я				В	Л		Я

Е	Ш		Т	С			Я		
И				Ф		Р	Р	Ч	
	Е	А			Ш	С			Е
Т			Т	Н			К	Ы	
	А	М	С		Л				У
		Я			В	Л		Ч	Я

Т	С	В	О	П	О	К	Р
Е	У	В	Л	Ь	П	В	И
И	Т	К	Е	У	Ш	О	Ж
Ч	Л	О	Т	М	И	Р	Ш
М	П	Е	О	А	О	Й	И
О	Х	А	Н	Н	Н	А	Л
Т	И	Л	А	И	К	Л	Р
А	М	Е	М	И	С	Н	В

А. Ю. Зубов, А. В. Зязин, Н. В. Никонов,
С. М. Рамоданов, А. А. Фролов

ОЛИМПИАДЫ ПО КРИПТОГРАФИИ И МАТЕМАТИКЕ ДЛЯ ШКОЛЬНИКОВ

Электронное издание

Москва
Издательство МЦНМО
2015

Зубов А. Ю., Зязин А. В., Никонов Н. В., Рамоданов С. М.,
Фролов А. А.
Олимпиады по криптографии и математике для школьников.
Электронное издание
М.: МЦНМО, 2015
180 с.
ISBN 978-5-4439-2303-1

В сборник включены условия, ответы и решения двадцати олимпиад по криптографии и математике, проведенных в Москве с 1991/92 по 2010/11 уч. г. Условия задач предварены элементарным введением в криптографию, использующим сюжеты из известных литературных произведений.

Книга предназначена для учащихся старших классов, учителей математики и информатики, а также студентов младших курсов, интересующихся вопросами информационной безопасности.

Подготовлено на основе книги: *Зубов А. Ю.* и др. Олимпиады по криптографии и математике для школьников / А. Ю. Зубов, А. В. Зязин, Н. В. Никонов, С. М. Рамоданов, А. А. Фролов. — 2-е изд., перераб. и доп. — М.: МЦНМО, 2013.

Издательство Московского центра
непрерывного математического образования
119002, Москва, Большой Власьевский пер., 11. Тел. (499) 241-74-83
<http://www.mccme.ru>

ISBN 978-5-4439-2303-1
© А. Ю. Зубов, А. В. Зязин, Н. В. Никонов,
С. М. Рамоданов, А. А. Фролов, 2015
© МЦНМО, 2015

Предисловие

Эта книга имеет две основные цели. С одной стороны — дать популярное изложение основных понятий не всем хорошо известной и даже таинственной науки криптографии. Криптография возникла в глубокой древности первоначально как искусство защиты письменных сообщений. В настоящее время в развитых странах она является большой и сложной научно-технической областью деятельности, обеспечивающей защиту важной для государства как передаваемой по линиям связи, так и хранимой в файлах информации. С другой стороны, в книге обобщается многолетний опыт проведения Олимпиад для школьников по математике и криптографии и приводятся задачи, которые предлагались школьникам начиная с 1991 года. Задачи снабжены подробными решениями и ответами. Знакомство с этими задачами и их внимательный разбор могут помочь школьникам подготовиться и принять участие в Олимпиадах последующих лет. Книга написана квалифицированными математиками и криптографами и представляет значительный интерес как для школьников старших классов, так и для преподавателей математики в школе.

В современной криптографии проводятся глубокие научные исследования, опирающиеся на достижения математики, физики, информатики, электроники и теории связи. Традиционно особо тесную связь в этих исследованиях криптография имеет с математикой. Поэтому соединение в Олимпиадах задач по этим родственным дисциплинам является органичным и позволяет школьникам приобщиться к интересной области знаний и решению нестандартных задач, имеющих наряду с занимательной формой строгие математические постановки и нередко неожиданные оригинальные решения. Участие в Олимпиадах по математике и криптографии для учеников средней школы может послужить хорошим началом пути становления будущих специалистов в этих непростых, но увлекательных областях науки.

Юные участники и талантливые победители Олимпиад — это источник надежды, что через некоторое время в ряды отечественных криптографов и математиков вольются свежие силы, которые скажут новое слово в этих важных для нашей страны областях науки и техники.

Вице-президент Академии криптографии
Российской Федерации,
доктор физико-математических наук, профессор,
заслуженный деятель науки Российской Федерации
В. Н. Сачков

От авторов

С 1991/92 учебного года Академия криптографии Российской Федерации и Институт криптографии, связи и информатики Академии ФСБ России проводят ежегодную олимпиаду школьников по математике и криптографии для учащихся 8–11 классов. Олимпиада вызывает большой интерес у школьников необычностью своего жанра и уже с первых лет собирала несколько сотен участников из Москвы и Подмосковья.

С 2007/08 учебного года олимпиада стала межрегиональной. Благодаря помощи вузов, входящих в состав Учебно-методического объединения по образованию в области информационной безопасности, к настоящему времени очный тур проводится в более чем 30 регионах России, а участвуют в нём около 2000 школьников.

С 2008/09 года олимпиада по математике и криптографии ежегодно включается в Перечень олимпиад школьников, утверждаемый Министерством образования и науки России, что позволяет предоставлять льготы победителям и призёрам при поступлении в вузы.

Школьники часто спрашивают, с какой литературой по криптографии им следует ознакомиться, чтобы успешно выступить на олимпиаде. Никаких специальных знаний для решения задач не требуется — в этом вы убедитесь сами, ознакомившись с задачами, которые приводятся в этой книге. Вместе с тем мы не можем отрицать, что предварительное знакомство с криптографией полезно хотя бы с психологической точки зрения, поскольку «внешний вид» задач может показаться необычным. Многие задачи нашей олимпиады — криптографические. Часть задач имеют криптографическую окраску, но их суть — математическая. Отдельные задачи — просто математические.

Тематика предлагаемых задач весьма разнообразна. Задачи первых олимпиад в основном были посвящены так называемым ручным шифрам, некоторые из которых применялись ещё до нашей эры. Позднее появились задачи, в которых затрагиваются и разделы современной криптографии, такие как криптосистемы с открытым ключом и криптографические протоколы. Также возник цикл задач, относящихся скорее к области защиты информации, чем собственно к криптографии.

При составлении вариантов заданий олимпиады для различных возрастных категорий особое внимание уделяется оценке сложности задач и времени, отводимому на их решение. Благодаря этому практически каждый год находятся участники олимпиады, решившие все задачи.

При подведении итогов каждой олимпиады мы с удовлетворением отмечаем наличие в работах отдельных участников оригинальных решений, более красивых, чем исходно предполагавшиеся составителями.

Олимпиада имеет свой интернет-сайт www.cryptolymp.ru, на котором размещается информация о сроках и местах проведения туров олимпиады, результаты проверки прошедших туров, а также архив задач с решениями. На сайте размещаются методические материалы по математическим методам криптографии, специально адаптированные для школьников. Их цель — не только способствовать подготовке к успешному участию в олимпиаде, но и сформировать понимание математической сути задач защиты информации.

Мы считаем главной задачей олимпиады поддержание интереса школьников к математике, популяризацию её приложений, в первую очередь криптографии. Судя по количеству участников олимпиады в самых разных регионах России, нам это удаётся.

В последнее время книг по криптографии появилось достаточно много. Однако эти книги либо слишком сложны для школьников, либо, наоборот, поверхностны или недостаточно полны. Поэтому авторы при создании этой книги ставили перед собой две основные цели: во-первых, предложить элементарное введение в криптографию, используя при этом чудесные детективные сюжеты известных произведений Ж. Верна, А. Конан Дойла, Э. По, В. Каверина, связанные с зашифрованными сообщениями; во-вторых, привести условия задач всех наших олимпиад прошедших лет с ответами и решениями.

Представляя данную книгу, авторы считают своим долгом с благодарностью вспомнить своего коллегу и товарища П. А. Гырдымова (1954–2004), чей вклад в становление олимпиады по криптографии трудно переоценить. Авторы выражают также глубокую признательность всем своим коллегам, которые когда-либо предлагали готовые задачи и идеи новых задач, поддерживая тем самым саму олимпиаду, и энтузиазм её организаторов.

Работа над книгой выполнена при поддержке гранта Президента РФ (НШ-6260.2012.10).

1. Введение

Если вы хотите передать текстовое сообщение (последовательность символов некоторого алфавита) адресату так, чтобы оно осталось тайным для посторонних, то у вас есть по крайней мере две возможности. Вы можете попытаться скрыть сам факт передачи сообщения, то есть прибегнуть к методам стеганографии, в арсенале которой симпатические (невидимые) чернила, микроточки и тому подобные средства. Другая возможность заключается в таком преобразовании сообщения, зависящем от секретного параметра (называемого ключом), которое делает его «бессмысленным» набором символов для любого лица, которому ключ неизвестен. В этом случае вы будете использовать методы криптографии. Термин *криптография* происходит от двух греческих слов: *криптос* — тайна и *графейн* — писать, и означает тайнопись. «Тайнопись» как раз и подразумевает, что вы скрываете смысл сообщения.

В этой книге мы используем ряд других криптографических терминов. Вкратце поясним их.

Сообщение, которое вы хотите передать, будем называть *открытым сообщением* (или *открытым текстом*). Например, в задаче 2.5 (раздел «Условия задач») открытым сообщением является фраза

КОРАБЛИ ОТХОДЯТ ВЕЧЕРОМ

Для сохранения сообщения в тайне оно преобразуется криптографическими методами и только после этого передаётся адресату. Преобразованное сообщение будем называть *шифрованным сообщением* (или *шифртекстом*). Иногда шифртекст называют также *криптограммой*. В задаче 2.5 шифртекст имеет вид:

ЮПЯТБНЩМСДТЛЖПСПГХСЦЦ

Шифрованное сообщение не обязательно является последовательностью букв, как в указанной задаче. Оно может состоять из цифр или специальных символов (например, «пляшущих человечков»).

Преобразование открытого сообщения в шифрованное будем называть *шифрованием* или *зашифрованием*. Адресату заранее сообщается, как из шифртекста получить открытый текст. Это преобразование будем называть *расшифрованием*. Для расшифрования получателю необходимо знать секретный ключ. При выборе способа шифрования надо стремиться к тому, чтобы лица, не знающие секретного ключа, не смогли восстановить открытый текст по шифртексту, используя любые доступные средства. В этом случае вы скроете содержание сообщения и обеспечите «тайнопись».

Для удобства изложения введём ряд обозначений. Пусть A — открытый текст, B — шифртекст, E — правило зашифрования, D —

правило расшифрования. В этих обозначениях зашифрование запишется в виде $E(A) = B$, а расшифрование — в виде $D(B) = A$. Преобразования E и D должны быть взаимно обратными, чтобы получатель мог однозначно восстановить открытый текст по полученному шифртексту. Однотипные правила зашифрования объединяют в классы. Внутри класса правила различаются по значениям некоторого параметра, который может быть числом, строкой чисел, таблицей и т. д. В криптографии конкретное значение такого параметра и называют ключом. По сути дела, ключ выбирает конкретное правило зашифрования из данного класса правил.

Зависимость E от ключа k будем указывать в виде E_k , а соотношения, связывающие открытый и шифрованный тексты, — в виде $E_k(A) = B$ и $D_k(B) = A$ соответственно. Пусть K — множество возможных ключей. Тогда совокупность $\{(E_k, D_k) : k \in K\}$ будем называть *шифром*.

Среди всего множества шифров выделяют шифры перестановки и шифры замены. Шифры перестановки изменяют порядок следования символов открытого текста. При этом состав символов сообщения не изменяется. Например, можно поменять местами символы открытого текста, расположенные на чётных и нечётных местах. Шифры замены делят последовательность символов открытого текста на отрезки одинаковой длины l и заменяют каждый отрезок своим эквивалентом, последовательность которых образует шифртекст. При $l = 1$ шифр замены называется *поточным*, а при $l > 1$ — *блочным*. Например, у А. Конана Дойла каждый символ открытого текста заменяется «пляшущим человечком», то есть используется поточный шифр замены. Современные стандарты шифрования используют блочные шифры замены.

Как правило, в задачах наших олимпиад шифр известен, а использованный ключ — нет. В этом случае для определения открытого текста по шифртексту возможны два подхода. Первый — определить ключ и с его помощью произвести расшифрование. Второй — попытаться восстановить открытый текст без определения ключа. Говорят, что шифр удалось «взломать», если удалось восстановить открытый текст по шифртексту в случае, когда секретный ключ неизвестен. Чем сложнее взломать шифр, тем он более стоек. Некоторые (не очень стойкие) шифры удаётся взломать, что и демонстрируют победители наших олимпиад.

При анализе стойкости шифра обычно исходят из принципа, сформулированного голландцем Огюстом Керкгоффсом (1835–1903). Согласно этому принципу, стойкость шифрования определяется лишь секретностью ключа. Имеется в виду, что даже осведомлённый противник, которому всё известно о шифре, не может его взломать, если ему неизвестен ключ. Стойкий шифр должен иметь достаточно много

ключей, иначе его можно взломать путём перебора всех ключей. Этот метод используется, например, в задаче 4.4, решение которой сводится к перебору 24 возможных ключей, лишь один из которых даёт при расшифровании «читаемый» текст. Поэтому многие участники олимпиады смогли восстановить сообщение на латинском языке, даже не зная этого языка.

Подчас смешивают два понятия — *шифрование* и *кодирование*. Как вы уже поняли, методы шифрования используются для обеспечения секретности передаваемых сообщений. В свою очередь, методы кодирования широко используются в технике передачи сообщений по различным каналам связи. Так, при передаче информации по компьютерной сети удобно использовать кодирование символов сообщения двоичными наборами, например, байтами. Методы кодирования направлены не на то, чтобы скрыть открытое сообщение, а на то, чтобы представить его в более удобном виде для передачи по техническим каналам связи, например, для уменьшения длины сообщения и т.п. При передаче сообщений по радиоканалу используют азбуку Морзе, и так далее. Вместе с тем кодирование может использоваться и для обеспечения секретности информации. С этой целью можно закодировать, например, пятизначными комбинациями цифр часто используемые слова, фразы, некоторые комбинации букв, а также отдельные буквы. Полученный весьма объёмный код (совокупность цифровых комбинаций) должен быть секретным. Текст передаваемого сообщения может быть естественным образом закодирован с помощью такого кода и передан по каналу связи в виде цифровой последовательности. Такой способ может обеспечить секретность информации лишь до тех пор, пока не перестанет быть секретным сам код. Формально такой код можно рассматривать как шифр с одним ключом.

В настоящее время для защиты информации широко используются электронные шифровальные устройства. Их важной характеристикой является не только стойкость реализуемого шифра, но и высокая скорость шифрования и компактность. Такими устройствами может оснащаться не только военная техника, но и используемые в повседневной жизни пластиковые карты. Кроме аппаратных реализаций алгоритмов шифрования широкое распространение получили их программные реализации. Сегодня шифрование используется, например, для защиты электронной почты.

Современная криптография бурно развивается. Появляются её новые направления и приложения, основанные на глубоких математических и физических методах. Вы, наверное, слышали о «квантовой криптографии», использующей методы квантовой физики для распределения криптографических ключей, и о криптографии «с открытым

ключом», использующей для зашифрования и расшифрования разные ключи. Криптография с открытым ключом, основанная на классических теоретико-числовых и алгебраических методах, позволила решить проблему цифровой подписи электронных документов, а также целый ряд других проблем, которые не могли быть решены методами традиционной криптографии. К ним относятся многие *криптографические протоколы*, решающие важные практические задачи. Это, например, «бросание жребия по телефону», «доказательства с нулевым разглашением», проведение электронных торгов и электронного голосования и другие. Об этом вы можете почитать сегодня во многих книгах, посвящённых криптографии.

2. Шифры замены

Наибольшее распространение на практике получили шифры замены. Это объясняется простотой их использования и достаточной стойкостью. Они эффективно реализуются как аппаратно, так и программно. Многие задачи наших олимпиад посвящены именно шифрам замены.

Пусть, например, шифруется сообщение на русском языке и при этом замене подлежит каждая буква сообщения. В этом случае шифр замены можно описать следующим образом. Для каждой буквы α исходного алфавита выбирается некоторое множество символов M_α таким образом, что при $\alpha \neq \beta$ множества M_α и M_β не пересекаются. M_α назовём множеством *шифробозначений* для буквы α . Таблица

a	b	c	\dots	α
M_a	M_b	M_c	\dots	M_α

(1)

служит ключом шифра замены. Зная её, можно осуществить как зашифрование, так и расшифрование. При зашифровании каждая буква α открытого текста заменяется любым символом из множества M_α . Если в сообщении содержится несколько букв α , то каждая из них заменяется любым символом из M_α . За счёт этого можно с помощью одного ключа (1) получить различные варианты зашифрования данного сообщения. Например, если ключом является таблица

а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п	р
21	37	14	22	01	24	62	73	46	23	12	08	27	53	35	04
40	26	63	47	31	83	88	30	02	91	72	32	77	68	60	44
10	03	71	82	15	70	11	55	90	69	38	61	54	09	84	45
с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	
20	13	59	25	75	43	19	29	06	65	74	48	36	28	16	
52	39	07	49	33	85	58	80	50	34	17	56	78	64	41	
89	67	93	76	18	51	87	66	81	92	42	79	86	05	57	

то сообщение «я знаком с шифрами замены» может быть зашифровано любым из следующих способов:

16 55 54 10 69 09 61 89 29 90 49 44 10 08 02 73 21 32 83 54 74
 41 55 77 10 23 68 08 20 66 90 76 44 21 61 90 55 21 61 83 54 42
 57 30 27 10 91 68 32 20 80 02 49 45 40 32 46 55 40 08 83 27 42

Так как множества $M_a, M_b, M_v, \dots, M_y$ попарно не пересекаются, по каждому символу шифртекста можно однозначно определить, какому множеству он принадлежит, то есть какую букву открытого текста он заменяет. Поэтому расшифрование возможно, и открытый текст определяется единственным образом.

Множества M_α состоят в большинстве случаев из одного элемента. Например, в романе Ж. Верна «Путешествие к центру Земли» в руки профессора Лиденброка попадает пергамент с рукописью из знаков рунического письма. Каждое множество M_α состоит из одного элемента. Элемент каждого множества выбирается из набора символов вида

1 11 111 1111 (2)

В рассказе А. Конан Дойла «Пляшущие человечки» каждый символ изображает пляшущего человечка в самых различных позах

(3)

На первый взгляд кажется, что чем «хитрее» символы, используемые в качестве шифробозначений, тем сложнее найти открытый текст, не имея ключа. Это, конечно, не так. Можно легко перейти от исходного шифртекста к шифртексту, состоящему из букв или чисел, заменив ими «хитрые» символы. Так герои романа Ж. Верна «Путешествие к центру Земли» заменили рунические символы буквами немецкого алфавита, и это облегчило получение открытого текста.

Рассмотрим примеры шифров замены.

Пусть каждое множество M_α состоит из одной буквы (такой шифр называется шифром *простой однобуквенной замены*). Например,

а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п	р
г	л	ь	п	д	р	а	м	ц	в	э	ъ	х	о	б	н

с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
с	ж	я	и	ю	к	щ	ф	е	у	ы	ч	ш	т	а

(4)

Ключ (4) удобно использовать для шифрования. При зашифровании каждая буква открытого текста ищется в верхней строке таблицы и заменяется расположенной под ней буквой второй строки. Расшифрование производится в обратном порядке. По сути дела, в приведённом приме-

ре ключом служит вторая строка таблицы (4), представляющая собой перестановку букв алфавита. Из истории криптографии известен ряд способов, позволяющих легко восстанавливать такие перестановки на основе некоторого простого правила. Это необходимо для того, чтобы исключить потерю ключа, записанного, например, на листе бумаги.

Одним из старейших шифров является шифр Цезаря. Это шифр простой однобуквенной замены, ключом которого служит таблица (4), вторая строка которой является циклическим сдвигом первой строки. Одним из ключей такого шифра является, например, таблица

$$\begin{array}{cccccccc} \text{а} & \text{б} & \text{в} & \dots & \text{ь} & \text{э} & \text{ю} & \text{я} \\ \text{г} & \text{д} & \text{е} & \dots & \text{я} & \text{а} & \text{б} & \text{в} \end{array} \quad (5)$$

Для восстановления такого ключа нужно знать лишь первую букву второй строки. Однако это удобство имеет и противоположную сторону: число ключей шифра Цезаря равно числу букв алфавита, и не представляет труда все их перебрать, чтобы определить истинный ключ по данной криптограмме путём расшифрования. Задача 4.4, например, именно на это и рассчитана. В одном из вариантов расшифрования участники олимпиады смогли узнать «читаемый» текст на латинском языке.

Другой пример шифра простой замены — так называемый *лозунговый шифр*. Для этого шифра вторая строка таблицы (4) начинается с легко запоминаемого слова — лозунга. Остальные буквы алфавита, не входящие в лозунг, следуют в их естественном порядке. Такую перестановку букв алфавита называют систематически перемешанным алфавитом. Выбрав, например, в качестве лозунга слово «учебник», получим систематически перемешанный алфавит

$$\begin{array}{cccccccccccccccc} \text{у} & \text{ч} & \text{е} & \text{б} & \text{н} & \text{и} & \text{к} & \text{а} & \text{в} & \text{г} & \text{д} & \text{ж} & \text{з} & \text{л} & \text{м} & \text{о} \\ \text{п} & \text{р} & \text{с} & \text{т} & \text{ф} & \text{х} & \text{ц} & \text{ш} & \text{щ} & \text{ъ} & \text{ы} & \text{ь} & \text{э} & \text{ю} & \text{я} \end{array}$$

Число ключей лозунгового шифра значительно больше, чем у шифра Цезаря.

Шифры простой однобуквенной замены имеют одну общую слабость. Заметим, что если в открытом тексте часто встречается какая-либо буква, то в шифртексте столь же часто встречается заменяющий её символ. То же касается и редких букв. Если имеется шифртекст достаточной длины, то указанное соответствие несложно использовать при идентификации букв открытого текста, даже если ключ неизвестен. В некоторых задачах олимпиад такая идентификация упрощается путём введения дополнительных условий. Например, в задаче 4.2 при шифровании сохранена разбивка текста на слова и указаны знаки препинания. Это позволяет выделить предлоги и союзы. Кроме того, текст сообщения содержит ряд удвоенных букв, которым скорее всего в открытом тексте соответствуют один из вариантов: НН, ОО, ИИ

и т. д. Если правильно идентифицированы несколько букв открытого текста (например, ряд частых букв), то дальнейшая работа по определению ключа не представляет особого труда. Решение подобных задач достаточно сложно формализовать, и в таких случаях уместно вспомнить высказывание о том, что криптография не только наука, но и искусство.

Популярные среди школьников криптограммы (типа криптограммы из задачи 1.5) фактически связаны с простой заменой, определяемой ключом

0	1	2	3	4	5	6	7	8	9
ш	и	ф	р	з	а	м	е	н	ы

в котором каждая цифра заменяется буквой. При этом должны соблюдаться правила арифметики. Эти правила значительно облегчают решение задачи, так же как правила русского языка облегчают в задаче 4.2 нахождение четверостишия В. Высоцкого.

Любые особенности текста, которые могут быть вам известны, — ваши помощники. Например, в задаче 5.2 прямо указано, что в тексте используются телеграфные сокращения «зпт» и «тчк». И эта подсказка указывает путь к решению задачи.

Одной из разновидностей шифров простой замены являются шифры *разнозначной замены*, заменяющие каждую букву одним или двумя символами (как в задаче 4.2). Например, ключ такого шифра задаётся таблицей

а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п	р
73	74	51	65	2	68	59	1	60	52	75	61	8	66	58	3
с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	
69	64	53	54	9	62	71	4	67	56	72	63	55	70	57	

Если шифртекст записан без знаков пробела, то при анализе шифра разнозначной замены появляется дополнительная трудность, связанная с разбиением сообщения на отдельные символы и слова. Взломать такой шифр сложнее, нежели шифр простой однобуквенной замены.

Другое усложнение шифра простой замены состоит в том, чтобы множества шифробозначений M_α содержали более одного элемента. Такие шифры получили название шифров *многозначной замены* (или *омофонов*). Эти шифры позволяют скрыть истинную частоту букв открытого текста, что существенно затрудняет их анализ. Однако при использовании омофонов возникает сложность, связанная с хранением ключа. Ключ представляет собой список множеств M_α для каждой буквы алфавита. Как правило, элементами этих множеств являются числа.






Пример омофона известен из художественной литературы и кинофильмов про разведчиков времён Второй мировой войны. Это — одна

из разновидностей так называемого *книжного шифра*. Ключом шифра служит книга. Множество шифробозначений для каждой буквы определяется пятизначными наборами цифр, в которых первые две цифры указывали номер страницы, третья цифра — номер строки, четвёртая и пятая цифры — номер позиции буквы в строке. Поэтому при поимке разведчика, который пользовался таким шифром, всегда пытались найти книгу, которая могла быть использована им в качестве ключа.

Мы не касаемся в нашем кратком введении более сложных методов построения шифров замены. Полагаем, что приведённых примеров достаточно для того, чтобы оценить многообразие шифров. Закончим рассказ о шифрах замены несколькими красивыми примерами, заимствованными из художественной литературы.

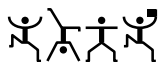
А. Конан Дойл, «Пляшущие человечки»

В этом рассказе Холмсу необходимо было прочитать тексты пяти записок:

- I. 
- II. 
- III. 
- IV. 
- V. 

Первая записка была так коротка, что дала возможность Холмсу сделать всего лишь одно правдоподобное предположение, оказавшееся впоследствии правильным. По-видимому, флаги употребляются лишь для того, чтобы отмечать концы отдельных слов. Больше ничего по первой записке установить было нельзя. Четвёртая записка, по всей видимости, содержала всего одно слово, так как в ней не было флагов.

Вторая и третья записки начинались, несомненно, с одного и того же слова из четырёх букв. Вот это слово:



Оно кончается той же буквой, какой и начинается. Счастливая мысль: письма обычно начинаются с имени того, кому письмо адресовано. Человек, писавший миссис Кьюбит эти послания, был, безусловно, близко

с ней знаком. Вполне естественно, что он называет её просто по имени. А зовут её Илси. Таким образом, Холмсу стали известны три буквы: И, Л и С.

В двух записках их автор обращается к миссис Кьюбит по имени и, видимо, чего-то требует от неё. Не хочет ли он, чтобы она пришла куда-нибудь, где он мог с ней поговорить? Холмс обратился ко второму слову третьей записки. В нём 7 букв, из которых третья и последняя — И. Холмс предположил, что слово это — ПРИХОДИ, и сразу оказался обладателем ещё 5 букв: П, Р, Х, О, Д.

Тогда он обратился к четвёртой записи, которая появилась на двери сарая. Холмс предположил, что она является ответом и что написала её миссис Кьюбит. Подставив в текст уже известные буквы, он получил: -И-О-Д-. Что же могла миссис Кьюбит ответить на просьбу прийти? Внезапно Холмс догадался: НИКОГДА

Возвратившись к первой записке, Холмс получил:

- -Д-С- А- СЛ-НИ

Он предположил, что четвёртое слово — СЛЕНИ Это — фамилия, чрезвычайно распространённая в Америке. Коротенькое слово из двух букв, стоящее перед фамилией, по всей вероятности, имя. Какое же имя может состоять из двух букв? В Америке весьма распространено имя Аб. Теперь остаётся установить только первое слово фразы; оно состоит всего из одной буквы, и отгадать его нетрудно: это — местоимение Я.

Далее Холмс восстанавливает содержание второй записки:

ИЛСИ Я -И- - - -ЛРИД-А
* * * *

Здесь указаны границы слов, а снизу одинаковыми символами отмечены одинаковые буквы. Четвёртое слово состоит из одной буквы (по-видимому, это союз или предлог). Буквы О и И уже определены, С, А и К — тоже. Остаются следующие возможности: это — либо В, либо У. Вряд ли это — В, так как в этом случае получилось бы «нечитаемое» третье слово -И-В. Поэтому, скорее всего — это предлог У. Небольшой перебор незадействованных букв даёт правдоподобную гипотезу о значении третьего слова: ЖИВУ. Скорее всего, последнее слово (-ЛРИДЖА) — мужское имя, в котором неизвестная буква — Э. Поэтому вторая записка гласит:

ИЛСИ Я ЖИВУ У ЭЛРИДЖА

Холмс послал телеграмму в нью-йоркское полицейское управление с запросом о том, кто такой Аб Слени. Поступил ответ: «Самый опасный бандит в Чикаго».

Сразу после этого появилась последняя (5-я) записка, в которой не хватало трёх букв: ИЛСИ ГО-ОВЬСЯ К С-ЕР-И, из которой сразу опреде-

ляются буквы М и Т:

ИЛСИ ГОТОВЬСЯ К СМЕРТИ

Шестая записка была направлена Холмсом преступнику:



Э. По, «Золотой жук»

Найден пергамент с текстом криптограммы. Для удобства пронумеруем по порядку все символы этого текста:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
5	3	#	#	+	3	0	5))	6	*	;	4	8	2	6)	4
20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36		
#	•)	4	#)	;	8	0	6	*	;	4	8	+	8	□		
37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52			
6	0))	8	5	;	;]	8	*	;	:	#	*	8			
53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69		
+	8	3	(8	8)	5	*	+	;	4	6	(;	8	8		
70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86		
*	9	6	*	?	;	8)	*	#	(;	4	8	5)	;		
87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102			
5	*	+	2	:	*	#	(;	4	9	5	6	*	2	(
103	104	105	106	107	108	109	110	111	112	113	114	115						
5	*	=	4)	8	□	8	*	;	4	0	6						
116	117	118	119	120	121	122	123	124	125	126	127	128						
9	2	8	5)	;)	6	+	8)	4	#						
129	130	131	132	133	134	135	136	137	138	139	140	141	142					
#	;	1	(#	9	;	4	8	0	8	1	;	8					
143	144	145	146	147	148	149	150	151	152	153	154	155	156					
:	8	#	1	;	4	8	+	8	5	;	4)	4					
157	158	159	160	161	162	163	164	165	166	167	168	169						
8	5	+	5	2	8	8	0	6	*	8	1	(
170	171	172	173	174	175	176	177	178	179	180	181	182						
#	9	;	4	8	;	(8	8	;	4	(#						
183	184	185	186	187	188	189	190	191	192	193	194	195						
?	3	4	;	4	8)	4	#	;	1	6	1						
196	197	198	199	200	201	202	203	204										
;	:	1	8	8	;	#	?	;										

Кроме того, на пергаменте изображены череп и козлёнок. Главный герой рассказа рассуждал следующим образом. По английски козлёнок — kid; череп связан с капитаном Киддом, по английски — kidd. Козлёнок

был нарисован на пергаменте в том месте, где ставится подпись. Изображение черепа в противоположном по диагонали углу наводило на мысль о печати или гербе. Капитан Кидд владел несметным богатством. Кидд, насколько мы можем судить о нём, не сумел бы составить истинно сложную криптограмму. По-видимому, это была простая замена. Возникает только вопрос о языке, на котором был написан текст. В данном случае трудностей с определением языка не было: подпись давала разгадку. Игра слов kid и kidd возможна лишь в английском языке.

Текст криптограммы идёт в сплошную строку. Задача была бы намного проще, если бы отдельные слова были отделены пробелами. Тогда можно было бы начать с анализа и сличения более коротких слов, и как только нашлось бы слово из одной буквы (например, местоимение «я» или союз «и» — для русского языка), начало было бы положено. Но просветов в строке не было.

Приходится подсчитывать частоты одинаковых символов, чтобы узнать, какие из них чаще, а какие реже встречаются в криптограмме. В результате получилась таблица частот всех символов:

8	;	4)	#	*	5	6	(+	1	0	2	9	:	3	?	□	•]	=
34	27	19	16	15	14	12	11	9	8	7	6	5	5	4	4	3	2	1	1	1

В английской письменной речи самая частая буква — е. Далее идут в нисходящем порядке: а, о, i, d, h, n, r, s, t, u, y, c, f, g, l, m, w, b, k, p, q, x, z. Буква е, однако, настолько часто встречается, что трудно построить фразу, в которой она не занимала бы господствующего положения. Итак, уже сразу у нас в руках путеводная нить. Составленная таблица, вообще говоря, может быть очень полезна, но в данном случае она понадобилась лишь в начале работы.

Поскольку символ 8 встречается чаще других, примем его за букву е английского алфавита. Для проверки этой гипотезы взглянем, встречается ли этот символ дважды подряд, так как в английском языке буква е часто удваивается, например, в словах meet, fleet, speed, seen, seed, beep, agree, и т. д. Хотя криптограмма невелика, пара 88 стоит в нём пять раз.

Самое частое слово в английском языке — определённый артикль the. Посмотрим, не повторяется ли у нас сочетание из трёх символов, расположенных в одинаковой последовательности и оканчивающихся символом 8. Если такое найдётся, то это будет, по всей вероятности, the. Приглядевшись, находим семь раз сочетание из трёх символов ;48. Итак, мы имеем право предположить, что символ ; — это буква t, а 4 — h; вместе с тем подтверждается, что 8 — это действительно е. Мы сделали важный шаг вперёд.

То, что мы расшифровали целое слово, потому так существенно, что позволяет найти границы некоторых других слов. Для примера возьмём

предпоследнее из сочетаний этого рода ;48 (позиции 172–174). Идущий сразу за 8 символ ; будет, как видно, начальной буквой нового слова. Выпишем, начиная с него, 6 символов подряд. Только один из них нам незнаком. Обозначим известные символы буквами и оставим свободное место для неизвестного символа (обозначим его точкой) t.eeth, ни одно слово, начинающееся с t и состоящее из 6 букв, не имеет в английском языке окончания th. В этом легко убедиться, подставляя на свободное место все буквы по очереди. Попробуем отбросить две последние буквы и получим t.ee, для заполнения свободного места можно снова взяться за алфавит. Единственно верным прочтением этого слова будет tree (дерево). В таком случае мы узнаём ещё одну букву — r, она обозначена символом (и мы можем прочитать два слова подряд the tree, в дальнейшем эта гипотеза может либо подтвердиться, либо привести к некоторому «нечитаемому» фрагменту. В последнем случае следует попытаться восстановить либо слово t.e, либо t.eet, либо слово, целиком включающее в себя t.eeth

Развиваем успех. Немного далее (186–188) находим уже знакомое нам сочетание ;48. Примем его опять за границу нового слова и выпишем целый отрывок, начиная с двух расшифрованных нами слов. Получаем такую запись:

the tree ;4(#?34 the

Заменим уже известные символы буквами:

the tree thr#?3h the

а неизвестные — точками:

the tree thr...h the

Нет никакого сомнения, что неясное слово — through (через). Это открытие даёт нам ещё три буквы — o, u и g, обозначенные в криптограмме символами # ? и 3.

Надписывая над уже определёнными символами криптограммы их значения, находим вблизи от её начала (позиции 54–58) группу символов 83(88, которая читается такegree, это, конечно, слово degree (градус) без первой буквы. Теперь мы знаем, что буква d обозначена символом +. Вслед за словом degree через 4 символа встречаем группу ;46(;88*. Заменим известные символы буквами, а неизвестные — точками th.rtee, по-видимому, перед нами слово thirteen (тринадцать). К известным нам буквам прибавились i и n, обозначенные в криптограмме символами 6 и *.

Криптограмма начинается так: 53##+. Подставляя буквы и точки, получаем .good, недостающая буква, конечно, a, и, значит, два первых слова будут читаться так: a good (хороший). Определены следующие 11 символов:

5	+	8	3	4	6	*	#	(;	?
a	d	e	g	h	i	n	o	r	t	u

На этом анализ Э. По заканчивается. Дальнейшую работу проделаем самостоятельно.

Четвёртый по частоте (16 вхождений) символ **)** ещё не определён. Возвратимся к диаграмме встречаемости букв английского языка. Среди первого десятка букв этой диаграммы у нас не встретились лишь буква **s**. Она — первый претендент на значение символа **)**. Эта гипотеза подтверждается тем, что вряд ли **)** обозначает гласную букву, так как в таком случае мы получили бы «нечитаемые» фрагменты

6	7	8	9	10	11	12
g	.	a))	i	n

или

37	38	39	40	41	42
i	.))	e	a

То, что символ **)** — это буква **s**, легко проверяется на участке криптограммы с 60-й по 89-ю позиции **.and thirteen .inutes north east and** Поэтому полагаем, что символ **)** — это **s**. Попутно определилось значение символа **9**, это — **m**.

Перебирая возможные значения символа **0**, стоящего на позициях 7 и 28 криптограммы, убеждаемся в том, что единственно возможным его значением может быть лишь буква **l** (**glass** — стекло, **hostel** — общежитие, гостиница или трактир).

Определяем, далее, значение символа **□** как **v** по фрагменту текста в позициях 107–113.

Теперь на участке текста с 22-й по 70-ю позиции остались неопределёнными лишь значения символов **] и :**, встретившихся по одному разу. Очевидно, что символ **]** — это **w**, а символ **:** — это **y**. Теперь на участке текста с 172-й по 204-ю позиции не выявлено лишь значение символа **1**, которое, как нетрудно заметить, может быть лишь буквой **f**.

Символ **2**, стоящий на позициях 117 и 90, очевидно, заменяет букву **b**.

Осталось определить лишь значения символов **• и =**. Небольшой перебор ещё неустановленных букв показывает, что символ **=** — это **c**, а символ **•** может обозначать одну из букв **k, p, q, x** или **z**. Обратившись к словарю, находим единственное подходящее окончание **p** слова **bishop** (епископ, слон).

Таким образом, однозначно определились значения всех 21 символов, встречающихся в криптограмме. Получился следующий открытый текст:

«A good glass in the bishop's hostel in the devil's seat twenty one degrees and thirteen minutes northeast and by north main branch seventh limb east side shoot from the left eye of the death's head a bee line from the tree through the shot fifty feet out».

В переводе на русский язык: «Хорошее стекло в трактире епископа на чёртовом стуле двадцать один градус и тринадцать минут северо-северо-восток главный сук седьмая ветвь восточная сторона стреляй из левого глаза мёртвой головы прямая от дерева через выстрел на пятьдесят футов».

Восстановленная простая замена:

A B C D E F G H I L M N O P R S T U V W Y
5 2 = + 8 1 3 4 6 0 9 * # • () ; ? □] :

Ж. Верн, «Путешествие к центру Земли»

В руки профессора Лиденброка попадает пергамент со следующей рукописью:

«Это — рунические письма; знаки эти совершенно похожи на знаки манускрипта Снорре. Но ... что же они означают? — спрашивает профессор, — ... Ведь это всё же древнеисландский язык, — бормотал он себе под нос». Изучение рукописи привело профессора к выводу о том, что это зашифрованное сообщение. Для его прочтения профессор решил заменить буквы сообщения их аналогами в современном немецком алфавите: «А теперь я буду диктовать тебе, — говорит он своему помощнику, — буквы нашего алфавита, соответствующие каждому из этих исландских знаков». Он называл одну букву за другой, и таким образом последовательно составлялась таблица непостижимых слов:

m . r n l l s	e s r e u e l	s e e c J d e
s g t s s m f	u n t e i e f	n i e d r k e
k t , s a m n	a t r a t e S	S a o d r r n
e m t n a e I	n u a e c t	r r i l S a
A t v a a r	. n s c r c	i e a a b s
c c d r m i	e e u t u l	f r a n t u
d t , i a c	o s e i b o	K e d i i I

Можно было предположить, что таинственная запись сделана одним

из обладателей книги, в которой находился пергамент. Не оставил ли он своего имени на какой-нибудь странице? На обороте второй страницы профессор обнаружил что-то вроде пятна, похожего на чернильную кляксу. Воспользовавшись лупой, он различил несколько наполовину стёртых знаков, которые можно было восстановить. Получилась запись **1 11 1 11 11 11 11 11 11** которая читалась как «Арне Сакнуссем» — имя учёного XVI столетия, знаменитого алхимика!

Далее профессор рассуждал так: «Документ содержит 132 буквы, 79 согласных и 53 гласных. Приблизительно такое же соотношение существует в южных языках, в то время как наречия севера бесконечно богаче согласными. Следовательно, мы имеем дело с одним из южных языков.» «... Сакнуссем, — продолжал профессор, — был учёный человек; поэтому раз он писал не на родном языке, то, разумеется, должен был отдавать предпочтение языку, общепринятому среди образованных умов XVI века, а именно — латинскому. Если я ошибаюсь, то можно будет испробовать испанский, французский, итальянский, греческий или еврейский. Но учёные XVI столетия писали обычно по-латински. Таким образом, я вправе признать не подлежащим сомнению, что это — латынь.»

«Всмотримся хорошенько, — сказал он, снова взяв исписанный листок. — Вот ряд из 132 букв, расположенных крайне беспорядочно. Вот слова, в которых встречаются только согласные, как, например, первое **m.rnlls**; в других, напротив, преобладают гласные, например, в пятом **unteief**, или в предпоследнем — **oseibo**. Очевидно, что эта группировка не случайна; она произведена автоматически, при помощи неизвестного нам соотношения, которое определило последовательность этих букв. Я считаю несомненным, что первоначальная фраза была написана правильно, но затем по какому-то принципу, который надо найти, подверглась преобразованию. Тот, кто владел бы ключом этого шифра, свободно прочёл бы её. Но что это за ключ?»

«При желании затемнить смысл фразы первое, что приходит на ум, как мне кажется, это написать слова в вертикальном направлении, а не в горизонтальном». Проверая эту гипотезу, он начал диктовать, называя сначала первые буквы каждого слова, потом вторые; он диктовал буквы в таком порядке:

**m e s s u n k a S e n r A . i c e f d o K . s e g n i t t a m u r t n e c e
r t s e r r e t t e , r o t a i v s a d u a , e d n e c s e d s a d n e l a k
a r t n i i i l u J s i r a t r a c S a r b m u t a b i l e d m e k m e r e t
a r c s i l u c o I s l e f f e n S n I**

С полученным текстом у профессора долго ничего не выходило. Это почти привело его в отчаяние. Однако «... совершенно машинально я стал обмахиваться этим листком бумаги, так что лицевая и оборот-

ная стороны листка попеременно представляли перед моими глазами. ... Каково же было моё изумление, когда вдруг мне показалось, что передо мной промелькнули знакомые, совершенно ясные слова, латинские слова: *craterem, terrestre!*» Дело в том, что читать этот текст нужно было не слева направо, как обычно, а наоборот! Таким образом, случай помог профессору найти ключ к решению задачи. Документ гласил следующее:

«In Sneffels Ioculis craterem kem delibat umbra Scartaris Julii intra calendas descende, audas viator, et terrestre centrum attinges. Kod feci. Arne Saknussem».

В переводе это означало: «Спустись в кратер Екуль Снайфедльс, который тень Скартариса ласкает перед июльскими календами, отважный странник, и ты достигнешь центра Земли. Это я совершил. Арне Сакнуссем».

3. Шифры перестановки

Как мы указывали ранее, шифр перестановки преобразует сообщение, лишь изменяя порядок следования его символов, но не изменяя самого состава символов. Перестановку символов сообщения длины n удобно представить в виде двустрочной таблицы

$$\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}, \quad (6)$$

в которой i_1 — номер места в шифртексте, на которое попадает первая буква сообщения, i_2 — номер места в шифртексте для второй буквы и т. д. Верхняя строка представляет собой отрезок натурального ряда от 1 до n , а нижняя строка — его перестановку. Такая таблица называется *подстановкой степени n* .

По подстановке, определяющей преобразование перестановки, можно осуществить как зашифрование, так и расшифрование сообщения. Например, в соответствии с подстановкой

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 3 & 1 & 4 & 6 \end{pmatrix}$$

слово МОСКВА будет зашифровано в слово КОСВМА. Попробуйте расшифровать криптограмму НЧЕИУК, полученную с помощью той же подстановки.

Читатель, знакомый с методом математической индукции, может легко убедиться в том, что существует $1 \cdot 2 \cdot 3 \cdot \dots \cdot n$ (это произведение обозначается $n!$ и читается как «эн факториал») перестановок множества из n элементов. Таким образом, число различных преобразований, осуществляемых шифром перестановки с текстом длины n , не превосходит $n!$. С увеличением n значение $n!$ очень быстро растёт. Приведём

значения $n!$ для первых 10 натуральных чисел:

n	1	2	3	4	5	6	7	8	9	10
$n!$	1	2	6	24	120	720	5040	40320	362880	3628800

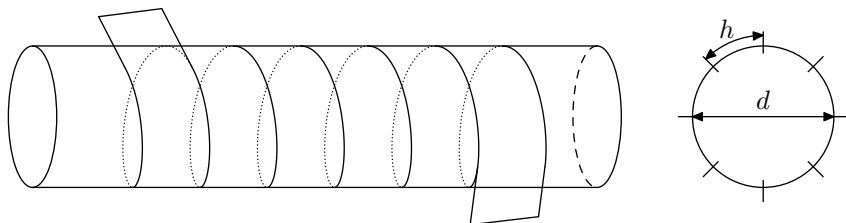
При больших n для приближённого вычисления $n!$ пользуются известной формулой Стирлинга

$$n! \approx \sqrt{2\pi n} \left(\frac{n}{e}\right)^n,$$

где $e = 2,718281828\dots$

Задание преобразований шифра перестановки с помощью подстановок нецелесообразно для текстов большой длины, поскольку работать с длинными таблицами неудобно. В связи с этим получили распространение более «компактные» методы построения перестановок. К ним относятся, в первую очередь, так называемые *геометрические* и *маршрутные* перестановки. Геометрические перестановки основаны на использовании размеров некоторой геометрической фигуры, а маршрутные перестановки — на возможности заполнения некоторой таблицы символами по различным «траекториям».

Классический пример геометрической перестановки — шифр под названием «Считала». Этот шифр использовался ещё во времена войны Спарты против Афин в V веке до н. э. Для шифрования использовался цилиндр (рукоятка меча, жезл и т. п.). На него виток к витку плотно наматывалась лента папируса, на которую «построчно» вдоль оси цилиндра записывался необходимый для передачи текст. Заполненная лента снималась с цилиндра и отправлялась адресату, который, имея точно такой же цилиндр, наматывал на него ленту и прочитывал сообщение. Нетрудно понять, что такой способ шифрования осуществлял перестановку букв сообщения, а ключом шифра служил цилиндр определённого диаметра.



Как следует из задачи 2.1, шифр «Считала» реализует не более чем n перестановок (где n — длина сообщения). В самом деле, этот шифр эквивалентен шифру маршрутной перестановки, для которого заши-

фрование состоит в построчной записи сообщения в прямоугольную таблицу и выписывания из неё шифртекста по столбцам. Число задействованных столбцов таблицы не превосходит длины сообщения. Имеются и геометрические ограничения в реализации шифра «Считала». Естественно предположить, что диаметр жезла d не должен превосходить 10 сантиметров. При высоте строки $h = 1$ сантиметр на одном витке такого жезла уместится не более 32 букв ($10\pi < 32$). Отсюда следует, что число перестановок, реализуемых «Считалой», вряд ли превосходит 32.

Другим примером геометрической перестановки является шифр под названием «Поворотная решётка». Для шифрования изготавлился ключ — трафарет в виде прямоугольного листа клетчатой бумаги размера $2m \times 2k$, в котором вырезается mk клеток так, чтобы при наложении трафарета на чистый лист бумаги того же размера четырьмя возможными способами вырезы полностью покрывали площадь листа. При шифровании буквы сообщения последовательно записывались в вырезы трафарета (построчно, слева направо) в каждом из четырёх возможных положений в заранее установленном порядке. Шифртекст выписывался из заполненного прямоугольника построчно. Если длина сообщения превосходила mk , то каждый следующий отрезок сообщения длины mk шифровался точно так же. Поясним процесс шифрования на примере.

Пусть ключом служит трафарет размера 6×10 , приведённый на рис. 1.

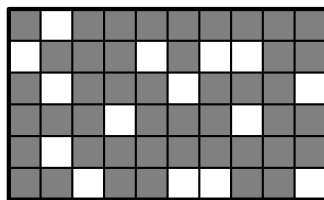


Рис. 1

Зашифруем с его помощью текст

ШИФРРЕШЕТКАЯВЛЯЕТСЯЧАСТНЫМСЛУЧАЕМШИФРАМАРШРУТНОЙПЕРЕСТАНОВКИ

Наложив трафарет на лист бумаги, записываем первые 15 букв текста (по числу вырезов): ШИФРРЕШЕКАЯВЛЯ. Сняв трафарет, мы увидим фрагмент текста, приведённый на рис. 2. Повернём трафарет на 180° . В новом положении вырезы трафарета оказываются незаполненными. Записываем в них следующие 15 букв. Получим фрагмент, приведённый на рис. 3. Переворачиваем трафарет на другую сторону и заполняем оставшиеся буквы текста аналогичным образом (рис. 4, 5).

	Ш							
И				Ф		Р	Р	
	Е				Ш			Е
			Т				К	
	А							
		Я			В	Л		Я

Рис. 2

Е	Ш		Т	С			Я	
И				Ф		Р	Р	Ч
	Е	А			Ш	С		Е
Т			Т	Н			К	Ы
	А	М	С		Л			У
		Я			В	Л	Ч	Я

Рис. 3

Е	Ш	А	Т	С	Е	М	Я		Ш
И	И			Ф		Р	Р	Ч	
	Е	А	Ф		Ш	С	Р		Е
Т	А		Т	Н	М		К	Ы	А
Р	А	М	С	Ш	Л	Р	У		У
	Т	Я			В	Л		Ч	Я

Рис. 4

Е	Ш	А	Т	С	Е	М	Я	Н	Ш
И	И	О	Й	Ф	П	Р	Р	Ч	Е
Р	Е	А	Ф	Е	Ш	С	Р	С	Е
Т	А	Т	Т	Н	М	А	К	Ы	А
Р	А	М	С	Ш	Л	Р	У	Н	У
О	Т	Я	В	К	В	Л	И	Ч	Я

Рис. 5

Осталось выписать шифртекст по строкам заполненного листа (см. рис. 5):

ЕШАТСЕЯНШИИОЙФПРРЧЕРЕАФЕШСРСЕТАТНМАКЯРАМСШЛРУНОУТЯВКВЛИЧЯ

Получатель сообщения, имеющий точно такой же трафарет, без труда восстановит исходный текст, наложив трафарет на заполненный шифртекстом лист по порядку четырьмя способами.

Можно доказать, что число возможных трафаретов, то есть число возможных ключей шифра «Поворотная решётка», выражается величиной $T = 4^{mk}$ (см. задачу 1.1). Этот шифр предназначен для шифрования сообщений длины, кратной $4mk$. Для сообщения длины $4mk$ число возможных перестановок равно $(4mk)!$, что во много раз превышает величину T . Тем не менее, уже при $m = k = 4$ число ключей шифра превосходит 4 миллиарда.

Широко распространена разновидность шифра маршрутной перестановки, называемая *шифром вертикальной перестановки* (ШВП). Шифрование использует прямоугольную клетчатую таблицу, в которую построчно записывается открытый текст. Число столбцов таблицы определяет длина числового ключа. Шифртекст выписывается из заполненной таблицы по столбцам, порядок которых определяется ключом. Пусть, например, ключом является (5, 4, 1, 7, 2, 6, 3), и с его помощью нужно зашифровать сообщение

ВОТПРИМЕРШИФРА ВЕРТИКАЛЬНОЙ ПЕРЕСТАНОВКИ

Запишем сообщение в таблицу, столбцы которой пронумерованы в соответствии с ключом:

5	1	4	7	2	6	3
В	О	Т	П	Р	И	М
Е	Р	Ш	И	Ф	Р	А
В	Е	Р	Т	И	К	А
Л	Ь	Н	О	Й	П	Е
Р	Е	С	Т	А	Н	О
В	К	И				

Выписывая теперь буквы по столбцам в соответствии с принятой нумерацией, получим шифртекст:

ОРЕЪЕКРФЙЙАМААЕОТШРНСИВЕВЛРВИРКПНППОТ

При расшифровании длина криптограммы (в данном примере равная 38) делится с остатком на длину ключа, равную 7. Остаток от деления (число 3) определяет число длинных столбцов в заполненной таблице. Эти столбцы расположены слева. Остальные 4-е столбца — короткие. Они расположены справа от длинных столбцов. Это наблюдение позволяет правильно записать шифртекст в таблицу, после чего выписать из неё открытый текст по строкам.

Число ключей ШВП не превосходит $m!$, где m — длина ключа. Как правило, m гораздо меньше длины сообщения n , поэтому число ключей шифра много меньше $n!$. Пользуясь приведённой выше формулой Стирлинга, попытайтесь оценить при больших значениях m и n , во сколько раз число возможных перестановок ШВП с ключом длины m меньше числа всех перестановок для текста длины n , кратной m .

