В июне 1815 года Наполеон проигрывал англичанам Битву при Ватерлоо. По легенде, за сражением внимательно наблюдали братья Ротшильды. Едва убедившись, что Наполеон проигрывает сражение, один из них, державший почтовых голубей, отправил их с зашифрованными инструкциями, привязанными к лапкам, в Лондон своим агентам.

Утром следующего дня, загнав дорогих лошадей, один из братьев Ротшильдов явился на Лондонскую биржу. Он был единственным в Лондоне, кто знал о поражении Наполеона. Притворно сокрушаясь по поводу успехов французского императора, он немедленно приступил к массовой продаже своих акций. Остальные биржевики сразу же последовали его примеру, так как решили, что сражение проиграли англичане. Английские, австрийские и прусские ценные бумаги дешевели с каждой минутой и оптом скупались агентами Ротшильда. О том, что Наполеон проиграл битву, на бирже узнали лишь через день. Многие держатели ценных бумаг покончили с собой, а Ротшильды заработали 40 миллионов фунтов стерлингов. Достоверная информация, полученная раньше других, позволила Ротшильдам вести беспроигрышную игру на бирже. Пожалуй, эта история и не стоила упоминания, если бы не дошедшая до наших дней знаменитая фраза одного из братьев-хитрецов: «Кто владеет информацией, тот владеет миром».

Во все времена люди пытались скрыть ту или иную информацию от других. По мере развития цивилизации информации становилось все больше, а необходимость ее скрывать все важнее и труднее. Так и появилась криптография — наука о методах сокрытия разнообразной информации. Развитием этих методов занимались лучшие умы человечества и, прежде всего, математики. Криптографические задачи являются сложнейшими прикладными задачами современной математики.

Как искусство криптография развивалась несколько тысяч лет, вплоть до середины XX века, пока не появились фундаментальные работы К. Шеннона по теории информации. С тех пор анализ и синтез шифров стал в большей степени опираться на научные методы. В начале XX века были известны десятки видов шифрсистем, с появлением же механических и затем электронных устройств их счет пошел на тысячи.

В настоящее время методы и средства криптографии используются для обеспечения информационной безопасности не только государства, но и частных лиц, и организаций. Дело здесь совсем не обязательно в секретах. Слишком много различных сведений «гуляет» по всему свету в цифровом виде, подвергаясь угрозам недружественного ознакомления, накопления, подмены, фальсификации и т. п. Наиболее надежные методы защиты от таких угроз дает именно криптография.

Решая задачи этого сборника, вы познакомитесь с основами интереснейшей науки и поймете, насколько необычен и сложен мир криптографии.

Клуб 4Ф, способствовавший появлению этой книги, объединяет людей, которые в той или иной степени занимались защитой информации. Среди нас есть математики, радиоинженеры, специалисты других областей знания. Мы очень хотим, чтобы наши ряды пополнялись умными, грамотными молодыми людьми, для которых слово Россия и Родина также важны, как и для нас. Путь познания всегда непрост, он долог и труден, но огромно счастье преодолевшего все трудности и постигшего глубины знания. Желаем вам счастья и успеха на этом пути.

От имени всех членов Клуба 4Ф,

Президент Клуба 4Ф
Величутин Иван Иванович
ivan-velich@yandex.ru
www.club-4f.ru

А. Ю. Зубов
А. В. Зязин
В. Н. Овчинников
С. М. Рамоданов

ОЛИМПИАДЫ ПО КРИПТОГРАФИИ И МАТЕМАТИКЕ ДЛЯ ШКОЛЬНИКОВ

Москва
Издательство МЦНМО
2006

УДК 003.26
ББК 32.937-082.03
З91

Издание осуществлено при поддержке гранта Президента РФ (НШ-8564.2006.10)

Зубов А. Ю. и др.

З91 Олимпиады по криптографии и математике для школьников / А. Ю. Зубов, А. В. Зязин, В. Н. Овчинников, С. М. Рамоданов. — М.: МЦНМО, 2006. — 136 с.: ил.

ISBN 5-94057-261-8

В сборник включены условия, ответы и решения пятнадцати олимпиад по криптографии и математике, проведенных в Москве с 1991 по 2005 гг. Условия задач предварены элементарным введением в криптографию, использующим сюжеты из известных литературных произведений.

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

ББК 32.937-082.03

ISBN 5-94057-261-8

Предисловие

С 1991 г. Институт криптографии, связи и информатики Академии ФСБ России проводит ежегодные олимпиады по криптографии и математике для учащихся 9–11 классов. Эти олимпиады вызывают большой интерес у школьников необычностью своего жанра и ежегодно собирают несколько сотен участников не только из Москвы и Подмосковья, но и из других регионов России.

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

При подведении итогов каждой олимпиады мы знакомим участников с общедоступными книгами по криптографии, которых в последние годы появилось достаточно много. Однако эти книги либо слишком сложны для школьников, либо поверхностны или недостаточно полны, либо малодоступны. Поэтому авторы поставили 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 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 подготовку и проведение олимпиад трудно переоценить.

Связаться с оргкомитетом олимпиады можно по электронной почте `olymp@academy.fsb.ru`. Информация и дате проведения очередной олимпиады обычно становится известной в октябре и размещается на сайте `www.academy.fsb.ru`.

1. Введение

Если вы хотите передать свое текстовое сообщение (последовательность символов некоторого алфавита) адресату так, чтобы оно осталось тайным для посторонних лиц, то у вас есть, по крайней мере, две возможности. Вы можете попытаться скрыть сам факт передачи текста, то есть прибегнуть к методам стеганографии, в арсенале которой — симпатические (невидимые) чернила, микроточки и тому подобные средства. Другая возможность заключается в попытке скрыть смысл сообщения от посторонних лиц, случайно или намеренно познакомившихся с передаваемым текстом. В этом случае вы можете прибегнуть к методам 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 своего сообщения.

Сообщение, которое вы хотите передать адресату, будем называть открытым сообщением. Например, в задаче 2.5 (раздел «Условия задач») одним из открытых сообщений является фраза:

КОРАБЛИ ОТХОДЯТ ВЕЧЕРОМ

Для сохранения сообщения в тайне оно преобразуется криптографическими методами и только после этого передается адресату. Преобразованное сообщение будем называть шифрованным сообщением (или зашифрованным сообщением). Другое название зашифрованного сообщения — криптограмма (или шифртекст). В задаче 2.5 зашифрованное сообщение выглядит так:

ЮПЯТБНЩМСДТЛЖГПСГХСЦЦ

Зашифрованное сообщение не обязательно должно быть последовательностью букв, как в указанной выше задаче. Часто зашифрованное сообщение может представлять собой последовательность цифр или специальных знаков (например, «пляшущих человечков»).

Процесс преобразования открытого сообщения в шифрованное будем называть *шифрованием* или *зашифрованием*. Адресату заранее сообщается, как из шифрованного сообщения получить открытое. Этот процесс получения исходного сообщения называют *расшифрованием*.

При выборе правила шифрования надо стремиться к тому, чтобы посторонние лица, не знающие правила расшифрования, не смогли восстановить по криптограмме открытое сообщение. В этом случае вы скроете смысл сообщения и обеспечите «тайнопись».

Для удобства дальнейшего изложения обозначим буквой A — открытое сообщение, B — шифрованное сообщение, f — правило шифрования, g — правило расшифрования. В этом случае зашифрование открытого сообщения A в шифрованное сообщение B можно записать в виде $f(A) = B$. Обратное преобразование (то есть получение открытого со-

общения A путем расшифрования B) запишется в виде соотношения $g(B) = A$.

Правило зашифрования f не может быть произвольным. Оно должно быть таким, чтобы по шифртексту B с помощью правила расшифрования g можно было однозначно восстановить открытое сообщение A. Однотипные правила зашифрования можно объединить в классы. Внутри класса правила различаются между собой по значениям некоторого параметра, которое может быть числом, таблицей и т. д. В криптографии конкретное значение такого параметра обычно называют *ключом*. По сути дела, ключ выбирает конкретное правило зашифрования из данного класса правил.

Зачем понадобилось вводить понятие ключа? Есть, по крайней мере, два обстоятельства, которые позволяют понять необходимость этого. Во-первых, обычно шифрование производится с использованием специальных устройств. У вас должна быть возможность изменять значение параметров устройства, чтобы зашифрованное сообщение не смогли расшифровать даже лица, имеющие точно такое же устройство, но не знающие выбранного вами значения параметра. Во-вторых, многократное использование одного и того же правила зашифрования f для зашифрования открытых текстов создает предпосылки для получения открытых сообщений по шифрованным без знания правила расшифрования g. Поэтому необходимо своевременно менять правило зашифрования.

Используя понятие ключа, процесс зашифрования можно описать в виде соотношения

$$f_\alpha(A) = B,$$

в котором α — выбранный ключ, известный отправителю и адресату.

Для каждого ключа α шифрпреобразование f_α должно быть обратимым, то есть должно существовать обратное преобразование g_α, которое при выбранном ключе α однозначно определяет открытое сообщение A по шифрованному сообщению B:

$$g_\alpha(B) = A.$$

Совокупность преобразований f_α и набор ключей, которым они соответствуют, будем называть *шифром*.

Среди всех шифров можно выделить два больших класса: шифры перестановки и шифры замены.

Шифрами перестановки называются такие шифры, преобразования из которых приводят к изменению только порядка следования символов исходного сообщения. Примером преобразования, которое может содержаться в шифре перестановки, является следующее правило. Каждая буква исходного сообщения, стоящая в тексте на позиции с четным номером, меняется местами с предшествующей ей буквой. В этом

случае ясно, что и исходное, и шифрованное сообщение состоят из одних и тех же букв.

Шифрами замены называются такие шифры, преобразования из которых приводят к замене каждого символа открытого сообщения на другие символы — шифробозначения, причем порядок следования шифробозначений совпадает с порядком следования соответствующих им символов открытого сообщения. В качестве примера преобразования, которое может содержаться в шифре замены, приведем такое правило. Каждая буква исходного сообщения заменяется на ее порядковый номер в алфавите. В этом случае исходный буквенный текст преобразуется в числовой.

Как правило, в задачах олимпиад шифр известен, а использованный ключ — нет. Для определения исходного текста по шифрованному при неизвестном ключе возможны два подхода: первый — определить ключ и затем найти исходное сообщение расшифрованием; второй — найти исходное сообщение без определения ключа. Получение открытого сообщения по шифрованному без заранее известного ключа называется *вскрытием шифра*, в отличие от расшифрования — когда ключ известен. Во многих случаях вскрытие шифра возможно, что и демонстрируют победители наших олимпиад.

Под стойкостью шифра, как правило, понимается способность противостоять попыткам провести его вскрытие. При анализе шифра обычно исходят из принципа, сформулированного голландцем Огюстом Керкгоффсом (1835–1903). Согласно этому принципу при вскрытии криптограммы противнику известно о шифре все, кроме используемого ключа. Одной из естественных характеристик шифра является число его возможных ключей. Ведь вскрытие шифра можно осуществлять перебором всех возможных его ключей. Мы уже говорили, что в приводимых ниже задачах олимпиад, как правило, шифр известен, но неизвестен выбранный ключ, что соответствует принципу Керкгоффса. Так, в задаче 4.4 все дело сводится к перебору 24 различных вариантов ключа, из которых только один дает читаемый текст. Поэтому многие участники олимпиады смогли восстановить сообщение на латинском языке, даже не зная этого языка.

Подчас смешивают два понятия: *шифрование* и *кодирование*. Мы уже договорились, что для шифрования надо знать шифр и секретный ключ. При кодировании нет ничего секретного, есть только определенная замена букв или слов на заранее определенные символы. Методы кодирования направлены не на то, чтобы скрыть открытое сообщение, а на то, чтобы представить его в более удобном виде для передачи по техническим средствам связи, для уменьшения длины сообщения и т. д. В принципе, кодирование, конечно же, можно рассматривать как шифр замены, для которого «набор» возможных ключей состоит только из

одного ключа (например, буква «а» в азбуке Морзе всегда кодируется знаками •— и это не является секретом).

В настоящее время для защиты информации широко используются электронные шифровальные устройства. Важной характеристикой таких устройств является не только стойкость реализуемого шифра, но и высокая скорость осуществления процессов шифрования и расшифрования. Для создания и обеспечения грамотной эксплуатации такой техники широко используются достижения современной криптографии, в основе которой лежат математика, информатика, физика, электроника и другие науки.

Современная криптография бурно развивается. В ней появляются новые направления. Так, с 1976 года развивается «открытая криптография». Ее отличительной особенностью является разделение ключей для зашифрования и расшифрования. При этом ключ для зашифрования не требуется делать секретным, более того, он может быть общедоступным и содержаться в телефонном справочнике вместе с фамилией и адресом его владельца. Подробнее об этом и других современных задачах криптографии можно прочитать в книгах по криптографии.

Наряду с термином «криптография» в литературе встречается термин «криптология», также происходящий от греческих корней, означающих «тайный» и «слово». Этот термин используется для обозначения всей области секретной связи. Криптологию делят на две части: криптографию и криптоанализ. Криптограф пытается найти методы обеспечения секретности сообщений, криптоаналитик пытается при неизвестном ключе выполнить обратную задачу. При этом часто говорят, что криптоаналитик вскрыл шифр, хотя чаще он вскрывает ключ заранее известного шифра.

2. Шифры замены

Наиболее известными и часто используемыми шифрами являются шифры замены. Они характеризуются тем, что отдельные части сообщения (буквы, слова, ...) заменяются на какие-либо другие буквы, числа, символы и т. д. При этом замена осуществляется так, чтобы потом по шифрованному сообщению можно было однозначно восстановить передаваемое сообщение.

Пусть, например, зашифровывается сообщение на русском языке и при этом замене подлежит каждая буква сообщения. Формально в этом случае шифр замены можно описать следующим образом. Для каждой буквы α исходного алфавита строится некоторое множество символов M_α так, что множества M_α и M_β попарно не пересекаются при $\alpha \neq \beta$, то есть любые два различные множества не содержат

одинаковых элементов. Множество M_α называется множеством шифр-обозначений для буквы α.

Таблица

$а$	$б$	$в$	...	$я$
$M_а$	$M_б$	$M_в$	...	$M_я$

(1)

является ключом шифра замены. Зная ее, можно осуществить как зашифрование, так и расшифрование.

При зашифровании каждая буква α открытого сообщения, начиная с первой, заменяется любым символом из множества M_α. Если в сообщении содержится несколько букв α, то каждая из них заменяется на любой символ из M_α. За счет этого с помощью одного ключа (1) можно получить различные варианты зашифрованного сообщения для одного и того же открытого 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, например, любым из следующих трех 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

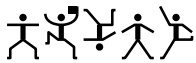
Так как множества $M_а$, $M_б$, $M_в$, ..., $M_я$ попарно не пересекаются, то по каждому символу шифрованного сообщения можно однозначно определить, какому множеству он принадлежит, и, следовательно, какую букву открытого сообщения он заменяет. Поэтому расшифрование возможно и открытое сообщение определяется единственным образом.

Часто M_α состоит 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

(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, тем труднее вскрыть сообщение, не имея ключа. Это, конечно, не так. Если каждому символу однозначно сопоставить какую-либо букву или число, то легко перейти к зашифрованному сообщению из букв или чисел. В романе Ж. Верна «Путешествие к центру Земли» каждый рунический знак был заменен на соответствующую букву немецкого языка, что облегчило восстановление открытого сообщения. С точки зрения криптографов использование различных сложных символов не усложняет шифра. Однако, если зашифрованное сообщение состоит из букв или цифр, то вскрывать такое сообщение удобнее.

Рассмотрим некоторые примеры шифров замены. Пусть каждое множество M_α состоит из одной буквы. 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)

Такой шифр называется шифром простой однобуквенной замены. По ключу (4) удобно проводить зашифрование и расшифрование: при зашифровании каждая буква открытого текста заменяется на соответствующую букву из второй строки (а на г и т. д.) При расшифровании, наоборот, г заменяется на а и т. д. При шифровании и расшифровании надо помнить вторую строчку в (4), то есть ключ.

Запомнить произвольный порядок букв алфавита достаточно сложно. Поэтому всегда пытались придумать какое-либо правило, по которому можно просто восстановить вторую строчку в (4).

Одним из первых шифров, известных из истории, был так называемый шифр Цезаря, для которого вторая строка в (4) является последовательностью, записанной в алфавитном порядке, но начинающейся не с буквы а:

а	б	в	...	ь	э	ю	я
г	д	е	...	я	а	б	в

(5)

В одной из задач (задача 4.4) используется шифр Цезаря. Запомнить ключ в этом случае просто — надо знать первую букву второй строки (4) (последовательность букв в алфавите предполагается известной). Однако такой шифр обладает большим недостатком. Число различных ключей равно числу букв в алфавите. Перебрав эти варианты, можно однозначно восстановить открытое сообщение, так как при правильном

выборе ключа получится «осмысленный» текст. В других случаях обычно получается «нечитаемый» текст. Задача 4.4 именно на это и рассчитана. Несмотря на то, что используется фраза на латинском языке, которого школьники не знают, многие участники олимпиады смогли указать открытое сообщение.

Другим примером шифра замены может служить лозунговый шифр. Здесь запоминание ключевой последовательности основано на лозунге — легко запоминаемом слове. Например, выберем слово-лозунг «учебник» и заполним вторую строку таблицы по следующему правилу: сначала выписываем слово-лозунг, а затем выписываем в алфавитном порядке буквы алфавита, не вошедшие в слово-лозунг. Вторая строка в (4) примет вид

```
у ч е б н и к а в г д ж з л м о
  п р с т ф х ц ш щ ъ ы ь э ю я
```

В данном случае число вариантов ключа существенно больше числа букв алфавита.

Рассмотренные шифры имеют одну слабость. Если в открытом сообщении часто встречается какая-либо буква, то в шифрованном сообщении часто будет встречаться соответствующий ей символ или буква. Поэтому при вскрытии шифра замены обычно стараются наиболее часто встречающимся символам шифрованного сообщения поставить в соответствие буквы открытого сообщения с наибольшей предполагаемой частотой появления. Если шифрованное сообщение достаточно большое, то этот путь приводит к успеху, даже если вы не знаете ключа.

