

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический
университет имени К. И. Сатпаева

О. Н. Жданов, К. К. Елемесов

**НАЧАЛА КРИПТОГРАФИИ В ЗАДАЧАХ И
УПРАЖНЕНИЯХ**

Рекомендовано Научно-методическим советом университета
в качестве учебного пособия

Алматы 2016

УДК 003. 26
ББК 81
Ж 42

Рецензенты:

Ахметов Б. С., д-р. техн. наук, проф. КазННТУ им. К. И. Сатпаева
Мукумбеков М. Ш., д-р. техн. наук, проф. КазНУ им. Аль-Фараби
Вальдемар Вайцек., д-р техн. наук, проф. Люблинского технического
университета (Польша)

Печатается по плану издания Министерства образования и науки Республики Казахстан на 2016 г.

Ж 42 **Жданов О. Н.**
Начала криптографии в задачах и упражнениях: Учеб. пособие / О. Н. Жданов,
К. К. Елемесов. – Алматы: КазННТУ имени К. И. Сатпаева, 2016. – 97 с.:
Ил. 13. Табл. 19. Библиогр. – 17 назв.

ISBN 978-601-228-857-5

При изучении криптографических методов защиты информации (КМЗИ) важным является решение задач по зашифровыванию и расшифровыванию текстов и задач криптоанализа текстов.

Авторами подготовлен сборник таких задач. В первую часть вошли задачи по большей части подготовительные, иллюстрирующие основные понятия криптографии. Как показала практика преподавания КМЗИ, решение таких задач позволяет студентам глубже, полнее понять современные алгоритмы шифрования.

При составлении сборника были использованы имеющиеся учебные пособия и задачки, особое влияние на составителей оказали книги: Зубов А. Ю., Зязин А. В., Овчинников В. Н., Рамоданов С. М. «Олимпиады по криптографии и математике для школьников». – М.: МЦНМО, 2006 и «Введение в криптографию» / Под общ. ред. В. В. Яценко. – М.: Моск. центр непрерыв. мат. образования, 2000.

Составители сборника старались всюду, где это оказывалось возможным, указывать авторство задач. Однако в настоящее время значительное количество задач распространяется как в печатном виде, так и в электронном, и часто установить «первого автора» не представляется возможным. Часть задач публикуется впервые.

Вторая часть сборника содержит задачи, связанные с алгоритмами DES, ГОСТ 28147–89, AES, RSA, а также с задачами генерации и проверки электронной подписи.

УДК 003. 26
ББК 81

ISBN 978-601-228-857-5

© Жданов О.Н. Елемесов К.К., 2016
© КазННТУ им. К. И. Сатпаева, 2016

ВВЕДЕНИЕ

Традиционной задачей криптографии является обеспечение конфиденциальности информации при передаче сообщений по контролируемому противником каналу связи. В простейшем случае эта задача описывается взаимодействием трех субъектов (сторон). Владелец информации, называемый обычно *отправителем*, осуществляет преобразование исходной (*открытой*) информации (сам процесс преобразования называется *шифрованием*) в форму передаваемых *получателю* по открытому каналу связи *шифрованных* сообщений с целью ее защиты от противника.

Под *противником* понимается любой субъект, не имеющий права ознакомления с содержанием передаваемой информации. В качестве противника может выступать *криптоаналитик*, владеющий методами раскрытия шифров. Законный получатель информации осуществляет *расшифровывание* полученных сообщений. Противник пытается овладеть защищаемой информацией (его действия обычно называют *атаками*). При этом он может совершать как пассивные, так и активные действия.

Пассивные атаки связаны с прослушиванием, анализом трафика, перехватом, записью передаваемых шифрованных сообщений, *дешифрованием*, т. е. попытками "*взломать*" защиту с целью овладения информацией.

При проведении *активных* атак противник может прерывать процесс передачи сообщений, создавать поддельные (сфабрикованные) или модифицировать передаваемые шифрованные сообщения. Эти активные действия называют попытками *имитации* и *подмены* соответственно.