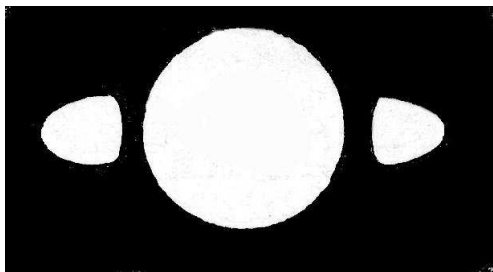
Как мы уже отмечали, ключ шифра желательно по возможности запоминать или извлекать его из какого-то легко запоминаемого слова или фразы. Для этого имеется несколько способов. Можно, например, отметить числами порядковые вхождения букв в некоторое «ключевое слово» и получить ключ. Поясним это на примере. Пусть ключевым является слово ПЕРЕСТАНОВКА. Отметим натуральными числами вхождения букв этого слова в алфавитном порядке. Первое вхождение буквы А получает номер 1, второе — номер 2. Поскольку ключевое слово не содержит буквы Б, буква В получает номер 3. Продолжая эту нумерацию, получим в результате следующий ключ:

П	Е	Р	Е	С	Т	А	Н	О	В	К	А
9	4	10	5	11	12	1	7	8	3	6	2

Ярким историческим примером применения шифров перестановки являются астрономические анаграммы. В период большого числа астрономических открытий в XVII в. существовал обычай закреплять за собой право на первенство, прибегая к помощи анаграмм — пере-

становки букв. Первооткрыватель кратко объявлял о сущности своего открытия в форме анаграммы (которая публиковалась), смысл которой был известен только ему одному. Это давало учёному время не спеша перепроверить своё открытие (например, используя более совершенную оптику), а в случае его правильности — раскрыть его суть общественности и подтвердить своё авторство. Одна из таких историй связана с именем Галилео Галилея.

С помощью своей несовершенной трубы, направленной на небесное тело, он увидел приблизительно вот что:



После этого Галилей поспешил сделать заявку на это открытие и опубликовал следующее, зашифрованное с помощью шифра перестановки, сообщение:

SMAISMRMIELMEPOETALEUMIBUVNEUGTTAVIRAS

В дальнейшем Галилей раскрыл смысл этого сообщения:

ALTISSIMUM PLANETAM TERGEMINUM OBSERVAVI,

что в переводе с латыни означает:

ВЫСОЧАЙШУЮ ПЛАНЕТУ ТРОЙНОЮ НАБЛЮДАЛ.

Галилей так и не догадался, что на самом деле открыл кольца Сатурна. И официально это открытие было сделано полвека спустя Гюйгенсом.

Приведём теперь некоторые общие идеи, используемые в анализе шифров перестановки. Мы можем попытаться восстановить исходное сообщение по шифртексту путём анаграммирования. Помните игру, в которой нужно составлять слова из букв данного слова? В ней выигрывает тот, кто составит больше слов. Участники этой игры и занимаются анаграммированием, то есть подбором букв друг за другом таким образом, чтобы получилось осмысленное слово. Шифртекст содержит все буквы, из которых состоит исходное сообщение. Нужно выяснить лишь порядок их следования друг за другом. Как мы уже убедились, число возможных перестановок букв длинного слова слишком велико при реализации полного перебора. Но, даже получив несколько подходящих вариантов перестановок, не всегда можно выделить из них истинный вариант. Например, из фрагмента шифртекста АОГР можно получить

осмысленные варианты ГОРА, РОГА и АРГО. Если нет дополнительных сведений о характере текста, то выбрать из этих трёх вариантов один невозможно.

Приведём пример ещё более запутанной ситуации. Пусть требуется восстановить сообщение по криптограмме

ААНИНК_ТЕОМЛ,З.ЬЪЗИВТЛП_ЬЮ

(«_» — обозначение пробела), полученной с помощью шифра перестановки. Возможны, как минимум, два варианта расшифрования:

КАЗНИТЬ, _НЕЛЬЗЯ_ПОМИЛОВАТЬ. и

КАЗНИТЬ_НЕЛЬЗЯ, _ПОМИЛОВАТЬ.

Эти варианты имеют прямо противоположный смысл, и без наличия дополнительной информации у нас нет возможности выбрать один из них.

В некоторых случаях за счёт особенностей в реализации шифра удаётся получить информацию об использованном преобразовании (перестановке). Например, в задаче 2.1, используя сведения о наклоне букв, удаётся из простых геометрических соображений определить диаметр Считалы, который является ключом шифра, и, следовательно, найти нужную перестановку.

В рассмотренном примере шифровальщик по неосторожности оставил на ленте папируса следы, которые позволили легко прочесть сообщение. Возможны и другие ситуации, когда не очень «грамотное» использование шифра позволяет его взломать. Так, в задаче 5.2 содержится пример текста, зашифрованного ШВП. По условию пробелы между словами при записи текста в таблицу опускались. Поэтому можно заключить, что столбцы, содержащие пробелы, располагались в исходной таблице справа. Это даёт возможность разбить множество столбцов на две группы (содержащие по 6 и по 5 букв). Для восстановления открытого текста остаётся найти порядок следования столбцов в каждой из групп, что гораздо проще.

Аналогичная ситуация возникает и для шифра «Поворотная решётка» при шифровании коротких сообщений, когда после записи открытого текста в вырезы трафарета не все клетки прямоугольника оказываются заполненными. Пусть, например, используется трафарет размера $m \times r$ и с его помощью зашифровано сообщение длины $mr - k$, где $1 < k \leq mr/4$. Незаполненные k клеток прямоугольника соответствуют вырезам трафарета в его четвёртом положении. Это наблюдение приводит к резкому сокращению числа допустимых трафаретов (их будет $4^{mr/4-k}$). Читателю предлагается самостоятельно найти число допустимых трафаретов при $k > mr/4$.

На примере задачи 5.2 продемонстрируем ещё один метод анализа шифров вертикальной перестановки — лингвистический. Он основан на том, что в естественных языках некоторые сочетания букв встреча-

ются часто, другие гораздо реже, а некоторые не встречаются вовсе (например, биграмма ЪЪ не встречается в русском языке).

Для решения задачи 5.2 будем подбирать порядок следования столбцов заполненной таблицы друг за другом так, чтобы в образовавшихся строках оказались «читаемые» отрезки текста. Приведённое решение задачи начинается с подбора трёх столбцов первой группы так, что в последней строке оказалась триграмма ТЧК. Это естественно, поскольку, скорее всего, сообщение заканчивается точкой. Далее подбираются столбцы, продолжающие фрагменты текста в других строках.

Сочетание лингвистического метода с учётом дополнительной информации позволяет довольно быстро восстановить открытый текст.

В заключение рассказа о шифрах перестановки приведём историю с зашифрованным автографом А. С. Пушкина, описанную в романе В. Каверина «Исполнение желаний».

Главный герой романа — студент-историк Н. Трубачевский, — занимавшийся работой в архиве своего учителя — академика Бауэра С. И., — нашёл в одном из секретных ящиков пушкинского бюро фрагмент недописанной X главы «Евгения Онегина». Это был перегнутый вдвое полулист плотной голубоватой бумаги с водяным знаком 1829 года. На листе было написано следующее.

- | | |
|--|--------------------------------------|
| 1. Властитель слабый и лукавый | 1. Нечаянно пригретый славой |
| 2. Его мы очень смирным знали | 2. Орла двуглавого щипали |
| 3. Гроза двенадцатого года | 3. Остервенение народа |
| 4. Но Бог помог — стал ропот ниже | 4. Мы очутились в Париже |
| 5. И чем жирнее, тем тяжеле | 5. Скажи, зачем ты в самом деле |
| 6. Авось, о Шиболет народный | 6. Но стихоплёт великородный |
| 7. Авось, аренды забывая | 7. Авось по манью Николая |
| 8. Сей муж судьбы, сей странник
бранный | 8. Сей всадник, папою венчанный |
| 9. Тряслися грозно Пиринеи | 9. Безрукий князь друзьям Морей |
| 10. Я всех уйму с моим народом | 10. А про себя и в ус не дует |
| 11. Потешный полк Петра Титана | 11. Предавших некогда тирана |
| 12. Россия присмирела снова | 12. Но искра пламени иного |
| 13. У них свои бывали сходки | 13. Они за рюмкой русской водки |
| 14. Витийством резким знамениты | 14. У беспокойного Никиты |
| 15. Друг Марса, Вакха и Венеры | 15. Свои решительные меры |
| 16. Так было над Невою льдистой | 16. Блестит над каменной
тенистой |
| 17. Плешивый щёголь, враг труда | 17. Над нами царствовал тогда |
| 18. Когда не наши повара | 18. У Бонапартова шатра |
| 19. Настала — кто тут нам помог? | 19. Барклай, зима иль русский бог? |
| 20. И скоро силою вещей | 20. А русский царь главой царей |
| 21. О русский глупый наш народ | 21. |
| 22. Тебе б я оду посвятил | 22. Меня уже предупредил |
| 23. Ханжа запрётся в монастырь | 23. Семействам возвратит Сибирь |

24. Пред кем унизились цари
 25. Волкан Неаполя пылал
 26. Наш царь в конгрессе говорил
 27. Дружина старых усачей
 28. И пуше царь пошёл кутить
 29. Они за чашею вина
 30. Сбирались члены сей семьи
 31. Тут Луин дерзко предлагал
 32. Но там, где ранее весна

24. Исчезнувший как тень зари
 25. Из Кишинёва уж мигал
 26. Ты александровский холоп (?)
 27. Свирепой шайке палачей
 28. Уже издавна, может быть
 29.
 30. У осторожного Ильи
 31. И вдохновенно бормотал
 32. И над холмами Тульчина

Без особых усилий Трубачевский прочитал рукопись, и ничего не понял. Он переписал её, получилась бессвязная чепуха, в которой одна строка, едва начавшая мысль, перебивается другой, а та — третьей, ещё более бессмысленной и бессвязной. Он попробовал разбить рукопись на строфы, — опять не получилось. Стал искать рифмы, — как будто и рифм не было, хотя на белый стих всё это мало похоже. Просчитал строку — четырёхстопный ямб, размер, которым написан «Евгений Онегин».

Трубачевский с азартом взялся за рукопись, пытался читать её, пропуская по одной строке, потом по две, по три, надеясь случайно угадать тайную последовательность, в которой были записаны строки. У него ничего не получалось. Тогда он стал читать третью строку вслед за первой, пятую за третьей, восьмую за пятой, предположив, что пропуски должны увеличиваться в арифметической прогрессии. Всё то же! Отчаявшись, он бросил эту затею. Однако, она не давала ему покоя ни на лекции, ни в трамвае. . . Как шахматист, играющий в уме, он не только знал наизусть каждую строчку, он видел её в десяти комбинациях сразу.

Прошло время. Однажды, когда он смотрел на светлые пятна окон подходящего к перрону поезда, каким-то внутренним зрением он увидел перед собой всю рукопись — и с такой необыкновенной отчётливостью, как это бывает только во сне.

Сможете ли вы прочитать эти стихи? Ответ вы найдёте в романе В. Каверина.

4. Многоалфавитные шифры замены

Шифр Цезаря относится к числу одноалфавитных шифров замены. Они фактически заменяют алфавит **A** открытого текста алфавитом **B** шифрованного текста. Для шифра Цезаря, например, алфавит **B** получается циклическим сдвигом алфавита **A** (в приведённом примере влево на три буквы):

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
B	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Основная слабость одноалфавитного шифра состоит в том, что частотные характеристики открытого и зашифрованного текстов одинаковы. Зная характерные особенности открытого текста, несложно восстановить алфавит шифртекста и зашифрованное сообщение. Указанная слабость была известна уже в средние века.

На смену одноалфавитным шифрам пришли более стойкие — *многоалфавитные шифры замены*. Такие шифры использовали несколько алфавитов шифртекста, выбор которых при зашифровании сообщения определяется некоторыми правилами. Большую популярность получили шифры, основанные на квадратной таблице, состоящей из алфавитов, записанных один под другим, причём каждый из них сдвинут на одну позицию влево по сравнению с предыдущим. Например, для английского алфавита такая таблица имеет следующий вид:

1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
3	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
4	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
5	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
6	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
7	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
8	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
9	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
10	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
11	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
12	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
13	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
14	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
15	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
16	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
17	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
18	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
19	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
20	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
21	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
22	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
23	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
24	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
25	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
26	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Шифр Цезаря может использовать в качестве алфавита шифртекста любую (но лишь одну) строку этой таблицы. Иоганнес Тритемий в

1518 году предложил использовать строки этой таблицы периодически: 1-я буква текста шифруется с помощью 1-го алфавита, 2-я буква — с помощью 2-го, 26-я буква — последнего, 27-я — опять с помощью 1-го и т. д.

Блез де Виженер в 1585 году изложил идею *ключевого слова*. Она состоит в следующем. Последовательность букв открытого текста шифруется с помощью периодической последовательности шифралфавитов в соответствии с выбранным секретным ключевым словом. Если, например, это слово — CRYPTOGRAPHY, то 1-я буква текста шифруется с помощью алфавита, который начинается буквой С, 2-я буква — с помощью алфавита, начинающегося буквой R, и т. д. После того как будет использована последняя буква ключевого слова — Y, для зашифрования следующей буквы вновь используется первая буква ключевого слова. Таблица 1 стала называться таблицей Виженера, а сам шифр — шифром Виженера.

Позже граф Гронсфельд усовершенствовал практическое использование шифра Виженера, предложив в качестве ключевого слова числовую последовательность. При этом буква открытого текста заменялась буквой, отстоящей от неё в естественном алфавите (1-й алфавит в таблице Виженера) на расстоянии, равном соответствующему числу ключевой последовательности. Например, если ключевая последовательность равна 3, 5, 11, 23, 7, 15, 3, а открытый текст — это слово GERMANY, то шифртекст имеет вид JJSJNSB.

Ещё более прозрачным процесс шифрования с помощью шифра Виженера стал после того, как буквенный алфавит был заменён числовым. В самом деле, заменим букву x алфавита её порядковым номером \bar{x} (начиная с 0) в этом алфавите. Например, $\bar{a} = 0$, $\bar{b} = 1$, и т. д. Тогда если \bar{x} — очередной знак открытого текста, а $\bar{\gamma}$ — знак ключевой последовательности, то соответствующий знак \bar{y} шифртекста равен остатку $r_n(\bar{x} + \bar{\gamma})$ от деления суммы чисел $\bar{x} + \bar{\gamma}$ на число n букв алфавита. Применительно к английскому алфавиту, если, например, $\bar{x} = 14$, $\bar{\gamma} = 17$, то $\bar{y} = r_{26}(14 + 17) = 5$. Формула $\bar{y} = r_n(\bar{x} + \bar{\gamma})$ делает процесс зашифрования алгебраической операцией, для проведения которой не нужна таблица Виженера. Такая версия шифра получила название *шифра гаммирования*, а ключевая последовательность стала называться *гаммой*. Для шифра Виженера гамма представляет собой числовую последовательность короткого периода. История криптографии показала, что именно небольшой период гаммы является главным недостатком шифра. Для того чтобы шифр гаммирования был стойким, требуется, чтобы гамма имела очень большой период и обладала ещё рядом дополнительных свойств, приближающих её к совершенно случайной последовательности.

Алгебраическая форма удобна для представления частных случаев шифра гаммирования. Представим, например, в алгебраической форме

шифр Цезаря. Введём обозначение \mathbb{Z}_n для множества $\{0, 1, \dots, n-1\}$. Тогда открытый текст записывается строкой чисел из \mathbb{Z}_n . Множеством ключей шифра Цезаря служит \mathbb{Z}_n . Результатом зашифрования открытого текста x_1, \dots, x_l на ключе $k \in \mathbb{Z}_n$ является y_1, \dots, y_l , где $y_i = r_n(x_i + k)$, $i = \overline{1, l}$. Результатом расшифрования шифртекста y_1, \dots, y_l на ключе $k \in \mathbb{Z}_n$ является x_1, \dots, x_l , где $x_i = r_n(y_i - k)$, $i = \overline{1, l}$.

Шифр гаммирования является не единственным примером многоалфавитного шифра замены. Большой класс таких шифров составляют шифры, реализуемые дисковыми шифраторами типа известной шифрмашин «Энигма», использовавшейся немецкими войсками в период Второй мировой войны. Об устройстве дисковых шифраторов и их роли можно прочитать во многих книгах, посвящённых Второй мировой войне.

5. Современные приложения криптографии

До 1978 года были известны лишь *шифры с секретным ключом*. Так называются шифры, для которых расшифрование определяется тем же ключом, что и зашифрование. Поэтому ключ нужно хранить в секрете от посторонних. В связи с симметричностью ситуации при использовании секретного ключа используют термин *симметричное шифрование*.

Примером шифра с секретным ключом является шифр простой замены типа «пляшущих человечков». Ключом такого шифра служит таблица замены знаков алфавита «человечками». Обозначим через $E_k(u) = v$ результат зашифрования сообщения u на ключе k , а через $D_k(v)$ результат расшифрования v на ключе k . Преобразования, осуществляемые при зашифровании и расшифровании, должны быть такими, чтобы для любых u и k выполнялось соотношение $D_k(E_k(u)) = u$.

В 1978 году появился первый *шифр с открытым ключом* под названием RSA (образованным первыми буквами фамилий разработчиков: Рональд Линн Ривест, Ади Шамир, Леонард Адлеман). Для зашифрования и расшифрования RSA использует *разные ключи* (и, соответственно, разные преобразования). При этом ключ зашифрования объявляется *открытым*. Более того, нужно, чтобы этот ключ записывался в общедоступном справочнике вместе с именем пользователя и другими данными. *Секретным* является ключ расшифрования, причём принадлежать он должен лишь одному пользователю. В связи с асимметричностью ситуации при использовании ключей появился термин *асимметричное шифрование*.

Можно привести следующую аналогию асимметричного шифрования. Если отправитель желает передать секретное сообщение, он информирует об этом получателя (например, телефонным звонком). Получатель присылает по почте почтовый ящик с прорезью с закрытым

замком. Отправитель опускает в прорезь своё сообщение (тем самым, «шифрует» его) и отсылает ящик по почте получателю. Получатель вынимает сообщение (производит «расшифрование»), воспользовавшись своим ключом. Злоумышленнику, которому отправленный ящик попадает в руки, практически невозможно изъять из него сообщение через прорезь. В такой системе шифрования прямое и обратное преобразования информации имеют различный характер. «Открытый ключ» — это, по сути дела, — прорезь, «секретный ключ» — это ключ от замка почтового ящика. Знание открытого ключа не позволяет определить секретный ключ.

Обозначим через E_A (открытый) алгоритм зашифрования пользователя A , а через D_A — его (секретный) алгоритм расшифрования. Пусть $v = E_A(u)$ — результат зашифрования сообщения u , а $u = D_A(v)$ — результат расшифрования сообщения v . Преобразования должны быть такими, чтобы для любого u выполнялось равенство $D_A(E_A(u)) = u$ (далее понадобится также, чтобы выполнялось и равенство $E_A(D_A(u)) = u$, которое имеет место не для любой асимметричной системы).

Идея асимметричного шифрования появилась в 1976 году в статье американских математиков Уитфилда Диффи и Мартина Хеллмана. В этой статье была предложена идея гипотетической *однонаправленной функции с секретом* (кратко — ОФС). Упрощённое определение ОФС можно сформулировать следующим образом.

Однонаправленной функцией с секретом k называется всякое отображение $F_k: U \rightarrow V$ множества U в множество V , для которого выполняются три свойства:

- 1) значение $F_k(u)$ «легко» вычисляется для любого аргумента u ;
- 2) уравнение $F_k(x) = v$ «сложно» решается относительно x при известном k ;
- 3) уравнение $F_k(x) = v$ «легко» решается относительно x при известном k .

В точном определении термины «легко» и «сложно» имеют строгое толкование в смысле теории сложности алгоритмов.

Аналогией ОФС является разборка и сборка механических часов. Разобрать или собрать часы без инструкции несоизмеримо сложнее, чем с инструкцией, которая и является «секретом».

Сделаем замечание. До сегодняшнего дня ОФС остаётся гипотетическим понятием, поскольку ни для одной функции не доказано (в смысле точного, а не упрощённого определения), что она действительно является ОФС. Вместе с тем сегодня используется ряд «кандидатов на ОФС», для которых требования 1)–3) определения практически выполняются. Используем такие «кандидаты» для построения систем шифрования с открытым ключом.

Пусть открытые сообщения представлены элементами множества U . Тогда $F_k(u)$ — это результат зашифрования сообщения u . Если злоумышленник имеет $F_k(u)$, то, в силу свойства 2) ОФС, он (не зная секрета k) должен решить вычислительно сложную задачу для получения u , в то время как законный получатель (имеющий секрет k) может (в силу свойства 3)) сделать это сравнительно «легко».

Укажем теперь «кандидата на ОФС», используемого в RSA.

Пусть n — целое число вида $p \cdot q$, где p, q — простые числа, \mathbb{Z}_n — множество чисел $\{0, 1, \dots, n-1\}$ и m — подходящее целое число (оно должно быть взаимно просто с $(p-1) \cdot (q-1)$). В качестве «кандидата на ОФС» шифр RSA использует функцию $F_{m,n}: \mathbb{Z}_n \rightarrow \mathbb{Z}_n$, где для $u \in \mathbb{Z}_n$ значение $F_{m,n}(u)$ равно остатку от деления числа u^m на n . При достаточно больших значениях n функция $F_{m,n}$ удовлетворяет требованиям, предъявляемым к ОФС. При этом «секретом» служат числа p, q , в произведение которых раскладывается n . Стойкость шифрования с помощью RSA определяется сложностью решения задачи разложения на множители числа n (называемой также *задачей факторизации* числа n). Если n выбрано так, что на сегодняшний день эта задача вычислительно сложна, то стойкость RSA будет гарантирована. Отметим, что факторизация целых чисел n вида $p \cdot q$, где p и q — близкие простые числа, является одной из сложнейших математических задач.

Изначально шифрование использовалось лишь для обеспечения конфиденциальности информации. Целью шифрования была защита от *пассивных атак* злоумышленников. Так называются действия, связанные с перехватом информации и попытками взломать шифр. Развитие информационных технологий потребовало защиты информации и от *активных атак*. Дело в том, что появилась техническая возможность модификации и создания поддельных электронных сообщений. Стали необходимы методы проверки подлинности цифровой информации и выявления источника информации, или, выражаясь книжным языком, методы *аутентификации информации*. Для решения этой задачи был предложен ряд методов, основанных на использовании *криптографических контрольных сумм*.

Идея проста. К цифровому сообщению u добавляется контрольная сумма $S(u)$, которой служит результат зашифрования информации на секретном ключе. Получатель сообщения $(u, S(u))$ должен иметь возможность проверки контрольной суммы. Если используется симметричное шифрование (в этом случае $S(u) = E_k(u)$), то получатель должен иметь секретный ключ k источника. Тогда он сможет вычислить $E_k(u)$ и проверить, совпадает ли это значение с полученной контрольной суммой. Если используется асимметричное шифрование (в этом случае $S(u) = D_A(u)$), то получатель должен иметь открытый ключ источника, который берётся из справочника абонентов. Тогда он смо-

жет вычислить $E_A(D_A(u))$ и проверить, совпадает ли это значение с u . И в том и в другом случае совпадение является критерием подлинности сообщения u .

Если u — длинное сообщение, то контрольная сумма может быть чрезмерно длинной. Чтобы сделать её короче, цифровую информацию можно предварительно «сжать». Для этого используют так называемые *хеш-функции*, которые отображают битовые строки произвольной длины в битовые строки фиксированной длины, например, 128 или 160 и более бит. Если F — такая функция, то сообщение u снабжается контрольной суммой $S(F(u))$.

Развитие автоматизированных средств обработки информации и сетевых технологий породило ещё один тип угроз: возможность *отказа от авторства* или *приписывания авторства*, порождённую средой не доверяющих друг другу пользователей сети (свойственной сфере бизнеса). Суть проблемы состоит в следующем. Как доказать, например, что один из участников нарушил условия принятого им договора, отказавшись позже от выполнения его условий? Если бы в тексте договора стояли собственноручные подписи его участников, то это могло быть основанием для обращения в суд. А как быть, если договор был заключён, например, через Интернет, без встречи его участников? Для решения возникшей проблемы потребовался аналог собственноручной подписи — *электронная (цифровая) подпись*. Проблему цифровой подписи решило использование асимметричного шифрования. В самом деле, если зашифровать сообщение u на секретном ключе её владельца A , то результат — $D_A(u)$ можно рассматривать как «подписанное сообщение» u . Составить такое сообщение мог только владелец секретного ключа D_A . Кроме того, кто угодно может проверить «подпись», взяв из справочника открытый ключ абонента A и вычислив $E_A(D_A(u)) = u$. Теперь автора сообщения u легко привлечь к суду в случае, если он откажется от обязательств, принятых им в сообщении u . Как и выше, подпись можно укоротить, используя предварительное «сжатие» сообщение с помощью хеш-функции F .

Отметим, что для обеспечения секретности «подписанное сообщение» $D_A(F(u))$, передаваемое пользователю B по незащищённому каналу связи, может быть зашифровано на открытом ключе получателя. Тогда получив $v = E_B(A, u, D_A(F(u)))$, пользователь B вычисляет $D_B(v) = A, u, D_A(F(u))$, затем применяет к u функцию F , вычисляя $F(u) = F'$, выбирает из справочника абонентов открытый ключ абонента A и затем проверяет равенство $E_A(D_A(F(u))) = F'$. Таким образом, получатель такого сообщения может проверить, пришло оно от пользователя A или нет, а само сообщение передавалась в зашифрованном виде.

Помимо указанных основных задач защиты информации, к которым относятся обеспечение конфиденциальности, аутентификации и невоз-

возможности отказа от авторства, криптографические методы успешно используются для решения многих других важных приложений. Это — задачи разграничения доступа, идентификации удалённых пользователей компьютерных систем, организации неотслеживаемых электронных платежей, доказательств с нулевым разглашением и других. С этими вопросами вы можете познакомиться в книгах, которых в последние годы достаточно много появилось на полках магазинов. Многие из них доступны и школьникам.

6. Условия задач олимпиад по криптографии и математике

Ниже приводятся задачи двадцати олимпиад по криптографии и математике. Нумерация задач двойная: первая цифра — номер олимпиады, вторая — номер задачи в олимпиаде. Для решения задач не требуется специальных знаний. Все необходимые определения даны в условиях. Задачи рассчитаны на учащихся 9, 10 и 11 классов.

I Олимпиада по криптографии и математике

1.1. Ключом шифра, называемого «поворотная решётка», является трафарет, изготовленный из квадратного листа клетчатой бумаги размера $n \times n$ (n — чётно). Некоторые из клеток вырезаются. Одна из сторон трафарета помечена. При наложении этого трафарета на чистый лист бумаги четырьмя возможными способами (помеченной стороной вверх, вправо, вниз, влево) его вырезы полностью покрывают всю площадь квадрата, причём каждая клетка оказывается под вырезом ровно один раз.

Буквы сообщения, имеющего длину n^2 , последовательно вписываются в вырезы трафарета, сначала наложенного на чистый лист бумаги помеченной стороной вверх. После заполнения всех вырезов трафарета буквами сообщения трафарет располагается в следующем положении и т. д. После снятия трафарета на листе бумаги оказывается зашифрованное сообщение.

Найдите число различных ключей для произвольного чётного числа n .

1.2. В адрес олимпиады пришло зашифрованное сообщение:

Ф В М Е Ж Т И В Ф Ю

Найдите исходное сообщение, если известно, что шифрпреобразование заключалось в следующем. Пусть x_1, x_2 — корни трёхчлена $x^2 + 3x + 1$. К порядковому номеру каждой буквы в стандартном русском алфавите (33 буквы) прибавлялось значение многочлена $f(x) = x^6 + 3x^5 + x^4 + x^3 + 4x^2 + 4x + 3$, вычисленное либо при $x = x_1$, либо при $x = x_2$ (в неизвестном нам порядке), а затем полученное число заменялось соответствующей ему буквой.

1.3. Для передачи информации от резидента Гарриваса в Нагонии только что внедрённому разведчику был установлен следующий порядок.

Все сообщения резидента определены заранее и пронумерованы числами $1, 2, 3, \dots$. Разведчик, обладающий феноменальной памятью, полностью запомнил соответствие между сообщениями и их номерами. Теперь для того, чтобы передать информацию разведчику, достаточно было сообщить ему лишь соответствующее число.

Для передачи числа в условленном месте оставлялась равная этому числу денежная сумма.

На момент разработки операции в Нагонии имели хождение денежные купюры достоинством $1, 3, 7$ и 10 бут (бут — денежная единица Нагонии). Однако в результате денежной реформы купюры достоинством 1 и 3 бут были изъяты из обращения.

Выясните, начиная с какого номера можно передать разведчику любое сообщение, пользуясь только оставшимися в обращении купюрами.

1.4. Сколько существует упорядоченных пар натуральных чисел a и b , для которых известны их наибольший общий делитель $d = 6$ и их наименьшее общее кратное $m = 6930$. Сформулируйте ответ и в общем случае, используя канонические разложения d и m на простые множители.

1.5. Дана криптограмма:

$$\begin{array}{rclcl} \text{ФН} & \times & \text{Ы} & = & \text{ФАФ} \\ + & & \times & & - \\ \text{ЕЕ} & + & \text{Е} & = & \text{НЗ} \\ = & & = & & = \\ \text{ИША} & + & \text{МР} & = & \text{ИМН} \end{array}$$

Восстановите цифровые значения букв, при которых справедливы все указанные равенства, если разным буквам соответствуют различные цифры. Расставьте буквы в порядке возрастания их цифровых значений и получите искомый текст.

1.6. Одна фирма предложила устройство для автоматической проверки пароля. Паролем может быть любой непустой упорядоченный набор букв в алфавите $\{a, b, c\}$. Будем обозначать такие наборы большими латинскими буквами. Устройство перерабатывает введенный в него набор P в набор $Q = \varphi(P)$. Отображение φ держится в секрете, однако про него известно, что оно определено не для каждого набора букв и обладает следующими свойствами. Для любого набора букв P

1) $\varphi(aP) = P$;

2) $\varphi(bP) = \varphi(P)a\varphi(P)$;

3) набор $\varphi(cP)$ получается из набора $\varphi(P)$ выписыванием букв в обратном порядке.

Устройство признаёт предъявленный пароль верным, если $\varphi(P)=P$. Например, трёхбуквенный набор bab является верным паролем, так как $\varphi(bab) = \varphi(ab)a\varphi(ab) = bab$. Подберите верный пароль, состоящий более чем из трёх букв.

II Олимпиада по криптографии и математике

2.1. В древнем шифре, известном под названием «Считала», использовалась полоска папируса, которая наматывалась на круглый стержень виток к витку без просветов и нахлёстов. Далее, при горизонтальном положении стержня, на папирус построчно записывался текст сообщения. После этого полоска папируса с записанным на ней текстом посылалась адресату, имеющему точно такой же стержень, что позволяло ему прочесть сообщение.

В наш адрес поступило сообщение, зашифрованное с помощью шифра «Считала». Однако её автор, заботясь о том, чтобы строчки были ровные, во время письма проводил горизонтальные линии, которые остались на полоске в виде чёрточек между буквами. Угол наклона этих чёрточек к краю ленты равен α , ширина полоски равна d , а ширина каждой строки равна h . Укажите, как, пользуясь имеющимися данными, прочесть текст.

2.2. Исходное цифровое сообщение коммерсант шифрует и передаёт. Для этого он делит последовательность цифр исходного сообщения на группы по пять цифр в каждой и после двух последовательных групп приписывает ещё две последние цифры суммы чисел, изображённых этими двумя группами. Затем к каждой цифре полученной последовательности он прибавляет соответствующий по номеру член некоторой целочисленной арифметической прогрессии, заменяя результат сложения остатком от деления его на 10.

Найдите исходное цифровое сообщение по шифрованному сообщению:

4 2 3 4 6 1 4 0 5 3 1 3

2.3. Рассмотрим преобразование цифрового текста, в котором каждая цифра заменяется остатком от деления значения многочлена $F(x) = b(x^3 + 7x^2 + 3x + a)$ на число 10, где a, b — фиксированные натуральные числа.

Выясните, при каких значениях a, b указанное преобразование может быть шифрпреобразованием (т.е. допускает однозначное расшифрование).

2.4. При установке кодового замка каждой из 26 латинских букв, расположенных на его клавиатуре, сопоставляется произвольное натуральное число, известное лишь обладателю замка. Разным буквам сопоста-

вляются не обязательно разные числа. После набора произвольной комбинации попарно различных букв происходит суммирование числовых значений, соответствующих набранным буквам. Замок открывается, если сумма делится на 26.

Докажите, что для любых числовых значений букв существует комбинация, открывающая замок.

2.5. Сообщение, записанное в алфавите

АБВГДЕЖЗИКЛМНОПРСТУФХЦШЩЬЫЭЮЯ

зашифровывается при помощи последовательности букв этого же алфавита. Длина последовательности равна длине сообщения. Шифрование каждой буквы исходного сообщения состоит в сложении её порядкового номера в алфавите с порядковым номером соответствующей буквы шифрующей последовательности и замене такой суммы на букву алфавита, порядковый номер которой имеет тот же остаток от деления на 30, что и эта сумма.

Восстановите два исходных сообщения, каждое из которых содержит слово КОРАБЛИ, если результат их зашифрования при помощи одной и той же шифрующей последовательности известен:

ЮПТЦАРГШАЛЖЖЕВЩЫРВУУ и ЮПЯТБНЩМСДТЛЖПГСХСЦЦ

2.6. Буквы русского алфавита занумерованы в соответствии с таблицей:

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

Для зашифрования сообщения, состоящего из n букв, выбирается ключ K — некоторая последовательность из n букв приведённого выше алфавита. Зашифрование каждой буквы сообщения состоит в сложении её номера в таблице с номером соответствующей буквы ключевой последовательности и замене полученной суммы на букву алфавита, номер которой имеет тот же остаток от деления на 30, что и эта сумма.

Прочтите шифрованное сообщение: РБНТСИТСРРЕЗОХ, если известно, что шифрующая последовательность не содержала никаких букв, кроме А, Б и В.

III Олимпиада по криптографии и математике

3.1. Установите, можно ли создать проводную телефонную сеть связи, состоящую из 993 абонентов, каждый из которых был бы связан ровно с 99 другими.

3.2. Шифрпреобразование простой замены в алфавите $A = \{a_1, a_2, \dots, a_n\}$, состоящем из n различных букв, заключается в замене каждой буквы шифруемого текста буквой того же алфавита, причём разные

буквы заменяются разными. Ключом шифра простой замены называется таблица, в которой указано, какой буквой надо заменить каждую букву алфавита А. Если слово СРОЧНО зашифровать простой заменой с помощью ключа:

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я
Ч	Я	Ю	Э	Ы	Ъ	Щ	Ш	Ц	Х	Ф	У	Б	Д	Т	З	В	Р	П	М	Л	К	А	И	О	Ж	Е	С	Г	Н

то получится слово ВЗДАБД. Зашифровав полученное слово с помощью того же ключа ещё раз, получим слово ЮШЫЧЯЫ. Сколько всего различных слов можно получить, если указанный процесс шифрования продолжать неограниченно?

3.3. Сообщение, зашифрованное в пункте А шифром простой замены в алфавите из букв русского языка и знака пробела (–) между словами, передаётся в пункт Б отрезками по 12 символов. При передаче очередного отрезка сначала передаются символы, стоящие на чётных местах в порядке возрастания их номеров, начиная со второго, а затем — символы, стоящие на нечётных местах (также в порядке возрастания их номеров), начиная с первого. В пункте В полученное шифрованное сообщение дополнительно шифруется с помощью некоторого другого шифра простой замены в том же алфавите, а затем таким же образом, как и из пункта А, передаётся в пункт В. По перехваченным в пункте В отрезкам:

С	О	–	Г	Ж	Т	П	Н	Б	Л	Ж	О
Р	С	Т	К	Д	К	С	П	Х	Е	У	Б
–	Е	–	П	Ф	П	У	Б	–	Ю	О	Б
С	П	–	Е	О	К	Ж	У	У	Л	Ж	Л
С	М	Ц	Х	Б	Э	К	Г	О	Щ	П	Ы
У	Л	К	Л	–	И	К	Н	Т	Л	Ж	Г

восстановите исходное сообщение, зная, что в одном из переданных отрезков зашифровано слово КРИПТОГРАФИЯ.

3.4. Дана последовательность чисел $C_1, C_2, \dots, C_n, \dots$ в которой C_n есть последняя цифра числа n^n . Докажите, что эта последовательность периодическая и её наименьший период равен 20.

3.5. Исходное сообщение, состоящее из букв русского алфавита и знака пробела (–) между словами, преобразуется в цифровое сообщение заменой каждого его символа парой цифр согласно следующей таблице:

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	–
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Для зашифрования полученного цифрового сообщения используется отрезок последовательности из задачи 3.4, начинающийся с некоторого члена C_k . При зашифровании каждая цифра сообщения складывается

с соответствующей цифрой отрезка и заменяется последней цифрой полученной суммы. Восстановите сообщение:

2339867216458160670617315588

3.6. Равносторонний треугольник ABC разбит на четыре части так, как показано на рисунке, где M и N — середины сторон AB и BC соответственно. Известно, что $PK \perp MQ$ и $NL \perp MQ$. В каком отношении точки P и Q делят сторону AC , если известно, что из этих частей можно составить квадрат?

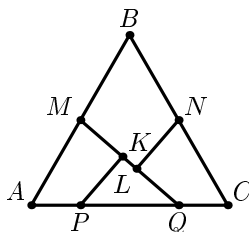


Рис. 6

IV Олимпиада по криптографии и математике

4.1. Ключом шифра, называемого «решёткой», является прямоугольный трафарет размера 6×10 клеток. В трафарете вырезаны 15 клеток так, что при наложении его на прямоугольный лист бумаги размера 6×10 клеток четырьмя возможными способами его вырезы полностью покрывают всю площадь листа.

Буквы сообщения (без пропусков) последовательно вписываются в вырезы трафарета (по строкам, в каждой строке слева направо) при каждом из четырёх его возможных положений. Прочтите исходный текст, если после зашифрования на листе бумаги оказался следующий текст (на русском языке):

Р	П	Т	Е	Ш	А	В	Е	С	Л
О	Я	Т	А	Л	—	Ь	З	Т	—
—	У	К	Т	—	Я	А	Ь	—	С
Н	П	—	Ь	Е	У	—	Ш	Л	С
Т	И	Ь	З	Ы	Я	Е	М	—	О
—	Е	Ф	—	—	Р	О	—	С	М

4.2. Криптограмма

12 2 24 5 3 21 6 29 28 2 20 18 20 21 5 10 27 17 2 11 2 16 —
 19 2 27 5 8 29 12 31 22 2 16, 19 2 19 5 17 29 8 29 6 29 16:
 8 2 19 19 29 10 19 29 14 19 29 29 19 10 2 24 2 11 2 16
 10 14 18 21 17 2 20 2 28 29 16 21 29 28 6 29 16.

получена заменой букв на числа (от 1 до 32) так, что разным буквам соответствуют разные числа. Отдельные слова разделены несколькими пробелами, буквы — одним пробелом, знаки препинания сохранены. Буквы «е» и «ё» не различаются. Прочтите четверостишие В. Высоцкого.

4.3. «Шифровальный диск» используется для зашифрования числовых сообщений. Он состоит из неподвижного диска и соосно вращающегося на нём диска меньшего диаметра. На обоих дисках нанесены цифры от 0 до 9, которые расположены в вершинах правильных 10-угольников, вписанных в диски.

Цифра X на неподвижном диске зашифровывается в цифру Y подвижного диска, лежащую на том же радиусе, что и X .

Для построения вписанного 10-угольника без транспортира надо уметь строить угол в 36° . Попробуйте вычислить с точностью до 0,1 значение какой-либо тригонометрической функции такого угла без таблиц и калькулятора.

4.4. Зашифрование фразы на латинском языке осуществлено в два этапа. На первом этапе каждая буква текста заменяется на следующую в алфавитном порядке (последняя Z заменяется на первую A). На втором этапе применяется шифр простой замены с неизвестным ключом. Его применение заключается в замене каждой буквы шифруемого текста буквой того же алфавита, при этом разные буквы заменяются разными буквами. Ключом такого шифра является таблица, в которой указано, какой буквой надо заменить каждую букву алфавита.

По данному шифртексту

OSZJX FXRE YOQJSZ RAYFJ

восстановите открытое сообщение, если известно, что для использованного (неизвестного) ключа результат шифрования не зависит от порядка выполнения указанных этапов для любого открытого сообщения. Пробелы в тексте разделяют слова.

Латинский алфавит состоит из следующих 24 букв:

A B C D E F G H I J L M N O P Q R S T U V X Y Z.

4.5. Для проверки телетайпа, печатающего буквами русского алфавита

А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я

передан набор из 9 слов, содержащий все 33 буквы алфавита. В результате неисправности телетайпа на приёмном конце получены слова

Г Ы Й А Э Б П Р К Е Ж Ц Ю Н М Ъ Ч С Ы Л З Ш Д У Ц Х О Т Я Ф В И

Восстановите исходный текст, если известно, что характер неисправности таков, что каждая буква заменяется буквой, отстоящей от неё в указанном алфавите не дальше, чем на две буквы. Например, буква Б может перейти в одну из букв {А, В, Г}.

4.6. Исходное сообщение из букв русского алфавита преобразуется в числовое сообщение заменой каждой его буквы числом по следующей таблице:

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

Для зашифрования полученного числового сообщения используется шифрующий отрезок последовательности A_1, A_2, \dots подходящей длины, начинающийся с A_{100} .

При зашифровании каждое число числового сообщения складывается с соответствующим числом шифрующего отрезка. Затем вычисляется остаток от деления полученной суммы на 30, который по данной таблице заменяется буквой. Восстановите сообщение КЕНЗЭРЕ, если шифрующий отрезок взят из последовательности, у которой $A_1 = 3$ и $A_{k+1} = A_k + 3(k^2 + k + 1)$ для любого натурального k .

4.7. Чтобы запомнить периодически меняющийся пароль в ЭВМ, математики придумали следующий способ. При известном числе a (например, номере месяца в году), пароль представляет собой первые шесть цифр наименьшего решения уравнения

$$a(x^2 - 1) = \sqrt{1 + x/a}.$$

(Число меньшей значности дополняется справа необходимым числом нулей.)

Решите такое уравнение при произвольном $a > 0$.

V Олимпиада по криптографии и математике

5.1. Комбинация (x, y, z) трёх натуральных чисел, лежащих в диапазоне от 10 до 20 включительно, является отпирающей для кодового замка, если выполнено соотношение $F(x, y, z) = 99$. Найдите все отпирающие комбинации для замка с

$$F(x, y, z) = 3x^2 - y^2 - 7z.$$

5.2. Сообщение было построчно записано в таблицу, имеющую 20 столбцов. При этом в каждую клетку таблицы записывалось по одной букве сообщения, пробелы между словами были опущены, а знаки препинания заменены на условные комбинации: точка — ТЧК, запятая — ЗПТ. Затем столбцы таблицы были некоторым образом переставлены, в результате чего был получен текст:

Я Н Л В К Р А Д О Е Т Е Р Г О М И З Я Е
 Й Л Т А Л Ф Ы И П Е У И О О Г Е Д Б О Р
 Ч Р Д Ч И Е С М О Н Д К Х И Н Т И К Е О
 Н У Л А Е Р Е Б Ы Ы Е Е З И О Н Н Ы Ч Д
 Ы Т Д О Е М П П Т Щ В А Н И П Т Я З С Л
 И К С И - Т Ч Н О - - Е - Л У Л - Т - Ж

Прочтите исходное сообщение.

5.3. Из точки O внутри треугольника ABC на его стороны AB , BC , AC опущены перпендикуляры OP , OQ , OR . Докажите, что $OA + OB + OC \geq 2(OP + OQ + OR)$.

5.4. Зашифрование сообщения состоит в замене букв исходного текста на пары цифр в соответствии с некоторой (известной только отправителю и получателю) таблицей, в которой разным буквам алфавита соответствуют разные пары цифр. Криптографу дали задание восстановить зашифрованный текст. В каком случае ему будет легче выполнить задание: если известно, что первое слово второй строки — «термометр» или что первое слово третьей строки — «ремонт»? Обоснуйте свой ответ. (Предполагается, что таблица зашифрования криптографу неизвестна).

5.5. Решите уравнение:

$$\sqrt{3x+1}\sqrt{3x+71} - (7 + \sqrt{2x-1})\sqrt{2x+14\sqrt{2x-1}+118} = 0.$$

5.6. При передаче сообщений используется некоторый шифр. Пусть известно, что каждому из трёх зашифрованных текстов

ЙМЫВОТСЬЛКЪГВЦАЯ
УКМАПОЧСРКШВЗАХ
ШМФЭОГЧСЙЪКФЬВЫЕАКК

соответствовало исходное сообщение МОСКВА. Попробуйте расшифровать три текста

ТПЕОИРВНТМОЛАРГЕИАНВИЛЕДНМТААГТДЪТКУБЧКГЕИШНЕИАЯРЯ
ЛСИЕМГОРТКРОМИТВАВКНОПКРАСЕОГНАЬЕП
РТПАИОМВСВТИЕОБПРОЕННИГЪКЕЕАМТАЛВТДЪСОУМЧШСЕОНШЬИАЯК

при условии, что двум из них соответствует одно и то же сообщение. Сообщениями являются известные крылатые фразы.

VI Олимпиада по криптографии и математике

6.1. В системе связи, состоящей из 1997 абонентов, каждый абонент связан ровно с N другими. Определите все возможные значения N .

6.2. Квадратная таблица размером 1997×1997 заполнена натуральными числами от 1 до 1997 так, что в каждой строке присутствуют все числа от 1 до 1997. Найдите сумму чисел, стоящих на диагонали, которая соединяет левый верхний и правый нижний углы таблицы, если заполнение таблицы симметрично относительно этой диагонали.

6.3. Текст

А М И М О П Р А С Т Е Т И Р А С И С П Д
И С А Ф Е И И Б О Е Т К Ж Р Г Л Е О Л О
И Ш И С А Н Н С Й С А О О Л Т Л Е Я Т У
И Ц В Ы И П И Я Д П И Щ П Ъ П С Е Ю Я Я

получен из исходного сообщения перестановкой его букв. Текст

У Щ Ф М Ш П Д Р Е Ц Ч Е Ш Ю Ш Ч Д А К Е
 Ч М Д В К Ш Б Е Е Ч Д Ф Э П Й Щ Г Ш Ф Щ
 Ц Е Ю Щ Ф П М Е Ч П М Е Р Щ М Е О Ф Ч Щ
 Х Е Ш Р Т Г Д И Ф Р С Я Ы Л К Д Ф Ф Е Е

получен из того же исходного сообщения заменой каждой буквы на другую букву так, что разные буквы заменены разными, а одинаковые — одинаковыми. Восстановите исходное сообщение.

6.4. На каждой из трёх осей установлено по одной вращающейся шестерёнке и неподвижной стрелке. Шестерёнки соединены последовательно. На первой шестерёнке 33 зубца, на второй — 10, на третьей — 7. На каждом зубце первой шестерёнки по часовой стрелке написано по одной букве русского языка в алфавитном порядке:

А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я

На зубцах второй и третьей шестерёнки в порядке возрастания по часовой стрелке написаны цифры от 0 до 9 и от 0 до 6 соответственно. Когда стрелка первой оси указывает на букву, стрелки двух других осей указывают на цифры.

Буквы сообщения шифруются последовательно. Зашифрование производится вращением первой шестерёнки против часовой стрелки до первого попадания шифруемой буквы под стрелку. В этот момент последовательно выписываются цифры, на которые указывают вторая и третья стрелки. В начале шифрования стрелка 1-го колеса указывала на букву А, а стрелки 2-го и 3-го колёс — на цифру 0.

а) зашифруйте слово О Л И М П И А Д А;

б) расшифруйте сообщение 2 4 8 0 9 2 8 3 9 1 1 2 1 1.

6.5. Цифры от 1 до 9 расположены на окружности в некотором неизвестном порядке. При зашифровании цифрового сообщения каждая отличная от 0 цифра заменяется на соседнюю с ней цифру на окружности по часовой стрелке, а при расшифровании — на соседнюю с ней цифру на окружности против часовой стрелки. Цифра 0 остаётся без изменения в обоих случаях.

Укажите условия, при которых порядок цифр на данной окружности можно однозначно восстановить по двум цифровым текстам — результатам расшифрования и зашифрования одного и того же цифрового текста с помощью данной окружности.

6.6. Докажите, что для каждого простого числа p последовательность a_1, a_2, a_3, \dots является периодической с периодом 2, если a_n равно остатку от деления числа p^{n+2} на 24 при всех $n \geq 1$.

6.7. Найдите все значения параметра a , при которых уравнение

$$\underbrace{\left| \dots \right|}_{1996 \text{ раз}} \left| x - a \right| - \underbrace{a \left| \dots \right|}_{1996 \text{ раз}} = 1996.$$

имеет ровно 1997 различных решений.

VII Олимпиада по криптографии и математике

7.1. Какое наименьшее число соединений требуется для организации проводной сети связи из 10 узлов, чтобы при выходе из строя любых двух узлов связи сохранялась возможность передачи информации между любыми двумя оставшимися (хотя бы по цепочке через другие узлы)?

7.2. В компьютерной сети используются пароли, состоящие из цифр. Чтобы избежать хищения паролей, их хранят на диске в зашифрованном виде. При необходимости использования происходит однозначное расшифрование соответствующего пароля. Зашифрование пароля происходит посимвольно одним и тем же преобразованием. Первая цифра остаётся без изменения, а результат зашифрования каждой следующей цифры зависит только от неё и от предыдущей цифры.

Известен список зашифрованных паролей:

4249188780319, 4245133784397, 5393511, 428540012393,
4262271910365, 4252370031465, 4245133784735

и два пароля 4208212275831, 4242592823026, имеющиеся в зашифрованном виде в этом списке. Можно ли определить какие-либо другие пароли? Если да, то восстановите их.

7.3. В результате перестановки букв сообщения получена криптограмма:

БТИПЧЬЛОЯЧЬБТОТПУНТНОНЗЛЖАЧЬОТУНИУХНИППОЛЮЧЬОЕЛОЛС

Прочтите исходное сообщение, если известно, что оно было разбито на отрезки одинаковой длины r , в каждом из которых буквы переставлены одинаково по следующему правилу. Буква отрезка, имеющая порядковый номер x ($x = 1, 2, \dots, r$), в соответствующем отрезке криптограммы имеет порядковый номер $f(x) = ax \oplus b$, где a и b — некоторые натуральные числа, $ax \oplus b$ равно остатку от деления суммы $ax + b$ на r , если остаток не равен нулю, и равно r , если остаток равен нулю.

7.4. Знаменитый математик Леонард Эйлер в 1759 г. нашёл замкнутый маршрут обхода всех клеток шахматной доски ходом коня ровно

по одному разу. Прочтите текст, вписанный в клетки шахматной доски по такому маршруту (см. рис. 7). Начало текста в а4.

7.5. При $a > 0$, $b > 0$, $c > 0$ докажите неравенство:

$$a^3 + b^3 + c^3 + 6abc > \frac{1}{4}(a + b + c)^3.$$

7.6. Для рисования на большой прямоугольной доске используется мел с квадратным сечением со стороной 1 см. При движении мела стороны сечения всегда параллельны краям доски. Как начертить выпуклый многоугольник площадью 1 м^2 с наименьшей площадью границы (площадь границы не входит в площадь многоугольника)?

7.7. Цифры $0, 1, \dots, 9$ разбиты на несколько непересекающихся групп. Из цифр каждой группы составляются всевозможные числа, для записи каждого из которых все цифры группы используются ровно один раз (учитываются и записи, начинающиеся с нуля). Все полученные числа расположили в порядке возрастания и k -ому числу поставили в соответствие k -ую букву алфавита

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЦЩЩЬЬЪЮЯ

Оказалось, что каждой букве соответствует число и каждому числу соответствует некоторая буква. Шифрование сообщения осуществляется заменой каждой буквы соответствующим ей числом. Если ненулевое число начинается с нуля, то при шифровании этот ноль не выписывается. Восстановите сообщение 873146507381 и укажите таблицу замены букв числами.

VIII Олимпиада по криптографии и математике

8.1. На рисунке изображена эмблема олимпиады. Она представляет собой замкнутую ленту, сложенную так, что образовавшиеся просветы являются одинаковыми равносторонними треугольниками. Если в некотором месте ленту разрезать перпендикулярно к её краям и развернуть, то получится прямоугольник. Найдите минимальное отношение его сторон.

8.2. Сообщение, составленное из нулей и единиц, шифруется двумя способами. При первом способе каждый ноль заменяется на

Д	Л	Р	И	Л	П	Н	Б
У	К	А	О	Т	У	С	Т
О	О	О	А	Н	О	И	Р
Т	Б	Г	К	Т	Т	У	К
К	О	Е	О	Р	А	В	О
К	Д	Г	П	В	Л	Е	Т
Т	А	Н	Р	М	А	Г	О
Е	А	О	В	И	Д	У	Л

Рис. 7



Рис. 8

последовательность из k_1 нулей и следующих за ними k_2 единиц, а каждая единица заменяется на последовательность из k_3 нулей. При втором способе шифрования каждая единица заменяется на последовательность из k_4 единиц и следующих за ними k_5 нулей, а каждый нуль заменяется на последовательность из k_6 нулей. При каких натуральных значениях k_i , $i = 1, 2, \dots, 6$, найдётся хотя бы одно сообщение, которое будет одинаково зашифровано обоими способами? Укажите общий вид таких сообщений.

8.3. Сообщение, подлежащее зашифрованию, представляет собой цифровую последовательность, составленную из дат рождения 6 членов оргкомитета олимпиады. Каждая дата представлена в виде последовательности из 8 цифр, первые две из которых обозначают день, следующие две — месяц, а остальные — год. Например, дата рождения великого математика Л. Эйлера 4 апреля 1707 года представляется в виде последовательности 04041707. Для зашифрования сообщения строится ключевая последовательность длины 48. Для её построения все нечётные простые числа, меньшие 100, выписываются через запятую в таком порядке, что модуль разности любых двух соседних чисел есть та или иная степень числа 2. При этом каждое простое число выписано ровно один раз, а числа 3, 5 и 7 записаны в виде 03, 05 и 07 соответственно. Удалив запятые из записи этой последовательности, получим искомую ключевую последовательность.