Кроме частоты появления букв, могут быть использованы другие обстоятельства, помогающие раскрыть сообщение. Например, может быть известна разбивка на слова, как в задаче 4.2, и расставлены знаки препинания. Рассматривая небольшое число возможных вариантов замены для предлогов и союзов, можно попытаться определить часть ключа. В этой задаче существенно используется, какие гласные или согласные могут быть удвоенными: «нн», «ее», «ии» и др.

При анализе шифрованного сообщения следует исходить из того, что число различных вариантов для части определяемого ключа не такое уж большое, если вы находитесь на правильном пути. В противном случае либо вы получите противоречие, либо число вариантов ключа будет сильно возрастать. Обычно, начиная с некоторого момента определение открытого сообщения становится делом техники. Так, в задаче 4.2, если вы определили «денно и нощно», то дальнейшее определение открытого текста не представляет труда.

Вообще-то можно сказать, что вскрытие шифров замены является искусством и достаточно трудно формализовать этот процесс.

Популярные у школьников криптограммы (типа рассмотренной в

задаче 1.5) по сути дела являются шифром замены с ключом

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

в котором каждой цифре ставится в соответствие буква. При этом должны соблюдаться правила арифметики. Эти правила значительно облегчают определение открытого текста, так же, как правила синтаксиса и орфографии в задаче 4.2 облегчают нахождение четверостишия В. Высоцкого.

Любые особенности текста, которые могут быть вам известны, — ваши помощники. Например, в задаче 5.2 прямо сказано, что в тексте есть выражения «зпт», «тчк», как часто бывает в реальных телеграммах. И эта подсказка — путь к решению задачи.

Шифрование даже относительно небольших текстов на одном ключе для рассмотренных шифров замены создает условия для вскрытия открытых сообщений. Поэтому такие шифры пытались усовершенствовать. Одно из направлений — построение шифров разнозначной замены, когда каждой букве ставится в соответствие один или два символа. (Простейшим примером является шифр, определяемый в задаче 4.2.) Например,

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 шифрованное сообщение написано без пробелов между символами, то появляется дополнительная трудность при разбиении шифрованного сообщения на отдельные символы и слова.

Другое направление создания шифров замены состоит в том, чтобы множества шифробозначений M_α содержали более одного элемента. Такие шифры получили название шифров многозначной замены. Они позволяют скрыть истинную частоту букв открытого сообщения, что существенно затрудняет вскрытие этих шифров. Главная трудность, которая возникает при использовании таких шифров, заключается в запоминании ключа. Надо запомнить не одну строчку, а для каждой буквы алфавита α — множество ее шифробозначений M_α. Как правило, элементами множеств M_α являются числа. Из художественной литературы и кинофильмов про разведчиков вам известно, что во время второй мировой войны часто использовались так называемые книжные шифры. Множество шифробозначений для каждой буквы определяется всеми пятизначными наборами цифр, в каждом из которых первые две цифры указывают номер страницы, третья цифра — номер строки, четвертая и пятая цифры — номер места данной буквы в указанной строке. Поэтому при поимке разведчика всегда пытались найти книгу,

которая могла быть использована им в качестве ключа.

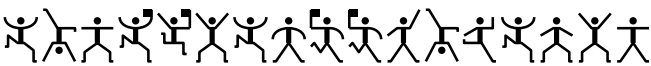
Мы не останавливаемся здесь на более сложных методах построения шифров замены. Приведенных примеров достаточно, чтобы оценить многообразие таких шифров. Но все они имеют серьезный недостаток — на одном ключе нельзя шифровать достаточно длинные сообщения. Поэтому, как правило, шифры замены используются в комбинации с другими шифрами. Чаще всего — с шифрами перестановки, о которых вы прочитаете в следующем разделе.

В заключение, следуя героям известных литературных произведений, вскроем некоторые шифры замены. Обратите внимание на то, какие неожиданные обстоятельства при этом используются. Действительно, вскрытие шифров — искусство.

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. Четвертая 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 четырех 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 ее просто по имени. А зовут ее 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 нее. Не хочет ли он, чтобы она пришла куда-нибудь, где он мог с ней поговорить? Холмс обратился ко второму слову третьей записки. В нем 7 букв, из которых третья и последняя — И. Холмс предположил, что слово это — ПРИХОДИ, и сразу оказался обладателем еще 5 букв: П, Р, Х, О, Д.

Тогда он обратился к четвертой записи, которая появилась на двери сарая. Холмс предположил, что она является ответом и что написала ее 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 четвертое слово — СЛЕНИ Это — фамилия, чрезвычайно распространенная 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 остается 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
          *  o   o       *
```

Здесь указаны границы слов, а снизу одинаковыми символами отмечены одинаковые буквы. Четвертое 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 дает 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 трех букв: ИЛСИ ГО-ОВЬСЯ К С-ЕР-И, из которой сразу определяются 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 козленок. Главный герой рассказа рассуждал следующим образом. По английски козленок — kid; череп связан с капитаном Киддом, по английски — kidd. Козленок

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 нем, 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 идет 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 — `e`. Далее идут в нисходящем порядке: `a, o, i, d, h, n, r, s, t, u, y, c, f, g, l, m, w, b, k, p, q, x, z`. Буква `e`, 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 `e` английского алфавита. Для проверки этой гипотезы взглянем, встречается ли этот символ дважды подряд, так как в английском языке буква `e` часто удваивается, например, в словах meet, fleet, speed, seen, seed, been, agree, и т. д. Хотя криптограмма невелика, пара *88* стоит в нем пять раз.

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

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

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 узнаем еще 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`*#?3*`h the`

а неизвестные — точками:

`the tree thr...h the`

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

Надписывая над уже определенными символами криптограммы их значения, находим вблизи от ее начала (позиции 54–58) группу символов *83(88*, которая читается так `egree`, 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.

Четвертый по частоте (16 вхождений) символ *)* еще не определен. Возвратимся к диаграмме встречаемости букв английского языка. Среди первого десятка букв этой диаграммы у нас не встретилась 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 неопределенными 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 еще 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».

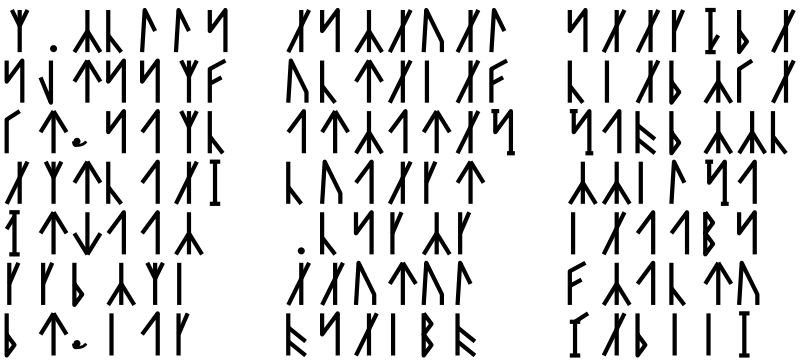
В переводе на русский язык: «Хорошее стекло в трактире епископа на чертовом стуле двадцать один градус и тринадцать минут северо-северо-восток главный сук седьмая ветвь восточная сторона стреляй из левого глаза мертвой головы прямая от дерева через выстрел на пятьдесят футов».

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*	***	*#*	*•*	*(*	*)*	*;*	*?*	□	*]*	*:*

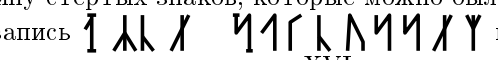
Ж. Верн, «Путешествие к центру Земли»

В руки профессора Лиденброка попадает пергамент со следующей рукописью:



«Это — рунические письмена; знаки эти совершенно похожи на знаки манускрипта Снорре. Но ... что же они означают? — спрашивает профессор, — ... Ведь это все 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 стертых знаков, которые можно было восстановить. Получилась запись  которая читалась как «арне сакнуссем» — имя ученого 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 ученый 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 ученые 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 прочел бы ее. 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». Проверяя эту гипотезу, он начал диктовать, называя сначала первые буквы каждого слова, потом вторые; он диктовал буквы в таком порядке:

```
messunkaSenrA.icefdoK.segnittamur tnece
rtserrette,rotaivsadua,ednecse dsadnelak
artniiiluJsiratracSarbmuta biledmekmeret
arcsilucoIsleffenSn 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 оборотная стороны листка попеременно представали перед моими глазами. ... Каково же было мое 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

Шифр, преобразования из которого изменяют только порядок следования символов исходного текста, но не изменяют их самих, называется шифром перестановки (ШП).

Рассмотрим преобразование из ШП, предназначенное для зашифрования сообщения длиной n символов. Его можно представить с помощью таблицы

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

где i_1 — номер места шифртекста, на которое попадает первая буква исходного сообщения при выбранном преобразовании, i_2 — номер места для второй буквы и т. д. В верхней строке таблицы выписаны по порядку числа от 1 до n, а в нижней — те же числа, но в произвольном порядке. Такая таблица называется подстановкой степени n.

Зная подстановку, задающую преобразование, можно осуществить как зашифрование, так и расшифрование текста. Например, если для преобразования используется подстановка

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

и в соответствии с ней зашифровывается слово `МОСКВА`, то получится `КОСВМА`. Попробуйте расшифровать сообщение `НЧЕИУК`, полученное в результате преобразования с помощью указанной выше подстановки.

В качестве упражнения читателю предлагается самостоятельно выписать подстановки, задающие преобразования в описанных ниже трех примерах шифров перестановки. Ответы помещены в конце раздела.

Читатель, знакомый с методом математической индукции, может легко убедиться в том, что существует $1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$ (обозначается $n!$, читается «n факториал») вариантов заполнения нижней строки таблицы (6). Таким образом, число различных преобразований шифра перестановки, предназначенного для зашифрования сообщений длины n, меньше либо равно $n!$ (заметим, что в это число входит и вариант преобразования, оставляющий все символы на своих местах!).

С увеличением числа n значение $n!$ растет очень быстро. Приведем таблицу значений $n!$ 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 приближенного вычисления $n!$ можно пользоваться известной формулой Стирлинга

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

где $e = 2,718281828\ldots$

Примером ШП, предназначенного для зашифрования сообщений длины n, является шифр, в котором в качестве множества ключей взято множество всех подстановок степени n, а соответствующие им преобразования шифра задаются, как было описано выше. Число ключей такого шифра равно $n!$.

Для использования на практике такой шифр не удобен, так как при больших значениях n приходится работать с длинными таблицами.

Широкое распространение получили шифры перестановки, использующие некоторую геометрическую фигуру. Преобразования из этого шифра состоят в том, что в фигуру исходный текст вписывается по ходу одного «маршрута», а затем по ходу другого выписывается с нее. Такой шифр называют маршрутной перестановкой. Например, можно вписывать исходное сообщение в прямоугольную таблицу, выбрав такой маршрут: по горизонтали, начиная с левого верхнего угла поочередно слева направо и справа налево. Выписывать же сообщение будем по другому маршруту: по вертикали, начиная с верхнего правого угла и двигаясь поочередно сверху вниз и снизу вверх.

Зашифруем, например, указанным способом фразу:

ПРИМЕРМАРШРУТНОЙПЕРЕСТАНОВКИ

используя прямоугольник размера 4×7:

П	Р	И	М	Е	Р	М
Н	Т	У	Р	Ш	Р	А
О	Й	П	Е	Р	Е	С
И	К	В	О	Н	А	Т

Зашифрованная фраза выглядит так:

МАСТАЕРРЕШРНОЕРМИУПВКЙТРПНОИ

Теоретически маршруты могут быть значительно более изощренными, однако запутанность маршрутов усложняет использование таких шифров.

Ниже приводятся описания трех разновидностей шифров перестановки, встречавшихся в задачах олимпиад.

Шифр «Сцитала». Одним из самых первых шифровальных приспособлений был жезл («Сцитала»), применявшийся еще во времена войны Спарты против Афин в V веке до н. э. Это был цилиндр, на который виток к витку наматывалась узкая папирусная лента (без просветов и нахлестов), а затем на этой ленте вдоль его оси записывался необходимый для передачи текст. Лента сматывалась с цилиндра и отправлялась адресату, который, имея цилиндр точно такого же диаметра, наматывал ленту на него и прочитывал сообщение. Ясно, что такой способ шифрования осуществляет перестановку местами букв сообщения.

Шифр «Сцитала», как видно из решения задачи 2.1, реализует не более n перестановок (n, по прежнему, — длина сообщения). Действительно, этот шифр, как нетрудно видеть, эквивалентен следующему шифру маршрутной перестановки: в таблицу, состоящую из m столбцов, построчно записывают сообщение, после чего выписывают буквы по столбцам. Число задействованных столбцов таблицы не может превосходить длины сообщения.

Имеются еще и чисто физические ограничения, накладываемые реализацией шифра «Сцитала». Естественно предположить, что диаметр жезла не должен превосходить 10 сантиметров. При высоте строки в 1 сантиметр на одном витке такого жезла уместится не более 32 букв ($10\pi < 32$). Таким образом, число перестановок, реализуемых «Сциталой», вряд ли превосходит 32.

Шифр «Поворотная решетка». Для использования шифра, называемого поворотной решеткой, изготавливается трафарет из прямоугольного листа клетчатой бумаги размера $2m \times 2k$ клеток. В трафарете вырезано mk клеток так, что при наложении его на чистый лист бумаги того же размера четырьмя возможными способами его вырезы полностью покрывают всю площадь листа.

Буквы сообщения последовательно вписываются в вырезы трафарета (по строкам, в каждой строке слева направо) при каждом из четырех его возможных положений в заранее установленном порядке.

Поясним процесс шифрования на примере. Пусть в качестве ключа используется решетка 6×10, приведенная на рис. 1.

Зашифруем с ее помощью текст

ШИФРРЕШЕТКАЯВЛЯЕТСЯЧАСТНЫМСЛУЧАЕМШИФРАМАРШРУТНОЙПЕРЕСТАНОВКИ

Наложив решетку на лист бумаги, вписываем первые 15 (по числу выре-

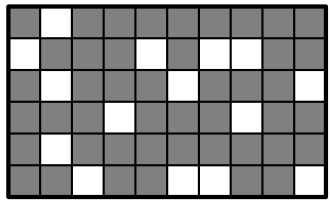


Рис. 1

зов) букв сообщения: ШИФРРЕШЕТКАЯВЛЯ.... Сняв решетку, мы увидим текст, представленный на рис. 2. Поворачиваем решетку на 180°. В окошечках появятся новые, еще не заполненные клетки. Вписываем в них следующие 15 букв. Получится запись, приведенная на рис. 3. Затем переворачиваем решетку на другую сторону и зашифровываем остаток текста аналогичным образом (рис. 4, 5).

	ь							
х				т		п	п		
	е				ь				е
			р				й		
	ю								
		ъ			б	к			ъ

Рис. 2

е	ь		р	я			ъ		
х				т		п	п	в	
	е	ю			ь	я			е
р			р	м			й	ш	
	ю	л	я		к				с
		ъ			б	к		в	ъ

Рис. 3

е	ь	ю	р	я	е	л	ъ		ь
х	х			т		п	п	в	
	е	ю	т		ь	я	п		е
р	ю		р	м	л		й	ш	ю
п	ю	л	я	ь	к	п	с		с
	р	ъ			б	к		в	ъ

Рис. 4

е	ь	ю	р	я	е	л	ъ	м	ь
х	х	н	и	т	о	п	п	в	е
п	е	ю	т	е	ь	я	п	я	е
р	ю	р	р	м	л	ю	й	ш	ю
п	ю	л	я	ь	к	п	с	м	с
н	р	ъ	б	й	б	к	х	в	ъ

Рис. 5

Получатель сообщения, имеющий точно такую же решетку, без труда прочтет исходный текст, наложив решетку на шифртекст по порядку четырьмя способами.

Можно доказать, что число возможных трафаретов, то есть количество ключей шифра «решетка», составляет $T = 4^{mk}$ (см. задачу 1.1). Этот шифр предназначен для сообщений длины $n = 4mk$. Число всех перестановок в тексте такой длины составит $(4mk)!$, что во много раз

больше числа T. Однако, уже при размере трафарета 8×8 число возможных решеток превосходит 4 миллиарда.

Широко распространена разновидность шифра маршрутной перестановки, называемая **«шифром вертикальной перестановки» (ШВП)**. В нем снова используется прямоугольник, в который сообщение вписывается обычным способом (по строкам слева направо). Выписываются буквы по вертикали, а столбцы при этом берутся в порядке, определяемом ключом. Пусть, например, этот ключ таков: (5,4,1,7,2,6,3), и с его помощью надо зашифровать сообщение:

ВОТПРИМЕРШИФРАВЕРТИКАЛЬНОЙПЕРЕСТАНОВКИ

Впишем сообщение в прямоугольник, столбцы которого 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	–	–	–	–

Теперь, выбирая столбцы в порядке, заданном ключом, и выписывая последовательно буквы каждого из них сверху вниз, получаем такую криптограмму:

ОРЕЬЕКРФИЙА-МААЕО-ТШРНСИВЕВЛРВИРКПН-ПИТОТ-

Число ключей ШВП не более $m!$, где m — число столбцов таблицы. Как правило, m гораздо меньше, чем длина текста n (сообщение укладывается в несколько строк по m букв), а, значит, и $m!$ много меньше $n!$.

Пользуясь приведенной выше формулой Стирлинга при больших m и n, попытайтесь оценить, во сколько раз число возможных перестановок ШВП с m столбцами меньше числа всех перестановок на тексте длины n, кратном m.