Под *шифром* обычно понимается семейство обратимых преобразований, каждое из которых определяется некоторым параметром, называемым *ключом*, а также порядком применения данного преобразования, называемым *режимом шифрования*.

Ключ – это важнейший компонент шифра, отвечающий за выбор преобразования, применяемого для зашифровывания конкретного сообщения. Обычно ключ представляет собой некоторую буквенную или числовую последовательность. Эта последовательность как бы "*настраивает*" алгоритм шифрования.

Каждое преобразование однозначно определяется ключом и описывается некоторым *криптографическим алгоритмом*. Один и тот же криптографический алгоритм может применяться для шифрования в различных режимах. Тем самым реализуются различные способы шифрования (простая замена, гаммирование и т. п.). Каждый режим шифрования имеет как свои преимущества, так и недостатки. Поэтому выбор режима зависит от конкретной ситуации. При расшифровывании используется криптографический алгоритм, который в общем случае может отличаться от алгоритма, применяемого для зашифровывания сообщения. Соответственно могут различаться ключи зашифровывания и расшифровывания. Пару алгоритмов зашифровывания и расшифровывания обычно называют *криптосистемой* (*шифрсистемой*), а реализующие их устройства – *шифртехникой*.

Если обозначить через M открытое, а через C зашифрованное сообщения, то процессы зашифровывания и расшифровывания можно записать в виде равенств

$$E_{k1}(M)=C, \quad D_{k2}(C)=M,$$

в которых алгоритмы зашифровывания E и расшифровывания D должны удовлетворять равенству

$$D_{k2}(E_{k1}(M))=M.$$

Рассмотрим вводные, подготовительные задачи.

Задача 1 [1]: Перед вами два зашифрованных текста. Один зашифрованный текст соответствует английскому открытому тексту, другой – русскому. Открытые тексты состоят только из букв. Шифрование заключалось в замене каждой буквы открытого текста двужначным числом. Разным буквам соответствуют разные числа, различия между строчной и прописной буквами не делались, знаки препинания опущены.

Определите, какой зашифрованный текст соответствует русскому открытому тексту.

Текст 1

11 25 28 33	35 42 47 53 69	72 83 11 19	22 17 31 47	39 45 17 11 57
83 91 19 11	59 62 53 45 11	51 11 65 25	25 28 11 83	91 51
45 11 19 25 33	62 35 69 72	83 19 25 65	51 83 91 11	

Текст 2

97 11 63	19 44	58 17 93	28 25 31	33 22 35 39	83 11 17 19
35 11 39					
59 47 51 17 91	69 33 28 42	45 17 53 57	62 33 65 22 72	97 11 63 69	
11 47 17 19	93 17 25 31	53 22 33 39 11	19 11 63 35		

Решение: Подсчитаем количество шифрообозначений в текстах. В первом тексте их 25, во втором – 28. Английский алфавит содержит 26 букв, следовательно, второй шифр-текст не может соответствовать английскому открытому тексту. Значит, второй текст – это зашифрованный русский текст.

Ответ: Первый текст – это зашифрованный английский текст, а второй – русский.

Решите самостоятельно следующую задачу. Проверить себя можно, обратившись к разделу «Ответы и указания».

Задача 2: Перед вами два зашифрованных текста. Открытые тексты состоят только из русских букв. Шифрование заключалось в замене каждой буквы открытого текста двузначным числом. Разным буквам соответствуют разные числа, различия между строчной и прописной буквами не делались, знаки препинания опущены.

Про какой из двух текстов сразу можно сказать, что он зашифрован с ошибками?

Текст 1

11 95 28 25	29 18 31	42 51 11 18	37 62 95	76 18 53 31
45 69 11	73 25 18	42 11 81	91 28 13 15	57 84 11 33 46 25
67 11 48 58 88	93 18 25	11 31 25 29	18 91 57 45 53 62	
37 18 29 67 73 67	11 25 18 11	29 31 62 31 37		

Текст 2

25 93 18 31	48 33 15 84 17	37 45	42 29 11	53 51	73 57 69 62 11
15 17 18 76 81	88 91 17 13	95 19 67 28 46 17	58 19 58 11		
23 18 23 76	81 61 99 88 25	11 44 19 23 17	18 11 51 42 51		
37 93 18 23 61	44 88 61 81 11				

Классификация шифров (подробнее см. [5]).