При зашифровании цифровой последовательности, представляющей сообщение, её цифры почленно складываются с соответствующими цифрами ключевой последовательности, при этом каждая полученная сумма заменяется её остатком от деления на 10. В результате зашифрования сообщения получена последовательность:

150220454213266744305682533362327363924975709849

Определите даты рождения членов оргкомитета олимпиады.

8.4. Квадрат размера 13×13 разбит на клетки размера 1×1 . В начальный момент некоторые клетки окрашены в чёрный цвет, а остальные — в белый. По клеткам квадрата прыгает Кристоша. В момент попадания Кристоши в очередную клетку происходит изменение цвета на противоположный у всех тех клеток, расстояния от центров которых до центра клетки с Кристошей есть натуральные числа. После того как Кристоша побывал в каждой клетке квадрата ровно 1999 раз, квадрат оказался раскрашенным так, как показано на рисунке. Восстановите цвет всех клеток квадрата в начальный момент.

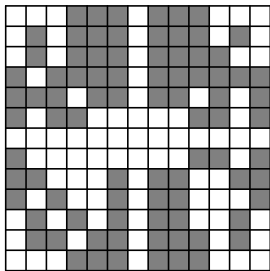


Рис. 9

8.5. Для всех действительных чисел a, b решите уравнение

$$\frac{a}{1-bx} = \frac{b}{1-ax}.$$

8.6. Разложите число $2^{30} + 1$ на простые сомножители.

IX Олимпиада по криптографии и математике

9.1. Суммой двух букв назовём букву, порядковый номер которой в алфавите имеет тот же остаток от деления на число букв в алфавите, что и сумма порядковых номеров исходных двух букв. Суммой двух буквенных последовательностей одинаковой длины назовём буквенную последовательность той же длины, полученную сложением букв исходных последовательностей, стоящих на одинаковых местах.

а) Докажите, что существует последовательность из 33 различных букв русского алфавита, сумма которой с последовательностью букв, представляющей собой сам этот алфавит, не содержит одинаковых букв.

б) Докажите, что сумма любой последовательности из 26 различных букв английского алфавита с последовательностью букв, представляющей собой сам этот алфавит, содержит не менее двух одинаковых букв.

9.2. Некоторую последовательность из букв русского алфавита

А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я

1949¹⁹⁹⁹ раз прибавили по правилу задачи 9.1 к слову КРИПТОША. Получили слово АНАЛИТИК. Найдите эту последовательность. Какое наименьшее число раз надо прибавить её к слову АНАЛИТИК, чтобы получить слово КРИПТОША?

9.3. Каждую букву исходного сообщения заменили её двузначным порядковым номером в русском алфавите согласно таблице

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	

Полученную цифровую последовательность разбили (справа налево) на трёхзначные цифровые группы без пересечений и пропусков. Затем, каждое из полученных трёхзначных чисел умножили на 77 и оставили только три последние цифры произведения. В результате получилась следующая последовательность цифр:

317564404970017677550547850355.

Восстановите исходное сообщение.

9.4. Клетки квадрата 4×4 пронумеровали так, что клетка в правом нижнем углу получила номер 1, а все остальные получили разные номера от 2 до 16. Оказалось, что суммы номеров клеток каждой строки, каждого столбца, а также каждой из двух диагоналей квадрата одинаковы («магический» квадрат). Клетки квадрата заполнили буквами некоторого сообщения так, что его первая буква попала в клетку с номером 1, вторая — в клетку с номером 2 и т. д. В результате построчного выписывания букв заполненного квадрата (слева направо и сверху вниз) получилась последовательность букв

Ы Р Е У С Т Е В Ъ Т А Б Е В К П.

Восстановите магический квадрат и исходное сообщение.

9.5. Окружность радиуса 5 с центром в начале координат пересекает ось абсцисс в точках $A(-5; 0)$ и $D(5; 0)$. Укажите все возможные расположения на окружности точек B , C и E , удовлетворяющие одновременно следующим четырём условиям:

- (1) координаты точек B , C и E — целые числа;
- (2) ордината точки E меньше нуля, а ординаты точек B и C больше нуля;
- (3) абсцисса точки B меньше абсциссы точки C ;
- (4) сумма площадей частей круга, лежащих внутри углов ABE и ECD равна половине площади круга, ограниченного исходной окружностью.

9.6. Для всех значений параметра a решите неравенство

$$\sqrt{-x^2 - x - 0,25 + a^2} \geq 1 + \sqrt{-x^2 + x + 3,75}.$$

X Олимпиада по криптографии и математике

10.1. Для изображения портрета Кристоши в квадратной таблице размера 15×15 каждую её клетку покрасили белой или чёрной краской. Назовём подряд идущие клетки одного цвета строки или столбца таблицы *полосой*, а число клеток в полосе — её *длиной*.

Восстановите изображение Кристоши по известным длинам полос чёрного цвета в каждой строке и в каждом столбце (следующих соответственно сверху вниз и слева направо). По строкам: 9; 11; 1, 1; 2, 3, 3, 2; 2, 2; 2, 1, 1, 1, 2; 2, 1, 2; 2, 2; 1, 5, 1; 2, 3, 2; 2, 2; 7; 1, 1; 6, 6; 1, 4, 1, 4, 1. По столбцам: 1; 5, 1; 9, 2; 2, 2, 2; 2, 1, 2, 2; 2, 1, 1, 1, 1, 2; 2, 1, 2, 3; 2, 2, 2, 1, 1; 2, 1, 2, 3; 2, 1, 1, 1, 1, 2; 2, 1, 2, 2; 2, 2, 2; 9, 2; 5, 1; 1. При этом полосы чёрного цвета одной строки или одного столбца не соприкасаются.

10.2. Решите уравнение

$$x^2 + y^2 + z^2 + xy - yz + xz - 5 =$$

$$= u^2 + v^2 + w^2 + uv - vw + uw + 2u - 2v + 2w,$$

если каждое неизвестное может принимать любое из двух значений, указанных в таблице

x	y	z	u	v	w
0	-1	1	-1	0	0
1	2	2	0	3	1

10.3. Буквы алфавита английского языка (I и J отождествлены)

ABCDEFGHIJKLMNOPQRSTUVWXYZ

вписаны в клетки таблицы 5×5 построчно слева направо, начиная с верхней строки. При этом сначала вписано слово английского языка из 6 попарно различных букв, которое назовём *ключевым словом*. Затем последовательно вписаны буквы, не вошедшие в ключевое слово, в их алфавитном порядке. Для зашифрования некоторого слова с помощью этой таблицы каждую его букву заменим парой цифр. Первая цифра — номер строки, а вторая — номер столбца таблицы, содержащих эту букву. Полученную цифровую последовательность запишем в обратном порядке, а затем каждую пару цифр (слева направо) последовательно заменим буквой по той же таблице. Найдите ключевое слово, если слово HANDWRITING (почерк) зашифровано в PVMTMEDWVAH.

10.4. Каждое число вида $x_n = 1 + 2 + 3 + \dots + n$, $n \in \mathbb{N}$, заменим последней цифрой s_n в его десятичной записи. Из последовательности s_1, s_2, s_3, \dots выпишем единицу и следующие за ней цифры до тех пор, пока не встретится уже выписанная цифра. Если при этом окажется, что выписаны не все десять цифр, то все отсутствующие допишем в порядке возрастания. Полученный отрезок из 10 различных цифр назовём *перестановкой*. Обозначим перестановку символом p_k , если её первая цифра является k -ой по счёту единицей в последовательности s_1, s_2, s_3, \dots .

а) Докажите, что цифровая последовательность s_1, s_2, s_3, \dots является периодической, и найдите её наименьший период.

б) Докажите, что последовательность перестановок p_1, p_2, p_3, \dots является периодической, и найдите её наименьший период.

10.5. С целью зашифрования разобьём текст на последовательные отрезки по 10 букв. Изменим порядок букв каждого отрезка с помощью перестановок из задачи 10.4. При этом для перестановки букв в k -ом от-

резке используется перестановка p_k . Например, из отрезка АБВГДЕЖЗИК с помощью перестановки 1 3 4 0 5 9 6 7 8 2 получим отрезок БГДАЕКЖЗИВ. Восстановите отрывок из книги Л. Кэррола, если после его зашифрования данным методом получен текст:

ООСХОРШКАЗЛЭНИАКОТАТТООНАРЗИСЧЗЕПОСТЕПЕНОАННИНЧАЯ
СОВАККНЧИХОТОСНИАКЧАЯЛУЫБКОЙКОТЯЕОЩАЕЫЛВКНААИДН
ЕООВТРОРЕЕМЯ

10.6. Докажите, что уравнение

$$x^5 + 5x^3 + 5x - 1 = 0$$

имеет один действительный корень и найдите его.

XI Олимпиада по криптографии и математике

11.1. Известно, что число вхождений некоторого символа в текст составляет от 10,5 % до 11 % длины текста. Найдите минимально возможную длину текста.

11.2. Во фрагменте литературного произведения известного автора, записанном без пробелов и знаков препинания, *заменяли* буквы. При этом, разные буквы заменили разными, а одинаковые — одинаковыми. В результате получили некоторую последовательность букв. Тот же фрагмент был разбит на целое число подряд идущих участков, состоящих из одинакового числа букв. В каждом участке буквы одинаково *переставили* между собой. В результате получили другую последовательность. Восстановите исходный фрагмент по двум полученным последовательностям:

МЗОБВЕСИАВЛИЕВСОДВОВМОНИОНЧЛГЕЕОТИЕПОРЗАНДСОТЮОВИЫСЧОНЕВИЛОО

РИЖХУВМРЭЭШБЯВРРЖШЬВЭРВУЧМЖЬВЕЖЭКВЖАБЬЯСВХВТРВШАВЕБГЭШВМВРЖЭ

если неизвестно, каким из указанных способов получена каждая из них. Также известно, что последовательность ШВМВРЖЭЭСВХБКЗНДЭЬ получена из названия произведения и фамилии автора той же *заменой* букв, которая использовалась при преобразовании исходного фрагмента.

11.3. Для передачи сообщений по телеграфу каждая буква русского алфавита (буквы Е и Ё отождествлены) представляется в виде пятизначной комбинации из нулей и единиц, соответствующих двоичной записи номера данной буквы в алфавите (нумерация букв начинается с нуля). Например, буква А представляется в виде 00000, буква Б — 00001, буква Ч — 10111, буква Я — 11111. Передача пятизначной комбинации производится по кабелю, содержащему пять проводов. Каждый двоич-

ный разряд передаётся по отдельному проводу. При приёме сообщения Криптоша перепутал провода, поэтому вместо переданного слова получен набор букв ЭАВЩОЩИ. Найдите переданное слово.

11.4. Клетку таблицы 8×8 назовём «хорошей», если все остальные клетки таблицы можно замостить прямоугольниками 3×1 .

а) Укажите все «хорошие» клетки таблицы.

б) Сообщение зашифровано по правилу, определяемому некоторым «ключевым словом». Например, если ключевое слово — ИКСИ, то каждая буква сообщения преобразуется с помощью соответствующей буквы последовательности ИКСИИКСИ... следующим образом. Если, например, 7-я буква сообщения — А, то она заменяется на 7-ю букву последовательности, т. е. на С, если Б, то она заменяется на Т, В — на У, ..., Я — на Р. Во все клетки таблицы, за исключением «хороших», построчно вписаны буквы шифрованного текста, а в «хорошие» клетки — буквы ключевого слова. Найдите ключевое слово и восстановите исходное сообщение по приведённой таблице.

щ	е	д	е	ю	у	я	б
б	в	ш	а	р	ш	д	н
п	ь	р	щ	е	у	в	ё
ъ	й	л	ё	и	ж	щ	е
д	е	ю	у	в	к	ч	ч
с	б	с	г	е	ь	р	е
ш	в	й	е	с	в	ь	о
э	ю	ь	ь	а	ь	з	ь

11.5. В углах квадрата со стороной 269 мм расположены прямоугольники со сторонами 100 мм и 90 мм. Можно ли перемещением прямоугольников внутри квадрата без пересечения друг с другом поменять место расположения каждого прямоугольника на симметричное относительно центра квадрата?

11.6. Решите систему уравнений

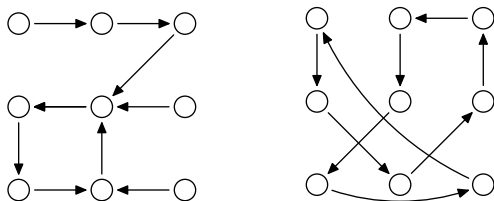
$$\begin{cases} \left(\left| y + x - \frac{5 + \sqrt{3}}{2} \right| + |x - 1| \right)^2 = \\ \quad = (|2x - \sqrt{2y} - 2| + |y - 1| + 1) \cdot (1 - |y - 1| - |2x - \sqrt{2y} - 2|), \\ x^2 + y^2 = 2(x + y) - 1. \end{cases}$$

ХII Олимпиада по криптографии и математике

12.1. Два криптографа выясняют, чей шифр содержит больше ключей. Первый говорит, что ключ его шифра состоит из 50 упорядоченных символов, каждый из которых принимает 7 значений. Второй говорит, что ключ его шифра состоит всего из 43 упорядоченных символов, зато каждый из них принимает 10 значений. Чей шифр содержит больше ключей?

12.2. Порядковый номер каждой буквы алфавита русского языка, состоящего из 32 букв (Е и Ё отождествлены), представлен в двоичной системе счисления пятизначным числом, начиная с нуля. Например, букве А соответствует двоичное число 00000, а букве Ч — 10111. Передача каждой буквы сообщения осуществляется путём передачи каждой из цифр соответствующего пятизначного двоичного числа по отдельному проводу. Криптоша случайно замкнул какие-то два из этих пяти проводов. В результате на других концах замкнутых проводов появляется 1, как только по одному из них передаётся 1. Найдите переданное слово, если получен текст ТЕЫЕУТАЦ.

12.3. Аладдин находится в подземелье, состоящем из девяти одинаковых залов, причём он не знает, в каком именно. Если он потрёт волшебную лампу, Большой Джинн перенесёт его в другой зал в соответствии со схемой на левом рисунке. Если Аладдин потрёт волшебное кольцо, Маленький Джинн перенесёт его в соответствии со схемой на правом рисунке.



Какую последовательность действий с лампой и кольцом надо сделать Аладдину, чтобы он мог утверждать, что находится в центральном зале? Выполнять какие-либо другие действия, например, ставить отметки в залах не разрешается. Схемы перемещения Аладдину известны.

12.4. В первую строку таблицы размером 3×10 вписали менее 10 различных букв русского алфавита (Е и Ё, И и Ъ, Ь и Ы отождествлены). Затем все оставшиеся буквы в естественном порядке построчно сверху вниз, слева направо вписали в свободные клетки таблицы. Можно ли слово АСТРАХАНЬ зашифровать с помощью этой таблицы в слово БУТЕРБРОД? Алгоритм шифрования изложен ниже на примере.

Пример. Исходное слово ИКСИ будет зашифровано в слово ИИНКЕ с помощью таблицы

	0	1	2	3	4	5	6	7	8	9
1	Ш	И	Ф	Р	А	Б	В	Г	Д	Е
2	Ж	З	К	Л	М	Н	О	П	С	Т
3	У	Х	Ц	Ч	Щ	Ы	Ь	Э	Ю	Я

по следующему правилу. Из номеров столбцов таблицы с буквами слова ИКСИ составим число 1281 и умножим его на 9. Получим 11529. Это будут последовательные номера столбцов таблицы с буквами шифрованного слова. Соответствующие номера строк таблицы с этими буквами будут 11221, где 1221 — соответствующие номера строк с буквами исходного слова, а первая 1 приписывается, если число цифр произведения больше числа букв исходного слова.

12.5. Предложение на русском языке в соответствии с некоторым правилом вписано в клетки таблицы:

Т	С	Ъ	О	Ц	О	К	Р
Е	У	В	Ц	Ь	П	В	И
И	Г	Ж	Э	У	Ц	О	Й
Ч	Г	С	Т	М	И	Р	Ц
М	П	Е	О	У	О	Й	И
О	Ж	А	Н	Н	Н	А	Г
Т	И	Г	У	И	К	Л	Р
А	М	Е	М	М	С	Н	Ъ

Найдите это правило и прочитайте предложение.

12.6. На плоскости изображён отрезок. Используя только циркуль, постройте середину этого отрезка. (Точка считается построенной, если она есть результат пересечения или касания окружностей.)

12.7. Найдите:

- последнюю цифру числа 2^{2002} ;
- три последние цифры числа 2^{2002} .

XIII Олимпиада по криптографии и математике

13.1. Пользователи сети связи для обеспечения секретности сообщений выбирают (независимо друг от друга) пары преобразований (E, D) , одно из которых, E (открытый ключ), публикуют в справочнике, а второе, D (личный ключ), держат в секрете. Известно, что значения $E(m)$ и $D(n)$ легко вычислить для любых сообщений m и n , причём из равенства $E(m) = n$ следует, что $D(n) = m$. В то же время нахождение m по $E(m)$ является сложной задачей, которую невозможно решить (любыми

средствами) за реальное время, если неизвестно D . Если пользователь A хочет послать пользователю B сообщение m , он берёт из справочника открытый ключ E_B пользователя B , вычисляет $n = E_B(m)$ и посылает n к B . Получив n , B вычисляет $D_B(n) = m$. Злоумышленник, перехвативший n , не сможет вычислить m . Это гарантирует секретность информации.

Ватсон предложил Холмсу способ передачи секретных сообщений с уведомлением о получении: A передаёт B сообщение $(A, E_B(m))$; B , получив сообщение, вычисляет m и направляет A уведомление $(B, E_A(m))$. Холмс возразил Ватсону, что этот способ не обеспечивает секретности информации от любого пользователя, который может перехватывать сообщения и как угодно их изменять. Дополнительно потребовав, чтобы для каждого преобразования E было сложно подобрать пару (m, n) , для которой $E(m) = E(n)$, Холмс предложил Ватсону свой способ: A передаёт B сообщение $E_B(A, m)$; B , получив сообщение, находит m и направляет A уведомление $E_A(B, m)$. Объясните, почему способ Холмса лучше способа Ватсона.

13.2. Шифр *Bifid*, имеющий простое правило зашифрования, использует в качестве ключа квадратную таблицу, в которую в некотором порядке записаны буквы английского алфавита (буквы I и J отождествлены). Результатом зашифрования фразы SIXTY EIGHT MILES на приведённом ключе является «фраза» RYXHT OFTXH LKSWH. Зашифруйте на том же ключе фразу ENTER OTHER LEVEL.

C	O	D	E	A
B	F	G	H	I
K	L	M	N	P
Q	R	S	T	U
V	W	X	Y	Z

13.3. Для доступа к управлению параметрами своего счёта клиенту Зазеркального банка необходимо связаться по телефону с банком и набрать семизначный пароль. После первой же неправильно набранной цифры пароля банк прерывает телефонное соединение. Как надо действовать, чтобы за наименьшее число попыток подобрать пароль?

13.4. Формулировка некоторого геометрического утверждения была вписана в клетки таблицы 10×10 построчно слева направо, начиная с верхней левой клетки. Знак переноса на следующую строку не ставился, но между соседними словами одной строки помещалась пустая клетка. Кристоша решил переставлять буквы в отдельных столбцах, сдвигая их все на одну позицию вверх и перенося самую верхнюю букву вниз (при этом пустую клетку он также считал буквой). Иногда

он менял местами сразу все строки, симметричные относительно средней линии, а именно 1-ю с 10-й, 2-ю с 9-й — и т. д., после чего снова брался за передвижение букв в столбцах. В результате таблица приняла представленный на рисунке вид. Прочитайте исходное геометрическое утверждение.

а	л	п	н	в	и		в	т	р
е	о	с	н	л	я		о	л	т
п		я	л	ы	е	о	ы	т	у
е	о	а	о	щ	д	р	р	а	е
н	р	у	и		о	н	с	т	в
п	к	и	м	е	ь		р		
е	в	о	ю	т	х	х	н	а	с
д	с	е	х	и	и	е	о	я	
о	к	ь	т	ы	п	ь	п	е	н
с	ж	с	с	е	л		о	о	о

13.5. Какое наименьшее количество натуральных чисел надо взять, чтобы любое число от 1 до 300 можно было представить в виде суммы подходящего набора различных указанных натуральных чисел.

13.6. Для зашифрования сообщения используют последовательность неотрицательных целых чисел x_1, x_2, \dots , удовлетворяющую соотношению $x_{k+3} = x_k + x_{k+2}$, $k = 1, 2, \dots$. Две строки известного стихотворения, последние 5 букв которых совпадают, зашифровали следующим образом. Первую букву заменили числом согласно таблице

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

и сложили с x_1 , вторую заменили и сложили с x_2 и т. д. Затем все суммы заменили остатками от деления на 31, а остатки заменили буквами согласно таблице. Получили текст

СЕЗНПКЬЛЧЕЮЩТНИЭЛЬЩБШЬЕЮ

ЛУАЕЧЖЪЭШЭЛЬЩХЧШДЮВЬЮИД.

Восстановите три буквы, соответствующие в таблице числам x_1, x_2, x_3 , и прочитайте двестише.

XIV Олимпиада по криптографии и математике

14.1. Числа, расположенные в клетках таблицы, указывают, сколько соседних по горизонтали, вертикали и диагонали клеток (включая ту, в которой находится само число) должны быть окрашены. Восстановите

картинку, которой соответствуют эти числа.

	5		2		0		0	1		2		1
		5		3			3			5		
3		4							6			4
			5	3		3				5		
				2		3	3	3	2			1
2		2								0		
	0		3		5				3			0
						3				1		
	1	3										
0				9			7		8		2	
		6			6							
	3									6		0
0				6			5					

14.2. Кодовая комбинация сейфа устанавливается на внутренней стороне дверцы с помощью трёх дисков. Каждый из них может быть установлен в одно из 20 положений, пронумерованных числами от 0 до 19, поворотом по часовой стрелке. В начальный момент диски установлены в положение (0, 0, 0). За положение с номером 19 диск не поворачивается. При повороте каждого диска на одно положение раздаётся щелчок. Сравните число возможных кодовых комбинаций, при установке которых раздаётся 33, 32, 25 щелчков.

14.3. На фирме работают P служащих. В гараже фирмы имеется B автомобилей. Каждый служащий имеет ключи от t автомобилей, причём ключи от разных автомобилей разные. (Будем говорить, что каждый служащий «владеет» i автомобилями.) Каждой машиной «владеют» ровно s служащих. При этом наборы ключей любых двух служащих содержат не более одного одинакового ключа. Известно также, что если служащий x не «владеет» автомобилем L , то из всех «владельцев» автомобиля L только у одного есть в наборе такой же ключ, как у служащего x .

Выразите числа P , B , а также общее количество ключей, имеющихся у служащих, через s и t . Числа s и t целые, большие 1.

14.4. Разложите на простые множители число $2^{22} + 39 \cdot 2^{10} + 81$.

14.5. Для зашифрования текста $v_1 v_2 \dots v_k$ на русском языке каждую его букву v_i заменили числом t_i согласно таблице

v_i	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П
t_i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

v_i	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
t_i	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

К каждому числу t_i из последовательности t_1, t_2, \dots, t_k прибавили число a_i из последовательности a_1, a_2, \dots, a_k , заданной соотношениями $a_1 = 1$, $a_{n+1} = 3a_n + 4$ при $n > 0$. Затем остаток от деления каждой суммы $t_i + a_i$ на 33 вновь заменили буквой по той же таблице. При переписывании зашифрованного текста несколько букв были пропущены. В результате получилось вот что:

Р Ч Ж Ъ Э Т С Ъ Ё Л Ж Ъ Я О Ш К С

Найдите исходный текст.

14.6. Имеется клетчатая бумага неограниченных размеров со стороной клетки, равной 1. Шаблоном размера k называется всякая плоская фигура, составленная путём соединения концами друг с другом k параллельных или перпендикулярных отрезков длины 1. Если существует отрезок длины 0,5, полностью размещаемый на шаблоне, то точки шаблона, общие с точками между концами этого отрезка, называются внутренними.

Найдите все шаблоны, которыми можно покрыть все линии клетчатой бумаги (шаблоны можно поворачивать и переворачивать). При покрытии разрешается использовать шаблоны одного вида, причём никакие два шаблона не могут иметь общих внутренних точек. Рассмотрите два случая:

а) $k = 2$; б) $k = 3$.

XV Олимпиада по криптографии и математике

15.1. Докажите, что десятичная запись квадрата натурального числа не может состоять из одинаковых цифр.

15.2. Для зашифрования текстов каждую букву заменяли парой цифр. При этом разные буквы текста заменялись разными парами, а одинаковые — одинаковыми. Даны два зашифрованных текста:

79 92 38 98 95 91 34 95 73 77 96 92 78 95 73 98 92 96 92 72 98
 96 77 72 92 34 77 96 75 90 76 95 38 98 92 70 33 90 96 79 90 96
 77 98 95 90 38 77 70 70 90 98 74 92 96 98 96 77 72 92 34 77 96
 75 73 77 96 92 98 74 92 79 96 90 79 92 96 98 94 90 76 98 74 92
 95 96 96 92 73 79 92 33 98 95 32 92 90 93 38 92 96 73 94 90 91
 96 91 73 92 98 74 95 73 33 72 96 90 34 95 73 73 91 36 71 92 33
 98 98 90 77 38 92 38 72 91 73 92 96 70 95 33 92 38 33 92

71 75 74 39 74 73 74 72 30 73 74 78 33 79 98 94 78 36 79 97 72
 29 78 74 96 74 92 30 38 79 70 72 94 78 79 22 92 92 79 98 37 70
 92 74 94 77 74 93 31 78 74 70 39 79 71 75 94 98 70 39 97 92 72
 22 23 39 78 94 70 74 76 78 94 78 78 30 77 39 94 74 75 94 39 79
 38 94 70 73 79 77 79 78 39 94 75 94 70 73 75 74 76 94 39 74 96
 74 76 78 74 96 79 94 39 79 71 30 27 39 79 32 71 75 74 39 74 73
 74 72 74 92 71 75 94 98 35 22 92 72 22 23 39

Известно, что один из них соответствует сообщению на русском языке, а другой — на английском (в текстах строчные и заглавные буквы не различались, а пробелы и знаки препинания опускались). Определите, какой зашифрованный текст соответствует сообщению на русском языке.

15.3. При зашифровании текста на русском языке (в текстах строчные и заглавные буквы не различались, а пробелы и знаки препинания опускались) каждую букву заменяли парой цифр. При этом разные буквы текста заменялись разными парами, а одинаковые — одинаковыми. Найдите все возможные места расположения слова ПОДЪЕЗД в исходном тексте по зашифрованному тексту:

92 97 36 72 97 92 70 73 97 90 97 72 38 39 74 76
 97 34 79 78 97 70 76 74 72 74 73 74 76 70 70 97
 76 74 96 74 37 39 75 97 70 39 74 79 39 37 71 74
 98 35 94 90 98 97 94 96 74 98 74 76 97

15.4. Центральный замок автомобиля открывается и закрывается с помощью брелка. При получении сигнала брелка замок открывается (если был закрыт) или закрывается (если был открыт). В брелке и замке имеются счётчики (назовём их СБ и СЗ), на которых изначально было выставлено одно и то же число. Пусть N — текущее значение СБ. При нажатии на кнопку брелка СБ меняет значение на $N + 1$, старое же значение N в зашифрованном виде передаётся замку. Микрокомпьютер замка расшифровывает полученный сигнал и находит число, переданное брелком. Если это число равно или превосходит значение СЗ, то замок срабатывает, а значение СЗ становится $N + 1$. Если это число оказывается меньше или при расшифровании обнаруживается ошибка, то замок остаётся в прежнем состоянии. Злоумышленник способен а) запоминать сигналы брелка, б) поставив помеху, исказить сигналы брелка (при этом сам злоумышленник получает сигнал без искажений), в) посылать замку ранее запомненные сигналы. Как злоумышленнику открыть замок? Алгоритмы зашифрования и расшифрования ему неизвестны.

15.5. Для всех $p \in (0; 1)$ найдите минимальное значение выражения $(x_1 + x_2) \cdot p + x_3 \cdot (1 - p)$ при условии, что

- 1) $0 < x_1 < 1; 0 < x_2 < 1; 0 < x_3 < 1$,
- 2) $x_1 + x_2 + x_3 = 1$,
- 3) $x_1 \leq x_2; x_3 \leq x_2; x_2 \cdot (1 - p) \leq x_1 \cdot p$.

XVI Олимпиада по криптографии и математике

16.1. Буквы фрагмента известного стихотворения Ф. И. Тютчева заменены некоторыми буквами так, что разным буквам соответствуют

разные буквы, а одинаковым — одинаковые. Пробелы между словами и знаки препинания сохранены.

*Гьюь Фюббин эй яюзовл,
Пфзшэюь юришь эй шчйфшвл:
Г эйц юбюрйэпо беввл —
С Фюббин ьюцэю вюльгю сйфшвл.*

Восстановите этот фрагмент.

16.2. Криптоша изобрёл устройство, которое позволяет вычислить среднее арифметическое любых 9 чисел или любых 223 чисел. Как правильно использовать это устройство, чтобы найти среднее арифметическое любых 2006 чисел? При необходимости Криптоша может дополнительно провести одно деление и одно умножение.

16.3. Для зашифрования сообщения на английском языке составляются две таблицы размера 5×5 . В клетки каждой таблицы в некотором порядке записываются буквы укороченного английского алфавита (в котором буквы *v* и *w* отождествлены) так, что каждая буква встречается в каждой таблице ровно один раз. Букву, расположенную в *i*-й строке и *j*-м столбце в первой таблице обозначим через a_{ij} , а во второй таблице — через b_{ij} . При зашифровании сообщение разбивается на пары подряд идущих букв и каждая пара заменяется другой парой следующим образом. Первая буква пары ищется в первой таблице, а вторая буква — во второй таблице. Если пара имеет вид $a_{ij}b_{lm}$, то при $i \neq l$ она заменяется парой $b_{im}a_{lj}$, а при $i = l$ — парой $b_{lj}a_{im}$. В результате зашифрования указанным способом сообщения

c r y p t o g r a p h i c a l a l g o r i t h m

был получен один из следующих шифртекстов:

p a b d g l i u r c a v t h o t u e a d s p,
d s z q u p h s b q i j d b m h p s j u i n.

Определите, какой именно. Ответ обоснуйте.

16.4. Пусть a_1, a_2, a_3, \dots и b_1, b_2, b_3, \dots числовые последовательности периодов 16 и 2006 соответственно. Найдите период последовательности $a_1, b_1, a_2, b_2, a_3, b_3, \dots$ (Периодом последовательности x_1, x_2, x_3, \dots называется такое наименьшее натуральное число T , что для всех натуральных n верно равенство $x_{n+T} = x_n$)

16.5. Бильярдные шары плотно уложены в правильный треугольник с основанием из 2006 шаров. На каждом шаре написано число. Сумма трёх чисел, написанных на шарах при вершинах исходного треугольника, а также любых треугольников со сторонами, параллельными исходному треугольнику, равна 0. Какие числа могут быть написаны на шарах?

16.6. Заполните неокрашенные клетки таблицы цифрами от 1 до 9 так, чтобы сумма цифр в каждой неокрашенной горизонтали совпала с числом, стоящим слева в верхней части окрашенного квадрата, а сумма цифр в каждой неокрашенной вертикали — с числом, стоящим сверху в нижней части окрашенного квадрата. При этом в каждой неокрашенной горизонтали и вертикали ни одна из цифр не должна повторяться.

		30	24		8	19	
	16			3			
	35						
5							17
25					9		
			20		26		
13			11				
	16	5	17			17	8
21				24			
10				15			

XVII Олимпиада по криптографии и математике

17.1. Сообщение на русском языке записано в 6 строк. В каждой строке, кроме последней, ровно 18 букв (буквы в строках стоят точно друг под другом). Для зашифрования сообщения каждую его букву заменили парой цифр в соответствии с её порядковым номером в алфавите (А — на 01, Б — на 02, ..., Я — на 33). В результате получилась таблица цифр, в которой 36 столбцов. Затем эту таблицу разделили на вертикальные полосы по три столбца в каждой. После чего полосы переставили в некотором порядке. Получили вот что:

```

316 001 190 014 013 150 171 240 120 131 105 614
010 810 050 610 012 161 121 200 614 120 401 117
619 501 172 327 171 041 061 221 010 033 801 016
115 313 192 312 030 130 160 103 210 013 620 016
512      060      061 250      061 825 16  103 310

```

Выясните, какой текст был зашифрован.

17.2. Пусть $C_n(a, b) = abab \dots ab$ — целое число, десятичная запись которого образована n -кратным повторением пары цифр a и b , где $a \neq 0$. Выясните, при каких n числа $C_n(a, b)$ делятся на 21 при любых значениях a и b .

17.3. Текстовое сообщение зашифровано следующим образом. Над его буквами надписывается числовая последовательность, образованная периодическим повторением шести цифр, образующих дату. Например, шестёрка цифр 181107 отвечает дате 18 ноября 2007 года. После этого каждая буква сообщения заменяется буквой, циклически отстоящей от неё в алфавите справа на число букв, указанное цифрой над ней.

Можно ли прочитать зашифрованное таким образом сообщение

Т П И Ё Р Ж Е М А А С Ф С Г Ъ О Г Х Ж П Н

если неизвестна дата его написания?

17.4. Сообщение на русском языке, состоящее из 63 букв и восклицательного знака, зашифровано с использованием так называемой «поворотной решётки», которая представляет собой трафарет, изготовленный из квадратного листа клетчатой бумаги размера 8 на 8. В трафарете некоторым образом вырезаны 16 клеток. Одна сторона трафарета помечена.

При наложении трафарета на чистый лист бумаги четырьмя возможными способами (помеченной стороной вверх, вправо, вниз, влево) его вырезы покрывают всю площадь квадрата, причём каждая клетка оказывается под вырезом ровно один раз.

Буквы сообщения построчно вписываются в вырезы трафарета (сверху вниз и слева направо, при этом пробелы между словами игнорируются). После того как буквы сообщения заполнят все вырезы трафарета, трафарет располагается в следующем положении (согласно указанному выше порядку) и т. д. Результат зашифрования сообщения представлен на рисунке. Найдите исходное сообщение.

т	я	с	а	п	м	р	е
в	щ	е	р	е	ш	ш	о
ч	и	ч	н	ф	и	т	р
ё	а	е	т	т	е	т	к
р	а	ь	п	а	п	о	ф
т	в	о	е	з	о	к	р
о	с	а	в	т	р	о	т
л	е	я	н	!	е	т	а

Рис. 10

17.5. В здании находится восемь серверов. Они расположены в вершинах куба. Эти серверы объединены в сеть, причём два сервера соединены линией связи «напрямую» в том и только том случае, когда они соответствуют двум соседним вершинам куба. Кроме того, два из этих серверов соединены дополнительно по радиоканалу.

Какое наименьшее число основных линий связи придётся вывести из строя злоумышленнику, для того чтобы потерялась связность сети (т. е. станет невозможно доставить информацию с одного из серверов на другой, даже через серверы-посредники).

17.6. Разложите на простые множители число $3^{20} + 3^4 + 1$, если известно, что оно делится на 167.

XVIII Олимпиада по криптографии и математике

18.1. Строка ПТИУААМДЛ получена перестановкой букв в некотором слове. Имеется последовательность цифр, задающая порядок, в котором надо выписать буквы строки для получения исходного слова. Каждая цифра записывалась в прямоугольный шаблон размера 5 на 3 пикселей по образцу



При передаче часть пикселей на местах, одинаковых для каждой цифры, стёрлись. Получилось вот что:



Восстановите исходное слово и перехваченную перестановку.

18.2. Фраза на русском языке записана два раза подряд без пробелов и знаков препинания и зашифрована с помощью шифра Виженера. Для зашифрования выбирается легко запоминаемое ключевое слово небольшой длины. Пусть k_1, k_2, \dots — последовательность букв, образованная периодическим повторением этого слова, и t_1, t_2, \dots — последовательность букв, представляющая собой данную фразу. Тогда результатом зашифрования фразы является последовательность s_1, s_2, \dots , в которой s_i — буква, порядковый номер которой в алфавите равен остатку от деления на 33 суммы порядковых номеров в алфавите букв t_i и k_i .

Известно, что сообщение было зашифровано с использованием ключевого слова из пяти букв. Результатом зашифрования является последовательность

МХЛЩЛИФЦБДЮГИШСПТАИВПБЬДЮОЛДЬУЭЮЕМХЛ

Восстановите исходное сообщение и ключевое слово.

В задаче используется полный русский алфавит, который мы приводим вместе с порядковыми номерами его букв (начиная с нуля):

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

18.3. На космической станции, состоящей из отсеков (круглых комнат) и соединяющих их коридоров, произошёл сбой электроснабжения, в результате чего связь с роботом, работающим на станции, прервалась. После восстановления работы станции выяснилось, что движение по коридорам, половина из которых оказались неосвещёнными, возмож-

но только по направлениям, указанным на схеме, и занимает 1 минуту для каждого коридора. При этом неизвестно, в каком отсеке находится робот. Робот управляется командами из нулей и единиц, при этом 0 соответствует движению по освещённому коридору, а 1 — по неосвещённому. Передайте команду роботу, которая приведёт его из любой комнаты в лабораторию (где находится выход). С момента начала движения робота его энергоснабжения хватит не более чем на 5 минут.

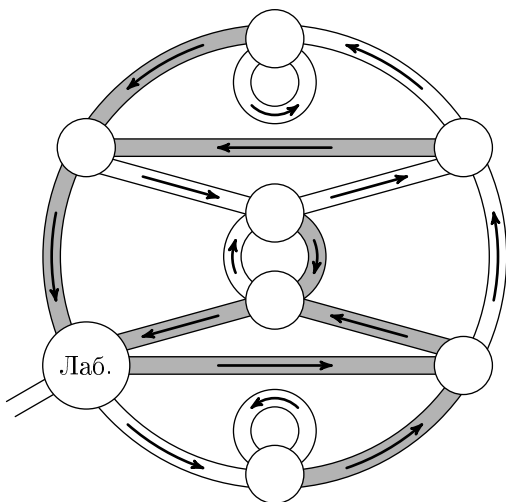


Рис. 11

18.4. В бесконечной последовательности цифр $2, 0, 0, 8, 0, 8, 6, \dots$ каждая цифра, начиная с пятой, равна последней цифре в десятичной записи суммы четырёх предыдущих цифр. Доказать, что в этой последовательности вновь встретятся подряд идущие цифры $2, 0, 0, 8$.

18.5. Для наблюдения за страной Криптоландией запущен разведывательный спутник. Страна Криптоландия имеет форму прямоугольника. При этом спутник находится на расстоянии 700 км от одной вершины прямоугольника, на расстоянии 330 км от противоположной вершины прямоугольника и на расстоянии 650 км от третьей вершины прямоугольника. Найти расстояние от спутника до четвертой вершины прямоугольника.

18.6. Число n представляется в виде произведения двух чисел $n = p \cdot q$. Найдите эти числа и приведите решение, если известно, что

а) $n = 40003200063$, а $|p - q| = 2$;

б) $n = 40000398401$, а p, q — простые и $|p - q| \leq 100$.

18.7. Делится ли число $2^{2^{2007}+3^{2008}-2009} - 1$ на 1155?

18.8. Для зашифрования сообщения на русском языке его записывают в одну строку без пробелов и знаков препинания. Заглавные буквы заменяются на строчные. В получившейся цепочке буквы нумеруются слева направо числами от 1 до L . Зашифрование происходит путём перестановки букв исходной цепочки по следующему правилу. Фиксируем два натуральных числа a и b . Буква с номером n в исходной цепочке должна в зашифрованной цепочке иметь номер, равный остатку от деления числа $a \cdot n + b$ на L (с одним исключением: если $a \cdot n + b$ нацело делится на L , то остаток полагается равным L). Например, если длина цепочки $L = 25$ и $a = 9$, $b = 11$, то третья буква исходной цепочки будет тринадцатой в зашифрованной цепочке (т. к. $9 \cdot 3 + 11 = 38$, а число 38 даёт остаток 13 при делении на 25). Известно, что в результате применения этого метода зашифрования к цепочке из 43 букв

св е т и т н е з н а к о м а я з в е з д а с н о в а м ы о т о р в а н ы о т д о м а

была получена цепочка

т а ы т о е о н с о о в з м е т р а д а з е д в а я н т о а ы с з а и м н о в к

При этих же значениях a , b проведено зашифрование ещё некоторой цепочки из 38 букв. Получилось вот что:

в и д и х в р л м а о я о а о д д с е м д р о и в в о е о з т о о б н з о

Найдите значения a и b и восстановите исходное сообщение.

18.9. На кодовом замке имеется круглый диск с риской. Вокруг диска нанесены числа от 0 до 99 по часовой стрелке. Для управления замком есть две кнопки: «вправо» и «влево». При нажатии на кнопку «вправо» диск вращается на 43 деления по часовой стрелке, при нажатии на кнопку «влево» — на 20 делений против часовой стрелки. Каждая из этих операций выполняется за 1 секунду. Изначально замок установлен на число 0. Замок открывается при его установке на число 50 — ключ замка.

а) За какое наименьшее время можно открыть замок при данном ключе 50?

б) Доказать, что замок можно открыть при любом ключе (ключ — число от 1 до 99).

в) За какое наименьшее время можно гарантированно открыть замок при любом ключе?

18.10. Решить уравнение при всех значениях параметра a

$$x^4 + 2x^3 - 4x^2 - 2(a+1)x - (a-3)(a+1) = 0.$$

18.11. При каких значениях параметра a уравнение

$$4(4a-1)x^2 + 2(4a+1)(x^2+1)x + (a+1)(x^2+1)^2 = 0$$

имеет ровно четыре различных решения?

XIX Олимпиада по криптографији и математици

19.1a. Подсчитайте, сколько всего существует натуральных чисел, которые не превосходят число 841 и не имеют с ним общих делителей, отличных от 1.

19.16. Известно, что число $N = 202718099$ является произведением двух простых чисел p и q , а количество натуральных чисел, меньших N и взаимно простых с N , равно 202687920. Найдите числа p и q .

19.2а. Для зашифрования фразы был взят кубик Рубика с нанесёнными на гранях русскими буквами. Развёртка кубика показана на рис. 12. Затем грани последовательно повернули по часовой стрелке на 90° определённое число раз: грань 1 — шесть раз; грань 2 — три раза; грань 3 — один раз; грань 4 — четыре; грань 5 — два и, наконец, грань 6 — пять раз. Затем каждая буква фразы находилась на грани кубика и заменялась буквой этой же грани, следующей за ней по часовой стрелке (например, на рис. 12 буква А переходит в букву Б, буква П в С). Буквы, находящиеся в центре грани, не заменяются.



Рис. 12

В результате получилась строка:

ОЕХДМАПРМКПДОПИМ.

Прочтите исходное сообщение.

19.26. Для зашифрования фразы был взят кубик Рубика с нанесёнными на гранях русскими буквами. Развёртка кубика показана на рис. 12. Три его грани повернули по часовой стрелке на 90° . При этом грань с меньшим номером поворачивалась раньше, чем грань с большим номером. Затем каждая буква фразы находилась на грани кубика и заменялась буквой этой же грани, следующей за ней по часовой стрелке (например, на рис. 12 буква А перейдёт в букву Б, буква П в С). Буквы, находящиеся в центре грани, не заменялись. Известно, что перед шифрованием запятая во фразе была заменена на ЗПТ, точка — на ТЧК, пробелы пропускались. В результате получилась строка:

ЕПОЕЪРИТСГХЖЗТЯПСТАПДСБИСТЧК.

Прочтите исходное сообщение.

19.3. Для передачи сообщения на русском языке Крокодил Гена и Чебурашка выполняют следующие действия. Каждый из них выбирает свою последовательность, состоящую из целых чисел в пределах от 0 до 32,

длина которой равна длине сообщения. Буквы сообщения заменяются числами по таблице.

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	0

Сначала Гена шифрует сообщение, используя свою последовательность. Для этого числовое значение первой буквы сообщения и первое число его последовательности складываются, а полученная сумма заменяется остатком от деления на 33 и вновь заменяется буквой по таблице. Затем эта процедура повторяется для вторых, третьих и т. д. чисел сообщения и последовательности. Полученный результат: ЁЛИСУВШОЮЦОМЮВЫЗПЭЪМО передаётся Чебурашке. После этого Чебурашка шифрует полученное сообщение с помощью своей последовательности. Получается строка ЪЭЛВШРЕЭТЖШОИГВФСЦХ. Эту строку он и передаёт Гене.

Гена вычитает из числовых значений букв полученного сообщения числа своей последовательности (к отрицательной разнице прибавляется число 33) и передаёт результат ЖЪХЙТСЖАШШЬЯМШЗЬВГ Чебурашке. Какое сообщение зашифровал Крокодил Гена?

19.4. Для доступа к общему почтовому ящику в Интернете Катя и Юра пользуются паролем СВЕЧА. Катя решает сменить этот пароль на новый (слово русского языка из пяти букв). Новый пароль передаётся по сети Юре в зашифрованном виде. Зашифрование осуществляется так. Первые буквы нового и старого пароля заменяются числами согласно таблице из задачи 19.3. Затем эти числа складываются, а полученная сумма заменяется остатком от деления на 33. Таким же образом поступают со вторыми буквами паролей, затем с третьими и т. д. После расшифрования Юра получил нечитаемый пароль из английских букв: SARCL. Оказалось, что программа расшифрования Юры была настроена на работу с английским алфавитом. При этом перед расшифрованием программа заменяла числовые значения поступившего зашифрованного пароля и старого пароля остатками от деления на 26, а расшифрование заключалось в нахождении их разностей (к отрицательной разнице прибавлялось число 26), которые приводились к буквенному виду согласно таблице

А	В	С	Д	Е	Ф	Г	Н	И	Ј	К	Л	М	Н	О	Р	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0

Помогите Юре понять, какой новый пароль установила Катя.

19.5. Торговые автоматы в Криптоландии принимают монетки номиналом только в 3 и 7 единиц. Укажите все цены, которые нельзя уста-

навливать на товары, продаваемые через автоматы подобного вида. Автоматы сдачу не дают.

19.6. Дан треугольник $\triangle ABC$, в котором $AB = 99$, $AC = 71$, $\angle BAC = 67^\circ$. Требуется только с помощью циркуля и линейки построить треугольник $\triangle DEF$ со сторонами $DE = 101$, $EF = 73$ и углом между ними $\angle DEF = 51^\circ$.

19.7. Четыре фразы на русском языке записываются без знаков препинания и пробелов. Для зашифрования каждой фразы используются неизвестные последовательности цифр x_1, x_2, \dots . Буквы во фразе последовательно заменяются на пары цифр согласно таблице из задачи 19.3 (к одноразрядным числам слева дописывается 0: например, А будет заменяться на 01). Зашифрование состоит в преобразовании получившейся строки цифр по следующему правилу. К первой цифре строки прибавляется цифра x_1 и записывается последняя цифра суммы, потом ко второй цифре строки прибавляется x_2 и также записывается последняя цифра суммы и т. д. Результат зашифрования выглядит следующим образом:

- 1) 0436389637110156289614062778022668915272874106897713780236,
- 2) 903913973306253415922423357601144271609271,
- 3) 17915094077497245567822036742365175971,
- 4) 37035325199253279170859097506579819015871949450238348350004529224.

Известно, что две фразы зашифрованы с помощью одной и той же последовательности. Укажите, какие именно (ответ обоснуйте).

19.8. Известно, что три числа a_1, a_2, a_3 были получены следующим образом. Сначала выбрали натуральное число A и нашли числа $A_1 = [A]_{16}$, $A_2 = [A/2]_{16}$, $A_3 = [A/4]_{16}$, где $[X]_{16}$ — остаток от деления целой части числа X на 16 (например, $[53/2]_{16} = 10$). Затем было выбрано целое число B такое, что $0 \leq B \leq 15$. Числа A_1, A_2, A_3 и B записали в двоичной системе счисления, т. е. представили каждое из них в виде строки из нулей и единиц длины 4, приписывая слева необходимое число нулей. Такие цепочки условимся складывать посимвольно «в столбик» без переносов в следующий разряд согласно правилу: $1 + 1 = 0 + 0 = 0$ и $0 + 1 = 1 + 0 = 1$, а саму операцию посимвольного сложения обозначим символом \oplus . Например, $3 \oplus 14 = (0, 0, 1, 1) \oplus (1, 1, 1, 0) = (1, 1, 0, 1) = 13$. Положим $a_1 = A_1 \oplus B$, $a_2 = A_2 \oplus B$, $a_3 = A_3 \oplus B$. Найдите все возможные значения числа a_3 , если известно, что $a_1 = 4$, $a_2 = 10$.

19.9. Для зашифрования сообщения на русском языке, записанного без знаков препинания и пробелов, используется последовательность натуральных чисел x_1, x_2, \dots , удовлетворяющая соотношению: $x_k = b \cdot 8^{a(k-1)}$, $k = 1, 2, \dots$. Здесь a и b — фиксированные (но неизвестные) натуральные числа. Зашифрование производится следующим образом.

Первая буква сообщения заменяется числом согласно таблице и складывается с x_1 . Потом также заменяется вторая буква и складывается с x_2 и т. д. Затем все суммы заменяются остатками от деления на 31, а остатки заменяются буквами согласно таблице.

А	Б	В	Г	Д	Е	Ё	Ж	З	И, Й	К	Л	М	Н	О	П
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь, Ы	Э	Ю	Я
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

В результате получился текст

ОЯФПРПЯФБКПЩСЬИЖЬИЯСЯЗТХЖУТНАЖБСЁНФВГМНУТУЁШЖФН

Найдите исходное сообщение, представляющее собой отрывок известного стихотворения, если известно, что в нём есть слово РАВНИНЫ.

19.10. Все 16 городов Криптоландии в качестве названий имеют различные четырёхразрядные комбинации, состоящие из нулей и единиц (например, «0011»). Все города попарно соединены непересекающимися дорогами, причём проезд из одного города в другой стоит столько криптов, в скольких разрядах различаются их имена (например, из «0011» в «1001» — 2 крипто). Путешественник, находящийся в «0000», хочет объехать все города страны и вернуться назад за минимальную цену. Как ему это сделать?

19.11а. Найдите число решений системы уравнений

$$\begin{cases} x + |y| = 1, \\ y + a|x| = 2 \end{cases}$$

при всех возможных значениях параметра a .

19.11б. Изобразите на плоскости Oxy множество всех точек с координатами $(x; y)$ таких, что $y \geq x^2 - 1$ и при любом значении параметра a выполняется неравенство $a^2y + 2ax - y - 2 \leq 0$. Ответ обоснуйте.

XX Олимпиада по криптографии и математике

20.1. В таблице приведена переписка двух абонентов (Godzilla и Фунтика) в чате.

Дата/время	Отправитель	Сообщение
10:11 28.11.2010	Godzilla	Привет. Как дела? Пришли пароль для почты.
10:14 28.11.2010	Фунтик	И усцрмс щюуьсэ ц Яспар-Джрюмгшмт пс вцю пювючж. Дсмьчз: Гшмтшпвжи.
10:21 28.11.2010	Godzilla	Когда доберёшься до Питера, позвони.

Фунтик отвечает Godzille и для конспирации каждую букву заменяет другой буквой (при этом разные буквы заменяются разными, а одинаковые — одинаковыми). Восстановите зашифрованное сообщение и пароль.

20.2. На клавиатуре мобильного телефона каждой кнопке сопоставлено по несколько букв: кнопке 2 соответствуют буквы ABC, 3 — DEF, 4 — GHI, 5 — JKL, 6 — MNO, 7 — PQRS, 8 — TUV, 9 — WXYZ. Выбор нужной буквы определяется числом нажатий на кнопку. Например, нажав на кнопку 4 один раз, получим букву G, а два нажатия на кнопку 4 дадут или букву H (если нажимать быстро) или две буквы G (если нажимать с паузой). Известно, что при наборе пароля из 10 букв были нажаты последовательно кнопки 777255899999. Определите число возможных вариантов паролей.

20.3. Для открытия подземелья в волшебной стране надо правильно назвать три целых числа a, b, c , служащих коэффициентами квадратичной функции $f(x) = ax^2 + bx + c$. Представителям четырёх рас были переданы следующие значения функции: троллям — значение $f(21)$, эльфам — $f(24)$, гномам — $f(25)$, оркам — $f(28)$. Когда представители рас встретились, чтобы совместно найти a, b, c и открыть подземелье, один из представителей, чтобы сорвать мероприятие, предъявил неверное значение. Выясните, кто это был, если известно, что тролли предъявили число 273, эльфы — 357, гномы — 391, орки — 497.

20.4. В концах диаметра окружности расположены числа 1 и 5, разбивающие окружность на две дуги. Совершим по окружности n оборотов по часовой стрелке, приняв за начало обхода один из концов диаметра. После прохождения каждой имеющейся на данный момент дуги делим её пополам и в середине записываем число $\frac{3x + 3y}{2}$, где x и y — числа, стоящие на концах пройденной дуги, взятые в порядке направления обхода. Найдите сумму всех записанных чисел после n оборотов.