В случае, когда ключ ШВП не рекомендуется записывать, его можно извлекать из какого-то легко запоминающегося слова или предложения. Для этого существует много способов. Наиболее распространенный состоит в том, чтобы приписывать буквам числа в соответствии с обычным алфавитным порядком букв. Например, пусть ключевым словом будет ПЕРЕСТАНОВКА. Присутствующая в нем буква А получает номер 1. Если какая-то буква входит несколько раз, то ее появления нумеруются последовательно слева направо. Поэтому второе вхождение буквы А получает номер 2. Поскольку буквы Б в этом слове нет, то буква В получает номер 3 и так далее. Процесс продолжается до тех пор, пока

все буквы не получат номера. Таким образом, мы получаем 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

Перейдем к вопросу о методах вскрытия шифров перестановки. Проблема, возникающая при восстановлении сообщения, зашифрованного ШП, состоит не только в том, что число возможных ключей велико даже при небольших длинах текста. Если и удастся перебрать все допустимые варианты перестановок, не всегда ясно, какой из этих вариантов истинный. Например, пусть требуется восстановить исходный текст по криптограмме АОГР, и нам ничего не известно, кроме того, что применялся шифр перестановки. Какой вариант «осмысленного» исходного текста признать истинным: ГОРА или РОГА? А может быть АРГО? Приведем пример еще более запутанной ситуации. Пусть требуется восстановить сообщение по криптограмме

ААНИНК-ТЕОМЛ,З.ЬЬЗИВТЛП-ЬЯО

полученной шифром перестановки. Возможны, как минимум, два варианта исходного сообщения:

КАЗНИТЬ,-НЕЛЬЗЯ-ПОМИЛОВАТЬ. и
КАЗНИТЬ-НЕЛЬЗЯ,-ПОМИЛОВАТЬ.

Эти варианты имеют прямо противоположный смысл и в имеющихся условиях у нас нет возможности определить, какой из вариантов истинный.

Иногда, за счет особенностей реализации шифра, удается получить информацию об использованном преобразовании (перестановке). Рассмотрим шифр «Сцитала» из задачи 2.1. Выше уже рассматривался вопрос о количестве перестановок, реализуемых «Сциталой». Их оказалось не более 32. Это число невелико, поэтому можно осуществить перебор всех вариантов. При достаточной длине сообщения, мы, скорее всего, получим единственный читаемый вариант текста. Однако, используя информацию о расположении линий, оставленных шифровальщиком, удается определить диаметр стержня, а значит, и возникающую перестановку букв (см. задачу 2.1).

В рассмотренном примере шифровальщик по неосторожности оставил на папирусе следы, позволяющие нам легко прочитать сообщение. Возможны и другие ситуации, когда не очень «грамотное» использование шифра облегчает вскрытие переписки.

В задаче 5.2 содержится пример текста, зашифрованного ШВП. По условию пробелы между словами при записи текста в таблицу опускались. Поэтому заключаем, что все столбцы, содержащие пробел в последней строке, должны стоять в конце текста. Таким образом, возникает разбиение столбцов на две группы (содержащие 6 букв, и

содержащие 5 букв). Для завершения восстановления исходного текста достаточно найти порядок следования столбцов в каждой из групп в отдельности, что гораздо проще.

Аналогичная ситуация возникает и при «неполном» использовании шифра «решетка» (см. задачу 4.1). Пусть имеется решетка размера $m \times r$, и зашифрованное с ее помощью сообщение длины $mr - k$, не содержащее пробелов. Незаполненные k мест в решетке при условии, что $k \leqslant mr/4$, соответствуют вырезам в четвертом положении решетки. На основе такой информации, происходит резкое уменьшение числа допустимых решеток (их будет $4^{mr/4-k}$). Читателю предлагается самостоятельно подсчитать число допустимых решеток при $k > mr/4$.

На примере решения задачи 5.2 продемонстрируем еще один подход к вскрытию шифров вертикальной перестановки — лингвистический. Он основан на том, что в естественных языках некоторые комбинации букв встречаются очень часто, другие — гораздо реже, а многие вообще не встречаются (например — «ыьъ»).

Будем подбирать порядок следования столбцов друг за другом так, чтобы во всех строках этих столбцов получались «читаемые» отрезки текста. В приведенном решении задачи восстановление текста начинается с подбора цепочки из трех столбцов первой группы, содержащей в последней строке сочетание ТЧК, так как естественно предположить, что сообщение заканчивается точкой. Далее подбираются столбцы, продолжающие участки текста в других строках, и т. д.

Сочетание лингвистического метода с учетом дополнительной информации довольно быстро может привести к вскрытию сообщения.

В заключение рассказа о шифрах перестановки приведем 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., — нашел 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
2. Его мы очень смирным знали
3. Гроза двенадцатого года
4. Но Бог помог — стал ропот ниже
5. И чем жирнее, тем тяжеле
6. Авось, о Шиболет народный
7. Авось, аренды забывая

1. Нечаянно пригретый славой
2. Орла двуглавого щипали
3. Остервенение народа
4. Мы очутилися в Париже
5. Скажи, зачем ты в самом деле
6. Но стихоплет великородный
7. Авось по манью Николая

8. Сей муж судьбы, сей странник бранный
9. Тряслися грозно Пиринеи
10. Я всех уйму с моим народом
11. Потешный полк Петра Титана
12. Россия присмирела снова
13. У них свои бывали сходки
14. Витийством резким знамениты
15. Друг Марса, Вакха и Венеры
16. Так было над Невою льдистой

17. Плешивый щеголь, враг труда
18. Когда не наши повара
19. Настала — кто тут нам помог?
20. И скоро силою вещей
21. О русский глупый наш народ
22. Тебе б я оду посвятил
23. Ханжа запрется в монастырь
24. Пред кем унизились цари
25. Волкан Неаполя пылал
26. Наш царь в конгрессе говорил
27. Дружина старых усачей
28. И пуще царь пошел кутить
29. Они за чашею вина
30. Сбирались члены сей семьи
31. Тут Лунин дерзко предлагал
32. Но там, где ранее весна

8. Сей всадник, папою венчанный
9. Безрукий князь друзьям Мореи
10. А про себя и в ус не дует
11. Предавших некогда тирана
12. Но искра пламени иного
13. Они за рюмкой русской водки
14. У беспокойного Никиты
15. Свои решительные меры
16. Блестит над каменкой тенистой
17. Над нами царствовал тогда
18. У Бонапартова шатра
19. Барклай, зима иль русский бог?
20. А русский царь главой царей
21. . . . . .
22. Меня уже предупредил
23. Семействам возвратит Сибирь
24. Исчезнувший как тень зари
25. Из Кишинева 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 ее, получилась бессвязная чепуха, в которой одна строка, едва начавшая мысль, перебивается другой, а та — третьей, еще 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 все это мало похоже. Просчитал строку — четырехстопный ямб, размер, которым написан «Евгений Онегин».

Трубачевский с азартом взялся за рукопись, пытался читать ее, 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. Все 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 ее 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 отчетливостью, как это бывает только во сне.

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

Ответы к упражнению.

1) Шифр маршрутной перестановки

1	2	3	4	5	6	7	8	9	10	11	12	13	14
25	24	17	16	9	8	1	2	7	10	15	18	23	26

15	16	17	18	19	20	21	22	23	24	25	26	27	28
27	22	19	14	11	6	3	4	5	12	13	20	21	28

2) Шифр «решетка»

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	11	15	17	18	22	26	30	34	38	42	53	56	57	60

16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	4	5	8	19	23	27	31	35	39	43	44	46	50	59

31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
3	6	7	10	12	24	28	32	36	40	41	45	47	48	52

46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
9	13	14	16	20	21	25	29	33	37	49	51	54	55	58

3) ШВП

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
23	1	17	34	7	29	12	24	2	18	35	8	30	13	25

16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
3	19	36	9	31	14	26	4	20	37	10	32	15	27	5

31	32	33	34	35	36	37	38
21	38	11	33	16	28	6	22

4. Многоалфавитные шифры замены с периодическим ключом

Рассмотрим 30-буквенный алфавит русского языка:

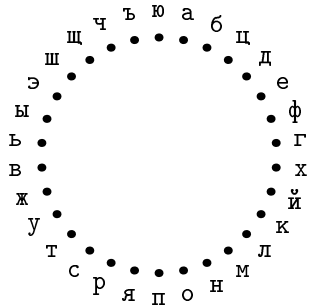
А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Э Ю Я.

В этом алфавите отсутствуют буквы Ё, Й и Ъ, что практически не ограничивает возможностей по составлению открытых сообщений на русском языке. В самом деле, замена буквы Ё на букву Е, буквы Й — на

букву И, а буквы Ъ — на букву Ь позволяет понять смысл открытого сообщения, написанного с использованием этого алфавита.

В алфавите любого естественного языка буквы следуют друг за другом в определенном порядке. Это дает возможность присвоить каждой букве алфавита ее естественный порядковый номер. Так, в приведенном алфавите букве А присваивается порядковый номер 1, букве О — порядковый номер 14, а букве Ы — порядковый номер 27. Если в открытом сообщении каждую букву заменить ее естественным порядковым номером в рассматриваемом алфавите, то преобразование числового сообщения в буквенное позволяет однозначно восстановить исходное открытое сообщение. Например, числовое сообщение 1 11 20 1 3 9 18 преобразуется в буквенное сообщение: АЛФАВИТ.

Дополним естественный порядок букв в алфавите. Будем считать, что за последней буквой алфавита следует его первая буква. Такой порядок букв достигается, если расположить их на окружности в естественном порядке по часовой стрелке. При таком расположении можно каждой из букв присвоить порядковый номер относительно любой буквы алфавита. Такой номер назовем относительным порядковым номером. Заметим, что если число букв в алфавите равно z, то относительный порядковый номер данной буквы может принимать все значения от 0 до $(z-1)$ в зависимости от буквы, относительно которой он вычисляется. Для примера рассмотрим исходный 30-буквенный алфавит русского языка, расположенный на окружности (см. рис.).



В этом случае порядковый номер буквы А относительно буквы А равен 0, относительно буквы Я он уже равен 1 и так далее, относительно буквы Б порядковый номер А равен 29. Значения относительных порядковых номеров букв алфавита из z букв совпадают со значениями всевозможных остатков от деления целых чисел на натуральное число z. Убедитесь в том, что порядковый номер какой-либо буквы алфавита относительно другой буквы равен остатку от деления разности их естественных порядковых номеров на число букв в алфавите.

Обозначим символами:

$D(N_1, N_2)$ — порядковый номер буквы с естественным порядковым номером N_1 относительно буквы с естественным порядковым номером N_2;

$r_m(N)$ — остаток от деления целого числа N на натуральное число m.

При этом справедливо равенство $D(N_1, N_2) = r_z(N_1 - N_2)$, где z — число букв в алфавите.

Для удобства обозначим $N_1 \boxminus N_2 = r_z(N_1 - N_2)$, $N_1 \boxplus N_2 = r_z(N_1 + N_2)$. Тогда имеют место равенства:

$$D(N_1, N_2) = N_1 \boxminus N_2, \tag{7}$$

$$N_1 = N_2 \boxplus D(N_1, N_2). \tag{8}$$

Формула (8) непосредственно получается из (7) и ее можно использовать для замены буквы с естественным порядковым номером N_2 на букву с естественным порядковым номером N_1. Число $D(N_1, N_2)$ называется знаком гаммы.

Для уяснения введенных обозначений читателю предлагается самостоятельно решить следующие задачи.

1. Докажите, что для любых целых N_1, N_2 и любого натурального z справедливо равенство: $D(N_1, N_2) = N_1 - N_2 - \left[\dfrac{N_1 - N_2}{z}\right] \cdot z$, где $[X]$ — целая часть числа X (наибольшее целое число, не превосходящее числа X).

2. Докажите равенство (8) и равенство:

$$N_2 = N_1 \boxminus D(N_1, N_2). \tag{9}$$

Для зашифрования некоторого открытого сообщения, состоящего из N букв, с помощью указанной замены требуется N знаков гаммы: по одному на каждую букву сообщения. Последовательность знаков гаммы, необходимая для зашифрования открытого сообщения, является ключом данного шифра.

Если последовательность знаков гаммы имеет небольшой (по сравнению с длиной открытого текста) период, то соответствующий шифр называется шифром замены с периодическим ключом. Ключом такого шифра, по существу, является отрезок гаммы, равный по длине периоду.

Число отрезков некоторой длины T, состоящих из чисел от 0 до $(z-1)$ равно z^T, так как на каждой из T позиций отрезка может быть любое из z чисел (независимо от чисел, находящихся на других позициях). Для наглядности приведем значения z^T при $z = 30$ в зависимости от значений T:

T	1	2	3	4	5	6	7
30^T	30	900	27000	810000	24300000	$0,729 \cdot 10^9$	$0,2187 \cdot 10^{11}$

T	8	9	10
30^T	$0,6561 \cdot 10^{12}$	$0,19683 \cdot 10^{14}$	$0,59049 \cdot 10^{15}$

Как видно из приведенной таблицы, число ключей рассматриваемого шифра замены с ключом периода 10, достаточно внушительно и составляет уже сотни триллионов. Это обстоятельство делает практиче-

ски невозможным вскрытие шифра методом перебора всех его ключей даже при меньших значениях периода гаммы.

Для рассматриваемого шифра характерно то, что буквы открытого текста, зашифрованные одним и тем же знаком гаммы, по сути, зашифрованы одним и тем же шифром простой замены. Например, ключевая таблица этого шифра простой замены при знаке гаммы, равном 1, имеет вид:

АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯ
БВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯА

Вторую строку этой ключевой таблицы называют алфавитом шифрования, соответствующим данному знаку гаммы. Поскольку в рассматриваемом шифре возможны все значения гаммы от 0 до 29, то данный шифр можно рассматривать как 30-алфавитный шифр замены. Если каждому из этих алфавитов поставить в соответствие его первую букву, то каждый знак гаммы можно заменить этой буквой. В этом случае ключ рассматриваемого шифра можно взаимнооднозначно заменить соответствующим словом в этом же алфавите. Такой многоалфавитный шифр замены был описан в 1585 году французом Блезом де Виженером в его «Трактате о шифрах»:

ABCDEFGHIJKLMNOPQRSTUVWXYZ
BCDEFGHIJKLMNOPQRSTUVWXYZA
CDEFGHIJKLMNOPQRSTUVWXYZAB
DEFGHIJKLMNOPQRSTUVWXYZABC
EFGHIJKLMNOPQRSTUVWXYZABCD
FGHIJKLMNOPQRSTUVWXYZABCDE
GHIJKLMNOPQRSTUVWXYZABCDEF
HIJKLMNOPQRSTUVWXYZABCDEFG
IJKLMNOPQRSTUVWXYZABCDEFGH
JKLMNOPQRSTUVWXYZABCDEFGHI
KLMNOPQRSTUVWXYZABCDEFGHIJ
LMNOPQRSTUVWXYZABCDEFGHIJK
MNOPQRSTUVWXYZABCDEFGHIJKL
NOPQRSTUVWXYZABCDEFGHIJKLM
OPQRSTUVWXYZABCDEFGHIJKLMN
PQRSTUVWXYZABCDEFGHIJKLMNO
QRSTUVWXYZABCDEFGHIJKLMNOP
RSTUVWXYZABCDEFGHIJKLMNOPQ
STUVWXYZABCDEFGHIJKLMNOPQR
TUVWXYZABCDEFGHIJKLMNOPQRS
UVWXYZABCDEFGHIJKLMNOPQRST
VWXYZABCDEFGHIJKLMNOPQRSTU
WXYZABCDEFGHIJKLMNOPQRSTUV
XYZABCDEFGHIJKLMNOPQRSTUVW
YZABCDEFGHIJKLMNOPQRSTUVWX
ZABCDEFGHIJKLMNOPQRSTUVWXY

Все алфавиты шифрования относительно латинского алфавита были сведены им в таблицу, получившую впоследствии название ее автора. Выше приведена таблица Виженера для современного латинского алфавита, она состоит из списка 26 алфавитов шифрования. Способ зашифрования с помощью таблицы Виженера заключается в том, что первый из алфавитов соответствует алфавиту открытого текста, а букве ключевого слова соответствует алфавит шифрования из данного списка, начинающийся с этой буквы. Буква шифрованного текста находится в алфавите шифрования на месте, соответствующем данной букве открытого текста. Простота построения таблицы Виженера делает эту систему привлекательной для практического использования. Рассмотрим пример вскрытия многоалфавитного шифра замены с периодическим ключом, содержащийся в рассказе Жюля Верна «Жангада». Вот текст, который был получен с помощью такого типа шифра:

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

Догадавшись, что ключом является натуральное число, персонаж «Жангады», судья Жаррикес, объясняет сыну обвиняемого Маноэлю, как был зашифрован документ: —«Давайте возьмем фразу, все равно какую, ну хотя бы вот эту:

У СУДЬИ ЖАРРИКЕСА ПРОНИЦАТЕЛЬНЫЙ УМ

А теперь я возьму наудачу какое-нибудь число, чтобы сделать из этой фразы криптограмму. Предположим, что число состоит из трех цифр, например, 4, 2 и 3. Я подписываю число 423 под строчкой так, чтобы под каждой буквой стояла цифра, и повторяю число, пока не дойду до конца фразы. Вот что получится:

У С У Д Ь И Ж А Р Р И К Е С А П Р О Н И Ц А Т Е Л Ь Н Ы Й У М
4 2 3 4 2 3 4 2 3 4 2 3 4 2 3 4 2 3 4 2 3 4 2 3 4 2 3 4 2 3 4

Будем заменять каждую букву нашей фразы той буквой, которая стоит после нее в алфавите

АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

на месте, указанном цифрой. Например, если под буквой А стоит цифра 3, вы отсчитываете три буквы и заменяете ее буквой Г. Если буква

находится в конце алфавита и к ней нельзя прибавить нужного числа букв, тогда отсчитывают недостающие буквы с начала алфавита.

Доведем до конца начатую криптограмму, построенную на числе 423, и исходная фраза заменится следующей:

Ч У Ц И Ю Л К В У Ф К Н Й У Г У Т С С К Щ Д Ф И П Ю Р Я Л Ц Р

Но как найти числовой ключ? Подсчет, проведенный Жаррикесом, показывает, что поиск ключа перебором всех возможных чисел, состоящих не более чем из 10 цифр, потребует более трехсот лет. Судья пытается наудачу отгадать заветное число. Наступает день казни. Обвиняемого Жоама Дакосту ведут на виселицу...