В качестве первичного признака, по которому проводится классификация шифров, используется тип преобразования, осуществляемого с открытым текстом при шифровании. Если фрагменты открытого текста (отдельные буквы или группы букв) заменяются некоторыми их эквивалентами в шифр-тексте, то соответствующий шифр относится к классу *шифров замены*. Если буквы открытого текста при шифровании лишь меняются местами друг с другом, то мы имеем дело с *шифром перестановки*. С целью повышения надежности шифрования шифрованный текст, полученный применением некоторого шифра, может быть еще раз зашифрован с помощью другого шифра.

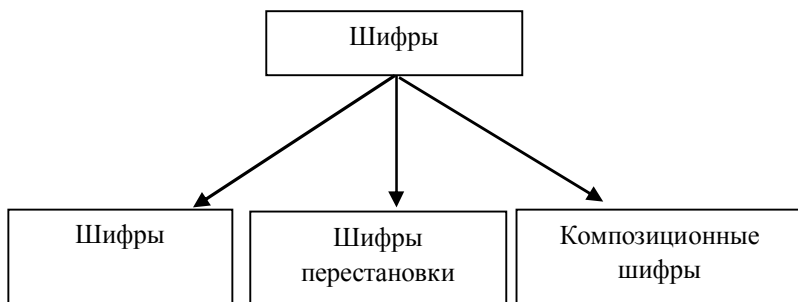


Рис. 1. Классификация шифров

Всевозможные такие композиции различных шифров приводят к третьему классу шифров, которые обычно называют *композиционными шифрами*. Заметим, что композиционный шифр может не входить ни в класс шифров замены, ни в класс шифров перестановки (рис. 1).

1. ШИФРЫ ПЕРЕСТАНОВКИ

Шифры перестановки или транспозиции изменяют только порядок следования символов или других элементов исходного текста.

Классическим примером такого шифра является система, использующая карточку с отверстиями – *решетку Кардано*, которая при наложении на лист бумаги оставляет открытыми лишь некоторые его части. При зашифровке буквы сообщения вписываются в эти отверстия. При расшифровке сообщение вписывается в диаграмму нужных размеров, затем накладывается решетка, после чего на виду оказываются только буквы открытого текста.

Следующая задача посвящена поворотной решетке.

Задача 3 [1, с. 38]: Ключом шифра, называемого «*поворотная решётка*», является трафарет, изготовленный из квадратного листа клетчатой бумаги размером $n \times n$ (n – чётно). Некоторые из клеток вырезаются. Одна из сторон трафарета помечена. При наложении этого трафарета на чистый лист бумаги четырьмя возможными способами (помеченной стороной вверх, вправо, вниз, влево) его вырезы полностью покрывают всю площадь квадрата, 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 n .

Решение: 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:

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

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 $4^{n^2/4}$.

Приведем пример шифра перестановки, основанного на иной идее.

Задача 4 [6]: Шахматная перестановка. Зашифровано высказывание, ключом является маршрут движения по доске, неизвестный вам. Движение начинается с отмеченной клетки. Переход в следующую клетку осуществляется ходом шахматного коня. Клетки, где нет букв, определяют пробел между словами.

Н	А	Р			Ь		У
Е	Т	О	Ш	В	Ю	С	Л
Я	Ж	А	Э	Т	И	К	А
О	М		С	Т	–	О	Д
О	А	Т	Р	Н	А	Т	,
О	Л	Е		Ь	А	Е	Б
М	М	К	Т	Я	А	К	А
Ь		А	Т	О	Р		Л

Решение: Сделав несколько пробных «ходов коня», можно определить первые три буквы. После этого уже легко дойти до конца первого слова. Дальше просто.

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

Самая большая трата, какую только можно сделать – это трата времени (Теофраст).

Также возможны и другие варианты шифра перестановки, например, шифры столбцовой и двойной перестановки.