20.5. Для зашифрования натурального числа m используется граф, представляющий собой множество вершин, некоторые из которых соединены друг с другом прямой линией. Вершины графа, соединённые друг с другом, называют *соседними*. Зашифрование состоит в выполнении следующих действий. В вершины графа записываются натуральные числа так, чтобы их сумма была равна m . Затем к числу в каждой вершине прибавляются числа в соседних вершинах. В результате получается граф, в котором «зашифровано» число m . Пример: для зашифрования числа 8 будем использовать граф на рис. 13. В его вершины поместим числа, сумма которых равна 8 (рис. 14). Затем к каждому числу прибавим числа в соседних вершинах. Результат зашифрования

указан на рис. 15. На рис. 16 приведён результат зашифрования некоторого числа. Найдите его.

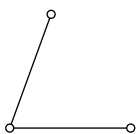


Рис. 13

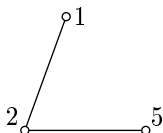


Рис. 14

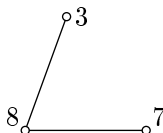


Рис. 15

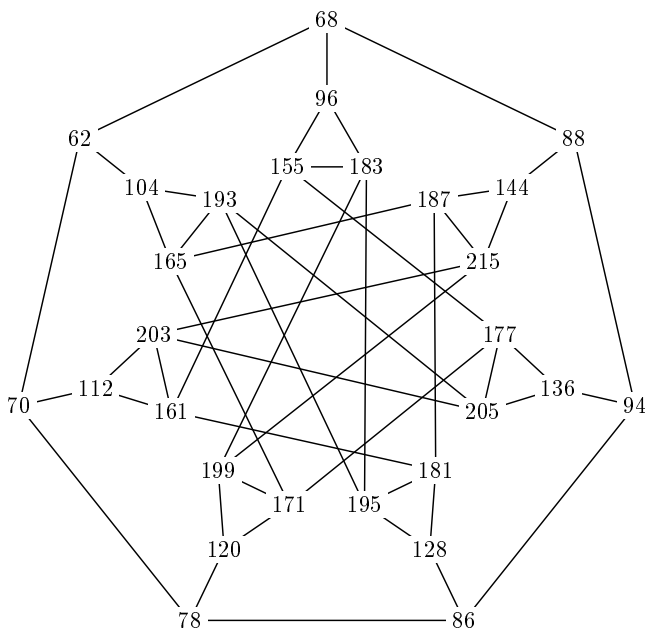


Рис. 16

20.6. Для прохода в учреждение необходимо предъявить пятизначную комбинацию, состоящую из нулей и единиц. Устройство распознавания представляет собой упрощённую модель нейрона — клетки головного мозга (см. рис. 17).

Пятизначная комбинация x_1, x_2, x_3, x_4, x_5 по пяти каналам поступает в клетку, где её компоненты умножаются на фиксированные целые числа a_1, a_2, a_3, a_4, a_5 и вычисляется сумма $S = a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 + a_5x_5$. Проход в учреждение открывается, только если $S \geq c$, где c — некоторое фиксированное целое число. В верхней таблице представлены те комбинации, при предъявлении которых проход открывается,

а в нижней таблице — для которых проход закрыт:

1, 0, 1, 1, 0	1, 1, 0, 1, 0	1, 1, 1, 1, 1	
1, 0, 1, 0, 0	0, 0, 1, 1, 0	1, 1, 0, 1, 1	1, 0, 1, 1, 1

Найдите ещё одну комбинацию, открывающую проход в учреждение.

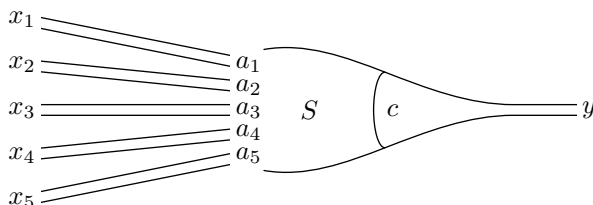


Рис. 17

20.7. В нейрокомпьютере используется упрощённая модель нейрона — клетки головного мозга (см. рис. 18). По четырём каналам x_1, x_2, x_3, x_4 в клетку поступают нули и единицы, из которых внутри неё формируется сумма $S = a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4$ (a_1, a_2, a_3, a_4 — целые). Затем S сравнивается с некоторым целым параметром c , и если $S \geq c$, то на выходе клетки формируется значение $y = 1$, иначе — $y = 0$. Найдите какие-либо целые параметры a_1, a_2, a_3, a_4, c такого нейрона, чтобы $y = 1$ на наборах $(1, 0, 1, 0)$, $(1, 1, 1, 0)$, $(0, 0, 1, 0)$, $(1, 0, 0, 1)$, $(1, 0, 1, 1)$, $(0, 0, 1, 1)$, $(1, 1, 1, 1)$ и $y = 0$ — на остальных наборах.

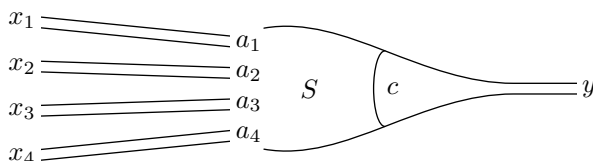


Рис. 18

20.8. В текстовом сообщении на русском языке, записанном без знаков препинания и пробелов, переставили буквы:

НКБАКМОРОЛААЕНТОИЕИБ.

Затем первую букву заменили буквой, следующей за ней через некоторое число позиций в алфавите, расположенном по кругу (см. рис. 19).



Рис. 19

Вторую букву заменили буквой, которая следует за ней через другое число позиций в алфавите, и так далее. При этом одинаковые буквы могут перейти в разные, а разные — в одинаковые. После этого получили:

ИКЛМНОИКЛМНОИКЛМНОСТ.

И, наконец, буквы в этой строке выстроили в исходном порядке:

ИКООКМТИСОНИЛНЛКМЛМН

(то есть если, например, первую букву исходного сообщения поставили на третье место, то теперь третью букву поставили на первое). Восстановите исходное сообщение.

20.9. Известно, что число 14197777 равно остатку от деления на 56887111 некоторого числа x , возведённого в куб. Числа x и 56887111 имеют общий делитель, отличный от 1, а число 56887111 является произведением двух простых чисел. Найдите хотя бы одно такое число x .

20.10. Крокодил Гена и Чебурашка могут связываться по двум каналам: радиоканалу и оптическому каналу. Используя эти каналы, они хотят договориться о кодовой комбинации сейфа, составленной из 20 букв К, З, С или Ч. Для этого Гена по оптическому каналу передаёт случайную комбинацию из 20 вспышек, причём каждая вспышка может быть красного (К), синего (С) или зелёного (З) цвета. Для каждой вспышки Чебурашка наугад выбирает светофильтр. Если его цвет совпадает с переданным цветом, то срабатывает датчик, а если не совпадает, то цвет вспышки остаётся для Чебурашки неизвестным. После замера всех вспышек Чебурашка по радиоканалу сообщает, какие светофильтры он выбрал. В результате Гена узнаёт номера вспышек, цвет которых Чебурашка определил. Гена устанавливает комбинацию на сейфе так: если цвет очередной вспышки Чебурашке определить удалось, то выбирается буква, соответствующая цвету вспышки (К, З либо С), если нет — выбирается Ч.

Шапокляк «встроилась» в оптический канал и прослушивает радиоканал. На пути передаваемых вспышек она выставляла свои светофильтры: ККЗЗЗСКСКСЗЗСКСКСКЗК и одновременно передавала вспышки тех же самых цветов Чебурашке. Срабатывание датчика у неё произошло на 6, 10, 11, 14, 17 и 19 вспышках. Чебурашка, не зная о вмешательстве, сообщил по радиоканалу свои цвета: СКЗККККЗЗККССККЗСЗСК. С учётом собранной Шапокляк информации определите число кодовых комбинаций, которые гарантированно не откроют сейф.

7. Указания и решения

1.1. Все клетки квадрата размера $n \times n$ разобьём на непересекающиеся группы по четыре клетки в каждой. Отнесём клетки к одной и той же группе, если при каждом повороте квадрата до его самосовмещения они перемещаются на места клеток этой же группы. На рисунке показано такое разбиение на группы всех клеток квадрата 6×6 , причём клетки одной группы помечены одной и той же цифрой. Всего таких групп будет $n^2/4$ (целое, так как n — чётное число). При наложении трафарета на квадрат ровно одна клетка из каждой группы окажется под его вырезами. Каждому трафарету поставим в соответствие упорядоченный набор всех клеток из таких групп, оказавшихся под вырезами трафарета при наложении его на квадрат помеченной стороной вверх. Такое соответствие является взаимнооднозначным, поскольку каждому ключу будет однозначно соответствовать упорядоченный набор из $n^2/4$ клеток (по одной из каждой группы), вырезанных в трафарете, и наоборот. Всего таких наборов $4^{n^2/4}$. В самом деле, существует ровно четыре различных варианта выбора клетки из каждой группы независимо от выбранных клеток из других таких групп. Таким образом, число различных ключей шифра «поворотная решётка» при чётных значениях n равно $4^{n^2/4}$.

1	2	3	4	5	1
5	6	7	8	6	2
4	8	9	9	7	3
3	7	9	9	8	4
2	6	8	7	6	5
1	5	4	3	2	1

1.2. Легко видеть, что $f(x) = (x^2 + 3x + 1)(x^4 + x + 1) + 2$. Отсюда $f(x_1) = f(x_2) = 2$, где x_1, x_2 — корни многочлена $x^2 + 3x + 1$. Получаем

Буква ш. с.	Ф	В	М	Е	Ж	Т	И	В	Ф	Ю
Номер	22	3	14	7	8	20	10	3	22	32

Номер	20	1	12	5	6	18	8	1	20	30
Буква о. с.	Т	А	К	Д	Е	Р	Ж	А	Т	Ь

Ответ: ТАКДЕРЖАТЬ

1.3. Ответ: начиная с 54.

1.4. Разложим числа m и d на простые множители: $d = 6 = 2 \cdot 3$; $m = 6930 = 2 \cdot 3 \cdot 3 \cdot 5 \cdot 7 \cdot 11$. Обозначим буквой t число m/d , равное произведению $3 \cdot 5 \cdot 7 \cdot 11$. Найдём все его делители q вида: $q = 3^x 5^y 7^z 11^u$, где числа x, y, z и u принимают только значения 0 и 1. Тогда, как нетрудно видеть, числа q и t/q окажутся взаимно простыми. Полагая $a = dq$ и $b = dt/q$, получим все искомые пары (a, b) . В самом деле, в указанных выше условиях наибольший общий делитель такой пары равен d , а её наименьшее общее кратное равно $dqt/q = dt = dm/d = m$. Таким

образом, искомое число упорядоченных пар совпадает с числом всех делителей q вида: $3^x 5^y 7^z 11^u$, которое равно числу всех упорядоченных наборов длины 4 и состоящих только из 0 и 1. Число всех таких наборов равно $2^4 = 16$, так как для каждого места в наборах существует ровно 2 варианта его значений независимо от значений на других местах. В общем случае число m/d представляется в виде $m/d = p^i r^j \dots s^h$, где p, r, \dots, s — различные простые числа, а i, j, \dots, h — натуральные числа. Число всех делителей вида: $q = p^x r^y \dots s^z$, где числа x, y, \dots, z принимают только по два значения (0 и соответствующий натуральный показатель степени в представлении числа m/d), равно 2^k , где k — число всех простых делителей числа m/d . Если число различных простых множителей в каноническом разложении числа m/d равно k , то число различных упорядоченных пар (a, b) равно 2^k .

Ответ: 16 пар (пары (a, b) и (b, a) разные). В общем случае число упорядоченных пар равно 2^k , где k — число всех простых делителей m/d .

1.5. Из последней строчки легко заметить, что $\text{Ш}=0$. Тогда из первого столбца находим, что $\text{И}=1$. Затем из последнего столбца находим $\text{Ф}=2$. Итак,

$$\begin{array}{rclcl} 2\text{Н} & \times & \text{Ы} & = & 2\text{А}2 \\ + & & \times & & - \\ \text{ЕЕ} & + & \text{Е} & = & \text{НЗ} \\ = & & = & & = \\ 10\text{А} & + & \text{МР} & = & 1\text{МН} \end{array}$$

Из средней строки ясно, что $\text{Н} > \text{Е}$. Из первого столбца находим $\text{Е}=7$. Из средней строки можно вычислить значения Н и З : $\text{Н}=8$ и $\text{З}=4$. Получим

$$\begin{array}{rclcl} 28 & \times & \text{Ы} & = & 2\text{А}2 \\ + & & \times & & - \\ 77 & + & 7 & = & 84 \\ = & & = & & = \\ 10\text{А} & + & \text{МР} & = & 1\text{М}8 \end{array}$$

Далее, последовательно вычисляем значения: $\text{А}=5$, $\text{Ы}=9$, $\text{М}=6$, $\text{Р}=3$. Расставим буквы в порядке возрастания их цифровых значений и получим текст **ШИФРЗАМЕНЫ**

Ответ: ШИФРЗАМЕНЫ

1.6. Обозначим $\overline{\varphi(P)}$ — набор $\varphi(P)$, выписанный в обратном порядке.

$$\begin{aligned} \varphi(\text{cbcacbc}) &= \overline{\varphi(\text{bcacbc})} = \overline{\varphi(\text{cacbc})a\varphi(\text{cacbc})} = \\ &= \overline{\varphi(\text{acbc})a\varphi(\text{acbc})} = \overline{\text{cbcacbc}} = \text{cbcacbc} = \text{cbcacbc}. \end{aligned}$$

Ответ: например, cbcacbc .

В общем случае можно показать, что множество искомых наборов состоит из слов вида:

$$P = \begin{cases} \underbrace{cb \underbrace{c \dots c}_{k \text{ раз}} acb \underbrace{c \dots c}_{k \text{ раз}}} & k \text{ — нечётное;} \\ \underbrace{b \underbrace{c \dots c}_{k \text{ раз}} ab \underbrace{c \dots c}_{k \text{ раз}}} & k \text{ — чётное.} \end{cases}$$

2.1. Рассмотрим один виток ленты на развёртке цилиндра (разрез по горизонтальной линии). По условию высота CE , опущенная на сторону AD , равна d . Угол DAC равен $(90 - \alpha)^\circ$. Отсюда AC равно $d / \cos \alpha$. Так как высота строки равна h , то всего на одном витке $n = d / (h \cdot \cos \alpha)$ букв.

Ответ: чтобы прочитать текст, надо разрезать ленту на участки по $n = d / (h \cdot \cos \alpha)$ букв и сложить их рядом.

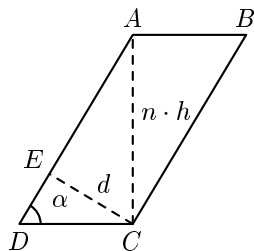


Рис. 20

2.2. Согласно условию, исходное сообщение состоит из двух пятёрок цифр: $A_1 A_2 A_3 A_4 A_5$ и $B_1 B_2 B_3 B_4 B_5$. Пусть $C_1 C_2$ — последние две цифры суммы чисел, изображённых этими пятёрками. Через $a \oplus b$ обозначим последнюю цифру суммы чисел a и b . Пусть D обозначает цифру переноса (цифру десятков) суммы $(A_5 + B_5)$. По условию имеем, что $A_5 \oplus B_5 = C_2$ и $(A_4 \oplus B_4) \oplus D = C_1$.

Пусть Γ_1 — первый член, а X — разность арифметической прогрессии, которую коммерсант использовал при шифровании. Тогда из условия получаем:

$$A_1 \oplus \Gamma_1 = 4, \quad (1)$$

$$A_2 \oplus (\Gamma_1 + X) = 2, \quad (2)$$

$$A_3 \oplus (\Gamma_1 + 2X) = 3, \quad (3)$$

$$A_4 \oplus (\Gamma_1 + 3X) = 4, \quad (4)$$

$$A_5 \oplus (\Gamma_1 + 4X) = 6, \quad (5)$$

$$B_1 \oplus (\Gamma_1 + 5X) = 1, \quad (6)$$

$$B_2 \oplus (\Gamma_1 + 6X) = 4, \quad (7)$$

$$B_3 \oplus (\Gamma_1 + 7X) = 0, \quad (8)$$

$$B_4 \oplus (\Gamma_1 + 8X) = 5, \quad (9)$$

$$B_5 \oplus (\Gamma_1 + 9X) = 3, \quad (10)$$

$$((A_4 \oplus B_4) \oplus D) \oplus (\Gamma_1 + 10X) = 1, \quad (11)$$

$$(A_5 \oplus B_5) \oplus (\Gamma_1 + 11X) = 3. \quad (12)$$

Обозначим символом $A \equiv B$ равенство остатков от деления на 10 чисел A и B . Тогда записи $A \oplus B = C$ и $(A + B) \equiv C$ имеют одинаковый

смысл. Если $A \equiv B$ и $C \equiv D$, то $A + B \equiv C + D$, $A - B \equiv C - D$. Всегда $A \equiv A$, так как остаток от деления единствен.

Из соотношений (4), (5), (9) и (10) находим соответственно:

$$A_4 \equiv 4 - (\Gamma_1 + 3X), \quad (13)$$

$$A_5 \equiv 6 - (\Gamma_1 + 4X), \quad (14)$$

$$B_4 \equiv 5 - (\Gamma_1 + 8X), \quad (15)$$

$$B_5 \equiv 3 - (\Gamma_1 + 9X). \quad (16)$$

Подставляя эти значения в равенства (11) и (12), получим следующие равенства: $9 + D - \Gamma - X \equiv 1$ и $9 - \Gamma - 2X \equiv 3$. Отсюда следует, что

$$X \equiv (-2 - D), \quad (17)$$

$$\Gamma_1 \equiv 2D. \quad (18)$$

Подставив X из (17) и Γ_1 из (18) в (1), (2), (3), (13), (14), (6), (7), (8), (15), (16), найдём выражения для цифр исходного сообщения:

$$A_1 \equiv 4 - 2D, A_2 \equiv 4 - D, A_3 \equiv 7, A_4 \equiv D, A_5 \equiv 4 + 2D,$$

$$B_1 \equiv 1 + 3D, B_2 \equiv 6 + 4D, B_3 \equiv 4 + 5D, B_4 \equiv 1 + 6D,$$

$$B_5 \equiv 1 + 7D.$$

Найденные выражения дают два варианта исходных сообщений:

$$4470416411 \text{ (при } D = 0),$$

$$2371640978 \text{ (при } D = 1).$$

2.3. Указание. Обозначим через $f(x)$ — остаток от деления значения многочлена $F(x)$ на 10. Для однозначного расшифрования необходимо и достаточно, чтобы разным значениям x соответствовали разные значения $f(x)$. Поэтому $f(0), f(1), \dots, f(9)$ принимают все значения от 0 до 9. Найдём эти значения:

$$f(0) = r_{10}(b(a + 0)) \quad f(1) = r_{10}(b(a + 1))$$

$$f(2) = r_{10}(b(a + 2)) \quad f(3) = r_{10}(b(a + 9))$$

$$f(4) = r_{10}(b(a + 8)) \quad f(5) = r_{10}(b(a + 5))$$

$$f(6) = r_{10}(b(a + 6)) \quad f(7) = r_{10}(b(a + 7))$$

$$f(8) = r_{10}(b(a + 4)) \quad f(9) = r_{10}(b(a + 3)),$$

где $r_{10}(y)$ — остаток от деления числа y на 10.

Отсюда, пользуясь свойствами остатков, замечаем, что b должно быть нечётным (иначе $f(x)$ будут только чётные числа) и b не должно делиться на 5 (иначе $f(x)$ будут только 0 и 5). Непосредственной проверкой можно убедиться, что при любом a и при всех b , удовлетворяющим приведённым условиям, гарантируется однозначность расшифрования.

Ответ: a — любое, b — не должно делиться на 2 и на 5.

2.4. Обозначим через $S(n)$ остаток от деления на 26 суммы чисел, которые соответствуют первым n буквам алфавита ($n = 1, 2, \dots, 26$) $0 \leq S(n) \leq 25$.

Если среди чисел $S(1), S(2), \dots, S(26)$ есть нуль: $S(t) = 0$, то искомой ключевой комбинацией является цепочка первых t букв алфавита.

Если среди чисел $S(1), S(2), \dots, S(26)$ нет нуля, то обязательно найдутся два одинаковых числа: $S(k) = S(m)$ (считаем, что $k < m$). Тогда искомой ключевой комбинацией является участок алфавита, начинающийся с $(k + 1)$ -й и заканчивающийся m -й буквой.

2.5. Если две буквы с порядковыми номерами T_1 и T_2 зашифрованы в буквы с порядковыми номерами C_1 и C_2 с помощью одной и той же буквы, то остатки от деления чисел $(C_1 - T_1)$ и $(C_2 - T_2)$ на 30 равны между собой и совпадают с порядковым номером шифрующей буквы (порядковым номером буквы $Я$ удобно считать число 0). Тогда, с учётом соглашения о порядковом номере буквы $Я$, справедливо, что T_1 равен остатку от деления числа $(T_2 + (C_1 - C_2))$ на 30, а, вместе с тем, T_2 равен остатку от деления числа $(T_1 + (C_2 - C_1))$ на 30. Если каждое из выражений в скобках заменить соответствующим остатком от деления на 30, то упомянутая связь не нарушится.

Представим в виде набора порядковых номеров известные шифрованные сообщения (обозначим их соответственно ш. с. 1 и ш. с. 2) и слово КОРАБЛИ:

слово	К	О	Р	А	Б	Л	И
T	10	14	16	1	2	11	9

ш. с. 1	Ю	П	Т	Ц	А	Р	Г	Ш	А	Л	Ж	Ж	Е	В	Ц	Щ	Ы	Р	В	У	У
C_1	29	15	18	22	1	16	4	24	1	11	7	7	6	3	22	25	27	16	3	19	19

ш. с. 2	Ю	П	Я	Т	Б	Н	Щ	М	С	Д	Т	Л	Ж	Г	П	С	Г	Х	С	Ц	Ц
C_2	29	15	0	18	2	13	25	12	17	5	18	11	7	4	15	17	4	21	17	22	22

Возможны 15 вариантов (номер варианта обозначим буквой k) расположения слова КОРАБЛИ в каждом из двух исходных сообщений (и. с. 1, и. с. 2).

Вначале для каждого из 15 вариантов расположения слова КОРАБЛИ в и. с. 1 найдём соответствующий участок и. с. 2. Имеем:

$C_2 - C_1$	0	0	12	26	1	27	21	18	16	24	11	4	1	1	23	22	7	5	14	3	3
-------------	---	---	----	----	---	----	----	----	----	----	----	---	---	---	----	----	---	---	----	---	---

T_1	10	14	16	1	2	11	9
T_2	T_{21}	T_{22}	T_{23}	T_{24}	T_{25}	T_{26}	T_{27}

Поэтому для участка и. с. 2 получаем следующие 15 вариантов:

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
T_{21}	10	10	22	6	11	7	1	28	26	4	21	14	11	11	3
T_{22}	14	26	10	15	11	5	2	0	8	25	18	15	15	7	6
T_{23}	28	12	17	13	7	4	2	10	27	20	17	17	9	8	23
T_{24}	27	2	28	22	19	17	25	12	5	2	2	24	23	8	6
T_{25}	3	29	23	20	18	26	13	6	3	3	25	24	9	7	16
T_{26}	28	2	29	27	5	22	15	12	12	4	3	18	16	25	14
T_{27}	0	27	25	3	20	13	10	10	2	1	16	14	23	12	12

Теперь для каждого из 15 вариантов расположения слова КОРАБЛИ в и. с. 2 найдём соответствующий участок и. с. 1. Имеем:

$C_1 - C_2$	0	0	18	4	29	3	9	12	14	6	19	26	29	29	7	8	23	25	16	27	27
-------------	---	---	----	---	----	---	---	----	----	---	----	----	----	----	---	---	----	----	----	----	----

T_2	10	14	16	1	2	11	9
T_1	T_{11}	T_{12}	T_{13}	T_{14}	T_{15}	T_{16}	T_{17}

Поэтому для участка и. с. 1 получаем следующие 15 вариантов:

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
T_{11}	10	10	28	14	9	13	19	22	24	16	29	6	9	9	17
T_{12}	14	2	18	13	17	23	26	28	20	3	10	13	13	21	22
T_{13}	4	20	15	19	25	28	0	22	5	12	15	15	23	24	9
T_{14}	5	0	4	10	13	15	7	20	27	0	0	8	9	24	26
T_{15}	1	5	11	14	16	8	21	28	1	1	9	10	25	27	18
T_{16}	14	20	23	25	17	0	7	10	10	18	19	4	6	27	8
T_{17}	18	21	23	15	28	5	8	8	16	17	2	4	25	6	6

Заменим порядковые номера в найденных вариантах участков и. с. 1 и и. с. 2 на буквы русского алфавита. Получаем следующие таблицы:

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
участок и. с. 2	К	К	Ц	Е	Л	Ж	А	Э	Ь	Г	Х	О	Л	Л	В
	О	Ь	К	П	Л	Д	Б	Я	З	Щ	Т	П	П	Ж	Е
	Э	М	С	Н	Ж	Г	Б	К	Ы	Ф	С	С	И	З	Ч
	Ы	Б	Э	Ц	У	С	Щ	М	Д	Б	Б	Ш	Ч	З	Е
	В	Ю	Ч	Ф	Т	Ь	Н	Е	В	В	Щ	Ш	И	Ж	Р
	Э	Б	Ю	Ы	Д	Ц	П	М	М	Г	В	Т	Р	Щ	О
	Я	Ы	Щ	В	Ф	Н	К	К	Б	А	Р	О	Ч	М	М

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
участок и.с.1	К	К	Э	О	И	Н	У	Ц	Ш	Р	Ю	Е	И	И	С
	О	Б	Т	Н	С	Ч	Ь	Э	Ф	В	К	Н	Н	Х	Ц
	Г	Ф	П	У	Щ	Э	Я	Ц	Д	М	П	П	Ч	Ш	И
	Д	Я	Г	К	Н	П	Ж	Ф	Ы	Я	Я	З	И	Ш	Ь
	А	Д	Л	О	Р	З	Х	Э	А	А	И	К	Щ	Ы	Т
	О	Ф	Ч	Щ	С	Я	Ж	К	К	Т	У	Г	Е	Ы	З
	Т	Х	Ч	П	Э	Д	З	З	Р	С	Б	Г	Щ	Е	Е

Из таблиц видно, что осмысленными являются варианты:

и.с.1 = К О Г Д А О Т К О Р А Б Л И

и.с.2 = К О Р А Б Л И В Е Ч Е Р О М

Естественно предположить, что в первом исходном сообщении речь идёт об отплытии кораблей. Предположив, что неизвестным участком первого исходного сообщения является подходящая по смыслу часть слова ОТПЛЫВАЮТ, находим неизвестную часть второго исходного сообщения: слово ОТХОДЯТ.

2.6. Каждую букву шифрованного сообщения расшифруем в трёх вариантах, предполагая последовательно, что соответствующая буква шифрующей последовательности есть буква А, Б или буква В:

шифрованное сообщение	Р	Б	Ь	Н	П	Т	С	И	Т	С	Р	Р	Е	З	О	Х
вариант А	П	А	Щ	М	О	С	Р	З	С	Р	П	П	Д	Ж	Н	Ф
вариант Б	О	Я	Ш	Л	Н	Р	П	Ж	Р	П	О	О	Г	Е	М	У
вариант В	Н	Ю	Ч	К	М	П	О	Е	П	О	Н	Н	В	Д	Л	Т

Выбирая из каждой колонки полученной таблицы ровно по одной букве, находим осмысленное сообщение НАШКОРРЕСПОНДЕНТ, которое и является искомым.

Замечание. Из полученной таблицы можно было найти такое исходное сообщение как

НАШ МОРОЗ ПОПОВ ЕМУ

которое представляется не менее осмысленным, чем приведённое выше. А если предположить одно искажение в шифрованном сообщении (скажем, в качестве 11-й буквы была бы принята не буква Р, а буква П), то, наряду с правильным вариантом, можно получить и такой:

НАШ МОРОЗ ПОМОГ ЕМУ

Число всех различных вариантов исходных сообщений без ограничений на осмысленность равно 3^{16} или 43046721, т. е. более 40 миллионов!

3.1. Если каждый из 993 абонентов связан с 99 абонентами, то для этого потребуется $993 \cdot 99/2$ линий связи, которое не может быть целым числом.

Ответ: нельзя.

3.2. Несложно заметить, что рассматриваемый шифр обладает тем свойством, что при зашифровании разные буквы заменяются разными. Следовательно, при зашифровании разных слов получаются разные слова. С другой стороны, одинаковые буквы заменяются на одинаковые независимо от цикла шифрования, так как используется один и тот же ключ. Следовательно, при зашифровании одинаковых слов получаются одинаковые слова. Таким образом, число различных слов, которые можно получить в указанном процессе шифрования с начальным словом СРОЧНО, совпадает с наименьшим номером цикла шифрования, дающем это начальное слово.

Так как буква С повторяется в каждом цикле шифрования, номер которого кратен 5, а буквы Р, О, Ч, Н — в каждом цикле, номера которых кратны 13, 7, 2 и 3 соответственно, то слово СРОЧНО появится впервые в цикле с номером, равным $\text{НОК}(2, 3, 5, 7, 13) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 = 2730$.

Ответ: 2730.

3.3. Если символы одного отрезка занумеровать последовательно числами от 1 до 12, то после передачи его из А в Б символы расположатся в порядке (2,4,6,8,10,12,1,3,5,7,9,11), а после передачи этого отрезка (замена символов не меняет порядка) из Б в В — в порядке (4,8,12,3,7,11,2,6,10,1,5,9). Переставим символы перехваченных отрезков в соответствии с их номерами до передачи из пункта А. Получим отрезки вида:

Л	П	Г	С	Ж	Н	Ж	О	О	Б	Т	-
Е	С	К	Р	У	П	Д	С	Б	Х	К	Т
Ю	У	П	-	О	Б	Ф	Е	Б	-	П	-
Л	Ж	Е	С	Ж	У	О	П	Л	У	К	-
Щ	К	Х	С	П	Г	Б	М	Ы	О	Э	Ц
Л	К	Л	У	Ж	Н	-	Л	Г	Т	И	К

Поскольку в пунктах А и Б одинаковые буквы заменялись одинаковыми, а разные — разными, то найденные отрезки можно рассматривать как замену одинаковых символов исходного текста одинаковыми, а разных — разными. Сравнивая места одинаковых букв слова КРИПТОГРАФИЯ и места одинаковых символов в отрезках, находим, что слово КРИПТОГРАФИЯ зашифровано во втором отрезке. Это даёт возмож-

ность найти исходное сообщение, используя гипотезы о частых буквах русского языка и смысле исходного сообщения.

Ответ:

С	О	В	Р	Е	М	Е	Н	Н	А	Я	-
К	Р	И	П	Т	О	Г	Р	А	Ф	И	Я
Э	Т	О	-	Н	А	У	К	А	-	О	-
С	Е	К	Р	Е	Т	Н	О	С	Т	И	-
Ш	И	Ф	Р	О	В	А	Л	Ь	Н	Ы	Х
С	И	С	Т	Е	М	-	С	В	Я	З	И

3.4. Докажем, что 20 является периодом рассматриваемой последовательности. Заметим, что у двух натуральных чисел a и b совпадают цифры единиц тогда и только тогда, когда их разность делится на 10. Таким образом, мы достигнем цели, если докажем, что разность $(n + 20)^{n+20} - n^n$ делится на 10 для всех натуральных значений n . Исходя из того, что $p^k - q^k$ делится на $(p - q)$, получаем, что $(n + 20)^{n+20} - n^{n+20}$ делится на $((n + 20) - n) = 20$. Кроме того, $n^{n+20} - n^n = n^n(n^{20} - 1) = n^n((n^4)^5 - 1)$ делится на $n(n^4 - 1)$ для всех $n > 1$. Вместе с тем,

$$\begin{aligned} n(n^4 - 1) &= n(n - 1)(n + 1)(n^2 + 1) = n(n - 1)((n + 2)(n - 2) + 5) = \\ &= (n - 2)(n - 1)n(n + 1)(n + 2) + 5(n - 1)n(n + 1), \end{aligned}$$

где каждое из слагаемых делится на 2 (так как содержит произведение $n(n + 1)$) и делится на 5 (поскольку первое слагаемое есть произведение пяти последовательных чисел, а второе содержит множитель 5). Следовательно, $n^{n+20} - n^n$ делится на 10. Число

$$(n + 20)^{n+20} - n^n = ((n + 20)^{n+20} - n^{n+20}) + (n^{n+20} - n^n)$$

делится на 10, так как каждое из слагаемых делится на 10.

Проверим, что 20 является наименьшим периодом. Выписывая первые 20 значений последовательности C_1, C_2, \dots

1 4 7 6 5 3 6 9 0 1 6 3 6 5 6 7 4 9 0

легко убедиться, что она не имеет периода меньшей длины.

3.5. Для того, чтобы найти исходное сообщение, найдём сначала цифровое сообщение, полученное из него с помощью таблицы замены. Согласно этой таблице на нечётных местах цифрового образа исходного сообщения могут быть только цифры 0, 1, 2 и 3. Последовательно рассматривая эти значения для каждого нечётного места цифрового сообщения с использованием соответствующей цифры шифрованного сообщения, найдём соответствующие варианты значений цифр шифрующего отрезка. Для этого вычислим остатки от деления разностей цифр

шифрованного и варианта цифрового сообщений:

порядковый номер места k	1	3	5	7	9	11	13	15	17	19	21	23	25	27
шифрованное сообщение S_k	2	3	8	7	1	4	8	6	6	0	1	3	5	8
вариант 0 для Γ_k	2	3	8	7	1	4	8	6	6	0	1	3	5	8
вариант 1 для Γ_k	1	2	7	6	0	3	7	5	5	9	0	2	4	7
вариант 2 для Γ_k	0	1	6	5	9	2	6	4	4	8	9	1	3	6
вариант 3 для Γ_k	9	0	5	4	8	1	5	3	3	7	8	0	2	5

По задаче 3.4 последовательность, из которой выбран шифрующий отрезок, является периодической с периодом 20. Из таблицы вариантов значений цифр шифрующего отрезка видим, что 5-я его цифра может быть равна 5, 6, 7 или 8, а его 25-я цифра — 2, 3, 4 или 5. Отсюда получаем, что $\Gamma_5 = \Gamma_{25} = 5$. На периоде последовательности, из которой выбран шифрующий отрезок, есть две цифры 5: C_5 и C_{15} . Поэтому рассмотрим два случая. Если $\Gamma_5 = C_5$, то $\Gamma_7 = C_7 = 3$. Это противоречит таблице вариантов значений цифр шифрующего отрезка, в которой Γ_7 может быть равна 4, 5, 6 или 7. Если же $\Gamma_5 = C_{15}$, то соответствующий шифрующий отрезок: 1636567490147656369016365674 хорошо согласуется с таблицей вариантов значений его цифр. Вычитая цифры найденного отрезка из соответствующих цифр шифрованного сообщения и заменяя разности их остатками от деления на 10, получим по таблице замены пар цифр на буквы исходное сообщение:

шифрованное сообщение	23	39	86	72	16	45	81	60	67	06	17	31	55	88
шифрующий отрезок	16	36	56	74	90	14	76	56	36	90	16	36	56	74
цифровое сообщение	17	03	30	08	26	31	15	14	31	16	01	05	09	14
исходное сообщение	С	В	Я	З	Ь	–	П	О	–	Р	А	Д	И	О

3.6. Обозначения понятны из рис. 21.

- 1) MK_1P_1B центрально симметричен $MKPA$ относительно M .
- 2) NL_1Q_1B центрально симметричен $NLQC$ относительно N .
- 3) $P_1K_2Q_1 = PKQ$ (параллельный перенос).
- 4) $LK_1K_2L_1$ — квадрат.
- 5) $MT \perp AC$, $NS \perp AC$.
- 6) $PMT = QNS$ ($MT = NS$, $PM = QN$, $\angle T = \angle S = 90^\circ$).
- 7) Без ограничения общности $AB = BC = CA = 1$.
- 8) $PT = QS = x$, $AP = \frac{1}{4} \mp x$, $PQ = \frac{1}{2}$, $QC = \frac{1}{4} \pm x$.

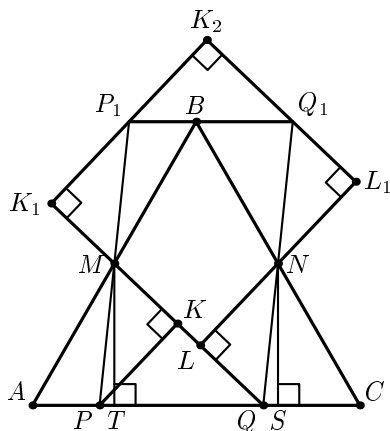


Рис. 21

9) $PMK = NQL$ ($PM=QN$, $\angle M=\angle Q$, $\angle K=\angle L=90^\circ$) $\Rightarrow MK = QL$.

10) $MQ = ML + LQ = ML + MK = ML + K_1M = K_1L = y$.

11) Площадь $ABC = \frac{\sqrt{3}}{4}$ равна площади $LK_1K_2L_1 = y^2$, $y = \frac{\sqrt[4]{3}}{2}$.

12) $MT = \frac{\sqrt{3}}{4}$ (половина высоты ABC).

13) $QT = PQ - PT = \frac{1}{2} \mp x$.

14) $MQ^2 = MT^2 + QT^2$ (теорема Пифагора), т. е.

$$\left(\frac{\sqrt[4]{3}}{2}\right)^2 = \left(\frac{\sqrt{3}}{4}\right)^2 + \left(\frac{1}{2} \mp x\right)^2 \stackrel{(x \leq 1/2)}{\iff} \sqrt{\frac{\sqrt{3}}{4} - \frac{3}{16}} = \left|\frac{1}{2} - x\right| \iff$$

$$\iff x = \frac{1}{2} - \frac{1}{4}\sqrt{4\sqrt{3}-3}.$$

$$\begin{aligned} 15) AP : PQ : QC &= \frac{1}{4} \left(\sqrt{4\sqrt{3}-3} - 1 \right) : \frac{1}{2} : \frac{1}{4} \left(3 - (\sqrt{4\sqrt{3}-3}) \right) = \\ &= \left(\sqrt{4\sqrt{3}-3} - 1 \right) : 2 : \left(3 - \sqrt{4\sqrt{3}-3} \right). \end{aligned}$$

Замечание. Точки P и Q можно построить с помощью циркуля и линейки. Подумайте, как это можно сделать.

$$\text{Ответ: } AP : PQ : QC = \left(\sqrt{4\sqrt{3}-3} - 1 \right) : 2 : \left(3 - \sqrt{4\sqrt{3}-3} \right).$$

4.1. Исходный текст состоит из 48 букв, следовательно, при зашифровании было использовано три положения решётки полностью и ещё три буквы вписаны в четвёртом положении. Значит, незаполненные 12 клеток совпадают с вырезами решётки в четвёртом положении. Так как

текст вписывается последовательно, то неизвестные нам три выреза могут располагаться только в первой строке таблицы и первых пяти клетках второй строки (до первого известного выреза). Считаем, что трафарет лежит в четвёртом положении. Учитывая, что в одну клетку листа нельзя вписать две буквы, получаем, что вырезы могут быть только в отмеченных знаком «?» местах трафарета («*» — места известных вырезов):

	?						?	
		?	?		*			*
*				*			*	
		*			*			
							*	
*		*	*			*		

Очевидно, что из отмеченных в первой строке двух клеток вырезается только одна (так как они совмещаются поворотом). Получаем два возможных варианта решётки (либо первый «?», либо второй «?» в первой строке). Читаемый текст получается при втором варианте.

Ответ: ПОЛЬЗУЯСЬШИФРОМРЕШЕТКАНЕЛЬЗЯОСТАВЛЯТЬПУСТЫЕМЕСТА

4.2. Один из вариантов решения состоит из следующих этапов.

1. 19=н из второй строки («19,2 19,5»).
2. 29=о из третьей строки («29,н,10») и 10=а или 10=и.
3. 14=щ из «но,14,но».
4. 8=д, 2=е, 10=и из «денно и ночью».

Получили текст:

12е245321 6о 28е2018 20215и 2717е11е16 —
не 275 до123122е16, не н5 17одо6о16:
денно и ночью они е24е11е16
ищ1821 17е20е28о16 21о286о16.

5. 5=а и 27=з из второй строки.
6. 17=в 6=п 16=й — последнее слово второй строки — водопой.

Получили текст:

12е24а321 по 28е2018 2021аи зв е11ей —
не за до123122ей, не на водопой:
денно и ночью они е24е11ей
ищ1821 ве20е28ой 21о28пой.

7. 21=т 18=у 28=л 20=с из последней строки «ищут веселой толпой».
8. 11=р из «зв е11ей» первой строки.

Итак,

12е24а3т по лесу стаи зверей —
незадо123122ей, не на водопой:
денно и ночью они е24ерей
ищут веселой толпой.

9. 24=г из «егерей».

10. 12=б 3=ю из «бегают».

11. 31=ы 22=ч из «добычей».

Ответ: Бегают по лесу стаи зверей —
Не за добычей, не на водопой:
Денно и ночью они егерей
Ищут веселой толпой.

4.3. *Ответ:* $\cos 36^\circ = (1 + \sqrt{5})/4 \approx 0,8$.

4.4. Занумеруем буквы латинского алфавита последовательно числами от 1 до 24. Пусть x — некоторое число от 1 до 24, а $f(x)$ — число, в которое переходит x на втором этапе. Тогда перестановочность этапов можно записать в следующем виде:

$$f(x+1) = f(x) + 1, \quad \text{т. е.} \quad f(x+1) - f(x) = 1.$$

Это означает, что соседние числа x и $x+1$ на втором этапе переходят в соседние же числа $f(x)$ и $f(x+1)$, т. е. второй этап — тоже сдвиг. Последовательное применение двух сдвигов — очевидно тоже сдвиг и остаётся рассмотреть 24 варианта различных сдвигов. Читаемый текст определяется однозначно. Осложнения, связанные с переходом Z в A, устраняются либо переходом к остаткам при делении на 24, либо выписыванием после буквы Z второй раз алфавита AB...Z.

Ответ: INTER ARMA SILENT MUSAE
('интер 'арма с'илент м'узэ —
когда гремит оружие, музы молчат).

4.5. Составим возможные варианты переданных букв:

ГЪЙ	АЭЕ	БПРК	ЕЖЩЮ	НМЬЧ	СЫЗЛ	ШДУ	ЦХОТ	ЯФВИ
БШЗ	АЫВ	АНОИ	ГЕЧЬ	ЛКЪХ	ПЩЕЙ	ЦВС	ФУМР	ЭТАЖ
ВЩИ	БЬЕ	БОПЙ	ДЁШЭ	МЛЫЦ	РЪЖК	ЧГТ	ХФНС	ЮУБЗ
ГЪЙ	ВЭЁ	ВПРК	ЕЖЩЮ	НМЬЧ	СЫЗЛ	ШДУ	ЦХОТ	ЯФВИ
ДЫК	ЮЖ	ГРСЛ	ЁЗЪЯ	ОНЭШ	ТЬИМ	ЩЕФ	ЧЦПУ	ХГЙ
ЕЬЛ	ЯЗ	СТМ	ЖИЫ	ПОЮЩ	УЭЙН	ЪЁХ	ШЧРФ	ЦДК

Выбирая вторую и последнюю группы букв (где есть короткие колонки букв), определяем слова, им соответствующие: ВЯЗ, ЭТАЖ. В исходных словах 33 буквы, поэтому буквы В, Я, З, Э, Т, А, Ж уже использованы и их можно вычеркнуть из всех колонок:

ГЪЙ	АЭЕ	БПРК	ЕЖЩЮ	НМЬЧ	СЫЗЛ	ШДУ	ЦХОТ	ЯФВИ
БШ		НОИ	ГЕЧЪ	ЛКЪХ	ПЩЕЙ	Ц С	ФУМР	ЭТАЖ
ЩИ		БОПЙ	ДЁШ	МЛЫЦ	РЪ К	ЧГ	ХФНС	
ГЪЙ	В	ПРК	Е Щ	НМЬЧ	СЪ Л	ШДУ	ЦХО	
		ГРСЛ	Ё Ъ	ОН	ЫМ	ЩЕФ	ЧЦПУ	
ЕЪЛ	ЯЗ	С М	ИЫ	ПО	У ЙН	ЪЁХ	ШЧРФ	

Из нескольких вариантов, например, в третьей группе:

ГНОЙ ГНОМ ГРОМ

выбираем варианты так, чтобы каждая буква использовалась один раз. Продолжая таким образом, получим ответ.

Ответ: БЫК ВЯЗ ГНОЙ ДИЧЬ ПЛЮЩ СЪЁМ ЦЕХ ШУРФ ЭТАЖ

4.6. Заметим, что $A_{k+1} - A_k = (k+1)^3 - k^3 + 2$ для всех натуральных k . Складывая почленно эти равенства при $k = 1, 2, \dots, (n-1)$, получим $A_n - A_1 = n^3 - 3 + 2n$. По условию $A_1 = 3$. Следовательно, справедливо соотношение $A_n = n^3 + 2n$.

Ясно, что при расшифровании так же, как и при зашифровании, вместо чисел $A_{100}, A_{101}, A_{102}, A_{103}, A_{104}, A_{105}, A_{106}$ можно воспользоваться их остатками от деления на 30. Так как для каждого целого неотрицательного i

$$(100 + i)^3 + 2(100 + i) = i^3 + 2i + 30z,$$

где z — некоторое целое число, то получаем следующие остатки при делении чисел A_{100}, \dots, A_{106} на 30:

A_{100}	A_{101}	A_{102}	A_{103}	A_{104}	A_{105}	A_{106}
0	3	12	3	12	15	18

Заключительный этап представлен в таблице:

шифрованное сообщение	К	Е	Н	З	Э	Р	Е
числовое шифрованное сообщение	9	5	12	7	27	15	5
шифрующий отрезок	0	3	12	3	12	15	18
числовое исходное сообщение	9	2	0	4	15	0	17
исходное сообщение	К	В	А	Д	Р	А	Т

4.7. Ответ: $x = \frac{1 + \sqrt{4a^2 + 1}}{2a}$ при $0 < a < 1$;

$$x_1 = \frac{1 + \sqrt{4a^2 + 1}}{2a}, \quad x_2 = \frac{-\sqrt{4a^2 + 1} - 1}{2a} \quad \text{при } a \geq 1.$$

5.1. Указание. Найдите допустимые варианты для остатков от деления неизвестных x и y на 7. Таких вариантов будет восемь. Учитывая принадлежность неизвестных к заданному диапазону, найдите допустимые варианты для (x, y) (19 вариантов). Для каждой пары (x, y) найдите z . В диапазон $10, \dots, 20$ попадают только три решения: (12,16,11), (13,17,17), (13,18,12).

5.2. Так как при записывании сообщения в таблицу пробелы опускались, можно сделать вывод, что столбцы, содержащие знак пробела в последней клетке, до перестановки были расположены в конце таблицы. Таким образом, столбцы можно разбить на две группы, как показано на рис. 22. При этом для получения исходного текста потребуется переставлять столбцы только внутри групп.

Я	Н	Л	В	Р	А	Л	О	Е	Г	О	М	З	Е
Й	Л	Т	А	Ф	Ы	И	П	И	О	Г	Е	Б	Р
Ч	Р	Д	Ч	Е	С	М	О	К	И	Н	Т	К	О
Н	У	Л	А	Р	Е	Б	Ы	Е	И	О	Н	Ы	Д
Ы	Т	Д	О	М	П	П	Т	А	И	П	Т	З	Л
И	К	С	И	Т	Ч	Н	О	Е	Л	У	Л	Т	Ж

К	Е	Т	Р	И	Я
Л	Е	У	О	Д	О
И	Н	Д	Х	И	Е
Е	Ы	Е	З	Н	Ч
Е	Щ	В	Н	Я	С
-	-	-	-	-	-

Рис. 22

Естественно предположить, что сообщение оканчивается точкой. Поэтому на третьем с конца месте в первой группе должен быть столбец, оканчивающийся на Т, на втором — на Ч, на последнем — на К. Получаем два варианта (рис. 23), из которых первый является явно «нечитаемым».

Р	А	Н	З	А	Н	Я	Л	В	Р	Л	О	Е	Г	О	М	З	Е
Ф	Ы	Л	Б	Ы	Л	Й	Т	А	Ф	И	П	И	О	Г	Е	Б	Р
Е	С	Р	К	С	Р	Ч	Д	Ч	Е	М	О	К	И	Н	Т	К	О
Р	Е	У	Ы	Е	У	Н	Л	А	Р	Е	Б	Ы	Е	И	О	Н	Ы
М	П	Т	З	П	Т	Ы	Д	О	М	П	Т	А	И	П	Т	З	Л
Т	Ч	К	Т	Ч	К	И	С	И	Т	Ч	Н	О	Е	Л	У	Л	Т

Рис. 23

З	А	Н	Я	Т	И	Е	К	Р
Б	Ы	Л	У	О	Д	Е	Л	О
К	С	Р	Е	Д	И	Н	И	Х
Ы	Е	У	Ч	Е	Н	Ы	Е	З
З	П	Т	С	В	Я	Щ	Е	Н
Т	Ч	К	-	-	-	-	-	-

Рис. 24

Таким образом, удалось зафиксировать последние три столбца первой группы. Переставляя столбцы второй группы, ищем «читаемые» продолжения зафиксированных столбцов (рис. 24). Действуя далее анало-

гичным образом с оставшимися столбцами первой группы, достаточно легко получаем исходное сообщение.

Ответ:

Д	О	Л	Г	О	Е	В	Р	Е	М	Я	З	А	Н	Я	Т	И	Е	К	Р
И	П	Т	О	Г	Р	А	Ф	И	Е	Й	Б	Ы	Л	О	У	Д	Е	Л	О
М	О	Д	И	Н	О	Ч	Е	К	Т	Ч	К	С	Р	Е	Д	И	Н	И	Х
Б	Ы	Л	И	О	Д	А	Р	Е	Н	Н	Ы	Е	У	Ч	Е	Н	Ы	Е	З
П	Т	Д	И	П	Л	О	М	А	Т	Ы	З	П	Т	С	В	Я	Щ	Е	Н
Н	О	С	Л	У	Ж	И	Т	Е	Л	И	Т	Ч	К						

5.4. Во втором случае известны пары цифр, которыми шифруются буквы «р», «е», «м», «о», «н», «т», а в первом — пары цифр для тех же букв, за исключением буквы «н».

Ответ: во втором случае легче.

5.5. *Ответ:* 481.

5.6. Можно заметить, что последовательность букв МОСКВА входит как подпоследовательность в каждый из шифртекстов первой тройки:

й МьвОт СьлКъГвц Аяя
укМапОч Ср Кщ Вэ Ах
ш МфэОгчСйъКфъВыеАкк

На основе этого наблюдения можно предположить, что шифрование заключается в следующем. В каждый промежуток между буквами исходного сообщения (начало и конец также считаются промежутками) вставляются одна либо две буквы в соответствии с известным только отправителю и получателю ключом.

Очевидно, что первая буква сообщения должна попасть на 2-е или 3-е место шифрованного текста. Сравнивая буквы, стоящие на указанных местах в подлежащих расшифрованию криптограммах, делаем вывод, что одно и то же исходное сообщение соответствует первому и третьему шифртексту и что первая буква этого сообщения — П.

Рассуждая далее аналогичным образом, заключаем, что второй буквой повторяющегося сообщения является О (сопоставили ОИ из 1-й криптограммы и ИО из 3-й) и так далее. В итоге получим, что первой и третьей криптограмме соответствует исходное сообщение

ПОВТОРЕНИЕМАТЬУЧЕНИЯ

Теперь расшифруем вторую криптограмму. Первой буквой сообщения могут быть только С или И. Далее, подбирая к каждой из них возможные варианты последующих букв и вычёркивая заведомо «нечитаемые» цепочки букв, получим:

СЕ, СМ, ИМ, ИГ

СЕГ, СЕӨ, СМО, СМР, ИМО, ИМР, ИГР, ИГГ

СЕГР, СЕГГ, СМОТ, СМОК, СМРК, СМРР, ИМОТ, ИМОК,

~~ИМРК, ИМРР, ИГРК, ИГРР~~

~~СМОТР, СМОТО, СМОКО, СМОКМ, ИМОТР, ИМОТО, ИМОКО, ИМОКМ~~

~~СМОТРМ, СМОТРИ,~~

~~СМОТОИ, СМОТОТ, СМОКОИ, СМОКОТ, ИМОТРМ, ИМОТРИ,~~

~~ИМОТОИ, ИМОТОТ, ИМОКОИ, ИМОКОТ~~

~~СМОТРИВ, СМОТРИА~~

~~СМОТРИВВ, СМОТРИВК, СМОТРИАК, СМОТРИАН~~ и так далее.

В итоге получим исходное сообщение СМОТРИВКОРЕНЬ.

Ответ: 1,3 — ПОВТОРЕНИЕМАТЬУЧЕНИЯ

2 — СМОТРИВКОРЕНЬ

5.7. Обратив внимание на то, что некоторые символы в тексте условий задач пятой олимпиады набраны выделенным шрифтом, и выписав эти символы в порядке их следования, получаем текст:

задача семь поясните как вы нашли текст задачи

6.1. Так как каждый из 1997 абонентов связан ровно с N другими, то общее число направлений связи равно $1997N$. Отсюда общее число связанных пар абонентов равно $1997N/2$, так как каждая связанная пара имеет ровно 2 направления связи. Поскольку число $1997N/2$ должно быть целым, а число 1997 — нечётное, то число N должно быть чётным.