Но все заканчивается благополучно. Помог счастливый случай. Другу Жоама удается узнать, что автора криптограммы звали Ортега. Поставив буквы О, Р, Т, Е, Г, А над последними шестью буквами документа и подсчитав, на сколько эти буквы по алфавиту сдвинуты относительно букв криптограммы, судья, наконец, находит ключ к документу:

исходное сообщение	О	Р	Т	Е	Г	А
шифрованное сообщение	Т	У	Ф	К	Д	Г
относительный сдвиг букв	4	3	2	5	1	3

Г. А. Гуревич в статье «Криптограмма Жюля Верна» (журнал «Квант» №9, 1985 г.) обращает внимание на то, что судья прошел практически весь путь до отгадки. Будучи уверенным, что в документе упоминается имя Жоама Дакосты, судья строит предположение: «Если бы строчки были разделены на слова, то мы могли бы выделить слова, состоящие из семи букв, как и фамилия Дакоста, и, опробуя их одно за другим, может быть и отыскали бы число, являющееся ключом криптограммы». Маноэль, в свою очередь, поняв основную идею судьи, предлагает опробовать возможные расположения слова ДАКОСТА в исходном тексте. Поскольку текст состоит из 252 букв, то достаточно опробовать не более 246 вариантов. В один прекрасный момент, записав над фрагментом ЙБНТФФЕ слово ДАКОСТА, мы определили бы последовательность цифр 5134325. Естественно предположить, что последняя цифра 5 — начало следующего периода:

исходное сообщение	...	Д	А	К	О	С	Т	А	...
шифрованное сообщение	...	Й	Б	Н	Т	Ф	Ф	Е	...
относительный сдвиг букв	...	5	1	3	4	3	2	5	...

Вместо ключа 432513 мы нашли его циклическую перестановку 513432, что ни в коей мере не мешает расшифрованию текста. Для этого достаточно для каждой буквы шифрованного текста определить букву, относительно которой данная буква сдвинута на величину соответствующей цифры ключа:

```
С Г У Ч П В Э Л Л З Й Р Т Е П Н Л Н Ф Г И Н Б О Р
4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4
Н А С Т О Я Щ И Й В И Н О В Н И К К Р А Ж И А Л М

Г Й У Г Л Ч Д К О Т Х Ж Г У У М З Д Х Р Ъ С Г С Ю
3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3
А З О В И У Б И Й С Т В А С О Л Д А Т О Х Р А Н Ы

Д Т П Ъ А Р В Й Г Г И Щ В Ч Э Е Ц С Т У Ж В С Е В
2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2
В Н О Ч Ь Н А Д В А Д Ц А Т Ь В Т О Р О Е Я Н В А

Х А Х Я Ф Б Ь Б Е Т Ф З С Э Ф Т Х Ж З Б З Ъ Г Ф Б
5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5
Р Я Т Ы С Я Ч А В О С Е М Ь С О Т Д В А Д Ц А Т Ь

Щ И Х Х Р И П Ж Т З В Т Ж Й Т Г О Й Б Н Т Ф Ф Е О
1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1
Ш Е С Т О Г О Г О Д А Н Е Ж О А М Д А К О С Т А Н

И Х Т Т Е Г И И О К З П Т Ф Л Е У Г С Ф И П Т Ь М
3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3
Е С П Р А В Е Д Л И В О П Р И Г О В О Р Е Н Н Ы Й

О Ф О К С Х М Г Б Т Ж Ф Ы Г У Ч О Ю Н Ф Н Ш З Г Э
4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4
К С М Е Р Т И А Я Н Е С Ч А С Т Н Ы Й С Л У Ж А Щ

Л Л Ш Р У Д Е Н К О Л Г Г Н С Б К С С Е П У Н Ф Ц
3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 1 5 3 4 3
И Й У П Р А В Л Е Н И Я А Л М А З Н О Г О О К Р У

Е Е Е Г Г С Ж Н О Е Ы И О Н Р С И Т К Ц Ь Е Д Б У
2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2
Г А Д А Я О Д И Н В Ч Е М И П О Д П И С Ы В А Ю С

Б Т Е Т Л О Т Б Ф Ц С Б Ю Й П М П З Т Ж П Т У Ф К
5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5
Ь С В О И М Н А С Т О Я Щ И М И М Е Н Е М О Р Т Е

Д Г
1 3
Г А
```

Итак, первая идея состоит в использовании вероятного слова, то есть слова, которое с большой вероятностью может содержаться в данном открытом тексте. Речь идет в том числе и о словах, часто встречающихся в любых открытых текстах. К ним, например, относятся такие слова как КОТОРЫЙ, ТОГДА, ЧТО, ЕСЛИ, приставки ПРИ, ПРЕ, ПОД и т. п.

Вторая идея основана на том, что буквы открытого сообщения находятся в открытом тексте на вполне определенных позициях. Если разность номеров их позиций окажется кратной периоду гаммы, то стоящие на этих позициях буквы будут зашифрованы одним и тем же знаком гаммы. Это означает, что определенные части открытого текста окажутся зашифрованными шифром простой замены. Эту идею можно использовать для определения периода ключа многоалфавитного шифра замены.

Для определения периода гаммы могут быть применены два способа. Первый из них известен как тест Казизки, второй способ использует так называемый индекс совпадения.

Тест Казизки был описан в 1863 году Фридрихом Казизки. Он основан на следующем наблюдении: два одинаковых отрезка открытого текста будут соответствовать двум одинаковым отрезкам шифрованного текста, если разность номеров позиций их начал кратна периоду гаммы. Следовательно, если мы обнаружим два одинаковых отрезка шифрованного текста, состоящих по крайней мере из трех букв, то с большой вероятностью им соответствуют одинаковые отрезки открытого текста (случайное совпадение маловероятно). Тест Казизки, по сути, заключается в том, что в шифрованном тексте надо найти пары одинаковых отрезков, вычислить разности номеров позиций их начал и определить общие делители найденных разностей. Как правило, один из этих общих делителей равен периоду гаммы.

Для уточнения значения периода гаммы может быть использован индекс совпадения, предложенный в 1920 году Уильямом Фридманом. Для последовательности букв индекс совпадения представляет собой число, равное количеству всех пар номеров позиций последовательности, на которых находятся одинаковые буквы, деленному на общее количество всех пар номеров позиций этой последовательности, т. е. среднему числу пар, состоящих из одинаковых букв. Примечательно то, что при зашифровании последовательности с помощью шифра простой замены указанное число не меняется.

Для иллюстрации этого подхода рассмотрим тот же самый шифрованный текст, записанный в виде последовательности столбцов, содержащих по шесть подряд идущих букв текста в каждом (подряд идущие буквы текста располагаются в столбцах сверху вниз):

```
СЭТФРЧЖДСАИЦСЯТТЪХТТТХИФФОМЫНЭДГСФГЫИДТЦМТ
ГЛЕГГДГХЮРЩСЕФФХГХЗГФТОЛИФГГФЛЕГСЦСИТБЛСПУ
УЛПИЙКУРДВВТВБЗЖФРВОФТКЕПОБУНЛННЕЕЖОКУОБЗФ
ЧЗННУОУЪТЙЧУХЬСЗБИТЙЕЕЗУТКТЧШШКСУЕННЦБТЮТК
ПЙЛБГТМСПГЭЖАБЭБЩПЖБОГПГЬСЖОЗРОБПЕОРЬТБЙЖД
ВРНОЛХЗГЪГЕВХЕФЗИЖЙНИИТСМХФЮГУЛКНГЕСЕЕФППГ
```

Составим для каждой из 6 получившихся строк соответствующий ей набор частот встречаемости букв в каждой из них:

	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
1 строка	1	0	0	2	3	0	1	0	3	0	0	0	2	1	1	0
2 строка	0	1	0	9	1	3	0	1	2	0	0	4	0	0	1	1
3 строка	0	3	4	0	1	3	2	2	1	1	3	2	0	3	4	2
4 строка	0	2	0	0	0	4	0	3	1	2	3	0	0	4	1	0
5 строка	1	6	0	4	1	1	4	1	0	2	0	0	1	0	4	5
6 строка	0	0	2	5	0	5	1	2	3	1	1	2	1	3	1	2

	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
1 строка	1	4	8	0	4	2	2	1	0	0	1	2	0	2	0	1
2 строка	1	4	2	1	5	3	1	0	0	1	0	0	0	0	1	0
3 строка	2	0	2	4	3	0	0	0	0	0	0	0	0	0	0	0
4 строка	0	2	6	4	0	1	1	3	2	0	1	0	1	0	1	0
5 строка	2	2	2	0	0	0	0	0	0	1	0	0	2	2	0	0
6 строка	1	2	1	1	3	3	0	0	0	0	1	0	0	0	1	0

По этой таблице частот встречаемости букв вычислим для каждой строки соответствующий ей индекс совпадения:

Номер строки	1	2	3	4	5	6
Индекс совпадения	0,060	0,077	0,045	0,053	0,057	0,057

Для всего шифрованного текста индекс совпадения равен 0,040, что заметно меньше, чем индекс совпадения для каждой из указанных строк. Это является хорошим подтверждением гипотезы о длине периода гаммы.

Другие идеи подходов к вскрытию рассматриваемых шифров основаны на тех или иных особенностях их построения и использования (см. решения задач 1.2, 2.2, 2.5, 2.6, 3.4, 3.5, 4.6).

5. Условия задач олимпиад по криптографии и математике

Ниже приводятся задачи пятнадцати 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 решетка», является трафарет, изготовленный из квадратного листа клетчатой бумаги раз-

мера $n \times n$ (n — четно). 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, причем 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 четного 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 трехчлена $x^2 + 3x + 1$. 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 внедренному разведчику был установлен следующий порядок.

Все сообщения резидента определены заранее и пронумерованы числами 1, 2, 3, ... 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:

ФН	×	Ы	=	ФАФ
+		×		−
ЕЕ	+	Е	=	НЗ
=		=		=
ИША	+	МР	=	ИМН

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

II Олимпиада по криптографии и математике

2.1. В древнем шифре, известном под названием «Сцитала», использовалась полоска папируса, которая наматывалась на круглый стержень виток к витку без просветов и нахлестов. 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 прочитать сообщение.

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

2.2. Исходное цифровое сообщение коммерсант шифрует и передает. Для этого он делит последовательность цифр исходного сообщения на группы по пять цифр в каждой и после двух последовательных групп приписывает еще две последние цифры суммы чисел, изображенных 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 сопоставляются 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

АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯ

зашифровывается при помощи последовательности букв этого же алфавита. Длина последовательности равна длине сообщения. Шифрование каждой буквы исходного сообщения состоит в сложении ее 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:

ЮПТЦАРГШАЛЖЖЕВЦЩЫРВУУ и ЮПЯТБНЩМСДТЛЖГПСГХСЦЩ

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 приведенного выше алфавита. Зашифрование каждой буквы сообщения состоит в сложении ее 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: РБЬНТСИТСРРЕЗОХ, 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 $A = \{a_1, a_2, \ldots, a_n\}$, состоящем из n различных букв, заключается в замене каждой буквы шифруемого текста буквой того же алфавита, причем разные буквы заменяются разными. Ключом шифра простой замены называется таблица, в которой указано, какой буквой надо заменить каждую букву алфавита A. 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	Ь	Ы	Э	Ю	Я
Ч	Я	Ю	Э	Ы	Ь	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 еще 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, передается в пункт Б отрезками по 12 символов. При передаче очередного отрезка сначала передаются символы, стоящие на четных местах в порядке возрастания их номеров, начиная со второго, а затем — символы, стоящие на нечетных 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, передается 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 $C_1, C_2, \ldots, C_n, \ldots$ в которой C_n есть последняя цифра числа n^n. Докажите, что эта последовательность периодическая и ее 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	Ь	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:

23398672164581606706173155 88

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?

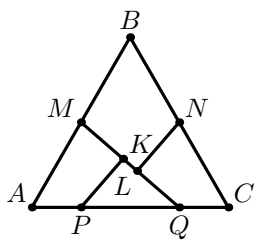


Рис. 6

IV Олимпиада по криптографии и математике

4.1. Ключом шифра, называемого «решеткой», 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 четырех 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 нем 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°. Попытайтесь 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

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

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

ГЪЙ АЭЕ БПРК ЕЖЩЮ НМЬЧ СЫЛЗ ШДУ ЦХОТ ЯФВИ

Восстановите исходный текст, если известно, что характер неисправности таков, что каждая буква заменяется буквой, отстоящей от нее в указанном алфавите не дальше, чем на две буквы. Например, буква Б может перейти в одну из букв {А, Б, 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	Ь	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 $A_1, A_2, \ldots$ 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

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

(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) трех 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 Й 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 $OA + OB + OC \geqslant 2(OP + OQ + OR)$.

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 трех шифрованных текстов

```
ЙМЫВОТСЬЛКЪГВЦАЯЯ
УКМАПОЧСРКЩВЗАХ
ШМФЭОГЧСЙЪКФЬВЫЕАКК
```

соответствовало исходное сообщение МОСКВА. Попробуйте расшифровать три текста

ТПЕОИРВНТМОЛАРГЕИАНВИЛЕДНМТААГТДЬТКУБЧКГЕИШНЕИАЯРЯ

ЛСИЕМГОРТКРОМИТВАВКНОПКРАСЕОГНАЬЕП

РТПАИОМВСВТИЕОБПРОЕННИГЬКЕЕАМТАЛВТДЬСОУМЧШСЕОНШЬИАЯК

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 Ь 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 трех осей установлено по одной вращающейся шестеренке и неподвижной стрелке. Шестеренки соединены последовательно. На первой шестеренке 33 зубца, на второй — 10, на третьей — 7. На каждом зубце первой шестеренки по часовой стрелке написано по одной букве русского языка в алфавитном порядке:

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

На зубцах второй и третьей шестеренки 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 шестеренки против часовой стрелки до первого попадания шифруемой буквы под стрелку. В этот момент по-

следовательно 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 колес — 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 остается 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 $a_1, a_2, a_3, \ldots$ является периодической с периодом 2, если a_n равно остатку от деления числа p^{n+2} на 24 при всех $n \geqslant 1$.

6.7. Найдите все значения параметра a, при которых уравнение

$$\underbrace{\Big|\ldots\Big|}_{\text{1996 раз}}\Big|x-\underbrace{a\Big|-a\Big|-\ldots-}_{\text{1996 раз}}\Big| = 1996.$$

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 остается без изменения, а результат зашифрования каждой следующей цифры зависит только от нее 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:

БТИПЧЬЛОЯЧЫЬТОТПУНТНОНЗЛЖАЧОЬОТУНИУХНИППОЛОЬЧОЕЛОЛС

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 ($x = 1, 2, \ldots, r$), 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. нашел 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 a4.

д	к	п	х	к	о	м	а
с	й	ю	н	р	с	я	р
н	н	н	ю	м	н	х	п
р	а	ц	й	р	р	с	й
й	н	е	н	п	ю	б	н
й	д	ц	о	б	к	е	р
р	ю	м	п	л	ю	ц	н
е	ю	н	б	х	д	с	к

Рис. 7

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 $0, 1, \ldots, 9$ 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

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

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 нуль не выписывается. Восстановите сообщение 873146507381 и укажите таблицу замены букв числами.

VIII Олимпиада по криптографии и математике

Рис. 8

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 ее 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 нуль заменяется на 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, $i = 1, 2, \ldots, 6$, найдется 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 ее построения все нечетные 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, ее цифры почленно складываются с соответствующими цифрами ключевой последовательности, при этом каждая полученная сумма заменяется ее 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 черный цвет, а остальные — в белый. По клеткам квадрата прыгает Криптоша. В момент попадания Криптоши в очередную клетку происходит изменение цвета на противоположный у всех тех клеток, расстояния от центров которых до центра клетки с Криптошей есть натуральные числа. После того как Криптоша побывал в каждой клетке квадрата ровно 1999 раз, квадрат оказался раскрашенным так, как показано на рисунке. Восстановите цвет всех клеток квадрата в начальный момент.

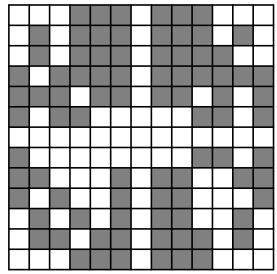


Рис. 9

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 назовем 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 назовем 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

1949^{1999} раз прибавили по правилу задачи 9.1 к слову КРИПТОША. Получили слово АНАЛИТИК. Найдите эту последовательность. Какое наименьшее число раз надо прибавить ее к слову АНАЛИТИК, чтобы получить слово КРИПТОША?

9.3. Каждую букву исходного сообщения заменили ее 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 трехзначные цифровые группы без пересечений и пропусков. Затем, каждое из полученных трехзначных 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 Ь 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 четырем 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

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

X Олимпиада по криптографии и математике

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

Восстановите изображение Криптоши по известным длинам полос черного 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 черного 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)

`ABCDEFGHIKLMNOPQRSTUVWXYZ`

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 назовем *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 $x_n = 1+2+3+\ldots+n$, $n\in\mathbb{N}$, заменим последней цифрой s_n в его десятичной записи. Из последовательности $s_1, s_2, s_3, \ldots$ 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 назовем *перестановкой*. Обозначим перестановку символом p_k, если ее первая цифра является k-ой по счету единицей в последовательности $s_1, s_2, s_3, \ldots$

а) Докажите, что цифровая последовательность $s_1, s_2, s_3, \ldots$ является периодической, и найдите ее наименьший период.

б) Докажите, что последовательность перестановок $p_1, p_2, p_3, \ldots$ является периодической, и найдите ее наименьший период.