ШИФР СТОЛБЦОВОЙ ПЕРЕСТАНОВКИ

При расшифровывании буквы шифротекста записываются по столбцам в соответствии с последовательностью чисел ключа, после чего исходный текст считывается по строкам. Для удобства запоминания ключа применяют перестановку столбцов таблицы по ключевому слову или фразе, всем символам которых ставятся в соответствие номера, определяемые порядком соответствующих букв в алфавите.

При решении заданий на криптоанализ шифров перестановки необходимо восстановить начальный порядок следования букв текста. Для этого используется анализ совместимости символов, в чем может помочь таблица сочетаемости.

Таблица 1

Сочетаемость букв русского языка (по [5])

Г	С	Слева		Справа	Г	С
3	97	л, д, к, т, в, р, н	А	л, н, с, т, р, в, к, м	12	88
80	20	я, е, у, и, а, о	Б	о, ы, е, а, р, у	81	19
68	32	я, т, а, е, и, о	В	о, а, и, ы, с, н, л, р	60	40
78	22	р, у, а, и, е, о	Г	о, а, р, л, и, в	69	31
72	28	р, я, у, а, и, е, о	Д	е, а, и, о, н, у, р, в	68	32
19	81	м, и, л, д, т, р, н	Е	н, т, р, с, л, в, м, и	12	88
83	17	р, е, и, а, у, о	Ж	е, и, д, а, н	71	29
89	11	о, е, а, и	З	а, н, в, о, м, д	51	49
27	73	р, т, м, и, о, л, н	И	с, н, в, и, е, м, к, з	25	75
55	45	ь, в, е, о, а, и, с	К	о, а, и, р, у, т, л, е	73	27
77	23	г, в, ы, и, е, о, а	Л	и, е, о, а, ь, я, ю, у	75	25
80	20	я, ы, а, и, е, о	М	и, е, о, у, а, н, п, ы	73	27
55	45	д, ь, н, о, а, и, е	Н	о, а, и, е, ы, н, у	80	20
11	89	р, п, к, в, т, н	О	в, с, т, р, и, д, н, м	15	85
65	35	в, с, у, а, и, е, о	П	о, р, е, а, у, и, л	68	32
55	45	и, к, т, а, п, о, е	Р	а, е, о, и, у, я, ы, н	80	20
69	31	с, т, в, а, е, и, о	С	т, к, о, я, е, ь, с, н	32	68
57	43	ч, у, и, а, е, о, с	Т	о, а, е, и, ь, в, р, с	63	37
15	85	п, т, к, д, н, м, р	У	т, п, с, д, н, ю, ж	16	84
70	30	н, а, е, о, и	Ф	и, е, о, а, е, о, а	81	19

Продолжение табл. 1

Г	С	Слева		Справа	Г	
90	10	у, е, о, а, ы, и	Х	о, и, с, н, в, п, р	43	57
69	31	е, ю, н, а, и	Ц	и, е, а, ы	93	7
82	18	е, а, у, и, о	Ч	е, и, т, н	66	34
67	33	ь, у, ы, е, о, а, и, в	Ш	е, и, н, а, о, л	68	32
84	16	е, б, а, я, ю	Щ	е, и, а	97	3
0	100	м, р, т, с, б, в, н	Ы	л, х, е, м, и, в, с, н	56	44
0	100	н, с, т, л	Ь	н, к, в, п, с, е, о, и	24	76
14	86	с, ы, м, л, д, т, р, н	Э	н, т, р, с, к	0	100
58	42	ь, о, а, и, л, у	Ю	д, т, щ, ц, н, п	11	89
43	57	о, н, р, л, а, и, с	Я	в, с, т, п, д, к, м, л	16	84

При анализе сочетаемости букв друг с другом следует иметь в виду зависимость появления букв в открытом тексте от значительного числа предшествующих букв. Для анализа этих закономерностей используют понятие условной вероятности.