Докажем, что для каждого $N = 2T$ существует система связи из 1997 абонентов, в которой каждый связан ровно с N другими. В самом деле, расположив всех абонентов на окружности и связав каждого из них с T ближайшими к нему по часовой стрелке и с ближайшими к нему против часовой стрелки, получим пример такой сети связи.

6.2. Покажем, что на диагонали присутствуют все числа от 1 до 1997. Пусть число a из множества $\{1, \dots, 1997\}$ не расположено на диагонали. Тогда, в силу симметрии таблицы, число a встретится в таблице чётное число раз. С другой стороны, поскольку a по одному разу встречается в каждой строке, всего в таблице имеется нечётное число вхождений числа a (1997). Получили противоречие. Количество клеток диагонали равно 1997, поэтому каждое число из множества $\{1, \dots, 1997\}$ встретится на диагонали ровно по одному разу. Вычисляя сумму арифметической прогрессии, находим ответ.

Ответ: 1995003.

6.3. *Указание.* Пусть некоторая буква α при зашифровании первым способом заменялась на букву β . Тогда количество вхождений буквы β в первой криптограмме будет равно числу вхождений буквы α во второй криптограмме.

Ответ: ШЕСТАЯ ОЛИМПИАДА ПО КРИПТОГРАФИИ ПОСВЯЩЕНА СЕМИДЕСЯТИ ПЯТИ ЛЕТИЮ СПЕЦИАЛЬНОЙ СЛУЖБЫ РОССИИ

6.4. а) Определим моменты остановок после начала шифрования. Для этого каждой букве русского алфавита припишем её порядковый номер: А — 0, Б — 1, и т. д. Тогда буквам из шифруемого слова будут соответствовать следующие номера: О — 15, Л — 12, И — 9, М — 13, П — 16, А — 0, Д — 4. Моменты остановок будем указывать числом одношаговых (на один зубец) поворотов 1-го колеса до соответствующей остановки.

№ остановки	1	2	3	4	5	6	7	8	9
Буква 1-го колеса	О	Л	И	М	П	И	А	Д	А
Число одношаговых поворотов от начала до остановки	15	45	75	79	82	108	132	136	165
Цифра 2-го колеса	5	5	5	1	8	2	8	4	5
Цифра 3-го колеса	1	2	5	2	5	3	6	3	4

Искомый шифртекст: 515355128523864354

б) Пусть t_k — количество одношаговых поворотов 1-го колеса от начала до остановки с номером k , $k = 1, 2, \dots$,

a_k — цифра, на которую указывает стрелка 2-го колеса в момент остановки с номером k ,

b_k — цифра 3-го колеса, на которую указывает стрелка 3-го колеса в момент остановки с номером k .

Тогда, учитывая, что начальное положение стрелок соответствует букве А на первом колесе и 0 на 2-м и 3-м колёсах, получаем равенства

$$t_k = 10m_k - a_k, \quad k = 1, 2, \dots \quad (1)$$

$$t_k = 7n_k + b_k, \quad k = 1, 2, \dots \quad (2)$$

для подходящих неотрицательных целых чисел m_k и n_k .

Заметим, что $1 = 7 \cdot 3 - 10 \cdot 2$. Отсюда получаем равенства

$$a_k = 7 \cdot (3a_k) - 10 \cdot (2a_k), k = 1, 2, \dots$$

$$b_k = 7 \cdot (3b_k) - 10 \cdot (2b_k), k = 1, 2, \dots$$

Подставляя эти значения в равенства (1) и (2), получим

$$t_k = 10(m_k + 2a_k) - 7(3a_k), k = 1, 2, \dots$$

$$t_k = 7(n_k + 3b_k) - 10(2b_k), k = 1, 2, \dots$$

Следовательно,

$$10(m_k + 2a_k) - 7(3a_k) = 7(n_k + 3b_k) - 10(2b_k), k = 1, 2, \dots$$

Правая и левая части делятся на 70, то есть имеют вид $70s_k$ для подходящего неотрицательного целого s_k . Поэтому

$$m_k = 7s_k - 2(a_k + b_k), k = 1, 2, \dots$$

$$n_k = 10s_k - 3(a_k + b_k), k = 1, 2, \dots$$

Подставляя m_k в (1), получим

$$t_k = 70s_k - 21a_k - 20b_k, k = 1, 2, \dots$$

Учитывая условие $0 < t_1 < t_2 < \dots < t_7$ и то, что остановка колёс происходит в момент первого появления шифруемой буквы под стрелкой 1-го колеса, получаем следующие итоговые значения:

k	1	2	3	4	5	6	7
a_k	2	8	9	8	9	1	1
b_k	4	0	2	3	1	2	1
$-(21a_k + 20b_k)$	-122	-168	-229	-228	-209	-61	-41
t_k	18	42	51	52	71	79	99
Буквы	С	И	С	Т	Е	М	А

6.5. Указание. Рассмотрим некоторую расстановку ненулевых цифр на окружности. Упорядоченную пару (a, b) соседних цифр на этой окружности назовём 1-соседней, если b является соседней с a по часовой стрелке. Пару (a, c) назовём 2-соседней, если существует цифра b , для которой пары (a, b) и (b, c) являются 1-соседними.

Каждой расстановке ненулевых цифр на окружности однозначно соответствует цепочка 1-соседних пар вида: $(1, a_1), (a_1, a_2), (a_2, a_3), \dots, (a_7, a_8), (a_8, 1)$, которой, в свою очередь, однозначно соответствует цепочка 2-соседних пар вида:

$$(1, a_2), (a_2, a_4), (a_4, a_6), (a_6, a_8), (a_8, a_1)(a_1, a_3)(a_3, a_5)(a_5, a_7)(a_7, 1), \quad (*)$$

где $a_2, a_3, \dots, a_8 \in \{2, \dots, 9\}$ и $a_i \neq a_j$ при $i \neq j$.

Если из цепочки $(*)$ удалить любую пару, то по оставшимся парам она восстанавливается однозначно.

Если из цепочки $(*)$ удалить две соседние пары, то она также восстанавливается однозначно.

Удаление из $(*)$ любых трёх пар приводит к неоднозначности восстановления цепочки $(*)$. В этом можно убедиться, рассмотрев следующие фрагменты цепочки вида $(*)$:

$$\begin{aligned} (a, b)(b, c)(c, d) \text{ и } (a, c)(c, b)(b, d), & \quad (a, b, c, d \text{ — различные цифры}), \\ (a, b)_{-}(c, d)(d, e) \text{ и } (a, d)(d, b)_{-}(c, e), & \quad (a, b, c, d, e \text{ — различные цифры}), \\ (a, b)_{-}(c, d)_{-}(e, f) \text{ и } (a, d)(e, b)_{-}(c, f), & \quad (a, b, c, d, e, f \text{ — различные} \\ & \quad \text{цифры}). \end{aligned}$$

Таким образом, при наличии двух указанных в условии задачи цифровых текстов нам будут известны некоторые 2-соседние пары, в которых первая цифра берётся из первой криптограммы, а вторая — из второй. Поэтому с учётом сказанного получаем условие однозначного восстановления порядка расстановки цифр на данной окружности.

Ответ: для однозначного восстановления расстановки цифр на окружности необходимо и достаточно, чтобы в одном из цифровых текстов было не менее 7 ненулевых цифр (это соответствует удалению из цепочки 2-соседних пар вида $(*)$ не более двух из них).

6.6. Последовательность остатков от деления чисел a_1, a_2, \dots на 24 — периодическая с периодом 2, так как для любого натурального n справедливо:

$$a_{n+2} - a_n = p^{n+4} - p^{n+2} = \begin{cases} 24 \cdot 2^{n-1}, & \text{при } p = 2 \\ p^{n+1}(p^3 - p), & \text{при } p \geq 3 \end{cases}.$$

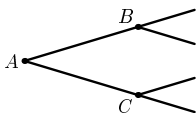
Кроме того, $p^3 - p = (p-1)p(p+1)$ кратно 24, то есть остатки у a_{n+2} и a_n равны.

6.7. *Указание.* При $a \leq 0$ рассматриваемое уравнение равносильно уравнению $|x-a| - 1995a = 1996$, которое имеет не более двух решений.

При $a > 0$ из графика функции $y = f(x)$, где $f(x)$ — это левая часть уравнения, видно, что если $1996 \in (0, a)$, то число решений будет чётным, и поэтому не может быть равным 1997. Если $1996 \in (a, +\infty)$, то уравнение имеет ровно 2 решения. Если же $a = 1996$, то уравнение имеет ровно 1997 решений.

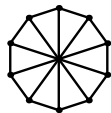
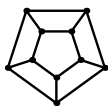
Ответ: $a = 1996$; все решения имеют вид $\pm 3992k + 1996$, $k = 0, 1, \dots, 998$.

7.1. Для того, чтобы сохранилась связь при выходе из строя любых двух узлов, необходимо, чтобы в каждый узел входило не менее трёх линий связи. Ситуация



недопустима, ибо при выходе из строя узлов B и C узел A становится недоступным. Значит, всего линий должно быть не менее $\frac{10 \times 3}{2} = 15$.

Вот два примера, удовлетворяющие условиям задачи с 15-ю линиями связи:



Приведём доказательство для первого примера. Если вышли из строя два узла на одном пятиугольнике, то связь сохранится через другие пятиугольники. Если вышли из строя по одному узлу на разных пятиугольниках, то связь сохранится по линиям, соединяющим эти пятиугольники.

Ответ: 15.

7.2. Процедура зашифрования может быть полностью описана с помощью квадратной таблицы размера 10×10 . На пересечении её строки с номером i и столбца с номером j записывается цифра, в которую при зашифровании переходит цифра j , если она расположена в пароле после цифры i . Из требования однозначности расшифрования следует, что в каждой строке таблицы каждая цифра встречается ровно один раз.

Обозначим через w_1, w_2, \dots, w_7 и o_1, o_2 зашифрованные пароли и два известных пароля в порядке, определяемом условием задачи. Процедура зашифрования сохраняет длину, поэтому w_3 и w_4 не могут соответствовать ни o_1 , ни o_2 . Предположив, что w_1 соответствует o_1 , получим часть таблицы, в которой в одной строке содержатся две одинаковые цифры. Это означает, что предположение неверно. Составляя таблицы, убеждаемся, что o_2 не шифруется ни в w_6 , ни в w_7 , ни в w_5 . В результате таких рассуждений остаётся только один вариант перехода $o_1 - w_2, o_2 - w_5$. Заполнение таблицы будет следующим:

	0	1	2	3	4	5	6	7	8	9
0									5	
1			3							
2	4	3	7					8		
3		7								
4			2							
5									3	
6										
7						4				
8			1	9						
9										

	0	1	2	3	4	5	6	7	8	9
0			6						5	
1			3							
2	4	3	7	0	6	2	5	8	9	
3	3	7								
4			2							
5									3	7
6										
7						4				
8			1	9						
9			1							

Очевидно, что в строке с номером 2 в последней клетке стоит 1. Знание этой таблицы позволяет однозначно расшифровать w_3 : получится 5830829. Пароли, соответствующие w_1, w_4, w_6, w_7 , восстанавливаются не полностью.

Ответ: полностью можно расшифровать только 5393511, получится 5830829.

7.3. Сообщение состоит из $3 \times 17 = 51$ буквы. Поэтому $r = 3$ или $r = 17$ (при $r = 1$ и $r = 51$ — получается нечитаемый текст). При $r = 3$ не получается осмысленного текста при всех шести возможных вариантах перестановки букв ($a = 1, 2, b = 0, 1, 2$). Рассмотрим случай $r = 17$:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Б	Т	И	П	Ч	Ь	Л	О	Я	Ч	Ы	Ь	Т	О	Т	П	У
Н	Т	Н	О	Н	З	Л	Ж	А	Ч	О	Ь	О	Т	У	Н	И
У	Х	Н	И	П	П	О	Л	О	Ь	Ч	О	Е	Л	О	Л	С

Соседние буквы при перестановке переходят в буквы, отстоящие друг от друга на одинаковое расстояние: буква на x -м месте переходит на место, определяемое остатком от деления $ax + b$ на 17, а буква на $(x+1)$ -м месте — на место, определяемое остатком от деления $(ax+b)+a$ на 17. Это верно для любого x . Поэтому есть всего 16 вариантов переходов соседних букв (исходный текст нечитаем), которые определяют однозначно переходы всех остальных букв. Перебирая их, получаем нечитаемые тексты во всех случаях, кроме одного, который даёт текст:

Ч	И	Т	Ь	П	Я	Т	Ь	Ч	Т	О	Б	Ы	П	О	Л	У
Ч	Н	О	З	Н	А	Т	Ь	Н	У	Ж	Н	О	О	Т	Л	И
Ь	Н	Е	П	Л	О	Х	О	П	О	Л	У	Ч	И	Л	О	С

Из трёх вариантов начала текста легко определяется истинный вариант.

Ответ:

ЧТОБЫ ПОЛУЧИТЬ ПЯТЬ НУЖНО ОТЛИЧНО ЗНАТЬ ПОЛУЧИЛОСЬ НЕ ПЛОХО

7.4. Последовательность обхода доски показана на рисунке:

37	62	43	56	35	60	41	50
44	55	36	61	42	49	34	59
63	38	53	46	57	40	51	48
54	45	64	39	52	47	58	33
1	26	15	20	7	32	13	22
16	19	8	25	14	21	6	31
27	2	17	10	29	4	23	12
18	9	28	3	24	11	30	5

Ответ:

Кавалергардов век недолог

И потому так сладок он.

Труба трубит, откинут полог...

7.5. Из однородности всех членов следует, что неравенство эквивалентно неравенству $a^3 + b^3 + c^3 + 6abc > 1/4$ при условии $a + b + c = 1$, $a > 0$, $b > 0$, $c > 0$.

Пусть c — минимальное из чисел a, b, c ($0 < c \leq 1/3$) и $a = x$. Тогда

$$\begin{aligned}
 A &= a^3 + b^3 + c^3 + 6abc - 1/4 = \\
 &= x^3 + (1 - c - x)^3 + c^3 + 6x(1 - c - x)c - 1/4 = \\
 &= 3(1 - 3c)x^2 - 3(1 - c)(1 - 3c)x + (1 - c)^3 + c^3 - 1/4.
 \end{aligned}$$

Находим минимум квадратного трёхчлена с параметром c и положительным коэффициентом при x^2 . Минимум достигается в точке $x = (1 - c)/2$, при этом значение A будет положительным.

7.6. Если мелом с квадратным сечением нарисовать на доске отрезок прямой так, чтобы стороны сечения были параллельны краям доски, то площадь полученной линии будет равна площади ступенчатой линии с такими же концами (см. рис. 25).

Если на доске нарисовать некоторый (выпуклый) многоугольник, то найдутся такие граничные «точки» этого многоугольника, которые являются ближайшими к одному из краёв доски. Площадь границы прямоугольника, содержащей все такие «точки», равна площади границы нарисованного выпуклого многоугольника (см. рис. 26).

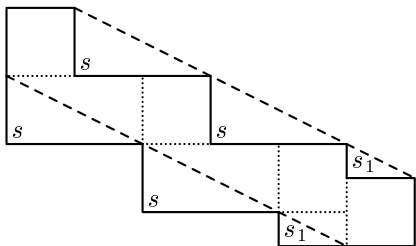


Рис. 25

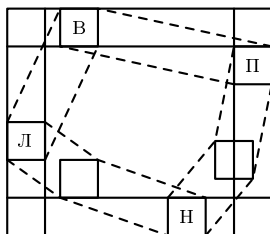


Рис. 26

Такой прямоугольник назовём окаймляющим. Ясно, что площадь окаймляющего прямоугольника не меньше площади соответствующего многоугольника. Значит, для любого многоугольника данной площади найдётся прямоугольник такой же площади, но с площадью границы не большей, чем площадь границы исходного многоугольника.

Если многоугольник со сторонами a и b имеет площадь 10000 см^2 , то площадь его границы равна

$$2a + 2b + 4 = 2a + \frac{20000}{a} + 4 = 2 \left(\sqrt{a} - \frac{100}{\sqrt{a}} \right)^2 + 404.$$

Минимум достигается в случае, когда возводимое в квадрат выражение равно 0. В этом случае $a = 100$, что влечёт $b = 100$. Таким образом, наименьшую площадь границы, равную 404 см^2 , имеет квадрат со стороной 1 м.

Ответ: квадрат со стороной 1 м; площадь его границы — 404 см^2 .

7.7. Если группа цифр, из которой образуются числа, состоит из k цифр, то существует ровно $k!$ различных чисел, для записи которых

используются все цифры группы ровно по одному разу. Группу из k цифр будем обозначать G_k .

Поскольку в сообщении отсутствуют цифры 2 и 9, эти цифры образуют либо две группы по одной цифре, либо одну группу из двух цифр. В обоих случаях эти цифры могут быть использованы для зашифрования ровно двух букв алфавита.

Так как $3! = 1! + 3! + 4!$, получаем $\{1, 3, 4, 5, 6, 7, 8, 0\} = G_1 \cup G_3 \cup G_4$.

Если $G_1 \neq \{1\}$, то из сообщения находим:

- а) $G_4 = \{1, 3, 7, 8\}$, $G_3 = \{0, 5, 6\}$, $G_1 = \{4\}$ либо
 б) $G_4 = \{1, 3, 7, 8\}$, $G_3 = \{4, 5, 6\}$, $G_1 = \{0\}$.

Случай а		Случай б		Случай а		Случай б		Случай а		Случай б	
А	2 (4)	0	К	1738	1738	Х	7183		7183		
Б	4 (29)	2 (29)	Л	1783	1783	Ц	7318		7318		
В	9 (56)	9 (92)	М	1837	1837	Ч	7381		7381		
Г	56 (65)	456	Н	1873	1873	Ш	7813		7813		
Д	65 (92)	465	О	3178	3178	Щ	7831		7831		
Е	506	546	П	3187	3187	Ъ	8137		8137		
Ё	605	564	Р	3718	3718	Ы	8173		8173		
Ж	650	645	С	3781	3781	Ь	8317		8317		
З	650	654	Т	3817	3817	Э	8371		8371		
И	1378	1378	У	3871	3871	Ю	8713		8713		
Й	1387	1387	Ф	7138	7138	Я	8731		8731		

Сообщение после расшифрования имеет вид: а) ЯАЗЧ или б) ЯДАЧ, т. е. не читается.

Если $G_1 = \{1\}$, то из сообщения находим $G_3 = \{3, 7, 8\}$, $G_4 = \{0, 4, 5, 6\}$. В этом случае таблица замены букв числами имеет вид:

А	1	Ё	465	Л	783	С	4560	Ч	5460	Э	6450
Б	2(29)	Ж	546	М	837	Т	4605	Ш	5604	Ю	6504
В	9(92)	З	564	Н	873	У	4650	Щ	5640	Я	6540
Г	378	И	645	О	4056	Ф	5046	Ъ	6045		
Д	387	Й	654	П	4065	Х	5064	Ы	6054		
Е	456	К	738	Р	4506	Ц	5406	Ь	6405		

Сообщение легко прочесть: НАУКА.

8.1. Проведём прямые, проходящие через точки пересечения границ сложенной ленты параллельно её краям. Очевидно, что тогда лента разобьётся на равные равносторонние треугольники. Отметим цифрой 0 все просветы, а цифрой 2 все треугольники, которые получились наложением друг на друга двух треугольников в сложенной ленте. Построим дополнительно ряд треугольников вне эмблемы, как показано на рисунке 27. В полученной фигуре число треугольников, отмеченных цифрой 2, равно числу треугольников, отмеченных цифрой 0. Поэтому площадь всей ленты равна площади трапеции $ABCD$. Количества треугольников в горизонтальных рядах $ABCD$ являются 9 последовательными членами арифметической прогрессии с первым членом, равным 3 (нижний ряд), и разностью 2. Следовательно, общее число треугольников равно

$$N = \frac{2 \cdot 3 + (9 - 1) \cdot 2}{2} \cdot 9 = 99.$$

Если h — ширина ленты, то площадь одного равностороннего треугольника с высотой h равна

$$S_0 = h^2 \operatorname{ctg} 60^\circ = h^2 / \sqrt{3}.$$

С другой стороны, если длина прямоугольника, полученного после разрезания ленты, равна l , то $S = lh$. Отсюда находим искомую величину: $l/h = 33\sqrt{3}$.

Ответ: $33\sqrt{3}$.

8.2. Последовательность из k нулей или k единиц обозначим соответственно через 0^k или 1^k . Тогда шифрование каждого знака сообщения состоит в замене

$$\begin{cases} 0 \rightarrow 0^{k_1} 1^{k_2} \\ 1 \rightarrow 0^{k_3} \end{cases} \quad \text{для I способа,} \quad \begin{cases} 1 \rightarrow 1^{k_4} 0^{k_5} \\ 0 \rightarrow 0^{k_6} \end{cases} \quad \text{для II способа.} \quad (1)$$

В зашифрованном сообщении все серии из единиц имеют длину k_2 для первого способа и длину k_4 для второго способа, поэтому, для совпадения результатов зашифрования необходимо, чтобы

$$k_2 = k_4. \quad (2)$$

Теперь легко получить, что в сообщении должно быть одинаковое число нулей и единиц.

Пусть n — число нулей в сообщении. Тогда число нулей в зашифрованном I способом сообщения равно $nk_1 + nk_3$, а II способом — $nk_5 + nk_6$. Таким образом,

$$nk_1 + nk_3 = nk_5 + nk_6. \quad (3)$$

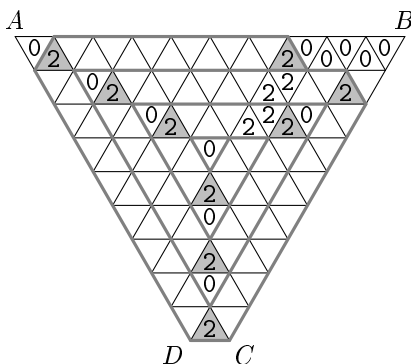


Рис. 27

Из (1) видно, что сообщение должно начинаться с нуля и оканчиваться единицей. Пусть перед первой единицей сообщения расположено a нулей. Тогда первые $a + 1$ знаков сообщения представляются при шифровании в виде:

$$\begin{aligned} \text{при } a = 1 & \quad \begin{cases} 0^{k_1} 1^{k_2} 0^{k_3} & \text{для I способа,} \\ 0^{k_6} 1^{k_4} 0^{k_5} & \text{для II способа,} \end{cases} \\ \text{при } a > 1 & \quad \begin{cases} 0^{k_1} 1^{k_2} 0^{k_1} 1^{k_2} \dots 0^{k_1} 1^{k_2} 0^{k_3} & \text{для I способа,} \\ 0^{ak_6} 1^{k_4} 0^{k_5} & \text{для II способа.} \end{cases} \end{aligned} \quad (4)$$

При $a = 1$ получаем необходимость равенства $k_1 = k_6$, а значит, с учётом (3) — равенства $k_3 = k_5$.

При $a > 1$ получаем условия:

$$\begin{aligned} k_1 &= ak_6, & a &\text{— натуральное,} \\ k_1 &= k_5 + bk_6, & b &\text{— натуральное или нуль.} \end{aligned}$$

Подставляя $k_1 = k_5 + bk_6$ в (3), получаем равенство $k_3 = (1 - b)k_6$, которое при натуральных k_3 , k_6 и $b \geq 0$ возможно лишь в случае $b = 0$. Следовательно, $k_3 = k_6$, а значит, с учётом (3) $k_1 = k_5$.

Таким образом, при $a > 1$ необходимы условия $k_2 = k_4$, $k_5 = k_1 = ak_6 = ak_3$, где a — натуральное. Из (4) следует, что сообщение должно иметь вид $0 \dots 01 \dots 1$, где число нулей и число единиц равно a .

Ответ: При $k_2 = k_4$, $k_1 = k_6$, $k_3 = k_5$ сообщения вида $0101 \dots 01$ шифруются одинаково.

При $k_2 = k_4$, $k_5 = k_1 = ak_6 = ak_3$, где a — натуральное, сообщения вида $(0 \dots 01 \dots 1) \dots (0 \dots 01 \dots 1)$ (группы из a нулей и a единиц) шифруются одинаково.

Замечание. Первый ответ не является частным случаем второго при $a = 1$.

8.3. Естественно предположить, что все члены оргкомитета родились в XX веке. Отсюда сразу замечаем, что на 3, 7, 11, 15, 19 и 23 местах последовательности простых чисел расположены числа 11, 17, 47, 53, 83 и 89 соответственно.

Выясним, какие числа являются соседними с указанными шестью числами. Для этого составим таблицу их возможных «соседей». В соответствии с условием имеем:

число	соседи
11	13, 19, 43, 7, 3
17	13, 19
47	79, 43, 31
53	61, 37
83	79, 67, 19
89	97, 73.

Учитывая, что первая цифра в номере месяца принимает значения только 0 или 1, построим следующую таблицу:

15	02	20	45	42	13	26	67	44	30	56	82	53	33	62	32	73	63	92	49	75	70	98	49
	19				19				19					19				19					19
	11				17				31 47					37 53 61				67 83					73 89 97
03	03			13	13				43									19					
07	07			19	19				79									79					
				13																			
				19																			
				43																			

где в первой строке расположено шифрованное сообщение, во второй строке — известные участки исходного сообщения, в третьей строке — ставшие известными участки ключевой последовательности, в остальных строках — возможные варианты ключевой последовательности в соответствующих позициях. При составлении таблицы учитывалось, что каждое число должно встретиться ровно один раз. Позиции чисел 31, 37, 67, 73 определяются однозначно. Их расположение однозначно определяет места для простых чисел 61 и 97.

Снова выпишем известные числа последовательности простых чисел и варианты для их соседей (первые две строки таблицы на этом шаге не понадобятся):

	11			17			31 47			37 53 61		67 83		73 89 97
03	03			13	13		43					19		
07	07			19	19		79					79		
				13										
				19										
				43										

Возможные соседи для числа 61 — лишь 59 и 29, а для 67 — лишь 59 и 3. Поэтому между 61 и 67 может находиться только число 59. Возможными соседями для числа 73 являются 89, 71 и 41. Ни одно из этих чисел не может быть соседом для 19, а для 79 может быть только 71. Таким образом, однозначно определяется расположение чисел 71 и 79. Для числа 47 остался только один кандидат в соседи справа — число 43. Общим соседом для 43 и 37 может быть только 41. Скорректируем таблицу с учётом сделанных выводов:

	11			17		31 47 43 41	37 53 61 59 67 83 79 71 73 89 97
03	03			13	13 29		
07	07			19	19 23		
				13			
				19			

Участок последовательности 17 * * 31 имеет только два варианта доопределения: (а) 17–19–23–31 и (б) 17–13–29–31. Рассмотрим оба случая.

а) Выпишем фрагмент таблицы для первого случая:

11	13 17 19 23 31
03	03
07	07

Очевидно, что числа 3 и 7 должны обязательно быть соседними с числом 11. Число 29 ещё не встречалось, значит оно должно располагаться либо на первом месте, либо на пятом. И то и другое невозможно, так как в обоих позициях оно является соседом либо для числа 3, либо для числа 7, что не соответствует условию (отличие соседних чисел на степень двойки). Следовательно, рассматриваемый случай невозможен.

б) Выпишем фрагмент таблицы для второго случая:

05	11	23 19 17 13 29 31
03	03	
07	07	

Очевидно, что числа 3 и 7 должны обязательно быть соседями для числа 11. Число 5 может попасть только на первую позицию (т.к. оно не может находиться рядом с 19). Значит, в пятой позиции должно быть число 23. Ясно, что числа 3 и 7 теперь расставляются однозначно.

Таким образом, приходим к выводу, что возможен всего один вариант ключевой последовательности. Получим окончательный вариант таблицы и найдём ответ:

15	02	20	45	42	13	26	67	44	30	56	82	53	33	62	32	73	63	92	49	75	70	98	49
10 09 19 48 29 04 19 54 25 09 19 49 12 06 19 71 24 06 19 70 04 07 19 52																							
05	03	11	07	23	19	17	13	29	31	47	43	41	37	53	61	59	67	83	79	71	73	89	97

Ответ: 10.09.1948 29.04.1954 25.09.1949 12.06.1971 24.06.1970 04.07.1952

8.4. Занумеруем горизонтали и вертикали квадрата натуральными числами от 1 до 13 сверху вниз и слева направо соответственно. Тогда каждая клетка квадрата однозначно определяется парой чисел $(i; j)$, где i — номер горизонтали, а j — номер вертикали, в которых находится клетка.

Расстояние между центром клетки $(a; b)$ и центром клетки $(c; d)$ равно $\sqrt{(a-c)^2 + (b-d)^2}$. Заметим, что $|a-c| \in \{0, 1, \dots, 12\}$ и $|b-d| \in \{0, 1, \dots, 12\}$. Обозначим $x = |a-c|$, $y = |b-d|$, $z = \sqrt{x^2 + y^2}$. Тогда z — число натуральное, если $x^2 = (z+y)(z-y)$. Отсюда получаем, что

$$1 = (z+y)(z-y) \iff \begin{cases} z = 1 \\ y = 0 \end{cases};$$

$$2^2 = (z+y)(z-y) \iff \begin{cases} z = 2 \\ y = 0 \end{cases};$$

$$3^2 = (z + y)(z - y) \iff \begin{cases} z = 3 \\ y = 0 \end{cases} \text{ или } \begin{cases} z = 5 \\ y = 4 \end{cases}; \text{ и т. д.}$$

$$12^2 = (z + y)(z - y) \iff \begin{cases} z = 12 \\ y = 0 \end{cases} \text{ или } \begin{cases} z = 15 \\ y = 9 \end{cases} \text{ или } \begin{cases} z = 20 \\ y = 16 \end{cases} \text{ или} \\ \begin{cases} z = 37 \\ y = 35 \end{cases} \text{ или } \begin{cases} z = 13 \\ y = 5 \end{cases}.$$

В общем случае, если $x^2 = mn$, то

$$\begin{cases} z = \frac{m+n}{2} \\ y = \left| \frac{m-n}{2} \right|. \end{cases}$$

Ясно, что m и n должны быть одинаковой чётности. По условию, $y \leq 12$, поэтому искомыми решениями будут только пары

$$(x; y) \in A = \{(3; 4), (4; 3), (6; 8), (8; 6), (9; 12), (12; 9), (5; 12), (12; 5)\} \cup \\ \cup \{(0; a), (a; 0), a = 1, \dots, 12\}.$$

Клетку $(a; b)$ назовём существенной для клетки $(c; d)$, если выполнено условие $(|a - c|; |b - d|) \in A$. Ясно, что цвет данной клетки менялся лишь тогда, когда Кристоша находился в какой-либо существенной для неё клетке. А так как в каждой клетке Кристоша побывал ровно 1999 раз (нечётное число), то цвет данной клетки изменился, если общее число существенных для неё клеток нечётно.

Для определения чётности числа всех существенных клеток для данной клетки воспользуемся тем, что у симметричных клеток относительно той или иной диагонали квадрата или относительно центрального вертикального или центрального горизонтального рядов эти числа будут одинаковы. Это, в частности, означает, что достаточно определить указанную чётность только для клеток $(a; b)$, где $a = 1, \dots, 5$, $b = a + 1, \dots, 6$ (этих клеток 15, занумеруем их, как показано на рис. 28). Кроме того, отметим, что у каждой из клеток на диагоналях квадрата, а также у каждой из клеток центрального вертикального и горизонтального рядов обязательно будет чётное число существенных для неё клеток.

Зоной асимметрии для той или иной клетки мы назовём множество тех клеток, которые в пределах исходного квадрата не имеют клеток, симметричных относительно вертикального, горизонтального и правого диагональных рядов, содержащих данную клетку. Ясно, что для данной клетки число существенных клеток, не лежащих в её зоне асимметрии, чётно.

На рис. 28 показана зона асимметрии для клетки 1, а также все клетки верхнего левого угла 6×6 , меняющие свой цвет.

Ответ на рис. 29.

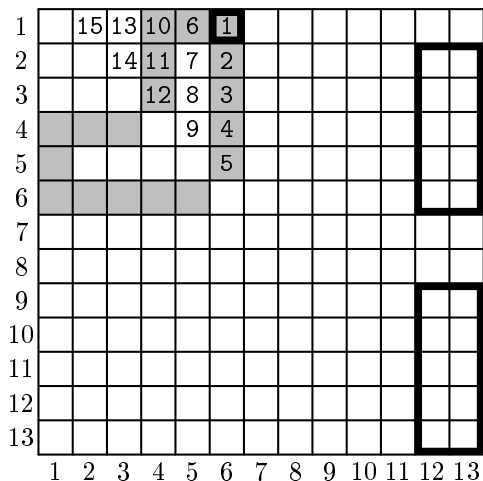


Рис. 28. Для клетки 1 жирными линиями выделена зона асимметрии. Серым цветом отмечены клетки верхнего левого угла 6×6 , меняющие свой цвет.

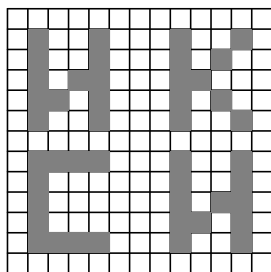


Рис. 29

8.5. При решении этого уравнения надо учитывать возможные ограничения: $a \neq 0$, $b \neq 0$, $a - b \neq 0$, $a + b \neq 0$. Поэтому целесообразно выделить их сразу.

1. Пусть $a = 0$, $b = 0$. Уравнение имеет вид $\frac{0}{1-0x} = \frac{0}{1-0x}$, то есть x — любое число.

2. Пусть $a = 0$, $b \neq 0$. Уравнение имеет вид $\frac{0}{1-bx} = \frac{b}{1-0x}$, или $0 = b$, то есть не имеет решений.

3. Аналогично, при $b = 0$, $a \neq 0$ нет решений.

4. При $a \neq 0$, $b \neq 0$ удобно рассмотреть три случая: а) $a = b$, б) $a = -b$, в) $a \neq \pm b$.

- a) $a = b$: $\frac{a}{1-ax} = \frac{a}{1-ax}$, $x \neq \frac{1}{a}$, x — любое, кроме $\frac{1}{a}$.
 b) $a = -b$: $\frac{a}{1+ax} = \frac{-a}{1-ax}$, $x \neq \pm \frac{1}{a}$, $\frac{1}{a} + x = -\frac{1}{a} + x$, $\frac{2}{a} = 0$, решений нет.
 c) $a \neq \pm b$:

$$\frac{a}{1-bx} = \frac{b}{1-ax}, \quad x \neq \frac{1}{a}, \quad x \neq \frac{1}{b},$$

$$\frac{1}{a} - \frac{b}{a}x = \frac{1}{b} - \frac{a}{b}x,$$

$$x \left(\frac{a}{b} - \frac{b}{a} \right) = \frac{1}{b} - \frac{1}{a},$$

$$x = \frac{(a-b)ab}{ab(a^2 - b^2)} = \frac{1}{a+b}.$$

Ответ. При $a = b = 0$ x — любое число.

При $a = b \neq 0$ $x \in \left(-\infty; \frac{1}{a}\right) \cup \left(\frac{1}{a}; \infty\right)$.

При $a = 0, b \neq 0$ или $a \neq 0, b = 0$ или $a = -b \neq 0$ решений нет.

$$\text{При } \begin{cases} a \neq -b \\ a \neq 0 \\ b \neq 0 \\ a \neq +b \end{cases} \quad x = \frac{1}{a+b}.$$

8.6. Число $2^{30} + 1$ представляет собой сумму кубов, сумму пятых степеней, а также из него можно выделить полный квадрат. Каждое из этих представлений позволяет найти некоторые делители исходного числа:

$$\begin{aligned} 2^{30} + 1 &= 2^{10 \cdot 3} + 1^3 = (2^{10} + 1)(2^{20} - 2^{10} + 1) = 1025 \cdot (2^{20} - 2^{10} + 1) = \\ &= 41 \cdot 25 \cdot (2^{20} - 2^{10} + 1). \end{aligned}$$

$$\begin{aligned} 2^{30} + 1 &= 2^{6 \cdot 5} + 1^5 = (2^6 + 1)(2^{24} - 2^{18} + 2^{12} - 2^6 + 1) = \\ &= 65 \cdot (2^{24} - 2^{18} + 2^{12} - 2^6 + 1) = \\ &= 13 \cdot 5 \cdot (2^{24} - 2^{18} + 2^{12} - 2^6 + 1). \end{aligned}$$

$$\begin{aligned} 2^{30} + 1 &= (2^{15} + 1)^2 - 2 \cdot 2^{15} = (2^{15} + 2^8 + 1)(2^{15} + 1 - 2^8) = \\ &= 33025 \cdot 32513 = 25 \cdot 1321 \cdot 32513. \end{aligned}$$

Таким образом, установлено, что среди простых делителей числа $2^{30} + 1$ содержатся 41, 13, 5. Непосредственной проверкой получаем равенство $32513 = 41 \cdot 793 = 41 \cdot 13 \cdot 61$.

Осталось проверить, что 1321 — простое число. Для этого достаточно показать, что 1321 не делится ни на одно простое число, меньшее $\sqrt{1321}$ ($37^2 = 1369$, $1369 > 1321$).

Ответ: $2^{30} + 1 = 5 \cdot 5 \cdot 13 \cdot 41 \cdot 61 \cdot 1321$.

9.1. а) Для доказательства достаточно указать хотя бы одну последовательность из 33 различных букв, сумма которой с русским алфавитом из 33 букв не содержит одинаковых букв. В качестве искомой последовательности возьмём сам алфавит. Докажем, что сумма алфавита с самим собой не содержит одинаковых букв. Пусть m и n — порядковые номера различных букв алфавита. Тогда по определению сложения букв достаточно показать, что числа $2m$ и $2n$ имеют разные остатки от деления на 33. В самом деле, если бы они были одинаковы, то число $2m - 2n$ делилось бы на 33 без остатка. В силу того что $\text{НОД}(2, 33) = 1$, разность $m - n$ также делилась бы на 33 без остатка, что невозможно. Утверждение пункта а) доказано.

Замечание. Утверждение пункта а) остаётся в силе для любого алфавита из нечётного числа букв.

б) При сложении двух последовательностей сумма порядковых номеров всех букв получаемой при этом последовательности и сумма порядковых номеров всех букв обоих слагаемых имеет один и тот же остаток от деления на 26. Значит, разность упомянутых сумм должна делиться на 26 без остатка. Докажем утверждение пункта б) методом от противного. В самом деле, если такая последовательность из 26 различных букв существует, то упомянутая разность равна сумме порядковых номеров букв алфавита. Однако сумма $1 + 2 + \dots + 26 = 13 \cdot 27 = 26 \cdot 13 + 13$ при делении на 26 имеет остаток 13. Это доказывает утверждение пункта б).

Замечание. Утверждение пункта б) остаётся в силе для любого алфавита из чётного числа букв.

Представляет интерес доказательство пункта б), предложенное участниками олимпиады.

При делении на любое чётное число суммы двух чётных или двух нечётных чисел получается чётный остаток, а при делении суммы чётного и нечётного чисел — нечётный остаток.

Соответствующие буквы складываемых последовательностей могут быть как одинаковой, так и различной чётности. (Для краткости мы называем букву чётной, если её номер чётен, и нечётной — если номер нечётен.) Будем решать задачу от противного. Предположим, что требуемая последовательность существует. Всего в сложении участвуют 52 буквы. Пар букв одинаковой и различной чётности должно быть одинаковое количество, а именно 13 (так как в результате сложения должно получиться 13 чётных и 13 нечётных букв). Пары букв различной чётности включают в себя 26 букв. Оставшиеся 26 букв входят в 13 пар букв одинаковой чётности. Однако, 13 пар букв одинаковой чётности не могут содержать одинаковое количество чётных и нечётных букв (так как 13 — нечётное число). Полученное противоречие доказывает утверждение пункта б).

9.2. В этой задаче условимся писать $a \equiv b$, если числа a и b имеют одинаковые остатки при делении на 33. Пусть n — номер первой буквы искомой последовательности. Эту букву указанное число раз прибавили к букве К, в результате получили букву А. Запишем соответствующее уравнение:

$$12 + 1949^{1999} \cdot n \equiv 1. \quad (1)$$

Имеем следующую цепочку соотношений:

$$1949^{1999} \equiv 2^{5 \cdot 399 + 4} \equiv (-1)^{399} \cdot 16 \equiv -16 \equiv 17.$$

Уравнение (1) принимает вид: $12 + 17 \cdot n \equiv 1$, или

$$17 \cdot n \equiv 22. \quad (2)$$

Пользуясь арифметикой остатков, несложно составить следующую таблицу

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
17	1	18	2	19	3	20	4	21	5	22	6	23	7	24	8	25	9	26	10	27	11	28	12	29	13	30	14	31	15	32	16	0

Здесь под каждой буквой подписан остаток от деления на 33 результата умножения её номера на 17. Как видно из таблицы, уравнение 2 имеет *единственное* решение $n = 11$, т.е. первая буква искомой последовательности — **Й**. Аналогично могут быть найдены и остальные буквы. Искомая последовательность имеет вид

$$\text{ЙЩНЧЛЖАФ}. \quad (3)$$

Если последовательность (3) прибавить 17 раз к слову КРИПТОША, то получится слово АНАЛИТИК. Ясно, что если последовательность (3) прибавить к слову КРИПТОША 33 раза, то вновь получится КРИПТОША. Значит, если (3) прибавить 16 раз к слову АНАЛИТИК, то получится КРИПТОША. Получить слово КРИПТОША меньше чем за 16 прибавлений не удастся. Действительно, рассмотрим предпоследние буквы в этих словах и в последовательности (3): Ш, И, А. Очевидно, что для получения буквы Ш из буквы И необходимо букву А прибавить к И по крайней мере 16 раз.

Ответ: **ЙЩНЧЛЖАФ**; 16 раз.

9.3. В этой задаче условимся писать $a \equiv b$, если числа a и b имеют одинаковые остатки при делении на 1000. Для нахождения последней буквы исходного сообщения необходимо решить уравнение

$$77 \cdot n \equiv 355. \quad (1)$$

Здесь n — пока неизвестное трёхзначное число. Пусть $n = 100 \cdot a + 10 \cdot b + c$ (a, b, c — цифры). Тогда

$$(100 \cdot a + 10 \cdot b + c) \cdot 77 \equiv 355 \iff$$

$$\iff 7000 \cdot a + 700 \cdot b + 70 \cdot c + 700 \cdot a + 70 \cdot b + 7 \cdot c \equiv 355 \iff$$

$$\iff 700 \cdot (a + b) + 70 \cdot (b + c) + 7 \cdot c \equiv 355.$$

Значит, $c = 5$. Далее,

$$700 \cdot (a + b) + 70 \cdot b + 30 \equiv 0.$$

Отсюда $b = 1$. Тогда

$$700 \cdot a + 800 \equiv 0.$$

Значит, $a = 6$ и поэтому $n = 615$.

Уравнение (1) могло быть решено иначе. Умножив обе части (1) на 13, получим $1001 \cdot n \equiv 13 \cdot 355$. Ясно, что последние три цифры числа, стоящего в левой части равенства, совпадают с тремя последними цифрами самого числа n . Вычислив $13 \cdot 355 = 4615$, найдём $n = 615$. Теперь аналогично решаем уравнение (1), в правой части которого стоят другие трёхзначные цифровые группы шифрсообщения (850, 547, 550 и т. д.).

Искомая цифровая последовательность имеет вид

121332252610221801150111050615.

Ответ: КЛЮЧИШИФРАНАЙДЕН.

9.4. Сначала восстановим магический квадрат. Сумма чисел во всех клетках квадрата равна $1 + 2 + \dots + 16 = \frac{16 \cdot 17}{2} = 136$, значит, в каждом столбце (а также в строке, на диагонали) сумма чисел составляет $136 : 4 = 34$. Попытаемся построить магические квадраты с суммой на линии, равной 34, и единицей в правом нижнем углу. Имеется несколько таких квадратов. Например,

4	10	7	13
5	15	2	12
9	3	14	8
16	6	11	1

10	5	11	8
6	9	7	12
3	4	14	13
15	16	2	1

12	2	5	15
7	13	10	4
9	3	8	14
6	16	11	1

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Расставляя буквы в соответствии с условием, только в одном случае, отвечающем четвёртому квадрату, получаем читаемый текст:

Ы	Р	Е	У
С	Т	Е	В
Ь	Т	А	Б
Е	В	К	П

П	Е	Р	Е
С	Т	А	В
Ь	Т	Е	Б
У	К	В	Ы

Ответ:

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

, ПЕРЕСТАВЬТЕ БУКВЫ.

9.5. Пусть $\angle AOB = \alpha$, $\angle COD = \beta$, $\angle AOE = \gamma$, r радиус окружности (см. рис. 30). Условие (4) задачи эквивалентно равенству

$$S_{ABE} + S_{CED} = S_{AED}.$$

С учётом выражений $S_{AOB} + S_{AOE} - S_{BOE} = S_{ABE}$ и $S_{EOD} + S_{OCD} - S_{COE} = S_{CED}$, это равенство можно записать в виде:

$$\begin{aligned} r^2(\sin \alpha + \sin \gamma) - r^2 \sin(\alpha + \gamma) + r^2(\sin \beta + \sin \gamma) - r^2 \sin(180^\circ - \gamma + \beta) = \\ = 2r^2 \sin \gamma \iff \sin \alpha + \sin \beta = \sin(\alpha + \gamma) + \sin(\gamma - \beta) \iff \\ \iff (1 - \cos \gamma) \cdot \sin \alpha + (1 + \cos \gamma) \cdot \sin \beta = \sin \gamma \cdot (\cos \alpha + \cos \beta). \quad (1) \end{aligned}$$

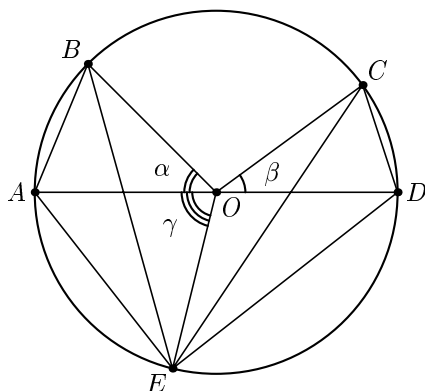


Рис. 30

Без ограничения общности можно считать, что $\gamma \leq 90^\circ$. Далее, поскольку координаты точки E — целые числа, меньшие 5, могут иметь место три случая.

Случай 1. $\sin \gamma = 1$. Равенство (1) примет вид: $\sin \alpha + \sin \beta = \cos \alpha + \cos \beta$. Это даёт два варианта расположения точек: 1) $B(-3; 4)$, $C(4; 3)$, $E(0; -5)$; 2) $B(-4; 3)$, $C(3; 4)$, $E(0; -5)$.

Случай 2. $\sin \gamma = \frac{3}{5}$, $\cos \gamma = \frac{4}{5}$. Из (1) получаем: $\sin \alpha + 9 \cdot \sin \beta = 3 \cdot \cos \alpha + 3 \cdot \cos \beta$. Последнее равенство невозможно, так как правая часть равенства строго меньше 6, а левая часть равенства не меньше, чем $\frac{3}{5} + 9 \cdot \frac{3}{5} = 6$.

Случай 3. $\sin \gamma = \frac{4}{5}$, $\cos \gamma = \frac{3}{5}$. Равенство (1) запишется в виде: $\sin \alpha + 4 \cdot \sin \beta = 2 \cdot \cos \alpha + 2 \cdot \cos \beta$. Это равенство невозможно, так как $\sin \alpha + 4 \cdot \sin \beta \geq \frac{3}{5} + 4 \cdot \frac{3}{5}$ и $2 \cdot \cos \alpha + 2 \cdot \cos \beta \leq 2 \cdot \frac{4}{5}$.

Ответ: 1) $B(-3; 4)$, $C(4; 3)$, $E(0; -5)$; 2) $B(-4; 3)$, $C(3; 4)$, $E(0; -5)$.

9.6. Выделим под знаками радикала полный квадрат:

$$\sqrt{-\left(x + \frac{1}{2}\right)^2 + a^2} \geq 1 + \sqrt{-\left(x - \frac{1}{2}\right)^2 + 4}.$$

В результате замены $x + \frac{1}{2} = t$ неравенство примет вид:

$$\sqrt{a^2 - t^2} \geq 1 + \sqrt{4 - (t - 1)^2}.$$

Для решения последнего неравенства изучим взаимное расположение на плоскости (t, y) полуокружностей

$$y_1(t) = \sqrt{a^2 - t^2} \text{ (центр } (0; 0), \text{ радиус } |a|)$$

и

$$y_2(t) = 1 + \sqrt{4 - (t - 1)^2} \text{ (центр } (1; 1), \text{ радиус } 2).$$

Точки пересечения полуокружностей (если этих точек две) расположены симметрично относительно прямой, соединяющей их центры. В данном случае это прямая $y = t$. Рассмотрим вначале качественно возможные взаимные расположения полуокружностей. Если величина $|a|$ мала, то полуокружности не пересекаются (рис. 31). С ростом $|a|$ у

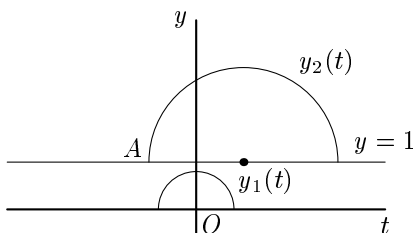


Рис. 31

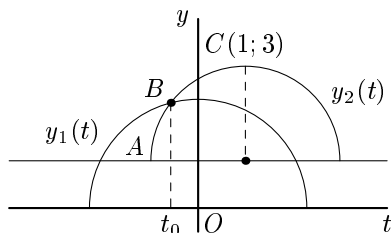


Рис. 32

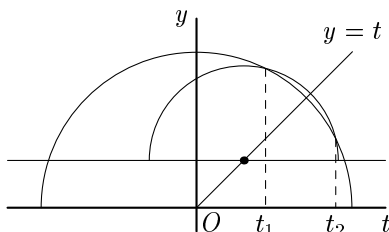


Рис. 33

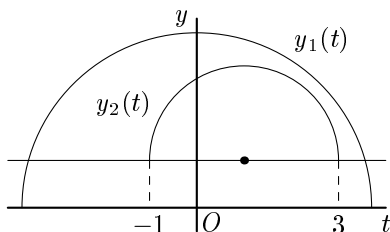


Рис. 34

полуокружностей появляется общая точка B (с абсциссой t_0) (рис. 32). При дальнейшем увеличении $|a|$ точка пересечения B «движется» по окружности $y_2(t)$ по часовой стрелке. Значение $|a|$, при котором точка B

совпадает с точкой $C(1; 3)$, является критическим, так как при дальнейшем увеличении $|a|$ полуокружности имеют две точки пересечения (рис. 33). И, наконец, при $|a|$, превосходящем некоторое значение, полуокружности вновь не пересекаются (рис. 34). Рассмотрим указанные случаи подробно.

Случай 1. При $|a| < OA = \sqrt{2}$ полуокружности не пересекаются, и неравенство решений не имеет (рис. 31).

Случай 2. Полуокружности имеют единственную точку пересечения с абсциссой $t_0 < 1$ (рис. 32). При этом $\sqrt{2} \leq |a| < OC = \sqrt{10}$. Решение неравенства имеет вид $t \in [-1; t_0]$.

Случай 3. Полуокружности имеют две точки пересечения (рис. 33). При этом $\sqrt{10} \leq |a| \leq 2 + \sqrt{2}$. Решение неравенства имеет вид $t \in [-1; t_1] \cup [t_2; 3]$. При $|a| = 2 + \sqrt{2}$ имеет место касание полуокружностей (можно считать, что точек пересечения по-прежнему две, но просто они совпадают).

Случай 4. При $|a| > 2 + \sqrt{2}$ полуокружности вновь не имеют общих точек, и $t \in [-1; 3]$.

Найдём теперь точные выражения для абсцисс t_1, t_2 точек пересечения окружностей. Эти величины удовлетворяют системе

$$\begin{cases} t^2 + y^2 = a^2 \\ (t-1)^2 + (y-1)^2 = 4 \end{cases} \iff \begin{cases} t^2 + y^2 = a^2 \\ t + y = \frac{a^2 - 2}{2} \end{cases} \implies t^2 + \left(\frac{a^2 - 2}{2} - t \right)^2 = a^2.$$

Решая квадратное уравнение, находим

$$t_{1,2} = \frac{a^2 - 2 \mp \sqrt{12 \cdot a^2 - a^4 - 4}}{4}.$$

Итак, решение неравенства имеет вид:

1. $|a| < \sqrt{2} \implies$ решений нет.
2. $\sqrt{2} \leq |a| < \sqrt{10} \implies t \in [-1; t_1]$.
3. $\sqrt{10} \leq |a| \leq 2 + \sqrt{2} \implies t \in [-1; t_1] \cup [t_2; 3]$.
4. $|a| > 2 + \sqrt{2} \implies t \in [-1; 3]$.

Переходя к переменной x и используя явные выражения для t_1, t_2 , получаем окончательный

Ответ:

1. $|a| < \sqrt{2} \implies$ решений нет.
2. $\sqrt{2} \leq |a| < \sqrt{10} \implies x \in \left[-\frac{3}{2}; \frac{a^2 - 2 - \sqrt{12 \cdot a^2 - a^4 - 4}}{4}\right]$.
3. $\sqrt{10} \leq |a| \leq 2 + \sqrt{2} \implies$
 $x \in \left[-\frac{3}{2}; \frac{a^2 - 2 - \sqrt{12 \cdot a^2 - a^4 - 4}}{4}\right] \cup \left[\frac{a^2 - 2 + \sqrt{12 \cdot a^2 - a^4 - 4}}{4}; \frac{5}{2}\right]$.
4. $|a| > 2 + \sqrt{2} \implies x \in \left[-\frac{3}{2}; \frac{5}{2}\right]$.