10.5. С целью зашифрования разобьем 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 отрезке 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
СОВАККНЧИХОТОСНИАКЧАЯЛУЫБКОЙКОТРЯЕОЩАЕБЫЛВКНААИДН
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, *заменили* 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
РИЖХУВМРЭЭШБЯВРРЖШЬВЭРВУЧМЖЬВЕЖЭКВЖАЬБЯСВХВТРВШАВЕЬГЭШВМВРЖЭ

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 двоичный разряд передается по отдельному проводу. При приеме сообщения Криптоша перепутал провода, поэтому вместо переданного слова получен набор букв ЭАВЩОЩИ. Найдите переданное слово.

11.4. Клетку таблицы 8×8 назовем «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-ая буква сообщения — А, то она заменяется на 7-ую 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 приведенной 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
з	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

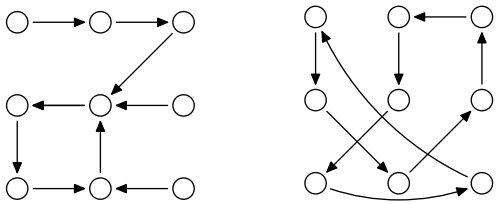
$$\begin{cases} \left(\left|y + x - \dfrac{5+\sqrt{3}}{2}\right| + |x-1|\right)^2 = \\ \qquad = \left(\left|2x - \sqrt{2y} - 2\right| + |y-1| + 1\right) \cdot \left(1 - |y-1| - \left|2x - \sqrt{2y} - 2\right|\right), \\ x^2 + y^2 = 2(x+y) - 1. \end{cases}$$

XII 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 путем 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 передается 1. Найдите переданное слово, если получен текст ТЕЫЕУТАЦ.

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



Какую последовательность действий с лампой и кольцом надо проделать 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 Й, Ь и Ъ 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 зашифровывается 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	Я	О	Л	О	К	Р
Е	А	В	Д	Ь	П	В	И
И	Т	Ж	Е	У	Д	О	И
Ч	Т	С	Т	М	И	Р	Ш
М	П	Э	О	А	О	Й	И
О	Ж	А	Н	Н	Н	А	Т
Т	И	Т	А	И	К	Л	Ч
А	М	Е	М	М	С	Н	Я

Найдите это правило и прочитайте предложение.

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

12.7. Найдите:

а) последнюю цифру числа 2^{2002};

б) 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, причем 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 берет 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 передает 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 передает 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 приведенном ключе является «фраза» `RYXXT OFTXT LKSWS`. 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 счета 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. Криптоша 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 $x_1, x_2, \ldots$, удовлетворяющую соотношению $x_{k+3} = x_k + x_{k+2}$, $k = 1, 2, \ldots$ 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

СЕЗНПБКЬЛЧЕЮЩЦТНИЭЛЬЩБШЬЕЮ

ЛУАЕЧЖЪЭШЭЛЪШЩХЧШДЮВЫЮИД.

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

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 трех 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 раздается щелчок. Сравните число возможных кодовых комбинаций, при установке которых раздается 33, 32, 25 щелчков.

14.3. На фирме работают P служащих. В гараже фирмы имеется B автомобилей. Каждый служащий имеет ключи от t автомобилей, причем 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 $2^{22} + 39 \cdot 2^{10} + 81$.

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 последовательности $t_1, t_2, \ldots, t_k$ прибавили число a_i последовательности $a_1, a_2, \ldots, a_k$, 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 Ь Э Т С Ъ Й 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 путем 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, причем никакие два шаблона не могут иметь общих внутренних точек.

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 шифрованный 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 шифрованному 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 счетчики (назовем 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 передается 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 остается в прежнем состоянии. Злоумышленник способен а) запоминать сигналы брелка, б) поставив помеху, искажать сигналы брелка (при этом сам злоумышленник получает сигнал без искажений), в) посылать замку ранее запомненные сигналы. Как злоумышленнику открыть замок? Алгоритмы шифрования 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) $x_1 \leqslant x_2$; $x_3 \leqslant x_2$; $x_2 \cdot (1-p) \leqslant x_1 \cdot p$.

6. Указания и решения

1.1. Все клетки квадрата размера $n \times n$ разобьем на непересекающиеся группы по четыре клетки в каждой. Отнесем 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, причем клетки одной группы помечены одной и той же цифрой. Всего таких групп будет $n^2/4$ (целое, так как n — четное 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 решетка» при четных 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 $3 \cdot 5 \cdot 7 \cdot 11$. Найдем 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 ее наименьшее общее кратное равно $dqt/q = dt = dm/d = m$. Таким

образом, искомое число упорядоченных пар совпадает с числом всех делителей q вида: $3^x5^y7^z11^u$, 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 $m/d = p^ir^j \dots s^h$, где $p, r, \dots, s$ — различные простые числа, а $i, j, \dots, h$ — натуральные числа. Число всех делителей вида: $q = p^xr^y \dots s^z$, 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 Ш=0. Тогда из первого столбца находим, что И=1. Затем из последнего столбца находим Ф=2. Итак,

$$\begin{array}{ccccccc} \texttt{2Н} & \times & \texttt{Ы} & = & \texttt{2А2} \\ + & & \times & & - \\ \texttt{ЕЕ} & + & \texttt{Е} & = & \texttt{НЗ} \\ = & & = & & = \\ \texttt{10А} & + & \texttt{МР} & = & \texttt{1МН} \end{array}$$

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

$$\begin{array}{ccccccc} \texttt{28} & \times & \texttt{Ы} & = & \texttt{2А2} \\ + & & \times & & - \\ \texttt{77} & + & \texttt{7} & = & \texttt{84} \\ = & & = & & = \\ \texttt{10А} & + & \texttt{МР} & = & \texttt{1М8} \end{array}$$

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

Ответ: ШИФРЗАМЕНЫ

1.6. *Ответ*: например, *cbcacbc*.

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

$$\varphi(cbcacbc) = \overline{\varphi(bcacbc)} = \overline{\varphi(cacbc)a\varphi(cacbc)} =$$
$$= \overline{\overline{\varphi(acbc)a\varphi(acbc)}} = \overline{\overline{cbc}\,\overline{acbc}} = \overline{cbcacbc} = cbcacbc.$$

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

$$P = \begin{cases} cb\underbrace{c\ldots c}_{k\text{ раз}}acb\underbrace{c\ldots c}_{k\text{ раз}} & k \text{ — нечетное;} \\ b\underbrace{c\ldots c}_{k\text{ раз}}ab\underbrace{c\ldots c}_{k\text{ раз}} & k \text{ — четное.} \end{cases}$$

2.1. Рассмотрим один виток ленты на развертке 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.

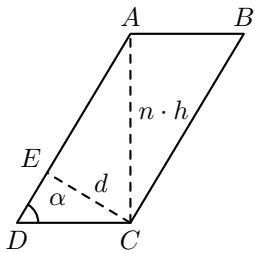


Рис. 10

2.2. Согласно условию, исходное сообщение состоит из двух пятерок цифр: $A_1A_2A_3A_4A_5$ и $B_1B_2B_3B_4B_5$. Пусть C_1C_2 — последние две цифры суммы чисел, изображенных этими пятерками. 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:

$$A_1 \oplus \Gamma_1 = 4, \tag{1}$$
$$A_2 \oplus (\Gamma_1 + X) = 2, \tag{2}$$
$$A_3 \oplus (\Gamma_1 + 2X) = 3, \tag{3}$$
$$A_4 \oplus (\Gamma_1 + 3X) = 4, \tag{4}$$
$$A_5 \oplus (\Gamma_1 + 4X) = 6, \tag{5}$$
$$B_1 \oplus (\Gamma_1 + 5X) = 1, \tag{6}$$
$$B_2 \oplus (\Gamma_1 + 6X) = 4, \tag{7}$$
$$B_3 \oplus (\Gamma_1 + 7X) = 0, \tag{8}$$
$$B_4 \oplus (\Gamma_1 + 8X) = 5, \tag{9}$$
$$B_5 \oplus (\Gamma_1 + 9X) = 3, \tag{10}$$
$$((A_4 \oplus B_4) \oplus D) \oplus (\Gamma_1 + 10X) = 1, \tag{11}$$
$$(A_5 \oplus B_5) \oplus (\Gamma_1 + 11X) = 3. \tag{12}$$

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:

$$A_4 \equiv 4 - (\Gamma_1 + 3X), \tag{13}$$

$$A_5 \equiv 6 - (\Gamma_1 + 4X), \tag{14}$$

$$B_4 \equiv 5 - (\Gamma_1 + 8X), \tag{15}$$

$$B_5 \equiv 3 - (\Gamma_1 + 9X). \tag{16}$$

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

$$X \equiv (-2 - D), \tag{17}$$

$$\Gamma_1 \equiv 2D. \tag{18}$$

Подставив X из (17) и Γ_1 из (18) в (1), (2),(3), (13), (14), (6), (7), (8), (15), (16), найдем 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 (при $D = 0$),
2371640978 (при $D = 1$).

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

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 $f(0)$, $f(1)$, ..., $f(9)$ принимают все значения от 0 до 9. Найдем эти значения:

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

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

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

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

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

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

Отсюда, пользуясь свойствами остатков, замечаем, что b должно быть нечетным (иначе $f(x)$ будут только четные 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 приведенным условиям, гарантируется однозначность расшифрования.

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

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

Если среди чисел $S(1), S(2), \ldots, S(26)$ 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 учетом 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 найдем 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 найдем 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
	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
участок	Э	М	С	Н	Ж	Г	Б	К	Ы	Ф	С	С	И	З	Ч
и.с.2	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
	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
участок	Г	Ф	П	У	Щ	Э	Я	Ц	Д	М	П	П	Ч	Ш	И
и.с.1	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 идет 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 трех 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 приведенное 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 $HOK(2,3,5,7,13) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 = 2730$.

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 дает возможность 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 $((n+20)-20) = 20$. 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,

$$n(n^4-1) = n(n-1)(n+1)(n^2+1) = n(n-1)((n+2)(n-2)+5) =$$
$$= (n-2)(n-1)n(n+1)(n+2) + 5(n-1)n(n+1),$$

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

$$(n+20)^{n+20} - n^n = \left((n+20)^{n+20} - n^{n+20}\right) + (n^{n+20} - n^n)$$

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

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

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

легко убедиться, что она не имеет периода меньшей длины.

3.5. Для того, чтобы найти исходное сообщение, найдем сначала цифровое сообщение, полученное из него с помощью таблицы замены. Согласно этой таблице на нечетных местах цифрового образа исходного сообщения могут быть только цифры 0, 1, 2 и 3. Последовательно рассматривая эти значения для каждого нечетного места цифрового сообщения с использованием соответствующей цифры шифрованного сообщения, найдем 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: 16365674901476563690163656 74 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. 11.

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) $PMT = QNS$ ($MT = NS$, $PM = QN$, $\angle T = \angle S = 90°$).

7) Без ограничения общности $AB = BC = CA = 1$.

8) $PT = QS = x$, $AP = \dfrac{1}{4} \mp x$, $PQ = \dfrac{1}{2}$, $QC = \dfrac{1}{4} \pm x$.

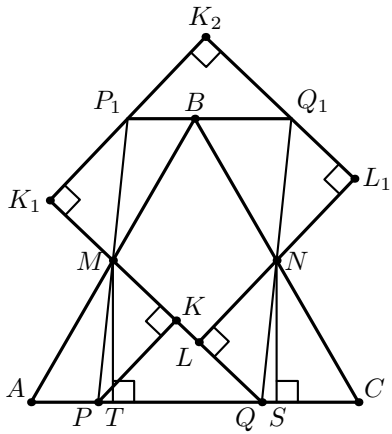


Рис. 11

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

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

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

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

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

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

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

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

15) $AP : PQ : QC = \dfrac{1}{4}\left(\sqrt{4\sqrt{3} - 3} - 1\right) : \dfrac{1}{2} : \dfrac{1}{4}\left(3 - (\sqrt{4\sqrt{3} - 3})\right) =$

$$= \left(\sqrt{4\sqrt{3} - 3} - 1\right) : 2 : \left(3 - \sqrt{4\sqrt{3} - 3}\right).$$

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

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 решетки полностью и еще три буквы вписаны в четвертом положении. Значит, незаполненные 12 клеток совпадают с вырезами решетки в четвертом 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 четвертом 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 решетки (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 нощно».

Получили текст:

12е24532 16о 28е2018 2021 5и 2717е11е16 —
не 275 до12312 2е16, не н5 17одо6о16:
денно и нощно 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 до12 31 22ей, не на водопой:
денно и нощно они е24е11ей
ищ1821 ве20е28ой 21о28пой.

7. 21=т 18=у 28=л 20=с из последней строки «ищут веселой толпой».
8. 11=р из «з в е 11 е й» первой строки.

Итак,

12е24а3т по лесу стаи зверей —
не за до12 31 22ей, не на водопой:
денно и нощно 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 нощно 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 остается 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 си́лент му́зэ —
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	ББЬЕ	БОПЙ	ДЁШЭ	МЛЫЦ	РЪЖК	ЧГТ	ХФНС	ЮУБЗ
ГЪЙ	ВЭЁ	ВПРК	ЕЖЩЮ	НМЬЧ	СЬЗЛ	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 группу 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	ГЕЧЬ	ЛКЪХ	ПЩЕЙ	Ц С	ФУМР	ЭТАЖ
ЩИ		БОПЙ	ДЁШ	МЛЫЦ	РЪ К	ЧГ	ХФНС	
ГЪЙ	В	ПРК	Е Щ	НМЬЧ	СЬ Л	ШДУ	ЦХО	
		ГРСЛ	Ё Ъ	ОН	ЬИМ	ЩЕФ	ЧЦПУ	
ЕЬЛ	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 $k=1,2,\ldots,(n-1)$, 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 $A_{100},\ldots,A_{106}$ 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*:

$$x = \frac{1+\sqrt{4a^2+1}}{2a} \text{ при } 0 < a < 1;$$

$$x_1 = \frac{1+\sqrt{4a^2+1}}{2a},\ x_2 = \frac{-\sqrt{4a^2-3}-1}{2a} \text{ при } a \geqslant 1.$$

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 $10, \ldots, 20$ 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 пробел в последней клетке, до перестановки стояли в конце таблицы. Таким образом, столбцы можно разбить на две группы, как показано на рис. 12. 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. 12

Естественно предположить, что сообщение оканчивалось 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. 13), из которых первый является явно «нечитаемым».

Р	А	Н
Ф	Ы	Л
Е	С	Р
Р	Е	У
М	П	Т
Т	Ч	К

З	А	Н
Б	Ы	Л
К	С	Р
Ы	Е	У
З	П	Т
Т	Ч	К

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

Рис. 13

З	А	Н	Я	Т	И	Е	К	Р
Б	Ы	Л	О	У	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. 14

Таким образом, удалось зафиксировать последние три столбца первой

группы. Переставляя столбцы второй группы, ищем «читаемые» продолжения зафиксированных столбцов (рис. 14). Действуя далее аналогичным 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 МывОт СьлКъгВц Аяя
укМапОч Ср Кщ Вэ Ах
ш МфэОгчСйъКфьВыеАкк

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 вычеркивая заведомо «нечитаемые» цепочки букв, получим:

СЕ, СМ, ИМ, ИГ
СЕГ, ~~сео~~, СМО, СМР, ИМО, ИМР, ИГР, ~~игт~~

~~сегр, сегт~~, 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:

задачасемьпояснитекаквынашлитекстзадачи

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 — нечетное, то число N должно быть четным.

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 $a \in \{1, \ldots, 1997\}$ не стоит на диагонали. Тогда, в силу симметрии таблицы, число a встречается четное количество раз. С другой стороны, так как число a по одному разу встречается в каждой строке, всего в таблице чисел a нечетное количество (1997). Получили противоречие.

Всего на диагонали 1997 клеток, поэтому каждое число из множества $\{1, \ldots, 1997\}$ встретится на диагонали ровно по одному разу. Вычисляя сумму арифметической прогрессии, находим ответ.

Ответ: 1995003.

6.3. *Ответ*: ШЕСТАЯОЛИМПИАДАПОКРИПТОГРАФИИПОСВЯЩЕНАСЕМИДЕСЯТИПЯТИЛЕТИЮСПЕЦИАЛЬНОЙСЛУЖБЫРОССИИ

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

6.4. а) Определим моменты остановок после начала шифрования. Для этого каждой букве русского алфавита припишем ее порядковый номер: А — 0, Б — 1, и т. д. Тогда буквам из шифруемого слова будут соответствовать 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 I колеса до соответствующей остановки.

№остановки	1	2	3	4	5	6	7	8	9
Буква I 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 II колеса	5	5	5	1	8	2	8	4	5
Цифра III колеса	1	2	5	2	5	3	6	3	4

Искомый шифртекст: 515355128523864354

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

a_k — цифра, на которую указывает стрелка II колеса в момент остановки с номером k,

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

Тогда, учитывая, что начальное положение стрелок соответствует букве А на первом колесе и 0 на II и III колесах, справедливы равенства

$$t_k = 10m_k - a_k, \quad k = 1, 2, \ldots \tag{1}$$

$$t_k = 7n_k + b_k, \quad k = 1, 2, \ldots \tag{2}$$

для подходящих неотрицательных целых чисел m_k и n_k.

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

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

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

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

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

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

Следовательно,

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

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

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

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

Подставляя m_k в (1), получим

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

Учитывая условие $0 < t_1 < t_2 < \cdots < t_7$ и то, что остановка колес происходит в момент первого появления шифруемой буквы под стрелкой I колеса, имеем

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 назовем 1-соседней, если b является соседней с a по часовой стрелке. Пару (a, c) назовем 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), $\ldots$, (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 $a_2, a_3, \ldots, a_8 \in \{2, \ldots, 9\}$ 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 трех пар приводит к неоднозначности восстановления цепочки $(*)$. В этом можно убедиться, рассмотрев следующие фрагменты цепочки вида $(*)$:

$(a, b)(b, c)(c, d)$ и $(a, c)(c, b)(b, d)$, (a, b, c, d — различные цифры),

$(a, b)\_(c, d)(d, e)$ и $(a, d)(d, b)\_(c, e)$, (a, b, c, d, e — различные цифры),

$(a, b)\_(c, d)\_(e, f)$ и $(a, d)(e, b)\_(c, f)$, (a, b, c, d, e, f — различные цифры).