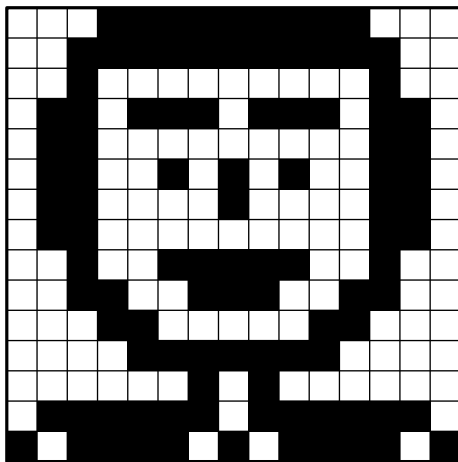


Рис. 36

тельно, для решения задачи перебором (а для таких сложных уравнений это зачастую единственный способ найти ответ) мы должны испытать каждый из этих наборов, т. е. провести вычисления 64 раза. Однако перебор перебору рознь! Обратите внимание на тот факт, что левая и правая части зависят только от трёх переменных. Значит, чтобы вычислить все значения, скажем, левой части потребуется только 2^3 вычислений. Найдя все значения левой и правой частей, немедленно получаем ответ. Заметим, что для этого пришлось провести вычисления (см. таблицы) всего 16, а не 64 раза.

x	y	z	левая часть	u	v	w	правая часть
0	-1	1	2	0	0	0	0
0	-1	2	2	0	0	1	3
0	2	1	-2	0	3	0	3
0	2	2	-1	0	3	1	3
1	2	1	2	-1	0	0	1
1	-1	2	2	-1	0	1	1
1	2	1	1	-1	3	0	-1
1	2	2	2	-1	3	1	-2

Ответ: $(0, -1, 1, -1, 3, 1)$, $(0, 2, 1, -1, 3, 1)$, $(0, 2, 2, -1, 0, 0)$, $(0, 2, 2, -1, 3, 0)$, $(1, -1, 1, -1, 3, 1)$, $(1, 2, 1, -1, 0, 1)$.

10.3. При зашифровании буква, содержащаяся в n -й строке и m -м столбце таблицы, заменяется буквой, содержащейся в m -й строке и n -м столбце. Такая замена соответствует симметрии относительно главной диагонали таблицы (главная диагональ образована клетками, у каждой

из которых номер строки и столбца совпадают). Запишем друг под другом буквы исходного слова и буквы, полученные после зашифрования:

H A N D W R I T I N G

H A V W D E M T M V P

Буквы H, A, T лежат на главной диагонали. Следующие пары букв симметричны относительно главной диагонали: (N, V), (D, W), (R, E), (I, M), (P, G). Тот факт, что некоторая буква, например G, содержится в n -й строке и m -м столбце, будем записывать так: $G = (n, m)$. Решение задачи представим в виде несложных вытекающих друг из друга утверждений.

1. $T = (4, 4)$. Если бы было $T = (5, 5)$, то ключевое слово состояло бы из шести последних букв алфавита и буква H не попадала бы на главную диагональ.

2. Используя симметрию, находим $N = (1, 5)$, $D = (2, 5)$.

3. $A = (2, 2)$. Это следует из того, что $D = (2, 5)$.

4. R входит в ключевое слово. Если это не так, то или $R = (4, 2)$, или $R = (4, 3)$. Оба варианта невозможны, так как R и E симметричны.

Итак, таблица имеет вид

	1	2	3	4	5
1		IV	III	II	N
2	IV	A	B	C	D
3	III			I	
4	II		I	T	U
5	V	W	X	Y	Z

Разместим пары (R, E), (I, M), (P, G). В таблице остались свободными 4 пары симметричных клеток. Они отмечены римскими цифрами I, II, III, IV.

5. Пара (P, G) в клетках I, I располагаться не может, так как в алфавите между D и G располагаются две буквы. В клетках II, II она также не может содержаться, так как буква G (из-за того что $D = (2, 5)$) должна находиться в третьей строке.

6. Пара (M, I) в клетках I, I располагаться не может, так как в алфавите между I и M есть только две буквы. В клетках III, III пара (M, I) также не может содержаться, так как иначе в ключевое слово вошли бы E, F, G, H. Этого не может быть, из-за того что ключевое слово состоит из 6 букв и по доказанному содержит R, N, а также M или I.

7. Пара (R, E) в клетках I, I располагаться не может, так как R входит в ключевое слово. В клетках II, II эта пара также не может содержаться, так как E следует сразу за D.

Возможные расположения пар отражены в таблице:

	I	II	III	IV
(P, G)	—	+	+	+
(M, I)	—	+	—	+
(R, E)	—	—	+	+

Имеются, таким образом, три варианта.

а) (P, G) — III, III; (M, I) — II, II; (R, E) — IV, IV.

б) (P, G) — IV, IV; (M, I) — II, II; (R, E) — III, III.

в) (P, G) — II, II; (M, I) — IV, IV; (R, E) — III, III.

8. Непосредственной проверкой легко убедиться, что таблица не может быть заполнена в соответствии с вариантом а).

9. С учётом б) таблица примет вид

	1	2	3	4	5
1		P	R	I	N
2	G	A	B	C	D
3	E				
4	M			T	U
5	V	W	X	Y	Z

Ключевое слово может быть одним из следующих:

OPRING, OGRINP, QPRING, QGRINP, SPRING, SGRINP.

10. Для варианта в) получим

	1	2	3	4	5
1		I	R	G	N
2	M	A	B	C	D
3	E				
4	P	Q	S	T	U
5	V	W	X	Y	Z

Ключевое слово может быть одним из следующих:

HIRGNM, HMRGNI, KIRGNM, KMRGNI, LIRGNM, LMRGNI, OIRGNM, OMRGNI.

11. Из приведённых ключевых слов осмысленным (словом английского языка) является SPRING.

Ответ: SPRING.

10.4. Пусть T — период последовательности s_n ; тогда разность $x_{n+T} - x_n$ должна делиться на 10 при любых натуральных n . Имеем

$$x_{n+T} - x_n = \frac{(n+T)(n+T+1)}{2} - \frac{n(n+1)}{2} = \frac{T(T+2n+1)}{2}.$$

Ясно, что $T = 20$ является периодом. Докажем, что любой другой период не меньше, чем 20. При $n = 1$ находим

$$x_{1+T} - x_1 = \frac{T(T+3)}{2}.$$

Правая часть делится на 10 при $T = 5, 12, 17$. Однако при этих значениях T разность

$$x_{2+T} - x_2 = \frac{T(T+5)}{2}$$

на 10 не делится. Следовательно, $T = 20$ — наименьший период последовательности.

Используя соотношение $x_n = x_{n-1} + n$, находим члены последовательности s_n :

$$1, 3, 6, 0, 5, 1, 8, 6, 5, 5, 6, 8, 1, 5, 0, 6, 3, 1, 0, 0, 1, 3, 6, 0, 5, \dots$$

Искомые подстановки имеют вид

$$p_1 = (1360524789), \quad p_2 = (1865023479), \quad p_3 = (1506324789), \\ p_4 = (1023456789), \quad p_5 = p_1, \quad p_6 = p_2.$$

Наименьший период последовательности p_n равен 4.

Ответ: а) 20; б) 4.

10.5. Ответ: ХОРОШО СКАЗАЛ КОТ И НА ЭТОТ РАЗ ОН ИСЧЕЗ ПОСТЕПЕННО НАЧИНАЯ С КОНЧИКА ХВОСТА И КОНЧАЯ УЛЫБКОЙ КОТОРАЯ ЕЩЕ БЫЛА ВИДНА НЕКОТОРОЕ ВРЕМЯ.

10.6. Пусть $f(x) = x^5 + 5x^3 + 5x - 1$. Тогда $f'(x) = 5x^4 + 15x^2 + 5 > 0$ для всех x , следовательно, функция $f(x)$ строго возрастает на всей числовой оси и уравнение $f(x) = 0$ имеет ровно один корень. (Поскольку $f(0) = -1$ и $f(1) = 10$, этот корень лежит на интервале $(0; 1)$.) Будем искать корень в виде $x = u + v$. Возведём это равенство в пятую степень:

$$x^5 = (u + v)^5 = u^5 + 5u^4v + 10u^3v^2 + 10u^2v^3 + 5uv^4 + v^5 = \\ = u^5 + v^5 + 5uv(u^3 + v^3) + 10u^2v^2(u + v).$$

Сумму кубов $u^3 + v^3$ запишем в виде $(u + v)((u + v)^2 - 3uv)$ и с учётом того, что $x = u + v$, получим $x^5 = u^5 + v^5 + 5uvx(x^2 - 3uv) + 10u^2v^2x$. Окончательно $x^5 - 5uvx^3 + 5u^2v^2x - (u^5 + v^5) = 0$. Сравнивая эту запись с исходным уравнением, получаем

$$\begin{cases} uv = -1, \\ u^5 + v^5 = 1. \end{cases}$$

Возведём первое уравнение системы в 5-ю степень и выполним замену $u^5 = a$, $v^5 = b$. Тогда

$$\begin{cases} ab = -1, \\ a + b = 1. \end{cases}$$

Отсюда $a = \frac{-1 + \sqrt{5}}{2}$, $b = \frac{-1 - \sqrt{5}}{2}$.

Ответ: $x = \sqrt[5]{\frac{-1 + \sqrt{5}}{2}} + \sqrt[5]{\frac{-1 - \sqrt{5}}{2}}$.

11.1. Пусть длина текста равна L . Пусть символ встречается в тексте x раз. Задачу можно переформулировать так: найти наименьшее натуральное число L , для которого существует такое натуральное число x , что

$$\frac{10,5}{100} < \frac{x}{L} < \frac{11}{100}.$$

При решении задачи некоторые участники руководствовались, вообще говоря, ошибочным утверждением, что чем меньше x , тем меньше соответствующее L . Однако при малых x это действительно так. При $x = 1$ не существует удовлетворяющего неравенству натурального L . При $x = 2$ находим $L = 19$. Из неравенства $L \geq 100x/11$ заключаем, что $L > 19$ при $x \geq 3$.

Ответ: 19.

11.2. Подсчитаем число появлений каждой из букв в шифртекстах. Первый текст: Б, Г, П, Р, Ы, Ю — 1 раз; А, Д, З, М, Т, Ч — 2 раза; Л — 3 раза; Н, С — 4 раза; Е, И — 6 раз; В — 7 раз; О — 12 раз. Второй текст: Г, И, К, С, Т, Ч — 1 раз; А, Б, Е, У, Х, Я — 2 раза; М — 3 раза; Ш, Ъ — 4 раза; Ж, Э — 6 раз; Р — 7 раз; В — 12 раз. Если текст получен перестановкой букв, то частоты встречаемости букв в нём должны быть характерны для текстов на русском языке. Во втором тексте отсутствует буква О, одна из самых частых букв. Поэтому можем сделать вывод, что первый текст получен перестановкой, а второй — заменой букв в исходном тексте.

При использовании шифра замены число вхождений буквы в исходный текст совпадает с числом вхождений заменяющей её буквы в шифрованный текст. Поэтому заключаем, что буква О заменялась на В, В — на Р, Л — на М. Кроме того, буквы Е и И заменялись на Ж и Э либо на Э и Ж, Н и С — на Ш и Ъ либо на Ъ и Ш.

Первая буква второго текста — Р; ей должна соответствовать буква В первого текста. Поэтому длина участков, на которые разбивался исходный текст при шифровании перестановкой, не менее пяти. Тогда в первый участок первого текста войдёт буква О, которой должна соответствовать буква В во втором тексте, поэтому длина участков не менее 6. Предположив, что длина участков равна 6, получаем, что внутри участка буквы переставлялись по схеме 1234546-546213, что приводит к осмысленному варианту восстановления исходного текста: В БЕЗМОЛВИИ САДОВ ВЕСНОЙ ВО МГЛЕ НОЧЕЙ ПОЕТ НАД РОЗОЮ ВОСТОЧНЫЙ СОЛОВЕЙ.

В названии произведения и фамилии автора стали известными почти все буквы: СОЛОВЕЙ РОЗА П??? И Н. Знаками вопроса обозначены

буквы, которые не встретились в исходном тексте. По смыслу легко догадаться, что автор — ПУШКИН.

11.3. Заметим, что после перепутывания проводков внутри каждой пятизначной комбинации число единиц не изменилось. Подпишем под каждой буквой полученного сообщения те буквы, которые представляют пятизначной комбинацией с тем же числом единиц:

Э	А	В	Щ	О	Щ	И
Ю	Б	З	З	З	Б	
Ы	Д	Л	Л	Л	В	
Ч	И	Н	Н	Н	Д	
П	Р	О	У	О	Р	
		У	Х	У		
		Х	Ц	Х		
		Ц	Щ	Ц		
		Ъ	Ъ	Ъ		
		Ь	Ь	Ь		

Выбирая по одной букве в каждом столбце таблицы, находим единственное «читаемое» слово ПАРОХОД.

Ответ: ПАРОХОД.

11.4. Раскрасим клетки таблицы в три цвета (назовём их условно 1, 2 и 3), как показано на рис. 37. Клетки, образующие линию, параллельную

1	2	3	1	2	3	1	2
3	1	2	3	1	2	3	1
2	3	1	2	3	1	2	3
1	2	3	1	2	3	1	2
3	1	2	3	1	2	3	1
2	3	1	2	3	1	2	3
1	2	3	1	2	3	1	2
3	1	2	3	1	2	3	1

Рис. 37

главной диагонали, окрашены в один цвет. Заметим, что прямоугольник 1×3 всегда покрывает клетки трёх разных цветов. Следовательно, «хорошие» клетки (если вообще таковые имеются) обязательно имеют цвет 1, потому что клеток цвета 1 на одну больше, чем клеток цвета 2 и цвета 3. По соображениям симметрии при повороте таблицы на 90° относительно её центра «хорошие» клетки переходят в «хорошие». Линии клеток цвета 1 до и после поворота указаны на рис. 38, а.

Ясно, что «хорошими» могут быть только те (четыре) клетки, в которых эти линии пересекаются. Непосредственной проверкой (рис. 38, б) убеждаемся, что найденные клетки «хорошими» являются. Таким обра-

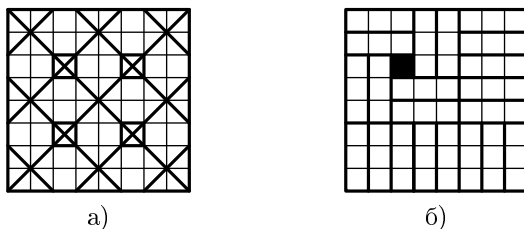


Рис. 38

зом, найдено ключевое слово РУСЬ. Укажем, как преобразуются буквы исходного сообщения:

	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
Р	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п
У	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т
С	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р
Ь	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы

Расшифрование сообщения осуществляется следующим образом. Пусть, например, девятая по счёту буква зашифрованного сообщения — д. Находим остаток от деления её номера на 4. Остаток равен 1. Находим в строке, начинающейся с заглавной Р, нашу д, тогда над ней в первой строке стоит искомая буква исходного сообщения — у. В результате расшифрования получаем

и	с	т	и	н	а	н	е
р	о	ж	д	а	е	т	с
я	и	■	з	и	■	с	т
и	н	ы	т	ч	к	и	с
т	и	н	а	р	о	ж	д
а	е	■	т	с	■	я	и
з	о	ш	и	б	о	к	т
ч	к	к	а	п	и	ц	а

Рис. 39

Ответ. а) «Хорошие» клетки указаны символом ■ на рис. 39.

б) Ключевое слово — РУСЬ. Исходное сообщение: Истина не рождается из истины. Истина рождается из ошибок. Капица

11.5. Покажем вначале, что каждый прямоугольник в своём углу может быть развёрнут на 90° . Рассмотрим, например, левый верхний прямоугольник (рис. 40). Как бы при этом ни располагались в углах другие

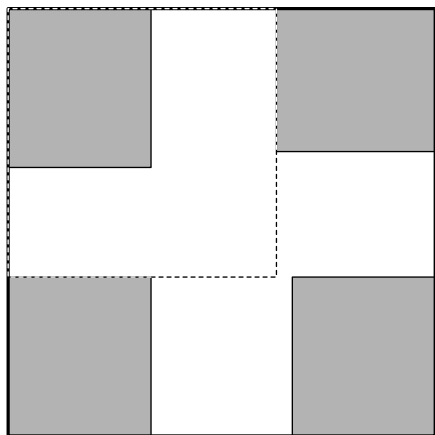


Рис. 40

прямоугольники, он, не задевая их, может перемещаться внутри указанного пунктиром квадрата со стороной 169 мм. Совместим центры прямоугольника и «пунктирного» квадрата. Используя теорему Пифагора, можно показать, что прямоугольник может вращаться вокруг центра, оставаясь при этом внутри «пунктирного» квадрата. Сдвинем теперь прямоугольники к центру квадрата, развернув их предварительно таким образом, чтобы они образовали квадрат со стороной 190 мм (рис. 41). Половина диагонали этого квадрата $d = 190 \cdot \sqrt{2}/2$, что меньше, чем 134,5 мм. Следовательно, мы можем повернуть образованный из прямоугольников квадрат относительно центра на 180° и тем самым поменять место расположения каждого прямоугольника на симметричное относительно центра квадрата.

Ответ: можно.

11.6. Используя в правой части первого уравнения исходной системы

$$\begin{cases} \left(\left| y + x - \frac{5 + \sqrt{3}}{2} \right| + |x - 1| \right)^2 = \\ = (|2x - \sqrt{2y} - 2| + |y - 1| + 1) \cdot (1 - |y - 1| - |2x - \sqrt{2y} - 2|), \\ x^2 + y^2 = 2(x + y) - 1 \end{cases}$$

формулу разности квадратов, преобразуем его к виду

$$\left(\left| y + x - \frac{5 + \sqrt{3}}{2} \right| + |x - 1| \right)^2 + (|2x - \sqrt{2y} - 2| + |y - 1|)^2 = 1.$$

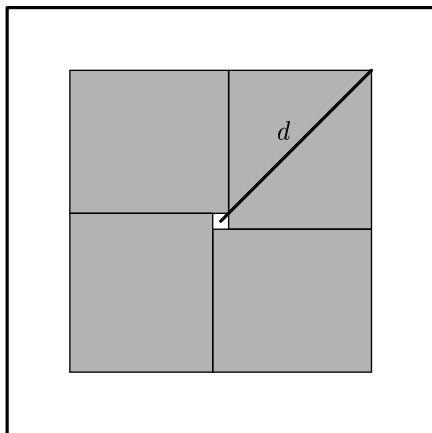


Рис. 41

Последнее уравнение системы $(x - 1)^2 + (y - 1)^2 = 1$ для наглядности запишем в виде

$$(0 + |x - 1|)^2 + (0 + |y - 1|)^2 = 1.$$

Следовательно, для доказательства совместности системы необходимо потребовать, чтобы выполнялись условия

$$2x - \sqrt{2y} - 2 = 0, \quad y + x - \frac{5 + \sqrt{3}}{2} = 0.$$

Отсюда $x = \frac{\sqrt{3}}{2} + 1$, $y = \frac{3}{2}$. Непосредственной подстановкой убеждаемся, что эта пара является решением исходной системы (отметим, что в данном случае достаточно было подставить эти числа лишь во второе уравнение).

Ответ: $x = \frac{\sqrt{3}}{2} + 1$, $y = \frac{3}{2}$.

12.1. У первого криптографа каждый из 50 символов ключа выбирается из 7 возможных значений. Значит, всего имеется $7 \cdot 7 \cdot \dots \cdot 7 = 7^{50}$ различных вариантов выбора ключа шифра. Аналогично у второго криптографа всего имеется 10^{43} различных вариантов выбора ключа. Задача сводится к сравнению чисел 7^{50} и 10^{43} . Это можно сделать несколькими способами:

а) $2^{25} = 2^{10} \cdot 2^{10} \cdot 2^5 > 10^3 \cdot 10^3 \cdot 32 > 10^7$, следовательно,

$$7^{50} = 49^{25} < 50^{25} = \frac{100^{25}}{2^{25}} < \frac{10^{50}}{10^7} = 10^{43};$$

б) $7^7 < 50 \cdot 50 \cdot 50 \cdot 7 = 125 \cdot 7 \cdot 10^3 < 900 \cdot 10^3 < 10^6$, следовательно,

$$7^{50} = 7^{7 \cdot 7 + 1} < (10^6)^7 \cdot 10 = 10^{43};$$

в) некоторые школьники использовали оценку $\frac{10}{7} = 1,42 \dots > 1,4$.

Основные недостатки в работах:

— часто сравнивали числа 350 и 430;

— использовали приближённые равенства без оценки сверху или снизу.

Ответ: шифр второго криптографа содержит больше ключей.

12.2. Запишем полученное сообщение в двоичном виде:

Т	10010
Е	00101
Ы	11011
Е	00101
У	10011
Т	10010
А	00000
Ц	10110

Если провода замкнуты, то по ним передаются одинаковые символы (0 или 1), т. е. замкнутым проводам соответствуют одинаковые столбцы цифр. Легко видеть, что это первый и четвёртый столбцы. Значит, во 2-м, 3-м и 5-м столбцах все символы правильные, кроме того, если в 1 и 4 столбцах стоят нули, то это тоже правильные знаки. Если в 1-м и 4-м столбцах стоят единицы, то возможны три варианта для знаков x и y этих столбцов:

10
01
11

Каждому варианту соответствует своя буква:

$x00y0$
00101
$x10y1$
00101
$x00y1$
$x00y0$
00000
$x01y0$

Заменяя каждый вариант на соответствующую букву, получим таблицу

Т		Ы		У	Т		Ц
Р	Е	Л	Е	Г	Р	А	Ж
В		Щ		С	В		Ф

Выбирая по одной букве в каждом столбце таблицы, находим «читаемое» слово ТЕЛЕГРАФ.

Ответ: ТЕЛЕГРАФ.

12.3. Задача имеет много решений. Приведём два решения, одно из которых структурное, а второе самое короткое из найденных участниками олимпиады.

Первое решение. Занумеруем залы в следующем порядке:

1	2	3
4	5	6
7	8	9

Если использовать лампу 3 раза (ллл), то Аладдин окажется в одном из залов 4, 5, 7, 8 независимо от того, где он находился первоначально:

1	2	3
•	•	6
•	•	9

Применив 3 раза кольцо и три раза лампу (ккк ллл), Аладдин окажется в одном из залов 4, 5, 7:

1	2	3
•	•	6
•	8	9

Повторив комбинацию (ккк ллл) ещё два раза, Аладдин окажется последовательно в одном из залов 5 или 7, а затем в зале 5:

1	2	3	1	2	3
4	•	6	4	•	6
•	8	9	7	8	9

Таким образом, последовательность действий

ллл ккк ллл ккк ллл ккк ллл

приводит к цели.

Второе решение. К цели приводит последовательность из 13 ходов:

ллл к л ккк лл к лл

Ответ: например,

ллл ккк ллл ккк ллл ккк ллл

или

ллл к л ккк лл к лл.

12.4. В первую строку вписано менее 10 букв, а далее буквы выписываются по алфавиту. Но А — первая буква алфавита. Значит А стоит в первой строке. Длины слов АСТРАХАНЬ и БУТЕРБРОД одинаковы, значит, Б тоже находится в первой строке. При умножении на 9 нет дополнительного переноса старшего разряда. Поэтому буква А стоит в первом столбце, а буква Б стоит в 9-м столбце. Буквы А и Б стоят в первой строке. Номера строк у букв А и Б, Б и Х, А и Р, Р и Е совпадают:

А	С	Т	Р	А	Х	А	Н	Ь
Б	У	Т	Е	Р	Б	Р	О	Д

Значит, буквы Р, Х и Е стоят в первой строке.

А	С	Т	Р	А	Х	А	Н	Ь
1	.	.	.	1	x	1	.	.
9								
9	.	.	.	p	9	p	.	.
Б	У	Т	Е	Р	Б	Р	О	Д

Пусть x , p — номера столбцов букв Х и Р. При умножении цифры 1 (соответствующей третьей по счёту букве А в слове АСТРАХАНЬ) на 9 либо нет переноса, тогда $9 \cdot x = \dots 9$, либо есть перенос единицы, тогда $9 \cdot x + 1 = \dots 9$. В первом случае получаем $x = 1$. Но в первом столбце первой строки уже стоит А, следовательно, такое невозможно. Во втором случае $x = 2$, откуда при дальнейшем умножении на 9 получаем, что $p = 0$.

А	С	Т	Р	А	Х	А	Н	Ь
1	.	.	0	1	2	1	.	.
9								
9	.	.	1	0	9	0	.	.
Б	У	Т	Е	Р	Б	Р	О	Д

Умножая далее, получим что Е стоит в первом столбце, что опять-таки невозможно, так как в первом столбце первой строки уже стоит А.

Ответ: нельзя.

12.5. Текст начинается с буквы Т, отмеченной чёрным кружком (хотя начинать читать можно с любого места). Листок с текстом следует развернуть так, чтобы буква Т приняла своё «естественное вертикальное» положение. Буква, оказавшаяся от Т справа (буква Е), будет второй буквой искомого текста. Справа от повернутой нужным образом буквы Е находится К, и т. д. Путь, вдоль которого прочитывается текст, указан на рис. 42.

Ответ: ТЕКСТ ЧИТАЕТСЯ ВДОЛЬ ПО КРИВОЙ ПРИДУМАННОЙ ИТАЛЬЯНСКИМ МАТЕМАТИКОМ ПЕАНО.

Т	С	В	О	Н	О	К	Р
Е	У	В	А	Б	Н	В	И
И	Г	К	Г	У	Н	О	И
Г	Е	О	Г	И	И	А	Н
М	Н	Е	О	У	О	И	И
О	У	А	Н	Н	Н	У	Г
Т	И	Г	У	И	К	А	Ч
А	И	Н	М	М	С	Н	В

Рис. 42

Замечание. В обыденном представлении «кривая» — это «тонкий штрих, вьющийся по плоскости». Рассмотрим, например, функции $x(t) = \sin t$, $y(t) = \cos t$. Если параметр t пробегает отрезок от 0 до 2π , то точка с координатами $(x(t), y(t))$ пробегает на декартовой плоскости окружность единичного радиуса с центром в начале координат ($x^2(t) + y^2(t) = 1$). Тригонометрические функции задают отображение отрезка $[0; 2\pi]$ в декартову плоскость. Это отображение *непрерывно* в том смысле, что если t «плавно» изменяется от 0 до 2π , то точка с координатами $(x(t), y(t))$ «плавно» пробегает всю окружность.

В 1890 г. итальянский математик Дж. Пеано (1862–1943) привёл поразительный пример, опровергающий представление о кривой как о «тонкой нити». Построенная им непрерывная кривая полностью заполняет квадрат (когда точка пробегает отрезок от 0 до 1, соответствующая точка на декартовой плоскости проходит через все точки квадрата). Вкратце построение можно описать так. Пусть A — точка отрезка (см. рис. 43). Поставим ей в соответствие точку квадрата. Разобьём отрезок и квадрат пополам (линия 1). Точка A оказалась в правой части

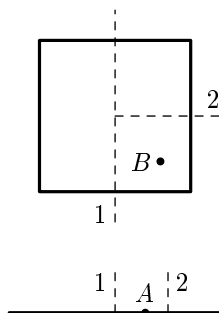


Рис. 43

отрезка, и поэтому берём правую часть квадрата. Половину отрезка, содержащую A , и правую часть квадрата делим пополам (линия 2). Точка A оказалась слева от точки деления, поэтому берём нижнюю половину половины квадрата. Далее вновь делим пополам четверть отрезка, содержащую A , и соответствующую ей четверть квадрата, и т. п. Продолжив бесконечно этот процесс, получим последовательность отрезков, стягивающихся к точке A , и соответствующую ей последовательность прямоугольников, стягивающихся к точке квадрата B . Каждой точке квадрата при таком отображении будет соответствовать, по крайней мере, одна точка отрезка.

Разбив отрезок на несколько равных частей и отобразив указанным способом точки разбиения, получим кривую наподобие кривой, приведённой на рис. 42.

12.6. Пусть дан отрезок AB . С помощью только циркуля можно построить такую точку C , что $AC = 2 \cdot AB$ (точка B — середина AC), используя свойства правильного шестиугольника.

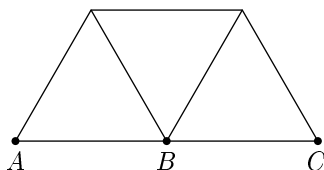


Рис. 44

Пересекая окружность радиуса AB с центром в точке A окружностью радиуса $2AB$ с центром в точке C , находим точку D . Находим

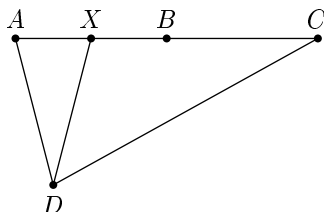


Рис. 45

пересечение окружности радиуса AB с центром в точке D с отрезком AB . Это искомая точка, так как треугольник ADX подобен треугольнику ADC с коэффициентом подобия 2.

12.7. а) Большинство участников с этой задачей справились. Для её решения надо рассмотреть последовательность степеней двойки и обнаружить закономерность: $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = \dots 6$, $2^5 = \dots 2$ и т. д.

Последние цифры 2, 4, 8, 6 периодически повторяются. Таким образом, $2^{2002} = (2^{500})^4 \cdot 2^2 = (\dots 6)^4 \cdot 4 = \dots 6 \cdot 4 = \dots 4$. Последняя цифра — 4.

б) Для решения задачи следует рассмотреть остатки степеней двойки при делении на 1000, т. е. три последние цифры. Предложим несколько решений данной задачи.

Первое решение. Некоторые школьники, используя умножение на 2, получили степени двойки до 2^{103} включительно и при этом заметили, что $2^3 = 8$ и $2^{103} = \dots 008$, а перед этим было число $2^{102} = \dots 504$. Значит, последовательность остатков 008, \dots , 504 длины 100 повторяется, начиная с 2^3 . Таким образом, на число 2002 приходится остаток 504.

Второе решение. Легко получить следующие соотношения:

$$2^{10} = 1024,$$

$$2^{20} = \dots 24 \cdot \dots 24 = \dots 576,$$

$$2^{40} = \dots 576 \cdot \dots 576 = \dots 776,$$

$$2^{80} = \dots 776 \cdot \dots 776 = \dots 176,$$

$$2^{160} = \dots 176 \cdot \dots 176 = \dots 976,$$

$$2^{320} = \dots 976 \cdot \dots 976 = \dots 576.$$

Выписав 4 произведения трёхзначных чисел, дальше сразу получаем

$$2^{640} = \dots 776,$$

$$2^{1280} = \dots 176.$$

Отсюда $2^{2002} = 4 \cdot 2^{1280} \cdot 2^{640} \cdot 2^{80} = 4 \cdot \dots 176 \cdot \dots 176 \cdot \dots 776 = 4 \cdot \dots 976 \cdot \dots 776 = \dots 504$.

В последней строке пользуемся тем, что $176^2 = \dots 976$.

Третье решение. Несложно вычислить следующее:

$$2^{10} = \dots 024,$$

$$2^{100} = ((\dots 24)^3)^3 \cdot \dots 24 = \dots 376,$$

$$376 \cdot 376 = \dots 376,$$

$$2^{2002} = 2^2 \cdot (2^{100})^{20} = 4 \cdot \dots 376 = \dots 504.$$

Общий подход. Имеет место соотношение $2^{2^k} \cdot 2^{2^k} = 2^{2^{k+1}}$. Следовательно, путём нескольких умножений трёхзначных чисел можно получить

$$2^{2^0} = 2, \quad 2^{2^1} = 4, \quad 2^{2^2} = 16, \quad 2^{2^3} = 256, \quad 2^{2^4} = \dots 536, \quad 2^{2^5} = \dots 296,$$

$$2^{2^6} = \dots 616, \quad 2^{2^7} = \dots 456, \quad 2^{2^8} = \dots 936, \quad 2^{2^9} = \dots 096, \quad 2^{2^{10}} = \dots 216$$

Раскладывая 2002 по степеням двойки:

$$2002 = 1024 + 512 + 256 + 120 + 64 + 16 + 2,$$

получим

$$2^{2002} = \dots 216 \cdot \dots 096 \cdot \dots 936 \cdot \dots 456 \cdot \dots 616 \cdot \dots 536 \cdot \dots 4.$$

Проведя несколько умножений, получим, что последние три цифры — 504.

Ответ: а) 4; б) 504.

13.1. Недостаток способа Ватсона состоит в том, что, перехватив сообщение $(A, E_B(m))$, злоумышленник C может заменить его на $(C, E_B(m))$, получив которое, B воспринимает его как первый шаг протокола передачи с уведомлением от C . Вычислив m , B затем уведомляет C о получении, посылая ему сообщение $(B, E_C(m))$. Из него C извлекает искомое m и от имени B уведомляет A о получении, посылая ему сообщение $(B, E_A(m))$.

Способ Холмса не позволяет злоумышленнику получить секретное сообщение m . В самом деле, получить его C может либо из перехваченных сообщений $E_B(A, m)$, $E_B(B, m)$, либо из направленного к нему сообщения $E_C(B, m)$. По $E_B(A, m)$ и $E_B(B, m)$ злоумышленнику невозможно найти m , поскольку для этого ему нужно решить сложную задачу обращения E_A или E_B . Исключая возможность сговора между B и C , считаем, что B «добровольно» не пошлёт к C сообщение $E_C(B, m)$. Значит, такое сообщение попадёт к C от B лишь в качестве уведомления о получении им сообщения $E_B(C, m)$. Такое сообщение к B может попасть лишь от C , который заменяет $E_B(A, m)$ на сообщение $E_B(C, m)$. По условию этого C также сделать не в состоянии.

13.2. Ключом шифра служит систематически перемешанный алфавит, записанный в квадратную таблицу. Такие алфавиты широко использовались в криптографии. Первые буквы алфавита составляли легко запоминаемое ключевое слово (в условии данной задачи это слово CODE), остальные же буквы следовали в их естественном порядке. Такое мнемоническое правило позволяло быстро восстановить ключ и произвести зашифрование или расшифрование.

	1	2	3	4	5
1	C	O	D	E	A
2	B	F	G	H	I
3	K	L	M	N	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Правило зашифрования шифра *Bifid* состоит в следующем. Строки и столбцы квадратной таблицы пронумеруем числами от 1 до 5, как показано на рисунке. Теперь каждая буква алфавита имеет свой номер,

состоящий из пары чисел $\binom{i}{j}$, где i — номер строки, а j — номер столбца. Например, буква S имеет номер $\binom{4}{3}$. Выпишем буквы открытого текста в строку, разделяя пробелом каждую пятёрку букв, а под ней — номера соответствующих букв. Фраза, взятая из условия задачи, запишется в виде

S	I	X	T	Y	E	I	G	H	T	M	I	L	E	S
4	2	5	4	5	1	2	2	2	4	3	2	3	1	4
3	5	3	4	4	4	5	3	4	4	3	5	2	4	3

Затем заменим номера букв. Для этого выпишем две строчки из пяти цифр под каждой пятёркой в одну строку из десяти цифр. Например, для второй пятёрки получается строка 1222445344. В получившейся строке каждая последовательная пара цифр и будет новыми номерами букв пятёрки, которые выпишем под соответствующими буквами. Так, для букв второй пятёрки получаем новые номера:

E	I	G	H	T
1	2	4	5	4
2	2	4	3	4
0	F	T	X	T

Наконец, заменяем буквы открытого текста буквами, номера которых в квадратной таблице указаны теперь под соответствующими буквами. В результате этой замены получаем зашифрованный текст. Например, пятёрка EIGHT будет зашифрована в пятёрку OFTXT.

Зашифруем на том же ключе фразу ENTER OTHER LEVEL, заполнив следующую таблицу:

E	N	T	E	R	O	T	H	E	R	L	E	V	E	L
1	3	4	1	4	1	4	2	1	4	3	1	5	1	3
4	4	4	4	2	2	4	4	4	2	2	4	1	4	2
1	4	4	4	4	1	2	4	4	4	3	5	3	4	4
3	1	4	4	2	4	1	2	4	2	1	1	2	1	2
D	Q	T	T	R	E	B	R	T	T	K	V	L	Q	R

Ответ: DQTTR EBRTT KVLQR.

13.3. Цифры пароля будем подбирать последовательно. Свяжемся с банком и наберём цифру 0. Если связь не оборвалась, то первая цифра пароля — 0. Если связь прервана, то первая цифра отлична от 0 и, связываясь заново с банком, пробуем набрать 1, и т. д. Не позднее чем через девять звонков мы будем точно знать, какая цифра стоит на первом месте в пароле, и сможем перейти к подбору второй цифры и т. д.

Общее количество звонков, которое понадобится для выяснения пароля, не более $7 \cdot 9 = 63$. Ещё один звонок может понадобиться для

получения доступа после полного выяснения пароля.

Заметим, что если бы решение о доступе или отказе принималось только после ввода *всего* пароля, то система защиты была бы гораздо надёжнее — последовательный подбор был бы невозможен и потенциально пришлось бы перебирать все 10^7 вариантов пароля.

13.4. Подходы участников олимпиады к решению этой задачи были весьма разнообразны. Предлагалось, например, решать эту задачу перебором, вырезав из бумаги три полосы, соответствующие первым трём строкам таблицы. Были попытки «увидеть» в зашифрованном тексте какое-либо слово, имеющее отношение к геометрической тематике, например, *прямая*, *точка* и т. п. Немаловажную роль в решении сыграло то естественное соображение, что круг слов, используемых в геометрических текстах, существенно ограничен.

В определённом смысле операции *сдвига букв в столбцах* и *отражения столбца относительно средней линии* перестановочны. (Действительно, сдвинуть столбец на одну позицию вверх и затем отразить — это всё равно что столбец сначала отразить, а затем сдвинуть вверх на девять позиций.) Поэтому можно считать, что сначала Кристоша передвигал буквы в столбцах, а затем, может быть, один раз отразил таблицу относительно средней линии. Рассмотрим букву *я* в предпоследнем столбце. Перед ней могут стоять буквы *о, п, н, р, с, ы, в*. Сочетание *оя* встречается в математических текстах в слове «постоянная», но необходимой буквы *т* в седьмом столбце нет. Сочетание *ря* может быть частью слова «прямая», но в седьмом столбце нет *р*. Сочетание *ся* (касающихся, пересекающихся и т. д.) представляется наиболее вероятным, и присутствие буквы *щ* в пятом столбце тому подтверждение. После того как столбцы с пятого по девятый выстроены так, чтобы прочитывалось *щикся*, получение ответа становится совсем простым делом.

п	о	с	л	е	д	о	в	а	т
е	л	ь	н	ы	е		о	т	р
а	ж	е	н	и	я		п	л	о
с	к	о	с	т	и		о	т	н
о	с	и	т	е	л	ь	н	о	
д	в	у	х		п	е	р	е	с
е	к	а	ю	щ	и	х	с	я	
п	р	я	м	ы	х		р	а	в
н	о	с	и	л	ь	н	ы		е
е		п	о	в	о	р	о	т	у

Мы не будем останавливаться здесь на доказательстве этого геометрического утверждения. Отметим только (большинством решавших это было упущено), что утверждение верно и в том случае, когда прямые не лежат в плоскости. Поворот осуществляется относительно прямой, перпендикулярной двум данным прямым и проходящей через точку их пересечения.

13.5. При решении этой задачи участники широко использовали двоичное представление чисел. Например, $105 = 1101001$. Известно, что в двоичном представлении степеней двойки присутствует лишь одна единица: $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 32$, $2^6 = 64$, $2^7 = 128$, $2^8 = 256$. Видим, что в двоичной записи числа 105 единицы стоят в 1-й, 4-й, 6-й и 7-й позициях (считаем слева направо). Значит, $105 = 2^0 + 2^3 + 2^5 + 2^6$. Поскольку двоичное число 11111111 (девять единиц) равно $511 > 300$, заключаем, что девяти чисел 1, 2, 4, 8, 16, 32, 64, 128, 256 вполне достаточно для представления любого натурального числа от 1 до 300 (и даже до 511).

Отметим, что использование двоичной системы записи не является ключевым при решении этой задачи. Например, участниками были предложены следующие девять чисел: 1, 2, 3, 7, 14, 28, 56, 112, 224.

Лишь в очень немногих работах присутствовало доказательство того, что искомый набор не может содержать менее девяти чисел. Действительно, пусть у нас есть восемь чисел и любое число от 1 до 300 представимо в виде суммы разных чисел из этого набора. Используя наш набор, мы можем закодировать любое число от 1 до 300: пусть, например, число a равно сумме первого и третьего чисел нашего набора, тогда будем писать $a = (1, 0, 1, 0, 0, 0, 0)$. Итак, число a получило свой код — строку из восьми символов, каждый символ или 0, или 1. Но нам надо закодировать триста чисел, а строк длины 8, как нетрудно видеть, всего 256. Значит, восьми чисел недостаточно.

13.6. Обозначим $a = x_1$, $b = x_2$, $c = x_3$. Так как эти числа соответствуют буквам в таблице, они принимают значения от 0 до 30. Из соотношения

$$x_{k+3} = x_k + x_{k+2}$$

последовательно получим

$$\begin{aligned} x_1 &= a, \\ x_2 &= b, \\ x_3 &= c, \\ x_4 &= a + c, \\ x_5 &= a + b + c, \\ x_6 &= a + b + 2c, \\ x_7 &= 2a + b + 3c, \end{aligned}$$

$$x_8 = 3a + 2b + 4c,$$

$$x_9 = 4a + 3b + 6c,$$

$$x_{10} = 6a + 4b + 9c,$$

и т. д.

При дальнейшем построении этой последовательности используем следующие правила.

1. Для построения следующей строки последнюю строку складываем с предпредпоследней.

2. Легко заметить, что столбцы чисел отличаются сдвигом по вертикали, поэтому сначала можно определить только коэффициенты при c .

3. Так как нас интересуют только остатки от деления на 31, то, например, $41c = 31c + 10c$ можно заменить на $10c$.

Продолжая аналогично, получим

$$x_{11} = 13,$$

$$x_{12} = 19,$$

$$x_{13} = 28,$$

$$x_{14} = 10,$$

$$x_{15} = 29,$$

$$x_{16} = 26,$$

$$x_{17} = 5,$$

$$x_{18} = 3,$$

$$x_{19} = 29,$$

$$x_{20} = 3,$$

$$x_{21} = 6,$$

$$x_{22} = 6a + 3b + 4c,$$

$$x_{23} = 7a + 4b + 13c,$$

$$x_{25} = 13a + 7b + 17c,$$

$$x_{26} = 17a + 13b + 24c.$$

Используя сдвиги столбцов, получили значения $x_{22}, x_{23}, x_{24}, x_{25}, x_{26}$. Продолжая аналогично, получим последние пять значений $x_{46}, x_{47}, x_{48}, x_{49}, x_{50}$:

$$x_{27} = 6,$$

$$x_{28} = 23,$$

$$x_{29} = 16,$$

$$x_{30} = 22,$$

$$x_{31} = 14,$$

$$\begin{aligned}
x_{32} &= 30, \\
x_{33} &= 21, \\
x_{34} &= 4, \\
x_{35} &= 3, \\
x_{36} &= 24, \\
x_{37} &= 28, \\
x_{38} &= 0, \\
x_{39} &= 24, \\
x_{40} &= 21, \\
x_{41} &= 21, \\
x_{42} &= 14, \\
x_{43} &= 4, \\
x_{44} &= 25, \\
x_{45} &= 8, \\
x_{46} &= 8a + 25b + 12c, \\
x_{47} &= 12a + 8b + 6c, \\
x_{48} &= 6a + 12b + 14c, \\
x_{49} &= 14a + 6b + 26c, \\
x_{50} &= 26a + 14b + 1c.
\end{aligned}$$

Итак, получено выражение чисел x_{22} , x_{23} , x_{24} , x_{25} , x_{26} и чисел x_{46} , x_{47} , x_{48} , x_{49} , x_{50} через a , b , c . Обозначим через O_i , Π_i числа, соответствующие i -м буквам стихотворения и полученного шифрованного текста. Тогда числа $O_{22} + x_{22}$ и Π_{22} имеют одинаковые остатки от деления на 31. То же самое и с числами $O_{46} + x_{46}$ и Π_{46} .

А так как числа O_{22} и O_{46} одинаковые, рассмотрев разности соответствующих частей, получим, что

$$x_{46} - x_{22} \quad \text{и} \quad \Pi_{46} - \Pi_{22} \tag{*}$$

дают одинаковые остатки от деления на 31.

Последним пяти буквам первой строки шифрованного текста соответствуют следующие числа Π_i :

$$\text{Б, Ш, Ъ, Е, Ю} — 1, 23, 27, 5, 29,$$

а последним буквам второй строки — следующие:

$$\text{В, Ы, Ю, И, Д} — 2, 26, 29, 8, 4.$$

Подставляя эти значения в (*) и выражая x_i через a , b , c , получаем

систему

$$\begin{cases} 2a - 9b + 8c = 1 \\ 8a + 2b - c = 3 \\ -a + 8b + c = 2 \\ a - b + 9c = 3 \\ 9a + b + 8c = 6, \end{cases}$$

где равенство означает равенство остатков от деления на 31. При этом использовали правило 3. Например, в первом уравнении $+22b$ заменили на $-9b$. Осталось решить полученную систему. Складывая второе и третье, четвёртое и пятое, третье и четвёртое уравнения, получим

$$\begin{cases} 7a + 10b = 5, \\ 10a + 17c = 9, \\ 7b + 10c = 5. \end{cases} \quad (**)$$

Выразим b и c через a и подставим в первое уравнение:

$$\begin{aligned} b &= \frac{5 - 7a}{10}, \quad c = \frac{9 - 10a}{17}, \\ 2a - 9 \frac{5 - 7a}{10} + 8 \left(\frac{9 - 10a}{17} \right) &= 1, \\ 340a - 9 \cdot 17(5 - 7a) + 80(9 - 10a) &= 170, \\ 611a &= 215, \\ 22a &= 29. \end{aligned}$$

Последнее уравнение можно решить методом подбора и обнаружить, что $22 \cdot 14$ и 29 дают одинаковые остатки от деления на 31. Итак,

$$a = 14.$$

Из системы (**) находим, что $10b = 0$ и $10c = 5$, откуда

$$\begin{aligned} b &= 0, \\ c &= 16. \end{aligned}$$

Зная a, b, c , можно последовательно найти все x_i и из соотношения $O_i = \Pi_i - x_i$ получить стихотворение:

ВЕЧОРТЫПОМНИШЬВЬЮГАЗЛИЛАСЬ
НАМУТНОМНЕБЕМГЛАНOSИЛАСЬ

14.1. Ответ: см. рис. 46.

14.2. Пусть MN — число различных комбинаций, при установке которых раздаётся N ($N \leq 57$) щелчков.

Заметим, что из соображений симметрии $M_N = M_{57-N}$. Для обоснования этого равенства достаточно установить взаимно однозначное

	5		2		0		0	1		2		1
		5		3			3			5		
3			4							6		4
				5	3		3			5		
					2		3	3	3	2		1
2		2								0		
	0		3		5					3		0
						3				1		
	1	3										
				9			7	8		2		
			6		6							
	3								6		0	
0				6	5							

Рис. 46

соответствие между комбинациями, получаемыми за N и за $57 - N$ поворотов. Это можно, например, сделать так: сопоставим комбинации (n_1, n_2, n_3) , где $n_1 + n_2 + n_3 = N$, комбинацию $(19 - n_1, 19 - n_2, 19 - n_3)$, получаемую за $19 - n_1 + 19 - n_2 + 19 - n_3 = 57 - (n_1 + n_2 + n_3) = 57 - N$ щелчков. Отсюда заключаем, что число комбинаций, при установке которых раздаётся 32 и 25 щелчков, одинаково ($M_{32} = M_{25}$).

Из предыдущего рассуждения также следует, что $M_{24} = M_{33}$. Поэтому для завершения решения достаточно сравнить числа M_{24} и M_{25} .

Комбинацию будем называть насыщенной, если один из дисков установлен в положение 19; остальные комбинации считаем ненасыщенными. Кроме того, будем отдельно рассматривать комбинации, в которых один из дисков установлен в положение 0.

Все комбинации, устанавливаемые за 24 щелчка, разделим на четыре группы: насыщенные и содержащие нуль, насыщенные без нуля, ненасыщенные с нулём, ненасыщенные без нуля. Легко подсчитать, что в первую группу входит 6 комбинаций (всевозможные перестановки чисел 19, 5 и 0), во вторую — $3 \cdot 4 = 12$ (три варианта места для числа 19; для каждого из них по четыре варианта значения первой незаполненной позиции, после чего оставшееся число находится однозначно), а в третью — $3 \cdot 13 = 39$ (три варианта выбора места для 0; для каждого из них возможно 13 вариантов выбора значения первой незаполненной позиции числами от 6 до 18). Число комбинаций в четвёртой группе находить не будем, а просто обозначим его через X .

Мысленно выпишем все комбинации, получаемые за 24 щелчка, в один столбец, а получаемые за 25 щелчков — в другой. Если какая-либо комбинация первого столбца с помощью ещё одного щелчка может быть преобразована в комбинацию второго столбца, то соединим

их стрелкой. Проведём все такие стрелки. Из каждой комбинации первой группы выходит ровно две стрелки. Шесть из них ведут к комбинациям, содержащим 0, а шесть — к не содержащим 0. Каждую комбинацию второй группы также можно продолжить двумя способами, и все получаемые стрелки (их 24) ведут к комбинациям, не содержащим 0. Каждая комбинация третьей группы продолжается тремя способами, всего при этом получится $39 \cdot 2$ стрелок к комбинациям с нулём и 39 — к комбинациям без нуля. Комбинации последней группы можно продолжить также тремя способами. При этом получится $3X$ стрелок, все ведут к комбинациям, не содержащим 0.

Всего получим $6 + 39 \cdot 2 = 84$ стрелки, ведущие к комбинациям с нулём, и $6 + 24 + 39 + 3X$ — без нуля.

С другой стороны, к каждой комбинации, получаемой за 25 щелчков и не содержащей 0, ведёт ровно три стрелки, а к комбинациям, содержащим 0, — ровно по две. Таким образом, число различных комбинаций, получаемых за 25 щелчков, составит $42 + 23 + X = 65 + X$, что на 8 больше, чем $6 + 12 + 39 + X = 57 + X$ — число различных комбинаций, получаемых за 24 щелчка.

Ответ: количества комбинаций, получаемых за 25 и 32 щелчка, совпадают, комбинаций для 33 щелчков меньше.

14.3. Сопоставим каждому служащему «точку», а каждому автомобилю — «линию». Если p — служащий, владеющий автомобилем L , то будем говорить, что точка p инцидентна линии L , а линия L инцидентна точке p . При этом пару (L, p) назовём «флагом». Условия задачи можно сформулировать в следующем виде:

1) для каждой точки p имеется ровно t флагов вида

$$(L_1, p), (L_2, p), \dots, (L_t, p);$$

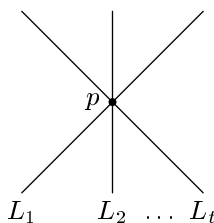
2) для каждой линии L имеется ровно s флагов вида

$$(L, p_1), (L, p_2), \dots, (L, p_s);$$

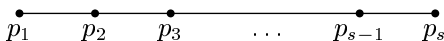
3) если точка x не инцидентна линии L , то имеются ровно одна такая линия M и одна такая точка y , что (L, y) , (M, x) и (M, y) — флаги.

Изобразим условия 1–3 графически:

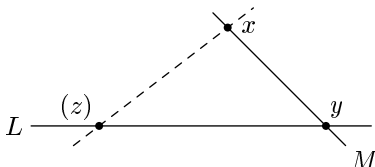
1) («пучок линий с центром в точке p »)



2) (точки «располагаются на линии L »)



3) («треугольники» (с точкой z) исключаются)



Вычисляя число F флагов двумя способами, получаем, согласно условиям 2 и 3, равенство $F = P \cdot t = B \cdot s$. Из условия 3 следует, что все точки располагаются на линиях пучков, центрами которых служат точки любой линии, например L . Отсюда (с учётом условий 1 и 2) следует, что число точек, не лежащих на линии L , равно $t \cdot (s - 1) \cdot 5$. Добавляя к этому число точек линии L , получаем общее число точек:

$$P = t \cdot (s - 1) \cdot s + s = s \cdot (t \cdot (s - 1) + 1).$$

Теперь находим число линий:

$$B = \frac{p \cdot t}{s} = t \cdot (t \cdot (s - 1) + 1).$$

Наконец, число флагов равно

$$F = t \cdot s(t \cdot (s - 1) + 1).$$

Ответ:

$$P = t \cdot (s - 1) \cdot s + s = s \cdot (t \cdot (s - 1) + 1);$$

$$B = t \cdot (t \cdot (s - 1) + 1);$$

$$F = t \cdot s(t \cdot (s - 1) + 1).$$

14.4. Обозначим $2^{10} = x$. Тогда исходное число имеет вид $4x^2 + 39x + 81$. Корни этого трёхчлена равны -3 и $-27/4$. Значит, $4x^2 + 39x + 81 = 4(x+3)(x+27/4)$. Далее, $(2^{10}+3)(2^{12}+27) = 1027 \cdot 4123 = 13 \cdot 79 \cdot 7 \cdot 19 \cdot 31$.