Таким образом, при наличии двух указанных в условии задачи цифровых текстов нам будут известны некоторые 2-соседние пары, в которых первая цифра берется из первой криптограммы, а вторая — из второй. Поэтому с учетом вышесказанного 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 $a_1, a_2, \ldots$ на 24 — периодическая с периодом 2, так как для любого натурального n справедливо:

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

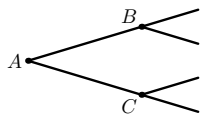
Кроме того, $p^3 - p = (p-1)p(p+1)$ кратно 24, то есть остатки у a_{n+2} и a_n равны.

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

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

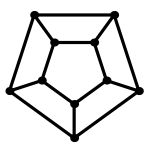
При $a > 0$ из графика функции в левой части уравнения видно, что если $1996 \in (0, a)$, число решений будет четным, поэтому не может быть равно 1997. Если $1996 \in (a, +\infty)$, то уравнение имеет ровно 2 решения. Если же $a = 1996$, то уравнение имеет ровно 1997 решений.

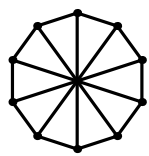
7.1. Для того, чтобы сохранилась связь при выходе из строя любых двух узлов, необходимо, чтобы в каждый узел входило не менее трех линий связи. Ситуация



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

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





Приведем 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 квадратной таблицей 10×10. На пересечении строки с номером i и столбца с номером j записываем цифру, в которую при зашифровании переходит цифра j, если она стоит в пароле после цифры i. Из однозначности расшифрования следует, что в каждой строке каждая цифра встречается ровно один раз.

Обозначим через $ш_1, ш_2, \ldots, ш_7$ и $о_1, о_2$ зашифрованные пароли и два известных пароля в порядке, определяемом условием задачи. Процедура зашифрования сохраняет длину, поэтому $ш_3$ и $ш_4$ не могут соответствовать ни $о_1$, ни $о_2$. Предположив, что $ш_1$ соответствует $о_1$, получим часть таблицы, в которой в одной строке две одинаковые цифры. Это означает, что предположение неверно. Составляя таблицы, убеждаемся, что $о_2$ не шифруется ни в $ш_6$, ни в $ш_7$, ни в $ш_5$. В результате таких рассуждений остается только один вариант перехода $о_1 - ш_2$, $о_2 - ш_5$. 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 $ш_3$: получится 5830829. Пароли, соответствующие $ш_1$, $ш_4$, $ш_6$, $ш_7$, 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 дает 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 трех вариантов начала текста легко определяется истинный вариант.

Ответ:

ЧТОБЫПОЛУЧИТЬПЯТЬНУЖНООТЛИЧНОЗНАТЬПОЛУЧИЛОСЬНЕПЛОХО

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 $(0 < c \leqslant 1/3)$ 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 трехчлена 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. 15).

Если на доске нарисовать некоторый (выпуклый) многоугольник, то найдутся такие граничные «точки» этого многоугольника, которые являются ближайшими к одному из краев доски. Площадь границы прямоугольника, содержащей все такие «точки», равна площади границы нарисованного выпуклого многоугольника (см. рис. 16).

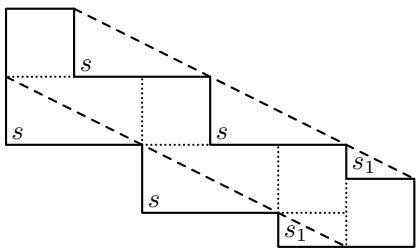


Рис. 15

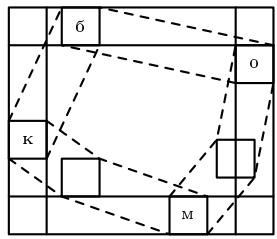


Рис. 16

Такой прямоугольник назовем окаймляющим. Ясно, что площадь окаймляющего прямоугольника не меньше площади соответствующего многоугольника. Значит, для любого многоугольника данной площади найдется 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 влечет $b = 100$. 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 $31 = 1! + 3! + 4!$, то $\{1, 3, 4, 5, 6, 7, 8, 0\} = G_1 \cup G_3 \cup G_4$.

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 прочитать: НАУКА.

8.1. Проведем прямые, проходящие через точки пересечения границ сложенной ленты параллельно ее краям. Очевидно, что тогда лента разобьется 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 17. 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: $l/h = 33\sqrt{3}$.

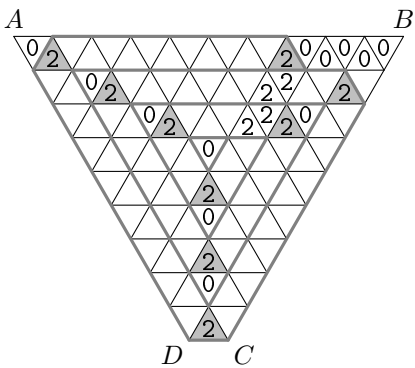


Рис. 17

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

$$\begin{cases} 0 \to 0^{k_1}1^{k_2} \\ 1 \to 0^{k_3} \end{cases} \text{ для I способа,} \qquad \begin{cases} 1 \to 1^{k_4}0^{k_5} \\ 0 \to 0^{k_6} \end{cases} \text{ для II способа.} \tag{1}$$

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

$$k_2 = k_4. \tag{2}$$

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 сообщении равно $nk_1 + nk_3$, а II способом — $nk_5 + nk_6$. Таким образом,

$$nk_1 + nk_3 = nk_5 + nk_6. \tag{3}$$

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:

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

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

При $a>1$ получаем условия:

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

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 $b\geqslant 0$ возможно лишь в случае $b=0$. Следовательно, $k_3=k_6$, а значит, с учетом (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.

Примечание. 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 учетом 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 еще 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 найдем 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 $|a-c| \in \{0, 1, \ldots, 12\}$ и $|b-d| \in \in \{0, 1, \ldots, 12\}$. 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

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

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

$$3^2 = (z+y)(z-y) \iff \begin{cases} z = 3 \\ y = 0 \end{cases} \text{ или } \begin{cases} z = 5 \\ y = 4 \end{cases}; \text{ и т. д.}$$

$$12^2 = (z+y)(z-y) \Longleftrightarrow \begin{cases} z = 12 \\ y = 0 \end{cases} \text{ или } \begin{cases} z = 15 \\ y = 9 \end{cases} \text{ или } \begin{cases} z = 20 \\ y = 16 \end{cases} \text{ или } \begin{cases} z = 37 \\ y = 35 \end{cases} \text{ или } \begin{cases} z = 13 \\ y = 5 \end{cases}.$$

В общем случае, если $x^2 = mn$, то

$$\begin{cases} z = \dfrac{m+n}{2} \\ y = \left|\dfrac{m-n}{2}\right| \end{cases}.$$

Ясно, что m и n должны быть одинаковой четности. По условию, $y \leqslant 12$, поэтому искомыми решениями будут только пары

$$(x;y) \in A = \{(3;4),(4;3),(6;8),(8;6),(9;12),(12;9),(5;12),(12;5)\} \cup \{(0;a),(a;0), a = 1,\ldots,12\}.$$

Клетку $(a;b)$ назовем существенной для клетки $(c;d)$, если выполнено условие $(|a-c|;|b-d|) \in A$. Ясно, что цвет данной клетки менялся лишь тогда, когда Криптоша находился в какой-либо существенной для нее клетке. А так как в каждой клетке Криптоша побывал ровно 1999 раз (нечетное число), то цвет данной клетки изменился, если общее число существенных для нее клеток нечетно.

Для определения четности 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 четность только для клеток $(a;b)$, где $a = 1,\ldots,5$, $b = a+1,\ldots,6$ (этих клеток 15, занумеруем их, как показано на рис. 18). Кроме того, отметим, что у каждой из клеток на диагоналях квадрата, а также у каждой из клеток центрального вертикального и горизонтального рядов обязательно будет четное число существенных для нее клеток.

Зоной асимметрии для той или иной клетки мы назовем 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 ее зоне асимметрии, четно.

На рис. 18 показана зона асимметрии для клетки 1, а также все клетки верхнего левого угла 6×6, меняющие свой цвет.

Ответ на рис. 19.

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.

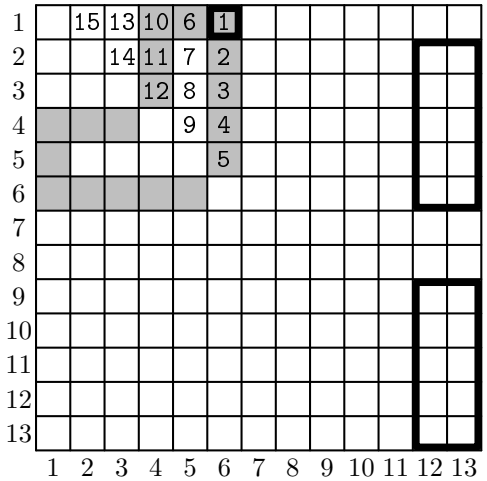


Рис. 18. Для клетки 1 жирными линиями выделена зона асимметрии. Серым цветом отмечены клетки верхнего левого угла 6×6, меняющие свой цвет.

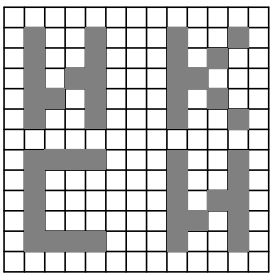


Рис. 19

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: a) $a = b$, b) $a = -b$, c) $a \neq \pm b$.

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) $a \neq \pm b$:

$$\frac{a}{1-bx} = \frac{b}{1-ax}, \qquad x \neq \frac{1}{a},\ x \neq \frac{1}{b},$$

$$\frac{1}{a} - \frac{b}{a}x = \frac{1}{b} - \frac{a}{b}x,$$

$$x\left(\frac{a}{b} - \frac{b}{a}\right) = \frac{1}{b} - \frac{1}{a},$$

$$x = \frac{(a-b)ab}{ab(a^2-b^2)} = \frac{1}{a+b}.$$

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.

При $\begin{cases} a \neq -b \\ a \neq 0 \\ b \neq 0 \\ a \neq +b \end{cases}$ $x = \frac{1}{a+b}$.

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:

$$\begin{aligned} 2^{30}+1 =& 2^{10\times 3}+1^3 = (2^{10}+1)(2^{20}-2^{10}+1) = 1025 \times (2^{20}-2^{10}+1) = \\ =& 41 \times 25 \times (2^{20}-2^{10}+1). \end{aligned}$$

$$\begin{aligned} 2^{30}+1 =& 2^{6\times 5}+1^5 = (2^6+1)(2^{24}-2^{18}+2^{12}-2^6+1) = \\ =& 65 \times (2^{24}-2^{18}+2^{12}-2^6+1) = \\ =& 13 \times 5 \times (2^{24}-2^{18}+2^{12}-2^6+1). \end{aligned}$$

$$\begin{aligned} 2^{30}+1 =& (2^{15}+1)^2 - 2 \times 2^{15} = (2^{15}+2^8+1)(2^{15}+1-2^8) = \\ =& 33025 \times 32513 = 25 \times 1321 \times 32513. \end{aligned}$$

Таким образом, установлено, что среди простых делителей числа $2^{30}+1$ содержатся 41, 13, 5. Непосредственной проверкой получаем равенство $32513 = 41 \times 793 = 41 \times 13 \times 61$.

Осталось проверить, что 1321 - простое число. Для этого достаточно показать, что 1321 не делится ни на одно простое число, меньшее 37 ($37^2 = 1369$, $1369 > 1321$).

Ответ: $2^{30}+1 = 5 \times 5 \times 13 \times 41 \times 61 \times 1321$.

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 возьмем 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 НОД$(2, 33) = 1$, разность $m-n$ также делилась бы на 33 без остатка, что невозможно. Утверждение пункта а) доказано.

Замечание. Утверждение пункта а) остается в силе для любого алфавита из нечетного 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 $1+2+\cdots+26=13\cdot 27=26\cdot 13+13$ при делении на 26 имеет остаток 13. Это доказывает утверждение пункта б).

Замечание. Утверждение пункта б) остается в силе для любого алфавита из четного числа букв.

Представляет интерес доказательство пункта б), предложенное участниками олимпиады.

При делении на любое четное число суммы двух четных или двух нечетных чисел получается четный остаток, а при делении суммы четного и нечетного чисел — нечетный остаток.

Соответствующие буквы складываемых последовательностей могут быть как одинаковой, так и различной четности. (Для краткости мы называем букву четной, если ее номер четен, и нечетной — если номер нечетен.) Будем решать задачу от противного. Предположим, что требуемая последовательность существует. Всего в сложении участвуют 52 буквы. Пар букв одинаковой и различной четности должно быть одинаковое количество, а именно 13 (так как в результате сложения должно получиться 13 четных и 13 нечетных букв). Пары букв различной четности включают в себя 26 букв. Оставшиеся 26 букв входят в 13 пар букв одинаковой четности. Однако, 13 пар букв одинаковой четности не могут содержать одинаковое количество четных и нечетных букв (так как 13 — нечетное 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:

$$12 + 1949^{1999} \cdot n \equiv 1. \tag{1}$$

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

$$17 \cdot n \equiv 22. \tag{2}$$

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
17	1	18	2	19	3	20	4	21	5	22	6	23	7	24	8	25	9	26	10	27	11

Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
28	12	29	13	30	14	31	15	32	16	0

Здесь под каждой буквой подписан остаток от деления на 33 результата умножения ее 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

$$\text{ЙЩНЧЛЖАФ}. \tag{3}$$

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

$$77 \cdot n \equiv 355. \tag{1}$$

Здесь n — пока неизвестное трехзначное число. Пусть $n = 100{\cdot}a{+}10{\cdot}b{+}c$ (a, b, c — цифры). Тогда

$$\begin{aligned}(100 \cdot a + 10 \cdot b + c) \cdot 77 \equiv 355 \iff \\ \iff 7000 \cdot a + 700 \cdot b + 70 \cdot c + 700 \cdot a + 70 \cdot b + 7 \cdot c \equiv 355 \iff \\ \iff 700 \cdot (a + b) + 70 \cdot (b + c) + 7 \cdot c \equiv 355.\end{aligned}$$

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 $13 \cdot 355 = 4615$, найдем $n = 615$. Теперь аналогично решаем уравнение (1), в правой части которого стоят другие трехзначные цифровые группы шифрсообщения (850, 547, 550 и т. д.).

Искомая цифровая последовательность имеет вид

$$12133225261022180115011105061 5.$$

Ответ: КЛЮЧШИФРАНАЙДЕН.

9.4. Сначала восстановим магический квадрат. Сумма чисел во всех клетках квадрата равна $1 + 2 + \ldots + 16 = \dfrac{16 \cdot 17}{2} = 136$, 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 четвертому 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

, ПЕРЕСТАВЬТЕБУКВЫ.

9.5. Пусть $\angle AOB = \alpha$, $\angle COD = \beta$, $\angle AOE = \gamma$, r радиус окружности (см. рис. 20). Условие (4) задачи эквивалентно равенству

$$S_{ABE} + S_{CED} = S_{AED}.$$

С учетом выражений $S_{AOB} + S_{AOE} - S_{BOE} = S_{ABE}$ и $S_{EOD} + S_{OCD} - S_{COE} = S_{ECD}$, это равенство можно записать в виде:

$$r^2(\sin\alpha + \sin\gamma) - r^2\sin(\alpha+\gamma) + r^2(\sin\beta + \sin\gamma) - r^2\sin(180^\circ - \gamma + \beta) =$$
$$= 2r^2\sin\gamma \iff \sin\alpha + \sin\beta = \sin(\alpha+\gamma) + \sin(\gamma-\beta) \iff$$
$$\iff (1-\cos\gamma)\cdot\sin\alpha + (1+\cos\gamma)\cdot\sin\beta = \sin\gamma\cdot(\cos\alpha + \cos\beta). \quad (1)$$

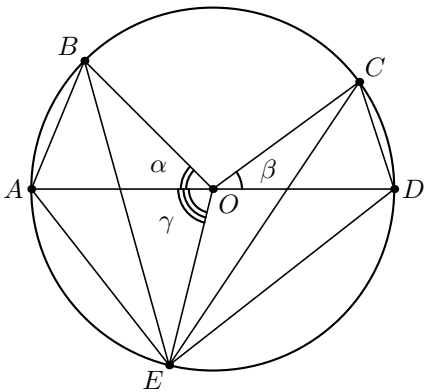


Рис. 20

Без ограничения общности можно считать, что $\gamma \leqslant 90^\circ$. 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 дает 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 $\sin\alpha + 4\cdot\sin\beta \geqslant \frac{3}{5} + 4\cdot\frac{3}{5}$ и $2\cdot\cos\alpha + 2\cdot\cos\beta \leqslant 2\cdot\frac{4}{5}$.

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:

$$\sqrt{-\left(x+\frac{1}{2}\right)^2+a^2}\geqslant 1+\sqrt{-\left(x-\frac{1}{2}\right)^2+4}.$$

В результате замены $x+\frac{1}{2}=t$ неравенство примет вид:

$$\sqrt{a^2-t^2}\geqslant 1+\sqrt{4-(t-1)^2}.$$

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. 21). С ростом $|a|$ у

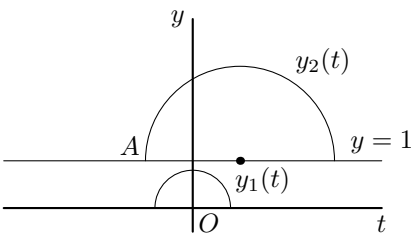


Рис. 21

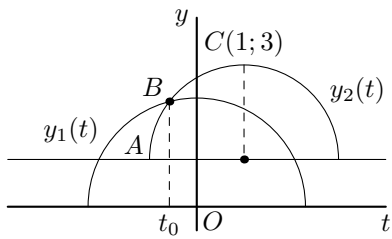


Рис. 22

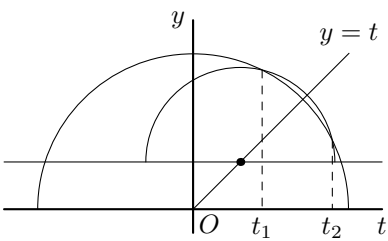


Рис. 23

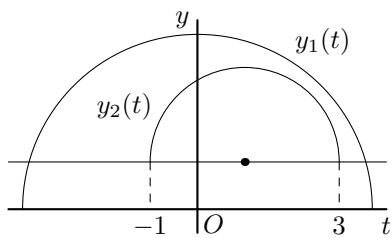


Рис. 24

полуокружностей появляется общая точка B (с абсциссой t_0) (рис. 22). 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. 23). И, наконец, при $|a|$, превосходящем некоторое значение, полуокружности вновь не пересекаются (рис. 24). Рассмотрим указанные случаи подробно.