Ответ: $7 \cdot 13 \cdot 19 \cdot 79 \cdot 31$.

14.5. Заменяя каждый член последовательности $a_1 = 1$, $a_{n+1} = 3a_n + 4$ остатком от его деления на 33, получим периодическую последовательность. Вот несколько первых членов этой последовательности:

$$1, 7, 25, 13, 10, 1, 7, 25, 13, 10, 1, 7, 25, 13, \dots$$

Так как каждый член этой последовательности остатков однозначно находится из предыдущего, заключаем, что её период равен пяти.

Будем вычитать из чисел, соответствующих буквам зашифрованного текста, числа этой периодической последовательности, а результаты заменять буквами согласно данной в условии задачи таблице:

Р	Ч	Ж	Ь	Э	Т	С	Ъ	Й	Л	...
17	24	7	29	30	19	18	27	10	12	...
1	7	25	13	10	1	7	25	13	10	...
16	17	15	16	20	18	11	2	30	2	...
П	Р	О	П	У	С	К	В	Э	В	...

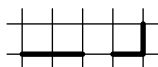
После слова ПРОПУСК идёт нечитаемый текст. Значит, или непосредственно после этого слова, или после буквы В пропущены буквы. (Перебор различных вариантов тривиален и поэтому здесь не приводится.) Сдвигая нашу периодическую последовательность относительно зашифрованного текста, находим такой вариант:

17	24	7	29	30	19	18		27	10	12	7	27	32	15	25	11	18
Р	Ч	Ж	Ь	Э	Т	С		Ъ	Й	А	Ж	Ъ	Я	О	Ш	К	С
1	7	25	13	10	1	7	25	13	10	1	7	25	13	10	1	7	25
16	17	15	16	20	18	11	2	14	0	11	0	2	19	5	24	4	26
П	Р	О	П	У	С	К		Н	А	К	А	В	Т	Е	Ч	Д	Щ

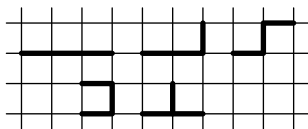
Естественно предположить, что на месте пропущенного знака в исходном тексте находилась буква З. Действуя далее аналогично, восстанавливаем весь текст.

Ответ: ПРОПУСК ЗНАКА В ТЕКСТЕ.

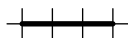
14.6. Сначала выясним, какие вообще могут быть шаблоны. Очевидно, что при $k = 2$ имеется 2 вида шаблонов:



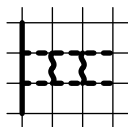
При $k = 3$ имеется 5 видов шаблонов:



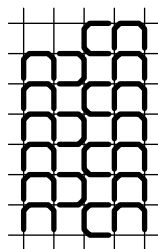
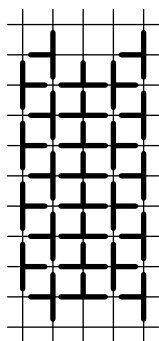
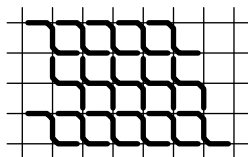
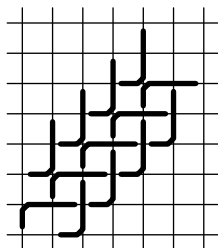
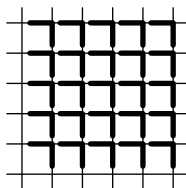
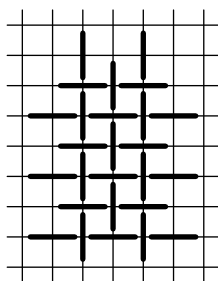
Оказывается, что все линии клетчатой бумаги можно покрыть любым из перечисленных выше шаблонов, кроме шаблона вида



Докажем последнее. Пусть требуемое покрытие существует. Рассмотрим одно наложение такого шаблона на клетчатую бумагу и некоторые соседние с ним клетки:



Из условия задачи и расположения первого шаблона следует, что пунктирные линии должны быть покрыты двумя другими шаблонами, но тогда волнистые линии без наложения внутренних точек шаблонов покрыть нельзя. Решение для остальных шаблонов показано ниже:



15.1. Квадрат натурального числа может оканчиваться только на цифры 0, 1, 4, 5, 6, 9. Число $0 \dots 0$ натуральным не является. Число $5 \dots 5$ не может быть квадратом, так как оно делится на 5, но не делится на 25. Аналогично $6 \dots 6 \neq n^2$, так как это число делится на 2, но не делится на 4. Числа $4 \dots 4$ и $9 \dots 9$ являются полными квадратами в том и только том случае, когда полным квадратом будет $1 \dots 1$.

Докажем, что $1 \dots 1 \neq n^2$. Предположим, что это не так: существует такое натуральное число n , что $1 \dots 1 = n^2$. Тогда $n = 10k \pm 1$ и, следовательно, $100k^2 \pm 20k = 1 \dots 10 \Leftrightarrow 10k^2 \pm 2k = 1 \dots 1$. Получили противоречие: нечётное число равно чётному.

15.2. Для решения этой задачи достаточно было заметить, что при указанном способе зашифрования количество различных букв в исходном тексте совпадает с числом различных пар в криптограмме. Первая из приведённых в условии задачи криптограмм содержит 23 различные пары, а вторая — 29. Так как латинский алфавит состоит из 26 букв, английскому исходному тексту может соответствовать только первая криптограмма.

15.3. Слово ПОДЪЕЗД состоит из семи букв, причём 3-я и 7-я совпадают. Найдём в тексте фрагменты длины семь с совпадающими парами в 3-й и 7-й позициях. Таких фрагментов получится семь:

```

36 72 97 92 70 73 97
74 76 97 34 79 78 97
70 76 74 72 74 73 74
73 74 76 70 70 97 76
74 37 39 75 97 70 39
71 74 98 35 94 90 98
98 35 94 90 98 97 94

```

Удалим из этого списка те, в которых есть другие повторы. Останется четыре варианта:

```

36 72 97 92 70 73 97
74 76 97 34 79 78 97
74 37 39 75 97 70 39
71 74 98 35 94 90 98

```

Отметим для первого случая ставшие известными буквы текста:

```

  Ъ Д П О Д Ъ Е З Д      Д
92 97 36 72 97 92 70 73 97 90 97
  О              Д      Д Е ...
72 38 39 74 76 97 34 79 78 97 70 ...

```

Видно, что уже в самом начале содержится «нечитаемая» последовательность букв. Отметим для остальных вариантов становящиеся из-

вестными буквы текста: Второй:

Д		Д		Д		Д				
92	97	36	72	97	92	70	73	97	90	97
			П	О	Д	Ъ	Е	З	Д	
72	38	39	74	76	97	34	79	78	97	70
	П		П		П	О			Д	О
76	74	72	74	73	74	76	70	70	97	76
П		П				Д			П	Е
74	96	74	37	39	75	97	70	39	74	79
			П						Д	
39	37	71	74	98	35	94	90	98	97	94
	П		П	О	Д					
96	74	98	74	76	97					

Третий:

Е		Е		З		Е		Е		
92	97	36	72	97	92	70	73	97	90	97
		Д	П		Е				Е	З
72	38	39	74	76	97	34	79	78	97	70
	П		П		П		З	З	Е	
76	74	72	74	73	74	76	70	70	97	76
П		П	О	Д	Ъ	Е	З	Д	П	
74	96	74	37	39	75	97	70	39	74	79
Д	О		П						Е	
39	37	71	74	98	35	94	90	98	97	94
	П		П		Е					
96	74	98	74	76	97					

Четвёртый:

									З	
92	97	36	72	97	92	70	73	97	90	97
			О							
72	38	39	74	76	97	34	79	78	97	70
	О		О		О					
76	74	72	74	73	74	76	70	70	97	76
О		О							О	
74	96	74	37	39	75	97	70	39	74	79
		П	О	Д	Ъ	Е	З	Д		Е
39	37	71	74	98	35	94	90	98	97	94
	О		О							
96	74	98	74	76	97					

Предполагалось, что участники на этом остановятся. Все решения с указанными тремя вариантами признавались правильными. Тем не менее, двое участников пошли ещё дальше — отсеяли ещё по одному варианту исходя из частот встречаемости букв в текстах (во втором и третьем вариантах слишком часто встречается буква П; кроме того, во втором варианте присутствует удвоение буквы З, что не характерно для обычных текстов).

15.4. Приведённый в задаче протокол работы брелка и замка был изобретён в ЮАР и практически без изменения использовался во многих известных противоугонных системах. Вызывает лишь удивление, что достаточно продолжительное время очевидная уязвимость этого протокола не была замечена (примечательно, что заметили и воспользовались ошибкой разработчиков непрофессионалы в области защиты информации).

Перейдём собственно к решению, пояснив предварительно одно из условий задачи. Пусть $СБ = k$ и $СЗ = m$, где k не меньше m . Отметим, что в данной ситуации при нажатии на кнопку брелка и срабатывании замка счётчик замка принимает значение не $m + 1$ (как ошибочно считали некоторые участники олимпиады), а $k + 1$. Это сделано для того, чтобы один и тот же сигнал брелка не мог быть использован дважды. Запишем теперь по пунктам действия злоумышленника.

1. Пусть сейчас замок открыт. Владелец хочет запереть машину и уйти. Пусть $СБ = k$ и $СЗ = m$, где k не меньше m . Владелец нажимает кнопку брелка. Злоумышленник запоминает посланный сигнал k и ставит помеху. В результате $СБ = k + 1$ и по-прежнему $СЗ = m$, т. е. замок не закрылся.

2. Заметив, что машина не заперта, владелец повторно нажимает кнопку брелка. Злоумышленник снова запоминает сигнал $k + 1$ брелка и опять ставит помеху. Значит, $СБ = k + 2$, а замок так и остаётся открытым, т. е. $СЗ = m$.

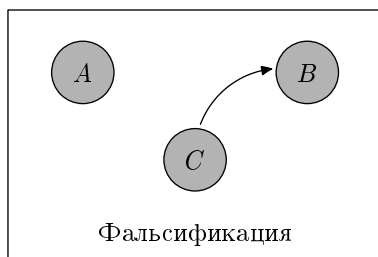
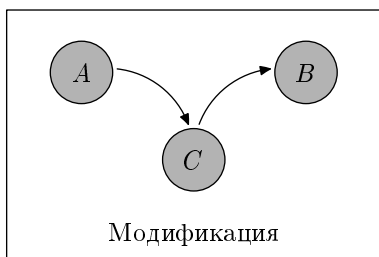
3. Выполнив действия пункта 2, злоумышленник немедленно посылает замку ранее запомненный сигнал k . Замок закрывается, и при этом $СЗ = k + 1$. Владелец уходит, полагая, что машину запер он сам.

4. Злоумышленник посылает замку ранее запомненный сигнал $k + 1$, и замок открывается.

К сожалению, многие участники решали задачу исходя из слишком упрощённой модели реальной ситуации, отводя владельцу роль эдакого простачка, который, запирая машину, то ли не может, то ли забывает проверить, сработал замок или нет: предлагалось выбрать момент, когда владелец попробует запереть автомобиль, поставить помеху, не дав тем самым замку сработать, а затем подождать, пока владелец уйдёт.

15.5. Предварим решение этой задачи небольшим отступлением о кодах аутентификации, поясняющим происхождение её формулировки.

При передаче информации по незащищённому (общедоступному) каналу связи возникает задача защиты от активных атак со стороны злоумышленника. Под активными атаками понимают попытки фальсификации (имитации) и модификации (подмены) сообщения. Цель ак-



тивных атак — дезинформация получателя. Не вдаваясь в детали, сообщим, что сегодня имеется техническая возможность проведения подобных атак.

Для противодействия активным атакам используются так называемые *коды аутентификации* (кратко — *A-коды*). Они дают возможность получателю сообщения проверить его подлинность (или аутентичность). Проверка использует некий секрет, известный лишь отправителю и получателю сообщения, точно так же, как при обеспечении секретности используется секретный ключ шифрования. В общем виде код аутентификации представляет собой совокупность (S, E, M) трёх конечных множеств, где S — множество *состояний источника*, E — множество *правил кодирования*, M — множество *сообщений*. Каждый элемент $e \in E$ представляет собой отображение $e: S \rightarrow M$. Правила кодирования «кодируют» состояния источника $s \in S$ в сообщения $m \in M$. Таким образом, сообщения передают информацию о наблюдаемом отправителем состоянии источника. Таковыми могут быть, например, результаты подбрасывания монеты при проведении жребия по телефону или обычные текстовые сообщения. Отображение $e \in E$ должно быть «обратимым», чтобы по данным m и e можно было однозначно восстановить s . Формально это требование записывается с помощью отображения $f_e: M \rightarrow S \cup \{0\}$, где 0 — число нуль (не принадлежащее S) и

$$f_e(m) = \begin{cases} s, & \text{если } e(s) = m, \\ 0, & \text{если такого } s \text{ не существует.} \end{cases}$$

Так вот, в определении A-кода требуется, чтобы выполнялось равенство $f_e(e(s)) = s$ для любых $s \in S$ и $e \in E$.

Как стороны A и B используют A -код для аутентификации передаваемой информации? Прежде всего, они сообща выбирают (втайне от злоумышленника) правило кодирования $e \in E$. Пусть A желает передать состояние источника $s \in S$. Тогда он вычисляет $m = e(s)$ и посылает m получателю B по каналу связи. Получив m , B использует то же правило кодирования e для вычисления $f_e(m)$. Если $f_e(m) \neq 0$, то m принимается как аутентичное, в противном случае — нет. На практике используются лишь такие A -коды, для которых вычисление $f_e(m)$ производится так же просто, как и $e(s)$.

При анализе надёжности защиты от активных атак с помощью A -кодов предполагается, что злоумышленник знает об A -коде всё, кроме секретного правила кодирования (ключа). Он (злоумышленник) проводит атаки на основе анализа свойств A -кода. При этом его действия являются наиболее целесообразными с точки зрения достижения успеха атаки. Приведём пример.

Рассмотрим A -код, для которого $S = \{H, T\}$ (сокращение от head — герб, tail — решка), $E = \{e_1, e_2, e_3\}$, $M = \{m_1, m_2, m_3\}$. Действие правил кодирования запишем в виде таблицы (матрицы кодирования):

$$\begin{array}{ccc} & m_1 & m_2 & m_3 \\ \begin{array}{c} e_1 \\ e_2 \\ e_3 \end{array} & \begin{pmatrix} H & T & 0 \\ T & 0 & H \\ 0 & T & H \end{pmatrix} \end{array}$$

В этой таблице указано, например, что состояние источника H кодируется с помощью правила e_1 в сообщение m_1 , и т. д.

Пусть состояние источника выбирается случайно (как при подбрасывании монеты). При этом одно из двух состояний появляется чаще другого (как при использовании несимметричной монеты). Пусть p — «доля» состояния H . Тогда $(1-p)$ — «доля» состояния T . Например, если при бросании монеты она в среднем в двух случаях из трёх выпадает гербом, то $p = 2/3$. С целью уменьшения шансов на успех злоумышленника A и B выбирают правило кодирования случайно. Пусть при этом $p(e_i) = x_i$ — «доля» e_i , $i = \overline{1, 3}$. Числа x_i лежат в интервале $(0, 1)$, и их сумма равна 1. Пусть $P(E) = (x_1, x_2, x_3)$. Эта тройка чисел называется *стратегией защиты*. Эта стратегия выбирается стороной защиты с таким расчётом, чтобы минимизировать «шансы» злоумышленника на успех.

Не вдаваясь в детали, укажем, что для данного A -кода при выбранной стратегии $P(E)$ эти шансы злоумышленника характеризуются величиной

$$L(\bar{x}) = \max\{px_1; (1-p)x_2\} + \max\{(1-p)x_1; (1-p)x_3\} + \max\{px_2 + px_3\}.$$

Сторона защиты выбирает *оптимальную стратегию* $P^{(0)}(E)$ так, чтобы минимизировать $L(\bar{x})$. Таким образом, возникает задача вычисления $\min_{\bar{x} \in \Delta} L(\bar{x})$, где

$$\Delta = \{(x_1, x_2, x_3) : 0 < x_i < 1, x_1 + x_2 + x_3 = 1\}.$$

Этот минимум можно вычислить, разбивая область Δ на подмножества Δ_j , $j = \overline{1, 8}$, в которых раскрывается каждый максимум в выражении $L(\bar{x})$. Например, в случае, когда

$$\begin{cases} x_1 p \geq x_2(1-p), \\ x_1 \leq x_2, \\ x_2 \geq x_3, \end{cases}$$

$L(\bar{x})$ имеет вид $L(\bar{x}) = p(x_1 + x_2) + (1-p)x_3$. Как раз эта задача была предложена на олимпиаде. Решается она, например, следующим образом.

Заметим, прежде всего, что из условий следует неравенство $p \geq 1/2$. В самом деле,

$$x_1 p \geq x_2(1-p) \geq x_1(1-p),$$

откуда $p \geq 1-p$ или $2p \geq 1$.

Выразив x_3 из условия $x_1 + x_2 + x_3 = 1$, получим следующее выражение:

$$L(\bar{x}) = (x_1 + x_2)(2p-1) + 1-p.$$

Легко видеть, что минимальное значение это выражение принимает при максимально большом значении x_3 . Остаётся найти достижимую верхнюю границу для значения x_3 .

Из цепочки неравенств $x_3 \leq x_2 \leq \frac{p}{1-p}x_1$ получаем

$$1 = x_1 + x_2 + x_3 \geq \frac{1-p}{p}x_3 + x_3 + x_3,$$

откуда следует, что $x_3 \leq \frac{p}{p+1}$. Ясно, что равенство $x_3 = \frac{p}{p+1}$ достигается лишь в случае, когда в указанной цепочке неравенств выполняются равенства, т. е. если $x_3 = x_2 = \frac{p}{1-p}x_1$. Мы нашли максимальное значение x_3 . Отсюда получаем, что

$$\min L(\bar{x}) = \left(\frac{1-p}{p+1} + \frac{p}{p+1} \right) p + \frac{p}{p+1}(1-p) = \frac{p(2-p)}{p+1}.$$

16.1. 1. Рассмотрим фрагменты шифртекста *эй* и *эйц*; это — слова из 2 и 3 букв. Одно из слов имеет суффикс *йээ*. Весьма вероятно, что *э* заменяет букву *н*, а *й* — одну из гласных: *о*, *а*, *и*, *е*. Тогда возможны следующие варианты окончания слова *юбюрйээпо*: *онная*, *онные*, *енные*, *енная*, *инная*, *инные*. Вариант окончания *ные* не подходит, так как при

этом n заменяет $ы$, и с буквы $ы$ начинается слово *пфзшэюь*. Поэтому n заменяет либо $а$, либо $о$.

2. Можно попытаться угадать слово *бвпвл*. Очевидно, что в нём $в$ — согласная. Сочетание вида *хох*, где $х$ — согласная, вряд ли возможно. Из вариантов *хах*, где $х$ — согласная, подходит, разве что *тат*. Проверим гипотезу, что $в$ заменяет $т$.

3. Заметим, что окончания четырёх слов — *овл*, *швл*, *пвл*, *швл* образуют рифму. С учётом шага 2, «напрашиваются» варианты окончаний *ать*, *ить*, *ять*.

4. Буква $ю$ часто встречается в шифртексте. Поэтому, скорее всего, она заменяет гласную букву. Она входит во фрагмент $\dots юбб\dots$. Так как буква $н$ уже занята, удвоение $бб$ скорее всего заменяет $сс$, и $юбб$ — это *асс*, *осс*, *есс* или *исс*. Возвращаясь к шагу 2, устанавливаем, что *бвпвл* заменяет *стать*.

5. Учитывая шаг 4, а также то, что заглавной буквой начинается имя собственное, попытаемся угадать что заменяет сочетание *Фюбб-ши*. «Напрашивается» вариант *Россия* или *Россию*, откуда находим, что $ю$ заменяет $о$, а $ш$ заменяет $и$.

6. Первое слово шифртекста — *Гьюь*. Ясно, что $ь$ заменяет согласную букву. Возможны следующие варианты из 4 букв: *удод*, *скок*, *умом*. Отсюда получаем первое предложение: *Умом Россию не понять*. Дальше легко догадаться.

Ответ:

*Умом Россию не понять,
Аршином общим не измерить:
У ней особенная стать —
В Россию можно только верить.*

16.2. Заметим, что $2007 = 223 \cdot 9$. Поэтому, используя данное устройство, можно было бы легко найти среднее арифметическое не 2006, а 2007 чисел. Действительно, обозначим эти 2007 чисел через a_1, \dots, a_{2007} , а их среднее арифметическое — через A_{2007} . Разобьём их на 9 групп по 223 числа в каждой: первая группа: a_1, \dots, a_{223} , вторая группа: a_{224}, \dots, a_{446} , ..., девятая группа: $a_{1785}, \dots, a_{2007}$. Для каждой из 9 групп найдём среднее арифметическое входящих в неё чисел. Затем вычислим среднее арифметическое найденных девяти средних арифметических. Это и будет среднее арифметическое 2007 чисел, поскольку

$$A_{2007} = (a_1 + \dots + a_{2007}) : 2007 = \\ = ((a_1 + \dots + a_{223}) : 9 + (a_{224} + \dots + a_{446}) : 9 + \dots + (a_{1785} + \dots + a_{2007}) : 9) : 223.$$

Итак, среднее арифметическое **любых** 2007 чисел мы находить умеем. Покажем теперь, как найти среднее арифметическое A_{2006} от 2006 чисел a_1, \dots, a_{2006} . Добавим к этим числам ещё одно число a_{2007} , равное

нулю, и вычислим среднее арифметическое A_{2007} теперь уже 2007 чисел. Воспользовавшись тем, что мы можем (дополнительно) выполнить одно умножение и одно деление, находим

$$A_{2006} = A_{2007} \cdot 2007 : 2006,$$

так как

$$\begin{aligned} A_{2006} &= (a_1 + \dots + a_{2006}) : 2006 = (a_1 + \dots + a_{2006} + a_{2007}) : 2006 = \\ &= (a_1 + \dots + a_{2006} + a_{2007}) : 2007 \cdot 2007 : 2006 = A_{2007} \cdot 2007 : 2006. \end{aligned}$$

Задача решена.

Отметим в заключение, что если разбить данные числа на несколько групп, найти среднее арифметическое каждой группы и затем взять среднее арифметическое полученных значений, то результат, вообще говоря, не будет совпадать со средним арифметическим исходных чисел, и вот простой пример:

$$\frac{1 + 2 + 3 + 4 + 5}{5} \neq \frac{\frac{1+2}{2} + \frac{3+4+5}{3}}{2}.$$

Тем не менее, таким способом среднее арифметическое вычислять можно, если разбивать исходные числа на группы, состоящие из одинакового количества чисел.

16.3. Указанный в задаче способ зашифрования обладает следующим свойством. Если ab заменяется на cd , то dc заменяется парой ba . Проверим наличие этого свойства в данных в условии открытом и зашифрованных текстах. Для первого шифртекста первая же пара cr заменяется на pa , а ar переходит в rc . Пара to заменяется на gl , а lg переходит в ot :

c r u p t o g r a p h i c a l g o r i t h m
p a b d g l i u r c a v t h o t u e a d s p

В рассмотренных заменах противоречий с указанным свойством мы не находим.

Для второго шифртекста это свойство не выполняется. Действительно, пара lg заменяется на mh , но при этом hm переходит в in :

c r u p t o g r a p h I c a l g o r i t h m
d s z q u p h s b q i j d b m h p s j u i n

Таким образом, первый шифртекст является единственным возможным вариантом.

Ответ: первый текст.

16.4. Представим последовательность $\{x_n\}$ в виде последовательности пар $(x_1, x_2), (x_3, x_4), \dots$, которая имеет вид $(a_1, b_1), (a_2, b_2), \dots$. Её период равен $c = \text{НОК}(16, 2006) = 16048$, так как равенство пар означает равенство их первых и равенство их вторых элементов. Поэтому при

всех натуральных n верно равенство $x_n = x_{n+2c}$. Покажем, что $2c$ — наименьшее число с таким условием. Пусть период последовательности $\{x_n\}$ равен t . Тогда число $2c$ должно делиться на t . Если t чётно ($t = 2k$), то из верных при всех натуральных m равенств

$$x_{2m-1+t} = x_{2m-1}, \quad x_{2m+t} = x_{2m}$$

следуют равенства

$$a_{m+k} = a_m, \quad b_{m+k} = b_m.$$

Таким образом, k делится на наименьшее общее кратное периодов исходных последовательностей. Отсюда

$$t = 2\text{НОК}(16, 2006) = 32096.$$

При нечётном t первая последовательность является «сдвигом» второй, что противоречит различию длин их периодов.

Ответ: 32096.

16.5. Рассмотрим фрагмент исходной фигуры, которая представляет собой правильный треугольник со стороной из четырёх шаров. Пусть на верхнем шаре написано число a , а на одном из примыкающих к нему снизу шаров — число b . Из условия задачи следует, что сумма чисел на любых трёх попарно касающихся шарах равна нулю. Поэтому числа на остальных шарах выражаются через a и b , как показано на рисунке 47. В вершинах фрагмента стоит число a , следовательно $a = 0$. Совершенно аналогично (при рассмотрении правильного треугольника со стороной из пяти шаров) доказывается, что $b = 0$.

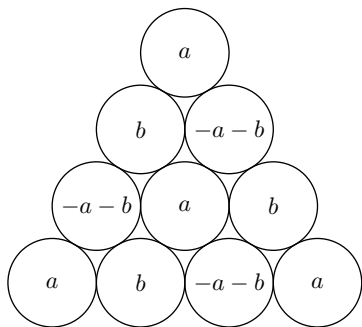


Рис. 47

Ответ: на всех шарах написано число 0.

16.6. *Ответ:* Единственно возможное заполнение таблицы показано на рис. 48.

17.1. Прежде всего определим, какие полосы находились на чётных, а какие — на нечётных местах перед перестановкой полос. Необходимым условием расположения полосы на нечётном месте является отсутствие в её первой колонке цифр, превосходящих 3. На рисунке соответствующие цифры выделим цветом. Всего получилось шесть полос, которые могли располагаться только на чётных местах до перестановки. Это полосы с номерами 1, 2, 4, 9, 11 и 12. Из того, что число полос равно 12, заключаем, что все остальные полосы располагались на нечётных

		30	24		8	19	
	16	7	9	3	1	2	
	35	6	8	5	7	9	17
25	1	8	7	9	9	1	8
13	4	9	20	1	3	7	9
	16	5	17	1	7	9	8
21	9	4	8	24	8	9	7
10	7	1	2	15	6	8	1

Рис. 48

местах.

316 001 190 014 013 150 171 240 120 131 105 614
 010 810 050 610 012 161 121 200 614 120 401 117
 619 501 172 327 171 041 061 221 010 033 801 016
 115 313 192 312 030 130 160 103 210 013 620 016
 512 060 061 250 061 825 16 103 310

Теперь обратим внимание на то, что полосы имеют разные длины. Это произошло из-за того, что последняя строка исходной таблицы была заполнена не целиком. Поэтому можно сделать вывод о том, что до перестановки на последних четырёх местах располагались полосы с номерами 10, 2, 7, 4, либо 10, 4, 7, 2. Первый вариант не подходит, т. к. в третьей строке возникает несуществующий номер буквы в алфавите — 35. Во втором варианте преобразуем пары цифр в буквы. Получим вот что:

ЛИМПИА
 КЕИКРИ
 ВЯЩЕНА
 АЯКОВЛ
 О

Далее, подбирая фрагменты слов по принципу «читаемости», последовательно двигаясь от последних столбцов к первым, восстанавливаем расположение остальных полос и исходный текст.

Ответ: Семнадцатая олимпиада по математике и криптографии посвящена столетию Ивана Яковлевича Верченко.

17.2. Заметим, что $abab \dots ab = ab \cdot x$, где $x = 0101 \dots 01$. Число в левой части равенства образовано n -кратным повторением пары цифр ab , поэтому в записи числа x пара 01 встречается также ровно n раз. Поскольку левая часть должна делиться на 21 при любых a и b , число n должно быть таким, чтобы на 21 делилось число x . Число делится на 21 в том и только том случае, когда оно делится на 3 и на 7. Для делимости на 3 необходимо и достаточно, чтобы сумма цифр числа делилась на 3, поэтому $n = 3k$. Оказывается, в нашем случае этого достаточно, чтобы число делилось и на 7. В самом деле, представим x в виде следующей суммы чисел:

$$0101 \dots 01 =$$

$$= 010101 + 010101 \cdot 10^6 + 010101 \cdot 10^{12} + \dots + 010101 \cdot 10^{6(k-1)}.$$

Тогда каждое слагаемое в правой части равенства делится на 7, так как $010101 = 7 \cdot 1443$.

Ответ: $n = 3k$, где k — произвольное натуральное число.

17.3. Используемые для зашифрования цифры (шестёрки) отвечают некоторой дате, и это накладывает на них определённые ограничения. Например, первой цифрой даты может быть только 0, 1, 2 или 3, третьей — только 0 или 1. Под каждой буквой шифрованного текста запишем возможные варианты букв сообщения:

Т	П	И	Ё	Р	Ж	Е	М	А	А	С	Ф	С	Г	Ь	О	Г	Х	Ж	П	Н
Т	П	И	Ё	Р	Ж	Е	М	А	А	С	Ф	С	Г	Ь	О	Г	Х	Ж	П	Н
С	О	З	Е	П	Ё	Д	Л	Я	Я	Р	У	Н	В	Ы	Н	В	Ф	Ё	О	М
Р	Н		Д	О	Е	Г	К		Ю	П	Т	П	Б		М	Б	У	Е	Н	
П	М		Г	Н	Д	В	Й		Э	О	С	О	А		Л	А	Т	Д	М	
	Л		В	М	Г		И		Ь	Н	Р		Я		К	Я	С		Л	
	К		Б	Л	В		З		Ы	М	П		Ю		Й	Ю	Р		К	
	Й		А	К	Б		Ж		Ъ	Л	О		Э		И	Э	П		Й	
	И		Я	Й	А		Ё		Щ	К	Н		Ь		З	Ь	О		И	
	З		Ю	Ч	Я		Е		Ш	Й	М		Ы		Ж	Ы	Н		З	
	Ж		Э	З	Ю		Д		Ч	И	Л		Ъ		Ё	Ъ	М		И	

Искомое сообщение получается выбором в каждом столбце по одной букве, так, чтобы выбранные буквы образовали «читаемую» строку. Например, в 15-м столбце присутствуют только буквы Ъ и Ы, что позволяет отсеять семь нижних вариантов букв в предыдущем столбце. Поскольку комбинация из шести цифр периодически повторялась, те же самые варианты можно отсеять во 2-м, 8-м и 20-м столбцах.

Т	П	И	Ё	Р	Ж	Е	М	А	А	С	Ф	С	Г	Ь	О	Г	Х	Ж	П	Н
Т	П	И	Ё	Р	Ж	Е	М	А	А	С	Ф	С	Г	Ь	О	Г	Х	Ж	П	Н
С	О	З	Е	П	Ё	Д	Л	Я	Я	Р	У	Н	В	Ы	Н	В	Ф	Ё	О	М
Р	Н		Д	О	Е	Г	К		Ю	П	Т	П	Б		М	Б	У	Е	Н	
П	М		Г	Н	Д	В	Й		Э	О	С	О	А		Л	А	Т	Д	М	
	Д		В	М	Г		И		Ь	Н	Р		Я		К	Я	С		Д	
	К		Б	Л	В		Э		Ы	М	П		Ю		Й	Ю	Р		К	
	Й		А	К	Б		Ж		Ъ	Л	О		Э		И	Э	П		Й	
	И		Я	Й	А		Ё		Щ	К	Н		Ь		З	Ь	О		И	
	Э		Ю	Ч	Я		Е		Ш	Й	М		Ы		Ж	Ы	Н		Э	

Теперь из первых двух столбцов видно, что во втором столбце единственно возможной является буква О. Учтём это наблюдение в 8, 14 и 20 столбцах. Теперь несложно подобрать искомое сообщение:

ПОЗДРАВЛЯЮ С НОВЫМ ГОДОМ

Используемая дата — 31.12.2007.

17.4. Для решения этой задачи участникам потребовалось проявить наблюдательность. При рассмотрении рисунка видно, что большинство букв расположено точно в центре клетки, а часть букв — смещена. Если выделить смещённые буквы, как это сделано на рисунке, то можно прочитать фрагмент текста: **авшифреповоротна.**

т	я	с	а	п	м	р	е
в	щ	е	р	е	ш	ш	о
ч	и	ч	н	ф	и	т	р
ё	а	е	т	т	е	т	к
р	а	ь	п	а	п	о	ф
т	в	о	е	з	о	к	р
о	с	а	в	т	р	о	т
л	е	я	н	!	е	т	а

Смещённых букв как раз 16 — по числу вырезов в трафарете. Поворачивая найденный трафарет в три оставшихся положения, находим остальные три фрагмента:

ярешёткапозволяе

тпрочитатьтекст!

смещениетрафарет

Осталось расположить эти фрагменты в «читаемом» порядке.

Ответ: Смещение трафарета в шифре поворотная решётка позволяет прочитать текст!

17.5. Так как неизвестно расположение радиоканала, после удаления проводных линий сеть должна разбиться не менее чем на три фрагмента (компоненты связности). Это легко сделать, удалив все линии связи у двух серверов, расположенных в соседних вершинах куба. Потребуется вывести из строя 5 линий.

Осталось показать, что четырьмя линиями обойтись нельзя. Так как число компонент не меньше трёх, а всего вершин — восемь, то компонента с наименьшим числом вершин содержит одну или две вершины. В первом случае для изолирования одного сервера нужно вывести из строя все три ведущие к нему проводные линии. Легко видеть, что оставшуюся часть сети удалением одной линии разделить на две части невозможно. Во втором случае для изолирования компоненты, состоящей из двух серверов, уже надо удалить четыре проводных линии. При этом оставшаяся часть сети не распадётся на две компоненты.

17.6. Несколько участников нашли правильный ответ, просто не побоявшись «в лоб» вычислить указанное число, поделить его на 167 и далее подбирать простые делители по возрастанию.

Решение с меньшим объёмом вычислительной работы выглядит так. Выполним замену $3^4 = x$. Тогда наше число примет вид $x^5 + x + 1$. Разложим его на множители:

$$\begin{aligned} x^5 + x + 1 &= x^5 + x + 1 + x^4 - x^4 + x^3 - x^3 + x^2 - x^2 = \\ &= x^5 + x^4 + x^3 + x^2 + x + 1 - x^4 - x^3 - x^2 = \\ &= x^3(x^2 + x + 1) + x^2 + x + 1 - x^2(x^2 + x + 1) = (x^2 + x + 1)(x^3 - x^2 + 1). \end{aligned}$$

Первый множитель $x^2 + x + 1$ также может быть разложен:

$$\begin{aligned} x^2 + x + 1 &= 3^8 + 3^4 + 1 = 3^8 + 2 \cdot 3^4 + 1 - 3^4 = (3^4 + 1)^2 - 3^4 = \\ &= (3^4 + 3^2 + 1)(3^4 - 3^2 + 1) = 91 \cdot 73 = 7 \cdot 13 \cdot 73. \end{aligned}$$

Со вторым множителем дело обстоит чуть сложнее. Постараемся воспользоваться уже имеющейся информацией. Воспользуемся тем, что

$$x^3 - x^2 + 1 = x \cdot (x^2 + x + 1) + x + 3.$$

Заметим, что $x + 3 = 81 + 3 = 84$ делится на 7. Кроме того, мы установили, что на 7 делится число $x^2 + x + 1$, а значит и число $x^3 - x^2 + 1$. Таким образом,

$$x^3 - x^2 + 1 = x \cdot 7 \cdot 13 \cdot 73 + 84 = 7 \cdot (3^4 \cdot 13 \cdot 73 + 12).$$

Вычисляя далее значение выражения в скобках и деля его на 167, получаем

$$3^4 \cdot 13 \cdot 73 + 12 = 167 \cdot 449.$$

Ответ: $3^{20} + 3^4 + 1 = 7^2 \cdot 13 \cdot 73 \cdot 167 \cdot 449$.

18.1. Исходя из характера стёртых пикселей, нетрудно восстановить возможную перестановку, которой соответствуют варианты слов.

3			3	3			3	3
5		1	5	5		4	5	5
6	7		6	6	2		6	6
8		4	8	8		1	8	8
9			9	9			9	9

И	0		И	И			И	И
А		П	А	А		П	А	А
А	М		А	А	Т		А	А
Д		У	Д	Д		У	Д	Д
Л			Л	Л			Л	Л

Ответ: слово — АМПЛИТУДА, перестановка — (571932486) или (671932485).

18.2. Убеждаемся, что зашифрованный текст имеет длину 38. Осмысленная фраза имеет тогда длину 19. Выписываем друг под другом известные 5 первых знаков второй и первой половины зашифрованного текста и находим разность позиций соответствующих букв.

В	П	Б	Ь	Д
М	Х	Л	Щ	Л
22	27	22	3	25

Если $x_1x_2x_3x_4x_5$ — ключевое слово, то при первом шифровании использовалось оно само, а при втором — $x_5x_1x_2x_3x_4$. Таким образом, найденные разности равны соответственно $x_5 - x_1$, $x_1 - x_2$, $x_2 - x_3$, $x_3 - x_4$, $x_4 - x_5$. Тогда при известной первой букве x_1 остальные вычисляются по формулам: $x_5 = r_{33}(x_1 + 22)$, $x_4 = r_{33}(x_1 + 14)$, $x_3 = r_{33}(x_1 + 17)$, $x_2 = r_{33}(x_1 + 6)$, где $r_{33}(z)$ — остаток от деления числа z на 33. Перебирая 33 варианта для буквы x_1 , получаем 33 варианта ключевого слова, среди которых находится единственное осмысленное слово: КРЫША. При расшифровании получаем исходное сообщение.

Ответ: ВЕРБЛЮДЫДУТНАСЕВЕРВЕРБЛЮДЫДУТНАСЕВЕР, КРЫША.

18.3. Одним из возможных способов решения поставленной задачи является нахождение путей длины 5, ведущих из лаборатории (вершины № 3), если двигаться против стрелок. Сначала из вершины № 3 можно попасть в вершины № 8 и № 2, двигаясь только по неосвещённым коридорам. Из вершин № 8 и № 2 пути ведут только по неосвещённым коридорам в вершины № 7, № 5 и № 1, № 6 и т. д. Это приводит к построению дерева, приведённого на рис. 49. Остаётся перебрать 5 вариантов, считывая последовательности (из нулей и единиц) справа налево. Истинный вариант: 01011 (выделен жирным шрифтом).

Ответ: 01011.

Замечание. На самом деле, граф, представленный на рисунке, является графом де Брейна некоторой равновероятной булевой функции. При этом задача сводится к поиску такой последовательности знаков

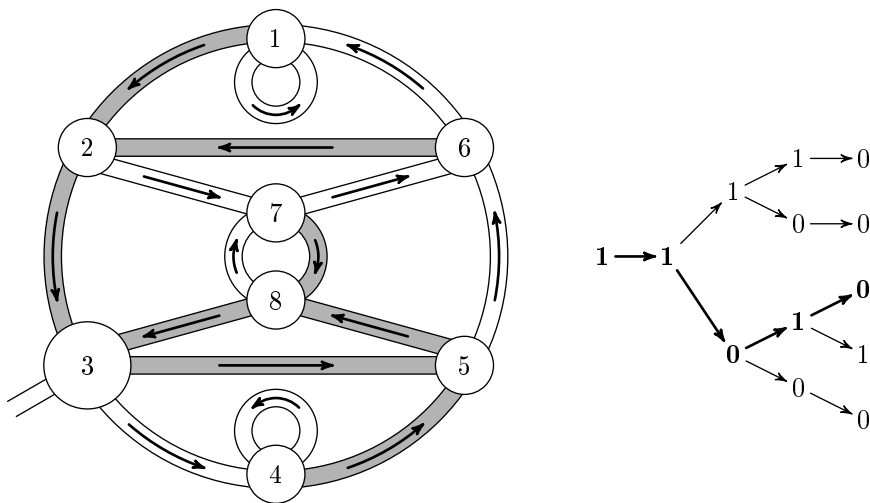


Рис. 49

выходной последовательности длины 5 (полузапрета), что в соответствующей системе уравнений определяются последние 3 неизвестные значениями $(0, 1, 1)$.

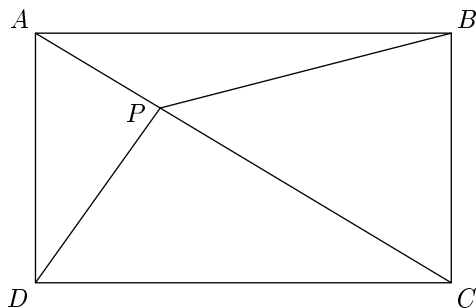
18.4. Последовательность состоит из цифр. Так как число четвёрок (a, b, c, d) конечно (и равно 10000), в данной последовательности рано или поздно встретятся две повторяющиеся четвёрки. Пусть они встретились на i -м и j -м местах, $0 \leq i < j$. Если $i = 0$, то всё доказано. Пусть $i > 0$.

Закон рекурсии:

$$u_{i+4} = r_{10}(u_{i+3} + u_{i+2} + u_{i+1} + u_i),$$

где $r_{10}(a)$ — остаток от деления числа a на 10. Заметим, что по заданным четырём членам последовательности можно однозначно восстановить предыдущий член. Другими словами, если цифры u_{i+4} , u_{i+3} , u_{i+2} , u_{i+1} известны, то существует единственная u_i , для которой выполняется описанное выше рекуррентное соотношение. Поэтому, если в последовательности совпали четвёрки на местах i и j , то совпадут четвёрки и на местах $i - 1$ и $j - 1$, и т. д. Поэтому совпадут четвёрки на местах 0 и $j - i$, ч. т. д.

18.5. Пусть дана четырёхугольная пирамида, основанием которой является прямоугольник. При этом расстояние от вершины пирамиды до одной вершины основания равно a , расстояние от вершины до противоположной вершины основания равно b , а расстояние до третьей вершины основания равно c . Найдём длину четвёртого бокового ребра d . Рассмотрим проекцию P вершины пирамиды на основание $ABCD$.



Пусть расстояние от точки P до сторон прямоугольника AB , BC , CD , AD равно x , y , z , v соответственно. Пусть h — высота пирамиды. Тогда имеем следующие равенства для определения длин боковых рёбер пирамиды:

$$x^2 + y^2 + h^2 = a^2,$$

$$v^2 + z^2 + h^2 = b^2,$$

$$y^2 + z^2 + h^2 = c^2.$$

Длина четвёртого (неизвестного) бокового ребра d выражается равенством

$$x^2 + v^2 + h^2 = d^2.$$

Из этих четырёх равенств нетрудно получить равенство

$$a^2 + b^2 = c^2 + d^2,$$

или $d^2 = a^2 + b^2 - c^2$. Осталось подставить в полученное выражение известные значения a , b , c , чтобы найти $d = 420$ км.

Ответ: 420 км.

18.6. а) $p = x - 1$, $q = x + 1$, $40003200063 = y^2 - 1$, $y^2 = 40003200064$. Нетрудно заметить, что $40003200064 = (200000 + z)^2$ и $z \in \{1, 2, \dots, 9\}$. Число 40003200064 заканчивается на 64, следовательно, $z = 8$.

Ответ: $p = 200007$, $q = 200009$.

б) $n = y^2 - t^2$, $y^2 = n + t^2$, где t — небольшое число, причём $y > \sqrt{n}$. Из представленных чисел легко определяется целая часть корня \sqrt{n} , она равна 200000. Оно увеличивается на единицу и возводится в квадрат (первый кандидат на y), и из полученного числа вычитается n (кандидат для t^2). Затем проверяется, извлекается ли квадратный корень из n — он извлекается и равен 40.

Ответ: $p = 199961$, $q = 200041$.

18.7. Да, делится. Число вида $2^k - 1$ делится на 3 тогда и только тогда, когда k чётно; на 5 — тогда и только тогда, когда k кратно 4; на 7 — тогда и только тогда, когда k кратно 3, а на 11 — тогда и только тогда,

когда k кратно 10. Показатель степени $2^{2007} + 3^{2008} - 2009$ делится на 4; он делится и на 3, т. к.

$$\begin{aligned} 2^{2007} + 3^{2008} - 2009 &= (2^{2007} - 2006) + (3^{2008} - 3) = \\ &= (2^{2007} - 2 - 2004) + (3^{2008} - 3) = 2 \cdot (2^{2006} - 1 - 1002) + (3^{2008} - 3), \end{aligned}$$

где $2^{2006} - 1 - 1002$ делится на 3. Поэтому в соответствии с первыми тремя критериями число, данное в условии задачи, делится на 3, 5 и 7. Числа 3^{2008} и 2^{2007} в десятичной записи оканчиваются на 1 и 8 соответственно, поэтому $2^{2007} + 3^{2008} - 2009$ делится на 10. Таким образом, число $2^{2^{2007} + 3^{2008} - 2009} - 1$ делится на $3 \cdot 5 \cdot 7 \cdot 11 = 1155$.

18.8. Сначала найдём в открытом тексте две уникальные буквы (по возможности близко расположенные). Это, например, К и Я, стоящие соответственно на 12-й и 16-й позициях в открытом тексте. В шифрованном тексте они стоят соответственно на местах 43 и на 28. Составляем систему уравнений

$$\begin{cases} 12a + b = 43k, \\ 16a + b = 28 + 43l. \end{cases}$$

Следовательно, $4a = 28 + 43t$. При $t = 0$ находим $a = 7$, из первого уравнения находим $b = 2$.

Расшифровав второй текст, получим искомое сообщение:

морозвоеводадозоромобходитвлaddenьясвои

18.9. а) При нажатии u раз на кнопку «вправо» и v раз на кнопку «влево» замок установится на деление с номером $r_{100}(43u - 20v)$, где $r_{100}(a)$ означает остаток от деления числа a на 100. Таким образом, нужно подобрать числа u, v такие, что $r_{100}(43u - 20v) = 50$.

Понятно, что достаточно подобрать число u , для которого $r_{100}(43u)$ будет равно 10, 30, 50, 70, 90, так как затем замок можно установить на ключ 50, вычитая 20 соответствующее число раз и вычисляя при этом остаток от деления на 100.

Будем действовать перебором ($u = 1, 2, \dots$): 43, 86, 129, 172, 215, 258, 301, 344, 387, 430. Поворачивая диск «вправо» 10 раз ($u = 10$) и 4 раза «влево» ($v = 4$), получаем: $r_{100}(30 - 80) = 50$. Итого, потребуется затратить 14 секунд. Из сделанных рассуждений видно, что за меньшее число секунд установить ключ в позицию 50 не удастся.

б) Продолжим перебор, показывающий, на какие деления можно установить замок только кнопкой «вправо»: 0, 43, 86, 129, 172, 215, 258, 301, 344, 387, 430, 473, 516, 559, 602, 645, 688, 731, 774, 817, 860. Далее кнопкой «влево» можно уменьшать эти числа на 20. Поэтому для того, чтобы можно было открыть замок при любом ключе, достаточно, чтобы среди перечисленных чисел встречались все остатки от деления на 20, что проверяется непосредственно. Следовательно, замок можно открыть при любом ключе.

в) Нужно найти u, v такие, что $r_{100}(43u - 20v) = k$, где k — ключ. Если $u \geq 20$, то можно уменьшить u на 20 следующим образом: $43u - 20v = 43(u - 20) - 20(v - 43)$. Следовательно, кнопку «вправо» имеет смысл жать не более 19 раз. При этом получим все остатки от деления на 20, как видно и из перебора, сделанного в п. б). Затем кнопку «влево» жмём не более 4 раз, так как $5 \cdot 20 = 100$ и за 5 раз диск сделает полный оборот. Таким образом, в выражении $r_{100}(43u - 20v) = k$ числа u, v заключены в пределах $0 \leq u \leq 19, 0 \leq v \leq 4$. Поэтому наименьшее время, необходимое для открытия любого замка, составит $19 + 4 = 23$ секунды.

18.10. Рассмотрим данное уравнение как уравнение второй степени относительно переменной a . При этом коэффициенты уравнения будут зависеть от x .

$$a^2 + (2x - 2)a - (x^4 + 2x^3 - 4x^2 - 2x + 3) = 0.$$

Решим это уравнение и получим, что

$$\begin{aligned} a &= 1 - x \pm \sqrt{(x - 1)^2 + x^4 + 2x^3 - 4x^2 - 2x + 3} = \\ &= 1 - x \pm \sqrt{x^4 + 2x^3 - 3x^2 - 4x + 4} = 1 - x \pm \sqrt{(x - 1)^2(x + 2)^2} = \\ &= 1 - x \pm (x - 1)(x + 2). \end{aligned}$$

Полученные равенства позволяют разложить исходное выражение на множители:

$$(a + x^2 + 2x - 3)(a - x^2 + 1) = 0.$$

Это позволяет свести решение исходного уравнения к решению двух уравнений меньшей степени.

$$1) \ x^2 + 2x + a - 3 = 0.$$

Дискриминант уравнения равен $16 - 4a$. Значит,

- при $a > 4$ уравнение не имеет решений,
- при $a = 4$ уравнение имеет единственное решение $x = -1$,
- при $a < 4$ уравнение имеет два решения $x = -1 \pm \sqrt{4 - a}$.

$$2) \ x^2 - (a + 1) = 0.$$

Дискриминант уравнения равен $4 + 4a$. Значит,

- при $a < -1$ уравнение не имеет решений,
- при $a = -1$ уравнение имеет единственное решение $x = 0$,
- при $a > -1$ уравнение имеет два решения $x = \pm\sqrt{1 + a}$.

Осталось объединить полученные ответы. Для этого необходимо дополнительно заметить, что при $a = 0$

$$x = -1 + \sqrt{4 - a} = \sqrt{1 + a} = 1,$$

а при $a = 3$

$$x = -1 - \sqrt{4 - a} = -\sqrt{1 + a} = -2.$$

При остальных значениях параметра a числа $x = -1 \pm \sqrt{4-a}$ и $x = \pm\sqrt{1+a}$ попарно различны.

Ответ:

- при $a < -1$ уравнение имеет два решения $x = -1 \pm \sqrt{4-a}$,
- при $a = -1$ уравнение имеет три решения $x = 0$ и $x = -1 \pm \sqrt{5}$,
- при $a = 0$ уравнение имеет три решения $x = -1$, $x = -3$, $x = 1$,
- при $a = 3$ уравнение имеет три решения $x = -2$, $x = 0$, $x = 2$,
- при $a = 4$ уравнение имеет три решения $x = -1$, $x = \pm\sqrt{5}$,
- при $-1 < a < 0$, при $0 < a < 3$ и при $3 < a < 4$ уравнение имеет четыре различных решения $x = -1 \pm \sqrt{4-a}$ и $x = \pm\sqrt{1+a}$,
- при $a > 4$ уравнение имеет два решения $x = \pm\sqrt{1+a}$.

18.11. Поскольку $x^2 + 1$ не обращается в ноль, можно разделить обе части уравнения на выражение $(x^2 + 1)^2$. Получим уравнение

$$(4a - 1) \cdot \left(\frac{2x}{x^2 + 1} \right)^2 + (4a + 1) \cdot \frac{2x}{x^2 + 1} + (a + 1) = 0.$$

Сделаем замену переменных $y = \frac{2x}{x^2 + 1}$. Рассмотрев график функции $y = \frac{2x}{x^2 + 1}$ (или любым другим стандартным способом), можно сделать вывод, что

- минимальное значение величины $y = \frac{2x}{x^2 + 1}$ равно -1 (при $x = -1$),

максимальное значение величины $y = \frac{2x}{x^2 + 1}$ равно 1 (при $x = 1$),

- множество значений величины $y = \frac{2x}{x^2 + 1}$ имеет вид $[-1; 1]$,
- для любого $c \in (-1; 0) \cup (0; 1)$ уравнение $\frac{2x}{x^2 + 1} = c$ имеет ровно два решения.

- Для $c \in \{-1; 1; 0\}$ уравнение $\frac{2x}{x^2 + 1} = c$ имеет единственное решение.

Теперь решим уравнение

$$(4a - 1) \cdot y^2 + (4a + 1) \cdot y + (a + 1) = 0.$$

Нам необходимо найти значения параметра a , при которых данное уравнение имеет ровно два решения, лежащие в множестве $(-1; 0) \cup (0; 1)$ (только при таких условиях исходное уравнение будет иметь четыре решения).

1) Если $a = -1$, то данное уравнение имеет решения $y = -\frac{3}{5}$, $y = 0$. В этом случае исходное уравнение имеет три решения. Кроме того, при $a \neq -1$ значение $y = 0$ не является решением уравнения.

2) Если $a = \frac{1}{4}$, то данное уравнение имеет решение $y = -\frac{5}{8}$. В этом случае исходное уравнение имеет два решения.

3) Пусть теперь $a > \frac{1}{4}$. В этом случае искомое множество значений параметра a описывается системой неравенств

$$\begin{cases} (4a+1)^2 - 4(4a-1)(a+1) > 0, \\ (4a-1) \cdot (-1)^2 + (4a+1) \cdot (-1) + a+1 > 0, \\ (4a-1) \cdot 1^2 + (4a+1) \cdot 1 + a+1 > 0, \\ -1 < -\frac{4a+1}{2(4a-1)} < 1. \end{cases}$$

(Здесь применяются известные факты о расположении корней квадратного трёхчлена.)

Решим эту систему при условии, что $a > \frac{1}{4}$.

$$\begin{cases} 5-4a > 0, \\ a-1 > 0, \\ 9a+1 > 0, \\ -2(4a-1) < -1-4a < 2(4a-1); \end{cases} \quad \begin{cases} a < \frac{5}{4}, \\ a > 1, \\ 4a > 3, \\ 12a > 1; \end{cases} \quad \begin{cases} a < \frac{5}{4}, \\ a > 1. \end{cases}$$

4) Пусть теперь $a < \frac{1}{4}$, $a \neq -1$. В этом случае искомое множество значений параметра a описывается системой условий

$$\begin{cases} (4a+1)^2 - 4(4a-1)(a+1) > 0, \\ (4a-1) \cdot (-1)^2 + (4a+1) \cdot (-1) + a+1 < 0, \\ (4a-1) \cdot 1^2 + (4a+1) \cdot 1 + a+1 < 0, \\ -1 < -\frac{4a+1}{2(4a-1)} < 1. \end{cases}$$

(Здесь применяются известные факты о расположении корней квадратного трёхчлена.) Решим эту систему при условии, что $a < \frac{1}{4}$, $a \neq -1$.

$$\begin{cases} 5-4a > 0, \\ a-1 < 0, \\ 9a+1 < 0, \\ -2(4a-1) > -1-4a > 2(4a-1); \end{cases} \quad \begin{cases} a < \frac{5}{4}, \\ a < -\frac{1}{9}, \\ 4a < 3, \\ 12a < 1; \end{cases} \quad \begin{cases} a < -\frac{1}{9}, \\ a \neq -1. \end{cases}$$

Ответ: $a \in (-\infty; -1) \cup \left(-1; -\frac{1}{9}\right) \cup \left(1; \frac{5}{4}\right)$.

19.1а. Заметим, что $841 = 29^2$ и что 29 — простое число. Теперь нетрудно сообразить, что существует $29(29-1) = 812$ натуральных чисел, которые не превосходят число 841 и не имеют с ним общих делителей, отличных от 1.

Ответ: 812.

19.16. Сначала заметим, что если $N = pq$, где p и q — простые числа, то количество натуральных чисел, меньших N и взаимно простых с N , равно $(p-1)(q-1)$ (обозначим это число $\varphi(N)$). Действительно, всего имеется $pq-1$ натуральных чисел, меньших N . Из них не взаимно просты с N те числа, которые делятся либо на p , а именно $p, 2p, \dots, (q-1)p$ (всего $q-1$ чисел), либо на q — это числа $q, 2q, \dots, (p-1)q$ (всего $p-1$ чисел). Значит,

$$\varphi(N) = pq - 1 - (p-1) - (q-1) = pq - p - q + 1 = (p-1)(q-1).$$

Получаем систему уравнений:

$$\begin{cases} pq = N, \\ (p-1)(q-1) = \varphi(N) \end{cases} \quad \text{или} \quad \begin{cases} pq = N, \\ p+q = N+1-\varphi(N). \end{cases}$$

По теореме Виета получаем, что p и q — корни уравнения

$$x^2 - (N+1-\varphi(N))x + N = 0.$$

$N = 202718099$, $\varphi(N) = 202687920$, и уравнение имеет вид

$$x^2 - 30180x + 202718099 = 0.$$

Корень из дискриминанта равен $\sqrt{D} = \sqrt{99960004}$. Чтобы извлечь квадратный корень из этого числа, можно заметить, что результат должен быть немного меньше, чем 10000, причём последняя цифра в этом числе должна быть 2 или 8. Претендентами будут следующие числа: 9998, 9992, 9988, 9982... Последовательно возводя их в квадрат, находим: $9998^2 = 99960004$. Итак:

$$x_1 = \frac{30180 - 9998}{2} = 10091 = p; \quad x_2 = \frac{30180 + 9998}{2} = 20089 = q.$$

Ответ: 10091 и 20089.

19.2а. Заметим, что четырёхкратный поворот грани ничего не изменяет, а трёхкратный поворот по часовой стрелке эквивалентен одному повороту против часовой стрелки. Таким образом, чтобы узнать, как были расположены буквы при шифровании, необходимо повернуть грань 1 — два раза; грань 2 — один раз (против часовой стрелки); грань 3 — один раз; грань 4 — не поворачивать; грань 5 — два и, наконец, грань 6 — один раз. После этого, исходя из расположения букв на полученном кубике, можно найти исходное сообщение, заменяя буквы шифртекста на буквы, стоящие в клетках против часовой стрелки. Отметим, что нет необходимости узнавать, куда перешли все написанные на кубе буквы. Достаточно узнать расположение букв шифртекста

ста после описанных преобразований. После этого следует выделить клетку, следующую против часовой стрелки за клеткой с рассматриваемой буквой шифртекста. Затем необходимо осуществить обратное преобразование, и в выделенной клетке на исходном кубе окажется соответствующая буква открытого текста.

Ответ: Джероламо Кардано.

19.26. Поскольку при данном способе шифрования буквы Т, Ч, К, Ф, Э, Ц не изменяются, можно предположить, что одно из вхождений буквы Т в зашифрованном тексте принадлежит трёхбуквенному сочетанию ЗПТ:

ЕП ОЕ Ъ Р И Т С Г Х Ж З Т Я П С Т А П Д С Б И С Т Ч К
 З П Т З П Т З П Т

Предположим, что это сочетание ЖЗТ. Отсюда следует, что при шифровании З переходит в Ж, а П переходит в З. Рассмотрим все возможные варианты поворота трёх граней и выделим из них те, при которых такие переходы возможны (см. таблицу ниже).

1	2	3	4	5	6	З → Ж	П → З
0	0	0	1	1	1	+	—
0	0	1	1	1	0	—	
0	1	1	1	0	0	+	—
1	1	1	0	0	0	+	—
0	0	1	0	1	1	—	
0	0	1	1	0	1	—	
0	1	0	1	1	0	—	
0	1	1	0	1	0	—	
1	0	1	1	0	0	—	
1	1	0	1	0	0	+	—
0	1	0	0	1	1	—	
0	1	1	0	0	1	+	—
1	0	0	1	1	0	+	—
1	1	0	0	1	0	—	
1	0	0	0	1	1	+	+
1	1	0	0	0	1	+	—
0	1	0	1	0	1	+	—
1	0	1	0	1	0	—	
1	0	0	1	0	1	—	
1	0	1	0	0	1	—	

Рассмотрим первый случай: 000111, который свидетельствует о том, что поворачивались грани 4, 5 и затем 6. Проследим движение выделен-

ных букв, исходя из такого вращения (рис. 50, первая строка). Заметим, что буквы З и П при шифровании будут переходить в буквы, стоящие в соответствующих окрашенных клетках (рис. 50, вторая строка, справа). Совершая обратное преобразование, находим эти буквы. Таким образом, при указанном движении З переходит в Ж, а П в З не переходит, о чём сделаем отметку в таблице. Продолжая эту процедуру для других возможных комбинаций движения, заполняем таблицу. Для перехода $З \rightarrow Ж$ существует девять вариантов. Отбросим из них те, для которых невозможен переход $П \rightarrow З$. Остаётся один вариант: **100011**. Следовательно, чтобы получить кубик, на котором проводилось шифрование, необходимо по одному разу повернуть первую грань, пятую и шестую. Производя расшифрование сообщения, получим открытый текст:

ДОЖДУСЬТЕБЯЗПТМОЕТВОРЕНЬЕТЧК.

Отметим, что для других вариантов расположения триграммы ЗПТ получается либо нечитаемый текст, либо нарушаются условия перехода выделенных букв.

Ответ: Дождусь тебя, моё творенье.

19.3. В условии задачи имеется 3 зашифрованных сообщения C_1, C_2, C_3 :

$$C_1 = M + K_{\Gamma} = \text{ЁЛИСУВШОЩОМОВЫЗПЭЪМО};$$

$$C_2 = C_1 + K_{\Psi} = M + K_{\Gamma} + K_{\Psi} = \text{ЪЭЛВШРЕЭТЖЩЮИГВФСЦХ};$$

$$C_3 = C_2 - K_{\Gamma} = M + K_{\Psi} = \text{ЖЪХЙТСЖЯШШЬЯМЫШЗЪВГ},$$

где M — исходное сообщение, K_{Γ} — последовательность, выбранная Крокодилом Геной; K_{Ψ} — последовательность, выбранная Чебурашкой. Тогда открытый текст можно найти следующим образом: $M = C_1 - C_2 + C_3$.

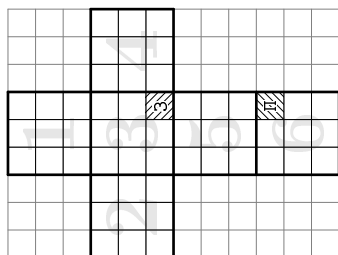
Ответ: ТИШЕ ЕДЕШЬ ДАЛЬШЕ БУДЕШЬ.

19.4. Рассмотрим сумму нового пароля SARCL и известного старого пароля СВЕЧА, от числовых значений которого взяты остатки от деления на 26. От значений полученной суммы также возьмём остатки от деления на 26:

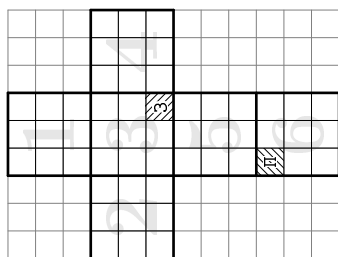
$$+ \begin{array}{ccccc} \text{S} & \text{A} & \text{R} & \text{C} & \text{L} \\ \text{C} & \text{В} & \text{Е} & \text{Ч} & \text{А} \end{array} = + \begin{array}{ccccc} 19 & 1 & 18 & 3 & 12 \\ 19 & 3 & 6 & 25 & 1 \end{array} = \begin{array}{ccccc} 12 & 4 & 24 & 2 & 13 \end{array}.$$

Таким образом, получено зашифрованное сообщение, переданное Катей и искажённое на приёмном конце программой Юры. На самом деле зашифрование осуществлялось в русском алфавите, поэтому для некоторых числовых значений зашифрованного сообщения возможны варианты:

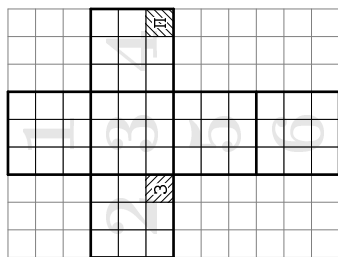
$$\begin{array}{ccccc} 12 & 4 & 24 & 2 & 13 \\ & 4+26 & & 2+26 & \end{array} = \begin{array}{ccccc} 12 & 4 & 24 & 2 & 13 \\ & 30 & & 28 & \end{array}.$$



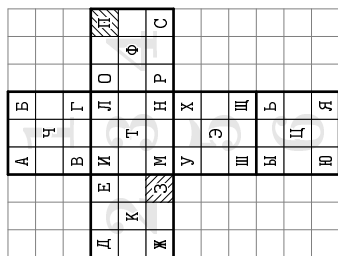
ВРАЩАЕМ
ГРАНЬ 6



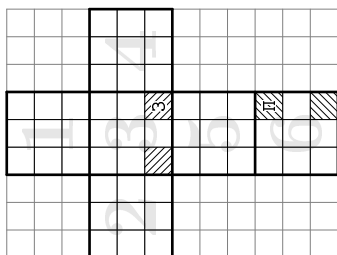
ВРАЩАЕМ
ГРАНЬ 5



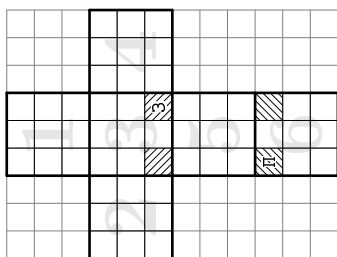
ВРАЩАЕМ
ГРАНЬ 4



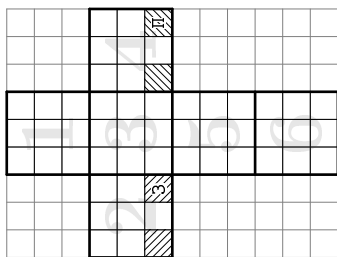
ВРАЩАЕМ
ГРАНЬ 4



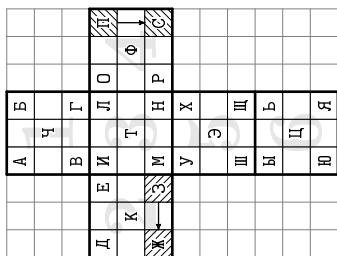
ВРАЩАЕМ
ГРАНЬ 6



ВРАЩАЕМ
ГРАНЬ 5



ВРАЩАЕМ
ГРАНЬ 4



ВРАЩАЕМ
ГРАНЬ 4

Рис. 50

Вычтем теперь из полученных числовых вариантов зашифрованного пароля числовые значения старого пароля в русском алфавите 19 3 6 25 1:

$$\begin{array}{cccc} -7 & 1 & 18 & -23 \\ & 27 & & 3 \end{array} \quad 12$$

и возьмём от полученных разностей остатки от деления на 33. Получим:

$$\begin{array}{cccc} 26 & 1 & 18 & 10 \\ & 27 & & 3 \end{array} \quad 12 = \begin{array}{c} \text{А} \\ \text{Щ} \end{array} \begin{array}{c} \text{Р} \\ \text{В} \end{array} \begin{array}{c} \text{И} \\ \text{К} \end{array}.$$

Единственный читаемый вариант — ШАРИК.

Ответ: ШАРИК.

19.5. Заметим, что $12 = 3 + 3 + 3 + 3$, $13 = 7 + 3 + 3$, $14 = 7 + 7$. Таким образом, имеется три подряд идущих числа, которые представимы в требуемом виде. Очевидно, что все последующие числа получаются прибавлением или к 12, или к 13, или к 14 нужного числа монет достоинством 3 единицы. Остаётся перебором чисел от 1 до 11 найти цены, которые нельзя устанавливать.

Приведём здесь ещё одно решение этой задачи, несколько более «математизированное», но вместе с тем познавательное и поучительное.

Фактически надо найти числа x, y такие, что $ax + by = n$ (в данном случае $a = 3$, $b = 7$). Уравнение $ax + by = n$, где $\text{НОД}(a, b) = 1$, неразрешимо в неотрицательных целых числах x, y при $n = F(a, b) = ab - a - b$ и разрешимо при всех натуральных $n > F(a, b) = ab - a - b$. Число $F(a, b)$ называется числом Фробениуса для пары (a, b) . Чтобы заметить это, покажем, что каждое из равносильных уравнений

$$ax + by = ab - a - b; \quad a(x + 1) + b(y + 1) = ab; \quad ax' + by' = c$$

не имеет натуральных решений x', y' при $c = ab$ и имеет такие решения при всех $c > ab$. Пусть при натуральных a, b, x', y' выполнено $ax' + by' = ab$. Тогда $ax' = b(a - y')$, т. е. x' делится на b (так как $\text{НОД}(a, b) = 1$ и у чисел a, b нет общих делителей, кроме 1). Следовательно $x' \geq b$. Тогда $ax' + by' > ab$, пришли к противоречию.

Пусть $c > ab$, тогда, в силу условия $\text{НОД}(a, b) = 1$, найдутся такие натуральные u, v (алгоритм Евклида), что $au - bv = c > ab$, т. е. $\frac{u}{b} - \frac{v}{a} > 1$. Следовательно, найдётся такое натуральное t , что $\frac{u}{b} > t > \frac{v}{a}$. Для этого t зададим натуральные числа x', y' следующим образом: $x' = u - bt$, $y' = at - v$. Тогда

$$ax' + by' = a(u - bt) + b(at - v) = au - bv = c.$$

Ответ: $\{1, 2, 4, 5, 8, 11\}$.

19.6. Способ 1. Поскольку для длин сторон $AB = 99$, $AC = 71$ и для значений углов 67° и 360° $\text{НОД}(99, 71) = 1$, $\text{НОД}(67, 360) = 1$, по схеме

алгоритма Евклида можно построить отрезок длины 1 и угол, равный 1° .

Схема алгоритма Евклида с помощью циркуля и линейки реализуется следующим образом. Сначала на большом отрезке AB последовательно от точки A засечками циркуля откладывается малый отрезок AC максимально возможное число раз (в данном случае 1 раз). Остаётся отрезок длины 18. Затем на AC максимальное число раз откладывается этот остаток. Получается новый остаток и т. д. В конце концов получится остаток длины 1.

Идейно так же построим угол 1° . Для этого опишем окружность произвольного радиуса с центром в точке A . Возьмём раствор циркуля, равный расстоянию между точками пересечения окружности с полупрямыми AB и AC . Этим раствором отложим последовательно на окружности дуги, соответствующие центральному углу $\angle BAC = 67^\circ$ максимально возможное количество раз. В результате получается угол, равный в градусах остатку от деления 360 на 67, т. е. 25° . Затем этот остаток раствором циркуля отложим наибольшее число раз на дуге, соответствующей центральному углу 67° (т. е. 2 раза). Получим остаток 17° и т. д. В итоге получится угол, равный 1° .

Способ 2. С помощью циркуля и линейки не составляет труда построить угол в 90° , а также угол в 30° и 60° . Кроме того, в условии дан угол в 67° . Искомый угол в 51° может быть построен, исходя из соотношения: $51^\circ = 67^\circ - 16^\circ$, поэтому достаточно научиться строить угол в 16° . Для этого можно заметить, что $16^\circ = 2 \cdot 90^\circ - 2 \cdot 67^\circ - 30^\circ$. Поэтому $51^\circ = 3 \cdot 67^\circ + 30^\circ - 2 \cdot 90^\circ$.

Для построения отрезков длины 101 и 73 можно заметить, что $101 = 7 \cdot 71 - 4 \cdot 99$; $73 = 8 \cdot 71 - 5 \cdot 99$.

19.7. Заметим, что на нечётных местах исходного текста могут появляться только цифры 0, 1, 2 и 3. Поэтому, если из одного шифртекста вычесть другой, зашифрованный с помощью той же последовательности, на нечётных местах разности могут получиться не любые цифры, а только 0, 1, 2, 3, 7, 8, 9, что будет являться критерием для выбора искомого цепочек.

Ответ: первая и вторая.

19.8. Пусть в двоичной системе счисления $A = (x_n, \dots, x_0)$. Тогда $A_1 = (x_3, x_2, x_1, x_0)$, $A_2 = (x_4, x_3, x_2, x_1)$, $A_3 = (x_5, x_4, x_3, x_2)$. Следовательно,

$$a_1 \oplus a_2 = (A_1 \oplus B) \oplus (A_2 \oplus B) = A_1 \oplus A_2 = (x_3 \oplus x_4, x_2 \oplus x_3, x_1 \oplus x_2, x_0 \oplus x_1),$$

$$a_3 \oplus a_2 = (A_3 \oplus B) \oplus (A_2 \oplus B) = A_3 \oplus A_2 = (x_5 \oplus x_4, x_4 \oplus x_3, x_3 \oplus x_2, x_2 \oplus x_1).$$

Итак, если вычислить $a_1 \oplus a_2$, то три младших бита $a_3 \oplus a_2$ будут найдены, а старший бит будет произвольным.

Вычислим значение $a_1 \oplus a_2$:

$$\begin{array}{cccc} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ \hline 1 & 1 & 1 & 0 \end{array}$$

Тогда возможные значения $(a_2 \oplus a_3)$ имеют вид $(*, 1, 1, 1)$, и $a_3 = a_2 \oplus (a_3 \oplus a_2)$:

$$\begin{array}{cccc} 1 & 0 & 1 & 0 \\ * & 1 & 1 & 1 \\ \hline * & 1 & 0 & 1 \end{array}$$

Итак, $a_3 = 13$, либо $a_3 = 5$. Можно убедиться в том, что оба варианта верны, если рассмотреть последовательности с параметрами $A = 20$, либо $A = 52$ и $B = 0$.

Ответ: 13 и 5.

19.9. Перемещаем указанное в условии слово под шифрованным текстом. При правильном расположении этого слова после его вычитания из фрагмента шифрованного текста получим значения, образующие геометрическую прогрессию, от членов которой взяты остатки от деления на 31 (см. таблицу).

...	Ф	Б	К	П	Щ	С	Ь	...
	Р	А	В	Н	И	Н	Ы	
...	20	1	10	15	25	17	27	...
...	16	0	2	13	9	13	26	...
...	4	1	8	2	16	4	1	...

Ответ: МОРОЗНО РАВНИНЫ БЕЛЕЮТ ПОДСНЕГОМ ЧЕРНЕЕТСЯ ЛЕС ВПЕРЕДИ, $b = 2$, $a = 1$.

19.10. Одно из возможных решений указано в таблице. Номеру поездки соответствует город прибытия. Для того чтобы такая таблица соответствовала решению, все комбинации, состоящие из четырёх цифр, каждая из которых равна либо 0, либо 1, должны быть перечислены и последовательные комбинации должны отличаться в одном разряде.

№ поездки	
1	0001
2	0011
3	0010
4	0110
5	0111
6	0101
7	0100
8	1100

№ поездки	
9	1101
10	1111
11	1110
12	1010
13	1011
14	1001
15	1000
16	0000

19.11а. Приведём геометрическое решение данной задачи.

а) Рассмотрим графики линий, задаваемых системой уравнений при $a > 0$ (рис. 51): $\begin{cases} |y| = 1 - x, \\ y = 2 - a|x|. \end{cases}$ Отсюда видно, что при $a > 0$ система может иметь 1, 2, 3 или 4 решения.

Ровно 3 решения система имеет при тех $a > 0$, при которых луч $y = 2 - ax$, $x > 0$, проходит через точку $B(1, 0)$, то есть при $a = 2$.

При $a > 2$ луч $y = 2 - ax$, $x > 0$, пересекает линию $|y| = 1 - x$ в двух точках. Поэтому в данном случае система имеет ровно 4 решения.

При $0 < a < 2$ луч $y = 2 - ax$, $x > 0$ не пересекает линию $|y| = 1 - x$. Поэтому в данном случае система имеет 1 или 2 решения. Два решения получаются пересечением луча $y = 2 - a|x|$, $x < 0$ и линии $|y| = 1 - x$ в двух точках. Это может быть, если луч $y = 2 - a|x|$, $x < 0$, имеет угловой коэффициент (равный a) больший, чем 1.

Итак, при $1 < a < 2$ система имеет ровно 2 решения.

Если же $0 < a \leq 1$, то система имеет 1 решение.

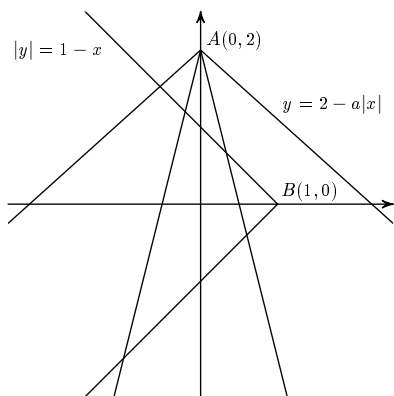


Рис. 51

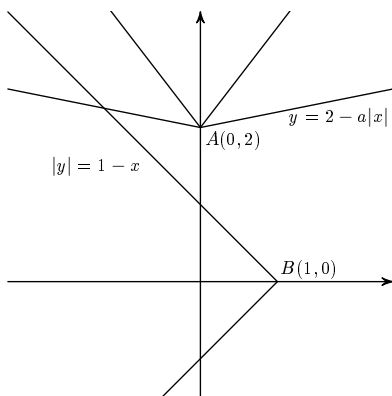


Рис. 52

б) Рассмотрим графики линий, задаваемых системой уравнений при $a < 0$ (рис. 52). Из рисунка видно, что при $a < 0$ система может иметь 0 или 1 решение.

Система не имеет решений при тех $a < 0$, при которых луч $y = 2 - a|x|$, $x < 0$, не пересекает линию $|y| = 1 - x$, то есть при $a \leq -1$.

При $-1 < a < 0$ луч $y = 2 - a|x|$, $x < 0$, пересекает линию $|y| = 1 - x$ ровно в одной точке. Поэтому в данном случае система имеет ровно 1 решение.

в) При $a = 0$ система, очевидно, имеет ровно 1 решение, а именно $(-1; 2)$.

Ответ:

- при $a \leq -1$ нет решений;
- при $-1 < a \leq 1$ система имеет 1 решение;
- при $1 < a < 2$ система имеет 2 решения;
- при $a = 2$ система имеет 3 решения;
- при $a > 2$ система имеет 4 решения.

19.116. Первое неравенство задаёт область внутри параболы $y = x^2 - 1$. Рассмотрим второе неравенство $ya^2 + (2x)a - (y + 2) \leq 0$. Для того чтобы данное неравенство выполнялось для всех значений параметра a при данных $(x; y)$, необходимо и достаточно выполнение условий

$$\begin{cases} y \leq 0, \\ x^2 + y(y + 2) \leq 0. \end{cases}$$

Этот вывод можно сделать, если рассмотреть многочлен $ya^2 + (2x)a - (y + 2)$ как квадратный трёхчлен относительно a с коэффициентами, зависящими от x, y .

В результате имеем систему условий

$$\begin{cases} y \geq x^2 - 1, \\ y \leq 0, \\ x^2 + y(y + 2) \leq 0; \end{cases} \quad \begin{cases} y \geq x^2 - 1, \\ y \leq 0, \\ x^2 + (y + 1)^2 \leq 1. \end{cases}$$

Множество всех точек на плоскости Oxy с координатами $(x; y)$, удовлетворяющими этой системе условий, указано на схематическом рисунке (см. рис. 53, заштрихованная область).

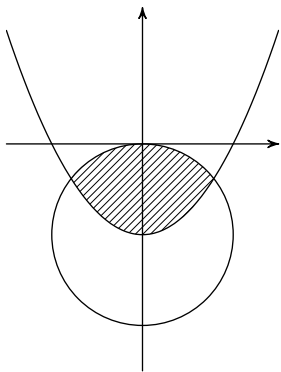


Рис. 53

20.1. Отметим, что восстановить исходный текст короткого сообщения, зашифрованного с использованием такого шифра (являющегося шифром простой замены), не так-то просто. Помогает здесь то, что в сообщении сохранена разбивка на слова, оставлены знаки пре-

пинания и заглавные буквы. Если обратить внимание на сочетание Яспар-Дюрюмгшт и содержащееся в ответе Godzilly упоминание города Питера, то можно предположить, что речь идёт о Санкт-Петербурге. Составим таблицу соответствий:

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
К				Б	П									Р				Н	Т	А	Г					У					Е	С

В соответствии с этими заменами некоторые буквы в зашифрованном тексте можно восстановить:

. .А.ТРА УЕ..А. . САНКТ-ПЕТЕРБУРГ НА ..Е НЕ.Е... . ПАР...:
БУРГУН...

Далее подбираем некоторые слова по смыслу. Весьма вероятно, что .А.ТРА — это ЗАВТРА, ПАР... — это ПАРОЛЬ. С учётом этих предположений сообщение примет вид:

. ЗАВТРА УЕЗ.А. В САНКТ-ПЕТЕРБУРГ НА .ВЕ НЕ.ЕЛ. . ПАРОЛЬ:
БУРГУН... .

Затем по смыслу окончательно получаем искомое сообщение.

Ответ: Я завтра уезжаю в Санкт-Петербург на две недели. Пароль: Бургундия.

20.2. Обозначим через x число букв, получившихся при наборе цифры 7 (их может быть от 1 до 3), y — число букв при наборе цифры 5 (1 или 2) и z — число букв при наборе цифры 9 (от 2 до 5). Перечислим возможные варианты представления числа 10 в виде суммы $x + 1 + y + 1 + z$:

- 1) $3 + 1 + 2 + 1 + 3$; 2) $3 + 1 + 1 + 1 + 4$; 3) $2 + 1 + 2 + 1 + 4$;
4) $2 + 1 + 1 + 1 + 5$; 5) $1 + 1 + 2 + 1 + 5$.

Для варианта 1 получить три буквы, нажимая 7, можно только одним способом; получить две буквы, нажимая 5, можно снова только одним способом; получить три буквы с помощью пяти девяток можно 6 способами. В итоге для варианта 1 имеем $1 \cdot 1 \cdot 6$ вариантов паролей, аналогично для варианта 2 будет $1 \cdot 1 \cdot 4$ вариантов паролей и т. д. Всего получаем $6 + 4 + 2 \cdot 4 + 2 + 1 = 21$ вариант.

Ответ: 21.

20.3. Разность значений квадратичной функции должна делиться на разность значений аргументов. Проверим выполнение этого факта для различных пар значений:

- для первого и второго: $357 - 273 = 84$ делится на 3;
- для третьего и четвёртого: $497 - 391 = 106$ не делится на 3; следовательно, значение исказили или гномы, или орки;
- для первого и третьего: $391 - 273 = 118$ не делится на 4, следовательно, значение исказили тролли или гномы.
- для второго и четвёртого: $497 - 357 = 140$ делится на 4.

Ответ: Гномы сообщили неверное значение.

Замечание. В данной задаче заложена идея, заключающаяся в разделении некоторого секрета между участниками. Пусть, например, для того чтобы открыть сейф, необходимо использовать t ключей, хранящихся у t различных лиц. То есть совершение действия по открытию сейфа подразумевает согласие группы лиц и их общую ответственность. Данный метод, называемый *схемой разделения секрета*, может быть реализован и при помощи математических средств. Например, для разделения секрета a_0 между t участниками может быть выбран многочлен степени $t-1$ вида $f(x) = a_0 + a_1x + \dots + a_{t-1}x^{t-1}$, коэффициенты которого a_0, a_1, \dots, a_{t-1} хранятся в секрете в некотором центре, которому доверяют все участники. Каждый участник выбирает своё число c_i , $c_i \neq 0$, предоставляет его в центр доверия, который возвращает значение многочлена $f(c_i)$. Таким образом, если участники обмениваются своими числами c_i и соответствующими значениями $f(c_i)$, то, имея в распоряжении t значений многочлена от различных чисел, возможно найти все его коэффициенты, в частности, секрет a_0 . Меньшее число участников однозначным образом сделать это не сможет.

Здесь необходимо сказать о задаче нахождения секрета в случае, если какие-то m , $m < t$, несогласных участников предъявляют ложные значения. Можно ли в этом случае найти a_0 ? Оказывается, что да, но при условии, что будет известно ещё $m+1$ значений многочлена от других значений честных участников. При этом можно распознать и несогласных участников.

20.4. Сначала заметим, что после первого оборота количество дуг равно 2^2 , после второго — 2^3 , после последнего — 2^{n+1} . Пусть после оборота с номером k , $1 \leq k \leq n$, в точках деления окружности на дуги расположены числа $x_1, x_2, \dots, x_{2^{k+1}}$. Тогда в ходе оборота с номером $k+1$ на окружности появятся следующие новые числа

$$y_1 = \frac{3x_1 + 3x_2}{2}, \quad y_2 = \frac{3x_2 + 3x_3}{2}, \quad \dots, \quad y_{2^{k+1}} = \frac{3x_{2^{k+1}} + 3x_1}{2}.$$

Очевидно, что

$$\sum_{i=1}^{2^{k+1}} y_i = 3 \cdot \sum_{i=1}^{2^{k+1}} x_i.$$

Значит, после $k+1$ оборота сумма всех чисел на окружности возрастет в 4 раза. Если учесть, что первоначальная сумма чисел на окружности равнялась 6, то получаем окончательный ответ.

Ответ: $6 \cdot 4^n$.

20.5. Граф, используемый в задаче, обладает следующим свойством: из множества всех его вершин можно выделить такое подмножество V (отмеченное на рис. 54 кружочками), что любая вершина графа лежит в

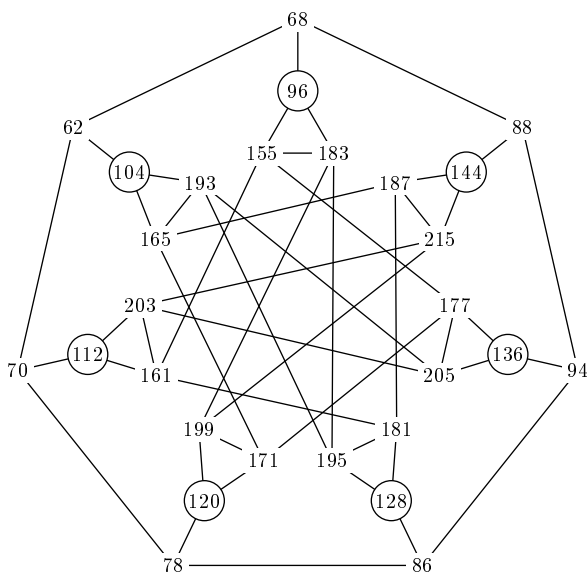


Рис. 54

окрестности ровно одной вершины из V . Окрестностью вершины графа называют множество соседних с ней вершин, включая её саму. Очевидно, что искомое число равно сумме чисел, расположенных в вершинах из множества V : $112 + 104 + 96 + 144 + 136 + 128 + 120 = 840$.

Ответ: 840.

Замечание. Задача нахождения подмножества V имеет следующую интерпретацию в теории помехоустойчивого кодирования. Вершины графа соответствуют блокам информации, которые можно передавать по некоторому каналу связи. Отдельно взятая вершина соединяется с другими вершинами, соответствующим тем блокам информации, в которые может перейти исходный блок при искажении, возникающем в канале связи. Для того чтобы на приёмном конце можно было однозначно распознать передаваемое сообщение, исходя из полученного искажённого, необходимо первоначально подобрать передаваемые блоки специальным образом, чтобы их окрестности не пересекались. Совокупность таких блоков и образует код. Сообщение перед передачей переводится в последовательность блоков из кода. Если любой блок, который можно передавать по каналу, можно получить из блока кода за счёт искажений, то код называют *совершенным*. Заметим, что множество V из решения задачи как раз является совершенным кодом.

Нахождение самого множества V по заданному графу (если оно существует) относится к классу вычислительно сложных задач (так называемых NP-полных задач). Это означает, что время работы алгоритма при увеличении количества вершин в графе растёт очень быстро. В то же время это обстоятельство не обеспечивает стойкости шифрования описанным способом, так как по известным данным возможно составить систему линейных уравнений и решить её (например, методом Гаусса). Известно, что этот метод позволяет сравнительно быстро решать эту задачу и при увеличении числа вершин. Для графа, приведённого в задании, в силу его небольшого размера, нахождение множества V оказывается более простой задачей, чем решение соответствующей системы линейных уравнений.

20.6. Для комбинации $1, 0, 1, 1, 0$ — проход открыт, а для $0, 0, 1, 1, 0$ — проход закрыт. То есть при изменении значения первой координаты с 1 на 0 значение суммы становится меньше c , поэтому очевидно, что $a_1 > 0$. Аналогично

$$\left. \begin{array}{l} 1, 1, 1, 1, 1 — \text{открыто} \\ 1, 0, 1, 1, 1 — \text{закрыто} \end{array} \right\} \Rightarrow a_2 > 0;$$

$$\left. \begin{array}{l} 1, 1, 1, 1, 1 — \text{открыто} \\ 1, 1, 0, 1, 1 — \text{закрыто} \end{array} \right\} \Rightarrow a_3 > 0;$$

$$\left. \begin{array}{l} 1, 0, 1, 1, 0 — \text{открыто} \\ 1, 0, 1, 0, 0 — \text{закрыто} \end{array} \right\} \Rightarrow a_4 > 0;$$

$$\left. \begin{array}{l} 1, 0, 1, 1, 0 — \text{открыто} \\ 1, 0, 1, 1, 1 — \text{закрыто} \end{array} \right\} \Rightarrow a_5 < 0.$$

Поэтому заведомо пройдёт комбинация, максимизирующая значение суммы S , а именно $1, 1, 1, 1, 0$. Отметим, что задача составлена таким образом, что других решений нет.

Ответ: $1, 1, 1, 1, 0$.

20.7. *Способ 1.* Составим, исходя из условия задачи, систему неравенств и запишем её в виде двух подсистем (без a_1 и с a_1):

$$\left\{ \begin{array}{l} 0 < c, \\ a_4 < c, \\ a_3 \geq c, \\ a_3 + a_4 \geq c, \\ a_2 < c, \\ a_2 + a_4 < c, \\ a_2 + a_3 < c, \\ a_2 + a_3 + a_4 < c; \end{array} \right. \quad \left\{ \begin{array}{l} a_1 < c, \\ a_1 + a_4 \geq c, \\ a_1 + a_3 \geq c, \\ a_1 + a_3 + a_4 \geq c, \\ a_1 + a_2 < c, \\ a_1 + a_2 + a_4 < c, \\ a_1 + a_2 + a_3 \geq c, \\ a_1 + a_2 + a_3 + a_4 \geq c. \end{array} \right.$$

Из первой подсистемы получаем:

$$\begin{cases} a_3 \geq c, \\ a_2 + a_3 + a_4 < c \end{cases} \implies a_2 + a_4 < 0.$$

Из второй подсистемы получаем:

$$\begin{cases} a_1 < c, \\ a_1 + a_4 \geq c \end{cases} \implies a_4 > 0;$$

$$\begin{cases} a_1 < c, \\ a_1 + a_2 + a_3 \geq c \end{cases} \implies a_2 + a_3 > 0.$$

Подбираем некоторые целые числа, удовлетворяющие полученным соотношениям, например $a_4 = 1$, $a_2 = -2$, $a_3 = 3$. Подставляем их в первую подсистему, тогда $2 < c \leq 3$. Полагаем $c = 3$ и подставляем во вторую подсистему, получаем $2 \leq a_1 < 3$, тогда выбираем $a_1 = 2$.

Способ 2. Определим меру влияния каждой переменной x_i , $i = \overline{1, 4}$, на значение линейной формы S , а именно оценим, как влияет изменение значения x_i при переходе с 0 на 1 на изменение значения S при каждой фиксации остальных переменных. Например, на наборе $(0, 0, 0, 1)$ формируется значение $y = 0$, а на наборе $(1, 0, 0, 1)$ получаем $y = 1$, поэтому в соответствующую клетку ставим 1 (в таблице она выделена жирным). Подсчитаем сумму таких знакоперемен для каждой переменной:

	0, 0, 0	0, 0, 1	0, 1, 0	0, 1, 1	1, 0, 0	1, 0, 1	1, 1, 0	1, 1, 1	сумма знакоперемен
x_1 : 0 1	0	1	0	0	0	0	1	1	3
x_2 : 0 1	0	0	-1	-1	0	-1	0	0	-3
x_3 : 0 1	1	1	0	0	1	0	1	1	5
x_4 : 0 1	0	0	0	0	1	0	0	0	1

Нетрудно сообразить, что соответствующий коэффициент при x_i будет тем больше, чем будет больше таких знакоперемен. Тогда выберем в качестве параметров a_i , $i = \overline{1, 4}$, значения, соответствующие числам в крайнем правом столбце в приведённой выше таблице: $a_1 = 3$, $a_2 = -3$, $a_3 = 5$, $a_4 = 1$.

Теперь необходимо найти c . Рассматривая все наборы, на которых $y = 1$, устанавливаем, что минимум линейной формы $S = 3x_1 - 3x_2 + 5x_3 + x_4$ достигается на наборе $(1, 0, 0, 1)$ и равен 4. Аналогично, рассматривая все наборы, на которых $y = 0$, получаем, что максимум линейной формы $S = 3x_1 - 3x_2 + 5x_3 + x_4$ достигается на $(0, 1, 1, 1)$ и

равен 3. Поэтому в качестве c можно взять произвольное число, удовлетворяющее двойному неравенству $3 < c \leq 4$, например, положить $c = 4$.

Способ 3. В задаче для 10-го класса, в которой рассматривалась клетка с тремя входами, было возможно решить задачу путём нахождения уравнения плоскости, отсекающей единичные вершины некоторого куба в трёхмерном пространстве с длиной стороны, равной единицы. Вершины этого куба либо белые, соответствующие тем наборам, на которых функция принимает значение 0, либо чёрные, соответствующие тем наборам, на которых функция принимает значение 1 (например, как это показано на рис. 55).

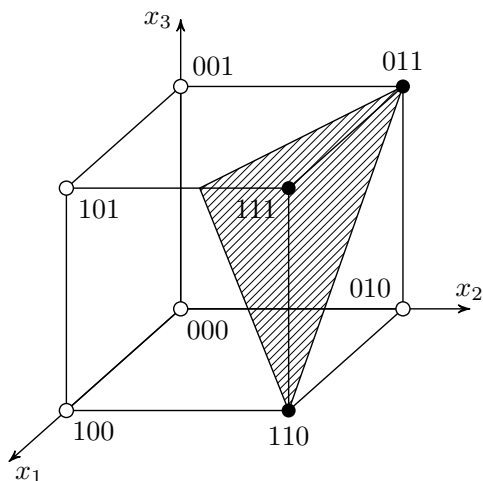


Рис. 55

Ответ: $a_1 = 2$, $a_2 = -2$, $a_3 = 3$, $a_4 = 1$, $c = 3$; $a_1 = 3$, $a_2 = -3$, $a_3 = 5$, $a_4 = 1$, $c = 4$.

Замечание. Многие важнейшие процессы в окружающем мире описываются с помощью пороговых соотношений, основанных на взвешенной оценке влияния различных параметров, в том числе противоборствующих. Пороговые явления наблюдаются как в микромире, например при распаде ядерного ядра, так и в повседневной жизни: в технике, экономике, медицине, социологии и т. д. Особое место здесь занимает нейрофизиология в связи с обнаружением учёными Уорреном МакКаллоком и Уолтером Питтсом в 1943 году пороговой природы работы нейронов живых организмов. Ими было показано, что суммарное возбуждение нервной клетки, возникающее в её теле (соне), формируется из входных сигналов x_i , $i = \overline{1, n}$, поступающих в клетку по n входным

нервным волокнам (дендритам). Это суммарное возбуждение представляет собой сумму $S = a_1x_1 + \dots + a_nx_n$, где a_1, \dots, a_n — параметры, хранящиеся в памяти клетки и которые могут корректироваться в течение её жизни. Выходной сигнал y формируется на выходе клетки (в аксоне) в случае, если суммарное возбуждение S будет больше некоторого параметра c , порога, который, наряду с a_1, \dots, a_n , также хранится в памяти клетки и, вообще говоря, может меняться. Вначале значения x_i , $i = \overline{1, n}$, и y считались двоичными, так как измерительные средства того времени могли улавливать только наличие сигнала или его отсутствие. Дальнейшие исследования в этой области привели к тому выводу, что сами сигналы могут принимать значения от 0 до $k-1$; при $k = 16$ такая модель достаточно точно описывает функционирование нейрона.

Работа Мак-Каллока и Питтса легла в основу построения нейрокомпьютеров с пороговыми операциями. Дело в том, что как показывает практика, такие нейрокомпьютеры на базе определённым образом сконструированных нейронных сетей позволяют решать некоторые типичные для живых организмов задачи (например, задачу распознавания образов) более эффективно по сравнению с другими алгоритмами. В частности, такие задачи могут возникнуть при построении системы, разрешающей или запрещающей допуск в учреждение на основании биологических параметров человека, таких как отпечаток пальца, радужная оболочка глаза, рисунок кровеносной системы.

20.8. По двум последним строкам можно восстановить обратную перестановку и использовать её для расшифрования первого сообщения. Из-за повторов букв в полученных строках сделать это однозначно удаётся не всегда. Таким образом, задача сводится к выбору букв из столбцов, содержащих не более трёх различных букв, которые дают читаемый текст. Жирным шрифтом выделены выбранные буквы, в серых клетках указаны уже использованные буквы, не участвующие в выборе.

И	К	Л	М	Н	О	И	К	Л	М	Н	О	И	К	Л	М	Н	О	С	Т
И	К	О	О	К	М	Т	И	С	О	Н	И	Л	Н	Л	К	М	Л	М	Н
Варианты обратной перестановки:																			
1	2	6	6	2	4	20	1	19	6	5	1	3	5	3	2	4	3	4	5
7	8	12	12	8	10	20	7	19	12	11	7	9	11	9	8	10	9	10	11
13	14	18	18	14	16	20	13	19	18	17	13	15	17	15	14	16	15	16	17
Варианты открытого текста:																			
Н	К	М	М	К	А	Б	Н	И	М	К	Н	Б	К	Б	К	А	Б	А	К
О	Р	А	А	Р	Л	Б	О	И	А	А	О	О	А	О	Р	Л	О	Л	А
Е	Н	Е	Е	Н	О	Б	Е	И	Е	И	Е	Т	И	Т	Н	О	Т	О	И

Ответ: ОКЕАН ОБНИМАЕТ КОРАБЛИ.

Замечание. В этой задаче фактически описан вариант так называемого *трёхэтапного бесключевого криптографического протокола Шамира*. Криптографический протокол — это заданная (строго определённая) последовательность шагов между взаимодействующими сторонами для достижения определённых целей. В данном случае такой целью является передача конфиденциального сообщения x от абонента A к абоненту B по общедоступному каналу связи. Сложность достижения такой цели в данном случае заключается в том, что абоненты A и B не имеют общего секретного ключа, который можно было бы использовать для зашифрования сообщения x перед его последующей передачей. Поэтому взаимодействующие стороны предпринимают указанную ниже последовательность действий.

1. Сначала абонент A выбирает некоторый ключ k_A и преобразование зашифрования E_{k_A} (в рассматриваемой задаче используется шифр перестановки), шифрует сообщение x и передаёт зашифрованное сообщение $E_{k_A}(x)$ абоненту B .

2. Абонент B не может расшифровать полученное сообщение, так как не знает, какое преобразование и ключ выбрал A . Вместо этого абонент B шифрует полученное сообщение $E_{k_A}(x)$ с помощью своего преобразования E' и ключа k_B (в рассматриваемой задаче используется так называемый шифр гаммирования) и возвращает теперь уже дважды зашифрованное сообщение x абоненту A .

3. Абонент A получает сообщение $E'_{k_B}(E_{k_A}(x))$. Если эти преобразования коммутируют (то есть выполняется равенство $E'_{k_B}(E_{k_A}(x)) = E_{k_A}(E'_{k_B}(x))$), то абонент A применяет к полученному сообщению своё преобразование расшифрования D_{k_A} и получает $E'_{k_B}(x)$, которое и отправляет B .

4. Абонент B , в свою очередь, применяет к полученному сообщению своё преобразование расшифрования D'_{k_B} и получает переданное от абонента A сообщение x .

Заметим, что стороннему наблюдателю будут известны следующие передаваемые сообщения: $E_{k_A}(x)$, $E'_{k_B}(E_{k_A}(x))$, $E'_{k_B}(x)$, при этом сообщение x не передавалось в открытом виде. Отметим, что в рассмотренной задаче выбранные абонентами преобразования не коммутируют.

20.9. Пусть $y = 14197777$, $N = p \cdot q = 56887111$, p, q — простые числа. По условию $\text{НОД}(x, N) = p > 1$, то есть $x = t \cdot p$, где t — натуральное число. Так как $y = r_N(x^3)$, где $r_N(x^3)$ — остаток от деления на N числа x^3 , то $\text{НОД}(y, N) = p$. Вычисляя $\text{НОД}(14197777, 56887111)$, находим, что $p = 10667$, тогда $y = 1331 \cdot p$, а $q = N/p = 5333$.

Деля обе части уравнения

$$1331 \cdot p = r_N((t \cdot p)^3)$$

на p , получаем:

$$1331 = r_q(t^3 \cdot p^2) = r_{5333}(t^3 \cdot 10667^2) = r_{5333}(t^3).$$

Поэтому $t = \sqrt[3]{1331} = 11$ и $x = t \cdot p = 11 \cdot 10667 = 117337$.

Ответ: $x = 117337$.

Замечание. Данная задача относится к криптографии с открытым ключом, или, более точно, с широко известной криптосистемой RSA. Напомним, что в этой системе ключ зашифрования e и ключ расшифрования d — различны, хотя и связаны между собой. Ключ расшифрования хранится в секрете. Для зашифрования сообщения $x \in \{0, \dots, N-1\}$ его необходимо возвести в степень e и взять остаток от деления на N , где N — произведение двух простых чисел p, q , а для расшифрования — получившееся число возвести в степень d и также взять остаток от деления на N . Стойкость криптосистемы RSA базируется на вычислительной сложности задачи разложения некоторого числа N на простые множители p, q (которые также необходимо хранить в секрете).

В приведённой задаче используется то, что если сообщение x , подлежащее шифрованию, имеет с N (нетривиальный, отличный от 1 и N) общий делитель (то есть делится на p или q), то это приводит к разложению N на простые множители и нахождению сообщения, которое было зашифровано. Поэтому при использовании такой системы шифрования необходимо следить за тем, чтобы сообщение x было взаимно просто с числом N . Заметим, что практически для всех x это условие выполняется.

20.10. Сравним посимвольно последовательности цветов, приведённые в условии, и сформируем таблицу:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
С	К	З	К	К	К	К	З	З	К	К	С	С	К	К	З	С	З	С	К	Светофильтры Чебурашки
К	К	З	З	З	С	К	С	К	С	З	З	С	К	С	К	С	К	З	К	Светофильтры Шапокляк
					*				*	*			*			*		*		Срабатывание датчика
	ч	ч			ч	ч			ч	ч		ч	К			С		ч	ч	Комбинация Гены

На каждой позиции возможны четыре варианта: совпали или нет цвета светофильтров Чебурашки и Шапокляк, сработал или нет у Шапокляк датчик. Рассмотрим эти варианты.

1. Цвета не совпали, датчик не сработал. Тогда в этой позиции кодовой комбинации Гена выставит чёрный цвет или цвет, выбранный Чебурашкой (всего два варианта).

2. Цвета совпали, датчик сработал, тогда Гена выставит тот же цвет (один вариант).

3. Цвета совпали, датчик не сработал или цвета не совпали, но датчик сработал. Тогда Гена выставит чёрный цвет (один вариант).

Ответом будем число $4^{20} - 2^k$, где k — число позиций, где (в которых) цвета не совпали и датчик не сработал. В данном случае $k = 9$.

Ответ: $4^{20} - 2^9$.

Замечание. Одной из важных задач современной криптографии является задача распределения ключей между взаимодействующими сторонами с использованием открытой сети связи. Возникает вопрос: как безопасно передать ключи по общедоступному каналу связи, чтобы этот ключ стал известным только тому, кому он предназначался? Одним из подходов к решению такой задачи является использование специальных криптографических протоколов *открытого распределения ключей* — правил обмена некоторыми сообщениями между участниками по сети связи. В приведённой задаче иллюстрируется идея использования одного типа такого протокола: *квантового протокола*.

В основе квантового протокола лежит передача по каналу связи некоторых физических объектов — фотонов с различными параметрами (поляризациями). Достоинство такого протокола состоит в следующем. Пусть злоумышленник «встроился» в оптический канал связи и пытается определить поляризацию передаваемых фотонов. Оказывается, правильно измерить поляризацию фотона можно лишь с некоторой вероятностью, а после самой попытки такого измерения информация о поляризации фотона теряется. Таким образом, попытка перехватить передаваемое сообщение приводит к его искажению, и на приёмной стороне этот факт вторжения будет обнаружен.

Данное свойство неопределённого изменения состояния фотона после измерения его параметров было обнаружено в 1927 году и известно как принцип неопределённости Гейзенберга. Спустя десятилетия это наблюдение привело к зарождению сравнительно нового направления — квантовой криптографии.

Рекомендуемая литература

- Болл У., Кокстер Г.* Математические эссе и развлечения. М.: Мир, 1986.
- Введение в криптографию / Под ред. В. В. Яценко. М.: МЦНМО, 2012.
- Верн Ж.* Жангада. М.: Детская литература, 1967. (Библиотечка приключений; Т. 9).
- Верн Ж.* Путешествие к центру Земли // Собрание сочинений в 12 т., т. 2. М.: Художественная литература, 1995. С. 7–225.
- Гарднер М.* От мозаик Пенроуза к надёжным шифрам. М.: Мир, 1993.
- Гуревич Г. А.* Криптограмма Жюль Верна // Квант. 1985. № 9. С. 30–35.
- Дориченко С. А., Яценко В. В.* 25 этюдов о шифрах. М.: ТЭИС, 1994.
- Жельников В.* Криптография от папируса до компьютера. М.: АБФ, 1996.
- Каверин В.* Исполнение желаний // Собрание сочинений в 6 т., т. 2. М.: Художественная литература, 1964. С. 211–552.
- Конан Дойл А.* Плывущие человечки // Записки о Шерлоке Холмсе. М.: Правда, 1983. С. 249–275.
- Основы криптографии. Учебное пособие / А. П. Алфёров, А. Ю. Зубов, А. С. Кузьмин, А. В. Черёмушкин. М.: Гелиос АРВ, 2005.
- По Э.* Золотой жук // Стихотворения. Проза. М.: Художественная литература, 1976. С. 433–462.
- Саломая А.* Криптография с открытым ключом. М.: Мир, 1995.
- Словарь криптографических терминов / Под ред. Б. А. Погорелова и В. Н. Сачкова. М.: МЦНМО, 2006.
- Соболева Т. А.* Тайнопись в истории России (История криптографической службы России XVIII – начала XX в.). М.: Международные отношения, 1994.
- Соболева Т. А.* История шифровального дела в России. М.: ОЛМА-ПРЕСС Образование, 2002.
- Уэзерелл Ч.* Этюды для программистов. М.: Мир, 1982.
- Фролов Г.* Тайны тайнописи. М., 1992.

Содержание

Предисловие	3
От авторов	4
1. Введение	6
2. Шифры замены	9
3. Шифры перестановки	21
4. Многоалфавитные шифры замены	29
5. Современные приложения криптографии	32
6. Условия задач олимпиад по криптографии и математике	36
7. Указания и решения	75
Рекомендуемая литература	179