Случай 1. При $|a| < OA = \sqrt{2}$ полуокружности не пересекаются, и неравенство решений не имеет (рис. 21).

Случай 2. Полуокружности имеют единственную точку пересечения с абсциссой $t_0 < 1$ (рис. 22). При этом $\sqrt{2} \leqslant |a| < OC = \sqrt{10}$. Решение неравенства имеет вид $t \in [-1; t_0]$.

Случай 3. Полуокружности имеют две точки пересечения (рис. 23). При этом $\sqrt{10} \leqslant |a| \leqslant 2 + \sqrt{2}$. Решение неравенства имеет вид $t \in \in [-1; t_1] \cup [t_2; 3]$. 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 $t \in [-1; 3]$.

Найдем теперь точные выражения для абсцисс t_1, t_2 точек пересечения окружностей. Эти величины удовлетворяют системе

$$\begin{cases} t^2 + y^2 = a^2 \\ (t-1)^2 + (y-1)^2 = 4 \end{cases} \iff \begin{cases} t^2 + y^2 = a^2 \\ t + y = \dfrac{a^2-2}{2} \end{cases} \Longrightarrow t^2 + \left(\frac{a^2-2}{2} - t\right)^2 = a^2.$$

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. $|a| < \sqrt{2} \Longrightarrow$ решений нет.
2. $\sqrt{2} \leqslant |a| < \sqrt{10} \Longrightarrow t \in [-1; t_1]$.
3. $\sqrt{10} \leqslant |a| \leqslant 2 + \sqrt{2} \Longrightarrow t \in [-1; t_1] \cup [t_2; 3]$.
4. $|a| > 2 + \sqrt{2} \Longrightarrow t \in [-1; 3]$.

Переходя к переменной x и используя явные выражения для t_1, t_2, получаем окончательный

Ответ:

1. $|a| < \sqrt{2} \Longrightarrow$ решений нет.
2. $\sqrt{2} \leqslant |a| < \sqrt{10} \Longrightarrow x \in [-\frac{3}{2}; \frac{a^2 - 2 - \sqrt{12 \cdot a^2 - a^4 - 4}}{4}]$.
3. $\sqrt{10} \leqslant |a| \leqslant 2 + \sqrt{2} \Longrightarrow$
$x \in [-\frac{3}{2}; \frac{a^2 - 2 - \sqrt{12 \cdot a^2 - a^4 - 4}}{4}] \cup [\frac{a^2 - 2 + \sqrt{12 \cdot a^2 - a^4 - 4}}{4}; \frac{5}{2}]$.
4. $|a| > 2 + \sqrt{2} \Longrightarrow x \in \left[-\frac{3}{2}; \frac{5}{2}\right]$.

10.1. Ход решения, а вернее та последовательность, в которой большинство участников определяло цвета клеток, изображен на рис. 25. Проанализировав по строкам длины черных полос, мы без труда определяем цвета некоторых клеток в первом, втором и 15-м рядах. Эти «сразу очевидные» клетки отмечены цифрой 1, причем если цифра обведена в кружок, то цвет клетки белый, если же в клетке стоит просто цифра, то это черная клетка. Анализируя затем длины полос по столбцам, отмечаем, что цвета клеток, помеченных цифрой 2, теперь однозначно определены. Вновь просматривая строки, определяем цвета очередной группы клеток и отмечаем их цифрой 3 и т. д.

									2				2						
									1		2		1						
								2	1	2	2	2	1	2					
							2	1	1	1	2	1	1	1	2				
						5	9	2	2	1	2	1	2	1	2	2	9	5	
					1	1	2	2	2	2	3	1	3	2	2	2	2	1	1
				9	②	⑤	⑫	12	4	3	1	1	1	3	4	12	⑫	⑤	②
				11	②	⑩	11	3	1	1	1	1	1	1	1	3	11	⑩	②
			1	1	②	⑪	10	⑪	④	④	②	②	②	④	④	⑪	10	⑪	②
	2	3	3	2	②	3	2	③	3	3	3	③	3	3	3	③	2	3	②
			2	2	②	4	2	⑤	④	④	④	⑤	④	④	④	⑤	2	4	②
2	1	1	1	2	②	6	2	⑦	⑧	8	⑦	6	⑦	8	⑧	⑦	2	6	②
		2	1	2	②	9	2	⑧	⑦	⑦	⑦	6	⑦	⑦	⑦	⑧	2	9	②
			2	2	②	9	2	⑧	⑤	⑤	⑤	⑤	⑤	⑤	⑤	⑧	2	9	②
		1	5	1	②	③	2	③	⑨	8	3	3	3	8	⑨	③	2	③	②
		2	3	2	②	④	10	7	⑩	⑦	6	6	6	⑦	⑩	7	10	④	②
			2	2	②	④	⑪	8	10	⑨	④	④	④	⑨	10	8	⑪	④	②
				7	②	④	⑨	⑧	9	9	4	3	4	9	9	⑧	⑨	④	②
			1	1	②	④	②	②	②	②	4	④	4	②	②	②	②	④	②
			6	6	②	3	2	2	2	2	3	②	3	2	2	2	2	3	②
1	4	1	4	1	1	①	1	1	1	1	①	1	①	1	1	1	1	①	1

Рис. 25

Ответ: см. рис. 26.

10.2. Наша цель — найти все наборы из шести чисел (x, y, z, u, v, w), удовлетворяющих уравнению. Поскольку каждое число в наборе может принимать ровно два значения, всего таких наборов $2^6 = 64$. Следова-

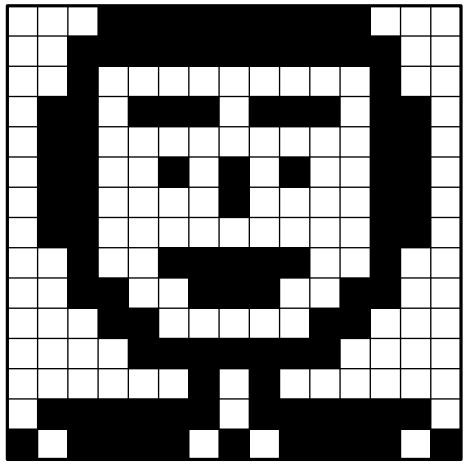


Рис. 26

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 трех 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
0	−1	1	2
0	−1	2	2
0	2	1	−2
0	2	2	−1
1	2	1	2
1	−1	2	2
1	2	1	1
1	2	2	2

u	v	w	правая часть
0	0	0	0
0	0	1	3
0	3	0	3
0	3	1	3
−1	0	0	1
−1	0	1	1
−1	3	0	−1
−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 в n-й строке и m-м столбце, будем записывать так: $\mathtt{G} = (n, m)$. Решение задачи представим в виде несложных вытекающих друг из друга утверждений.

1. $\mathtt{T} = (4, 4)$. Если бы было $\mathtt{T} = (5, 5)$, то ключевое слово состояло бы из шести последних букв алфавита и буква H не попадала бы на главную диагональ.

2. Используя симметрию, находим $\mathtt{N} = (1, 5)$, $\mathtt{D} = (2, 5)$.

3. $\mathtt{A} = (2, 2)$. Это следует из того, что $\mathtt{D} = (2, 5)$.

4. R входит в ключевое слово. Если это не так, то или $\mathtt{R} = (4, 2)$, или $\mathtt{R} = (4, 3)$. 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 $\mathtt{D} = (2, 5)$) 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 учетом 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 приведенных 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:

$$1, 3, 6, 0, 5, 1, 8, 6, 5, 5, 6, 8, 1, 5, 0, 6, 3, 1, 0, 0, 1, 3, 6, 0, 5, \ldots$$

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 $x = u + v$. Возведем 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 учетом 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

$$\begin{cases} uv = -1, \\ u^5 + v^5 = 1. \end{cases}$$

Возведем 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 $a = \dfrac{-1+\sqrt{5}}{2}$, $b = \dfrac{-1-\sqrt{5}}{2}$.

Ответ: $x = \sqrt[5]{\dfrac{-1+\sqrt{5}}{2}} + \sqrt[5]{\dfrac{-1-\sqrt{5}}{2}}$.

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 $L \geqslant 100x/11$ заключаем, что $L > 19$ при $x \geqslant 3$.

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, Ь — 4 раза; Ж, Э — 6 раз; Р — 7 раз; В — 12 раз. Если текст получен перестановкой букв, то частоты встречаемости букв в нем 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 ее 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 Ь либо на Ь 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 войдет 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: СОЛОВЕЙИРОЗАП???ИН. 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 представляются 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.

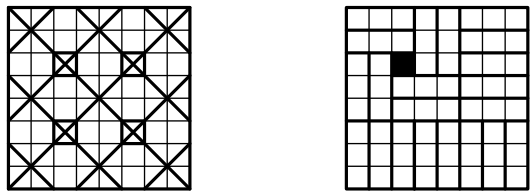
11.4. Раскрасим клетки таблицы в три цвета (назовем их условно 1, 2 и 3), как показано на рис. 27. Клетки, образующие линию, параллельную

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. 27

главной диагонали, окрашены в один цвет. Заметим, что прямоугольник 1×3 всегда накрывает клетки трех 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 ее центра «хорошие» клетки переходят в «хорошие». Линии клеток цвета 1 до и после поворота указаны на рис. 28, а.

Ясно, что «хорошими» могут быть только те (четыре) клетки, в которых эти линии пересекаются. Непосредственной проверкой (рис. 28, б) убеждаемся, что найденные клетки «хорошими» являются. Таким обра-



а) б)

Рис. 28

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 счету буква зашифрованного сообщения — д. Находим остаток от деления ее 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. 29

Ответ. а) «Хорошие» клетки указаны символом ■ на рис. 29.

б) Ключевое слово — РУСЬ. Исходное сообщение: Истина не рождается из истины. Истина рождается из ошибок. Капица

11.5. Покажем вначале, что каждый прямоугольник в своем углу может быть развернут на 90°. Рассмотрим, например, левый верхний прямоугольник (рис. 30). Как бы при этом ни располагались в углах другие

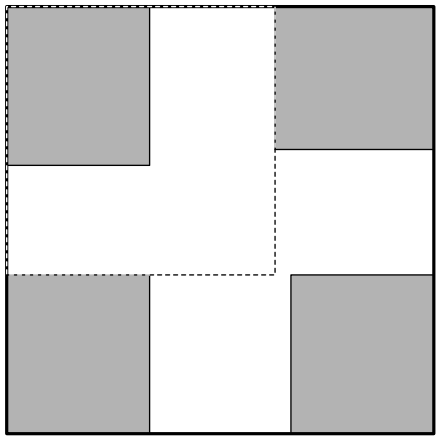


Рис. 30

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. 31). 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

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

формулу разности квадратов, преобразуем его к виду

$$\left(\left|y + x - \frac{5+\sqrt{3}}{2}\right| + |x-1|\right)^2 + \left(\left|2x - \sqrt{2y} - 2\right| + |y-1|\right)^2 = 1.$$

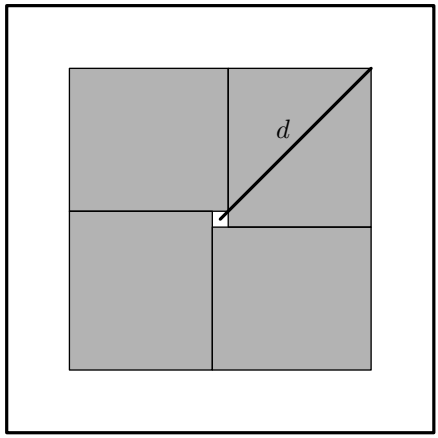


Рис. 31

Последнее уравнение системы $(x-1)^2+(y-1)^2=1$ для наглядности запишем как

$$(0+|x-1|)^2+(0+|y-1|)^2=1.$$

Следовательно, для совместности системы необходимо потребовать, чтобы выполнялись условия

$$2x-\sqrt{2y}-2=0, \qquad y+x-\frac{5+\sqrt{3}}{2}=0.$$

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 $7\cdot 7\cdot\ldots\cdot 7=7^{50}$ различных вариантов выбора ключа шифра. Аналогично у второго криптографа всего 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,

$$7^{50} = 7^{7 \cdot 7 + 1} < \left(10^6\right)^7 \cdot 10 = 10^{43};$$

в) некоторые школьники использовали оценку $\frac{10}{7} = 1{,}42\ldots > 1{,}4$.

Основные недостатки в работах:

— часто сравнивали числа 350 и 430;

— использовали приближенные 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 четвертый 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. Приведем 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**) еще 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 счету букве А в слове АСТРАХАНЬ) на 9 либо нет переноса, тогда $9 \cdot x = \ldots 9$, либо есть перенос единицы, тогда $9 \cdot x + 1 = \ldots 9$. 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 черным кружком (хотя начинать читать можно с любого места). Листок с текстом следует развернуть так, чтобы буква Т приняла свое «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. 32.

Ответ: ТЕКСТ ЧИТАЕТСЯ ВДОЛЬ ПО КРИВОЙ ПРИДУМАННОЙ ИТАЛЬЯНСКИМ МАТЕМАТИКОМ ПЕАНО.

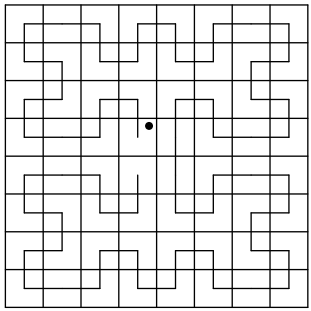


Рис. 32

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) привел 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. 33). Поставим ей в соответствие точку квадрата. Разобьем отрезок и квадрат пополам (линия 1). Точка A оказалась в правой части

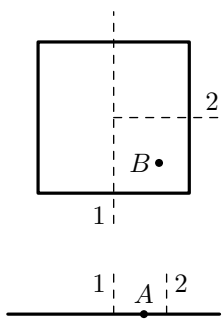


Рис. 33

отрезка, и поэтому берем правую часть квадрата. Половину отрезка, содержащую A, и правую часть квадрата делим пополам (линия 2). Точка A оказалась слева от точки деления, поэтому берем 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, приведенной на рис. 32.

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.

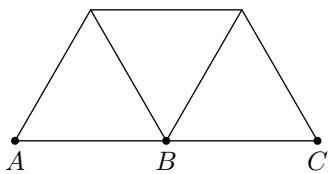


Рис. 34

Пересекая окружность радиуса AB с центром в точке A окружностью радиуса $2AB$ с центром в точке C, находим точку D. Находим

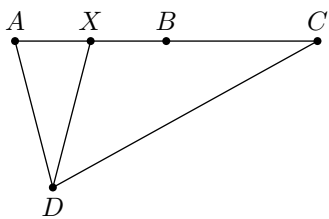


Рис. 35

пересечение окружности радиуса AB с центром в точке D с отрезком AB. Это искомая точка, так как треугольник ADX подобен треугольнику ACD с коэффициентом подобия 2.

12.7. а) Большинство участников с этой задачей справились. Для ее решения надо рассмотреть последовательность степеней двойки и обнаружить закономерность: $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = \ldots 6$, $2^5 = \ldots 2$ и т. д.

Последние цифры 2, 4, 8, 6 периодически повторяются. Таким образом, $2^{2002} = (2^{500})^4 \cdot 2^2 = (\ldots 6)^4 \cdot 4 = \ldots 6 \cdot 4 = \ldots 4$. 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 $2^{103} = \ldots 008$, а перед этим было число $2^{102} = \ldots 504$. Значит, последовательность остатков $008, \ldots, 504$ длины 100 повторяется, начиная с 2^3. Таким образом, на число 2002 приходится остаток 504.

Второе решение. Легко получить следующие соотношения:

$$\begin{aligned} 2^{10} &= 1024, \\ 2^{20} &= \ldots 24 \cdot \ldots 24 = \ldots 576, \\ 2^{40} &= \ldots 576 \cdot \ldots 576 = \ldots 776, \\ 2^{80} &= \ldots 776 \cdot \ldots 776 = \ldots 176, \\ 2^{160} &= \ldots 176 \cdot \ldots 176 = \ldots 976, \\ 2^{320} &= \ldots 976 \cdot \ldots 976 = \ldots 576. \end{aligned}$$

Выписав 4 произведения трехзначных чисел, дальше сразу получаем

$$\begin{aligned} 2^{640} &= \ldots 776, \\ 2^{1280} &= \ldots 176. \end{aligned}$$

Отсюда $2^{2002} = 4 \cdot 2^{1280} \cdot 2^{640} \cdot 2^{80} = 4 \cdot \ldots 176 \cdot \ldots 176 \cdot \ldots 776 = 4 \cdot \ldots 976 \cdot \ldots 776 = \ldots 504$.

В последней строке пользуемся тем, что $176^2 = \ldots 976$.

Третье решение. Несложно вычислить следующее:

$$\begin{aligned} 2^{10} &= \ldots 024, \\ 2^{100} &= \big((\ldots 24)^3\big)^3 \cdot \ldots 24 = \ldots 376, \\ 376 \cdot 376 &= \ldots 376, \\ 2^{2002} &= 2^2 \cdot (2^{100})^{20} = 4 \cdot \ldots 376 = \ldots 504. \end{aligned}$$

Общий подход. Имеет место соотношение $2^{2^k} \cdot 2^{2^k} = 2^{2^{k+1}}$. Следовательно, путем нескольких умножений трехзначных чисел можно получить

$$2^{2^0} = 2, \quad 2^{2^1} = 4, \quad 2^{2^2} = 16, \quad 2^{2^3} = 256, \quad 2^{2^4} = \ldots 536, \quad 2^{2^5} = \ldots 296,$$

$$2^{2^6} = \ldots 616, \quad 2^{2^7} = \ldots 456, \quad 2^{2^8} = \ldots 936, \quad 2^{2^9} = \ldots 096, \quad 2^{2^{10}} = \ldots 216$$

Раскладывая 2002 по степеням двойки:

$$2002 = 1024 + 512 + 256 + 120 + 64 + 16 + 2,$$

получим

$$2^{2002} = \ldots 216 \cdot \ldots 096 \cdot \ldots 936 \cdot \ldots 456 \cdot \ldots 616 \cdot \ldots 536 \cdot \ldots 4.$$

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 пошлет к C сообщение $E_C(B, m)$. Значит, такое сообщение попадет 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 пятерку 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 пятеркой в одну строку из десяти цифр. Например, для второй пятерки получается строка 1222445344. В получившейся строке каждая последовательная пара цифр и будет новыми номерами букв пятерки, которые выпишем под соответствующими буквами. Так, для букв второй пятерки получаем новые номера:

E	I	G	H	T
1	2	4	5	4
2	2	4	3	4
O	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 шифрованный текст. Например, пятерка EIGHT будет зашифрована в пятерку 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 наберем 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 $7 \cdot 9 = 63$. Еще 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 надежнее — 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 трем 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 определенном смысле операции *сдвига букв в столбцах* и *отражения столбца относительно средней линии* перестановочны. (Действительно, сдвинуть столбец на одну позицию вверх и затем отразить — это все равно что столбец сначала отразить, а затем сдвинуть вверх на девять позиций.) Поэтому можно считать, что сначала Криптоша 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 щихся, 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: $2^0 = 1$, $2^1 = 10$, $2^2 = 100$, ..., $2^8 = 100000000$. 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 111111111 (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 $a = (1, 0, 1, 0, 0, 0, 0, 0)$. 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

$$\begin{aligned}
x_{11} &= 13,\\
x_{12} &= 19,\\
x_{13} &= 28,\\
x_{14} &= 10,\\
x_{15} &= 29,\\
x_{16} &= 26,\\
x_{17} &= 5,\\
x_{18} &= 3,\\
x_{19} &= 29,\\
x_{20} &= 3,\\
x_{21} &= 6,\\
x_{22} &= 6a + 3b + 4c,\\
x_{23} &= 7a + 4b + 13c,\\
x_{25} &= 13a + 7b + 17c,\\
x_{26} &= 17a + 13b + 24c.
\end{aligned}$$

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}:

$$\begin{aligned}
x_{27} &= 6,\\
x_{28} &= 23,\\
x_{29} &= 16,\\
x_{30} &= 22,\\
x_{31} &= 14,
\end{aligned}$$

$$
\begin{aligned}
x_{32} &= 30,\\
x_{33} &= 21,\\
x_{34} &= 4,\\
x_{35} &= 3,\\
x_{36} &= 24,\\
x_{37} &= 28,\\
x_{38} &= 0,\\
x_{39} &= 24,\\
x_{40} &= 21,\\
x_{41} &= 21,\\
x_{42} &= 14,\\
x_{43} &= 4,\\
x_{44} &= 25,\\
x_{45} &= 8,\\
x_{46} &= 8a + 25b + 12c,\\
x_{47} &= 12a + 8b + 6c,\\
x_{48} &= 6a + 12b + 14c,\\
x_{49} &= 14a + 6b + 26c,\\
x_{50} &= 26a + 14b + 1c.
\end{aligned}
$$

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 О_i, Ш_i числа, соответствующие i-м буквам стихотворения и полученного шифрованного текста. Тогда числа $\text{О}_{22} + x_{22}$ и Ш_{22} имеют одинаковые остатки от деления на 31. То же самое и с числами $\text{О}_{46} + x_{46}$ и Ш_{46}.

А так как числа О_{22} и О_{46} одинаковые, рассмотрев разности соответствующих частей, получим, что

$$x_{46} - x_{22} \quad \text{и} \quad \text{Ш}_{46} - \text{Ш}_{22} \qquad (*)$$

дают одинаковые остатки от деления на 31.

Последним пяти буквам первой строки шифрованного текста соответствуют следующие числа Ш_i:

Б, Ш, Ь, Е, Ю — 1, 23, 27, 5, 29,

а последним буквам второй строки — следующие:

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, четвертое и пятое, третье и четвертое уравнения, получим

$$\begin{cases} 7a + 10b = 5, \\ 10a + 17c = 9, \\ 7b + 10c = 5. \end{cases} \qquad (**)$$

Выразим b и c через a и подставим в первое уравнение:

$$b = \frac{5 - 7a}{10}, \quad c = \frac{9 - 10a}{17},$$

$$2a - 9\frac{5 - 7a}{10} + 8\left(\frac{9 - 10a}{17}\right) = 1,$$

$$340a - 9 \cdot 17(5 - 7a) + 80(9 - 10a) = 170,$$

$$611a = 215,$$

$$22a = 29.$$

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

$$b = 0,$$

$$c = 16.$$

Зная a, b, c, можно последовательно найти все x_i и из соотношения $\text{О}_i = \text{Ш}_i - x_i$ получить стихотворение:

ВЕЧОРТЫПОМНИШЬВЬЮГАЗЛИЛАСЬ

НАМУТНОМНЕБЕМГЛАНОСИЛАСЬ

14.1. *Ответ*: см. рис. 36.

14.2. Пусть MN — число различных комбинаций, при установке которых раздается N ($N \leqslant 57$) щелчков.

Заметим, что из соображений симметрии $M_N = M_{57-N}$. Для обоснования этого равенства достаточно установить взаимно однозначное

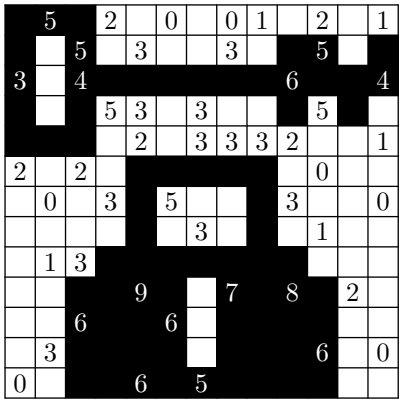


Рис. 36

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 раздается 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 нулем, 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 четвертой 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 еще одного щелчка может быть преобразована в комбинацию второго столбца, то соединим

их стрелкой. Проведем 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 нулем 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 нулем, и $6 + 24 + 39 + 3X$ — без нуля.

С другой стороны, к каждой комбинации, получаемой за 25 щелчков и не содержащей 0, ведет 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) назовем «флагом». Условия задачи можно сформулировать в следующем виде:

1) для каждой точки p имеется ровно t флагов вида

$$(L_1, p), (L_2, p), \ldots, (L_t, p);$$

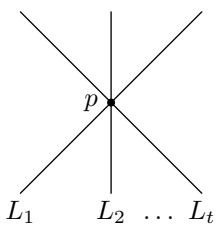
2) для каждой линии L имеется ровно s флагов вида

$$(L, p_1), (L, p_2), \ldots, (L, p_s);$$

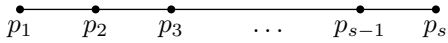
3) если точка x не инцидентна линии L, то имеются ровно одна такая линия M и одна такая точка y, что (L, y), (M, x) и (M, y) — флаги.

Изобразим условия 1–3 графически:

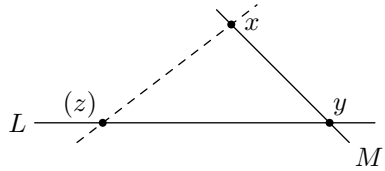
1) («пучок линий с центром в точке p»)



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 учетом 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 трехчлена 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 ее 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	...

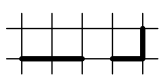
После слова ПРОПУСК идет нечитаемый текст. Значит, или непосредственно после этого слова, или после буквы В пропущены буквы. (Перебор различных вариантов тривиален и поэтому здесь не приводится.) Сдвигая нашу периодическую последовательность относительно зашифрованного текста, находим такой вариант:

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

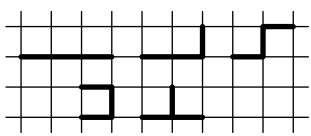
Естественно предположить, что на месте пропущенного знака в исходном тексте находилась буква З. Действуя далее аналогично, восстанавливаем весь текст.

Ответ: ПРОПУСК ЗНАКА В ТЕКСТЕ.

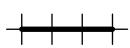
14.6. Сначала выясним, какие вообще могут быть шаблоны. Очевидно, что при $k = 2$ имеется 2 вида шаблонов:



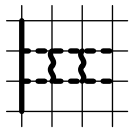
При $k = 3$ имеется 5 видов шаблонов:



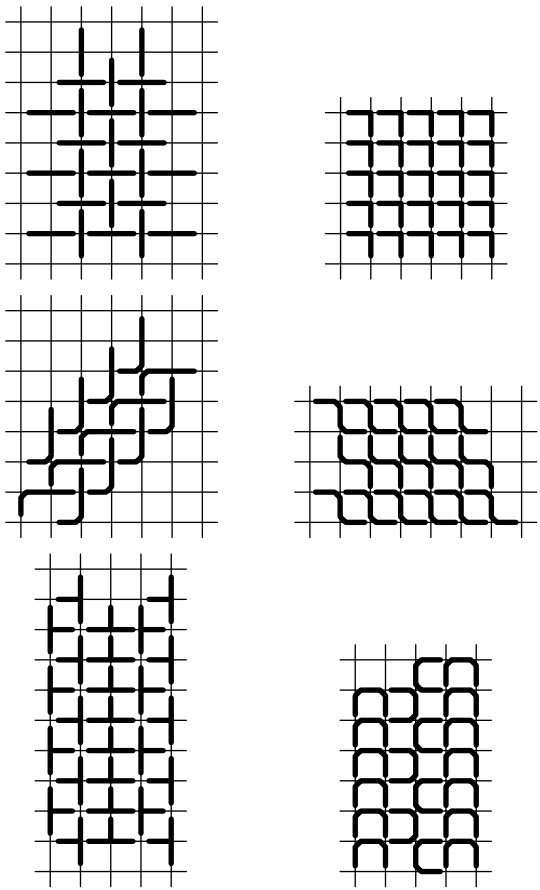
Оказывается, все линии клетчатой бумаги можно покрыть любым из перечисленных выше шаблонов, кроме шаблона вида



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 $0\ldots0$ натуральным не является. Число $5\ldots5$ не может быть квадратом, так как оно делится на 5, но не делится на 25. Аналогично $6\ldots6 \neq n^2$, так как это число делится на 2, но не делится на 4. Числа $4\ldots4$ и $9\ldots9$ являются полными квадратами в том и только том случае, когда полным квадратом будет $1\ldots1$.

Докажем, что $1\ldots1 \neq n^2$. Предположим, что это не так: существует такое натуральное число n, что $1\ldots1 = n^2$. Тогда $n = 10k \pm 1$ и, следовательно, $100k^2 \pm 20k = 1\ldots10 \Leftrightarrow 10k^2 \pm 2k = 1\ldots1$. Получили противоречие: нечетное число равно четному.

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 приведенных 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, причем 3-я и 7-я совпадают. Найдем 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
```

Четвертый:

```
                          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 еще дальше — отсеяли еще по одному варианту исходя из соображений 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. Приведенный в задаче протокол работы брелка и замка был изобретен 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).

Перейдем 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 счетчик 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 остается открытым, т. е. СЗ $= m$.

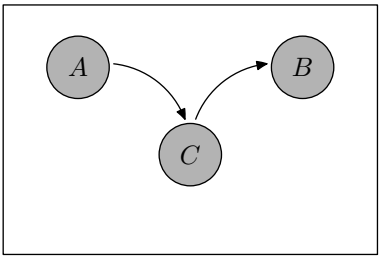
3. Выполнив действия пункта 2, злоумышленник немедленно посылает замку ранее запомненный сигнал k. Замок закрывается, и при этом СЗ $= k+1$. Владелец уходит, полагая, что машину запер он сам.

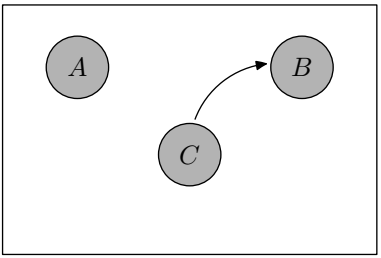
4. Злоумышленник посылает замку ранее запомненный сигнал $k+1$, и замок открывается.

К сожалению, многие участники решали задачу исходя из слишком упрощенной 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 уйдет.

15.5. Предварим решение этой задачи небольшим отступлением о кодах аутентификации, поясняющим происхождение ее формулировки.

При передаче информации по незащищенному (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) трех конечных множеств, где S — множество *состояний источника*, E — множество *правил кодирования*, M — множество *сообщений*. Каждый элемент $e \in E$ представляет собой отображение $e\colon S \to M$. 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 $f_e\colon M \to S \cup \{0\}$, 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 к 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 надежности защиты от активных атак с помощью A-кодов предполагается, что злоумышленник знает об A-коде все, 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. Приведем 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):

$$\begin{array}{c} \\ e_1 \\ e_2 \\ e_3 \end{array} \begin{array}{c} \begin{array}{ccc} m_1 & m_2 & m_3 \end{array} \\ \begin{pmatrix} H & T & 0 \\ T & 0 & H \\ 0 & T & H \end{pmatrix} \end{array}$$

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 трех 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 расчетом, 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 $\min\limits_{\bar{x}\in\Delta} L(\bar{x})$, где

$$\Delta = \{(x_1, x_2, x_3)\colon 0 < x_i < 1,\ x_1 + x_2 + x_3 = 1\}.$$

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

$$\begin{cases} x_1 p \geqslant x_2(1-p), \\ x_1 \leqslant x_2, \\ x_2 \geqslant x_3, \end{cases}$$

$L(\bar{x})$ 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 $p \geqslant 1/2$. В самом деле,

$$x_1 p \geqslant x_2(1-p) \geqslant x_1(1-p),$$

откуда $p \geqslant 1-p$ или $2p \geqslant 1$.

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. Остается найти достижимую верхнюю границу для значения x_3.

Из цепочки неравенств $x_3 \leqslant x_2 \leqslant \dfrac{p}{1-p} x_1$ получаем

$$1 = x_1 + x_2 + x_3 \geqslant \frac{1-p}{p} x_3 + x_3 + x_3,$$

откуда следует, что $x_3 \leqslant \dfrac{p}{p+1}$. Ясно, что равенство $x_3 = \dfrac{p}{p+1}$ достигается лишь в случае, когда в указанной цепочке неравенств выполняются равенства, т. е. если $x_3 = x_2 = \dfrac{p}{1-p} x_1$. Мы нашли максимальное значение x_3. Отсюда получаем, что

$$\min L(\bar{x}) = \left(\frac{1-p}{p+1} + \frac{p}{p+1}\right) p + \frac{p}{p+1}(1-p) = \frac{p(2-p)}{p+1}.$$

Рекомендуемая литература

У. Болл, Г. Кокстер. Математические эссе и развлечения. М.: Мир, 1986.

Ж. Верн. Жангада. М.: Детская литература, 1967. (Библиотечка приключений; Т. 9).

Введение в криптографию / Под ред. В. В. Ященко. М.: МЦНМО: ЧеРо, 2000.

Ж. Верн. Путешествие к центру Земли // Собрание сочинений в 12 т., т. 2. М.: Художественная литература, 1995. С. 7–225.

М. Гарднер. От мозаик Пенроуза к надежным шифрам. М.: Мир, 1993.

Г. А. Гуревич. Криптограмма Жюля Верна // Квант. 1985. № 9. С. 30–35.

С. А. Дорученко, В. В. Ященко. 25 этюдов о шифрах. М.: ТЭИС, 1994.

В. Жельников. Криптография от папируса до компьютера. М.: ABF, 1996.

В. Каверин. Исполнение желаний // Собрание сочинений в 6 т., т. 2. М.: Художественная литература, 1964. С. 211–552.

А. Конан Дойл. Пляшущие человечки // Записки о Шерлоке Холмсе. М.: Правда, 1983. С. 249–275.

Основы криптографии. Учебное пособие / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. М.: Гелиос АРВ, 2005.

Э. По. Золотой жук // Стихотворения. Проза. М.: Художественная литература, 1976. С. 433–462

А. Саломаа. Криптография с открытым ключом. М.: Мир, 1995.

Т. А. Соболева. Тайнопись в истории России (История криптографической службы России XVIII – начала XX в.). М.: Международные отношения, 1994.

Т. А. Соболева. История шифровального дела в России. М.: ОЛМА-ПРЕСС Образование, 2002.

Ч. Уэзерелл. Этюды для программистов. М.: Мир, 1982.

Г. Фролов. Тайны тайнописи. М., 1992.

Содержание

Анатолий Юрьевич Зубов
Андрей Валентинович Зязин
Валентин Николаевич Овчинников
Сергей Михайлович Рамоданов

ОЛИМПИАДЫ ПО КРИПТОГРАФИИ
И МАТЕМАТИКЕ ДЛЯ ШКОЛЬНИКОВ

Подписано в печать 02.10.2006 г. Формат $60 \times 90\ {}^{1}/_{16}$. Бумага офсетная.
Печать офсетная. Печ. л. 8,5. Тираж 3000 экз. Заказ № .

Издательство Московского центра
непрерывного математического образования
119002, Москва, Большой Власьевский пер., 11. Тел. 241-74-83.

Отпечатано с готовых диапозитивов в ФГУП «Полиграфические ресурсы».