Систематически вопрос о зависимости букв алфавита в открытом тексте от предыдущих букв исследовался известным русским математиком А. А. Марковым (1856–1922). Он доказал, что появления букв в открытом тексте нельзя считать независимыми друг от друга. В связи с этим А. А. Марковым отмечена еще одна устойчивая закономерность открытых текстов, связанная с чередованием гласных и согласных букв. Им были подсчитаны частоты встречаемости биграмм вида гласная–гласная (g, g), гласная–согласная (g, c), согласная–гласная (c, g), согласная–согласная (c, c) в русском тексте длиной в 10^5 знаков. Результаты подсчета отражены в следующей таблице:

Таблица 2

Чередование гласных и согласных

	Г	С	Всего
Г	6588	38310	44898
С	38296	16806	55102

Задача 5 [15]: Открытый текст, сохраняя пробелы между словами, записали в таблицу. Начало было в первой строке, текст записывали слева направо, переходя со строки на следующую, шифрование заключалось в перестановке столбцов. Найдите открытый текст.

Шифрованный текст:

Д	В			Ы	Т
	Г	О	Е	Р	О
У	Ь	Д		У	Б
М	М	Я	Ы	Р	П

Решение: Присвоим столбцам номера в порядке их следования. Наша задача – найти такой порядок столбцов, при котором текст будет осмысленным.

Составим таблицу:

	1	2	3	4	5	6
1	X					
2		X				
3			X			
4				X		
5					X	
6						X

Клетка (k, m) в этой таблице означает, что столбец с номером m следует за столбцом с номером k . Знаком «X» отметим невозможные случаи.

Сочетания столбцов 1, 2 и 5, 2 невозможны, так как гласная не может находиться перед мягким знаком. Невозможны и следования столбцов 2, 1 и 2, 5. Теперь из третьей строки следует, что 1, 5 и 5, 1 невозможны, так как УУ – нехарактерная для русского языка биграмма. Далее два пробела подряд не могут быть в тексте, значит, ставим «X» в клетках 3, 4 и 4, 3. Снова обратимся к третьей строке. Если бы столбец 2 следовал за столбцом 4, то слово начиналось бы с мягкого знака. Ставим «X» в клетке 4, 2. Из первой строки: невозможна комбинация 4, 5,

невозможна и 3, 5. Итог наших рассуждений представлен в таблице:

	1	2	3	4	5	6
1	X	X			X	
2	X	X			X	
3			X	X	X	
4		X	X	X	X	
5	X	X			X	
6						X

Итак, после столбца 6 обязательно следует столбец 5. Но тогда поставим «X» в клетке 6, 2 и получим: столбец 2 следует за столбцом 3. Далее мы вычеркнули 5, 1 и 2, 1, следовательно, надо проверить варианты: ...6532... и ...65 432... . Но (4, 3) вычеркнуто ранее. Итак, остались варианты расположения столбцов:

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

1

Запишем 6, 5, 3, 2 столбцы подряд:

т	ы	–	в
о	р	о	г
б	у	д	ь
п	р	я	м

Попытка поставить столбец 1 перед столбцом 6 приведет к биграмме МП в последней строке и сочетанию ДТЫ в первой. Остались варианты: 653241, 146 532.

Ответ: 653241 – ключ, открытый текст:

ты_в_д

ороге_

будь_у

прямым

(строка из популярной в 1970-е годы песни).

Приведем еще один пример криптоанализа шифра столбцовой перестановки.

Задача 6 [16]: Дан шифротекст:
СВПООЗЛУЙЬСТЬ_ЕДПСОКОКАЙЗО

Решение: Текст содержит 25 символов, что позволяет записать его в квадратную матрицу 5x5. Известно, что шифрование проводилось по столбцам, следовательно, расшифровывание следует проводить, меняя порядок столбцов.

С	В	П	О	О
З	Л	У	Й	Ь
С	Т	Ь	—	Е
Д	П	С	О	К
К	А	Й	З	О

Необходимо провести анализ совместимости символов (таблица сочетаемости букв русского и английского алфавита, а также таблицы частот биграмм представлена выше). В первом и третьем столбцах сочетание СП является крайне маловероятным для русского языка. Рассмотрим другие запрещенные и маловероятные сочетания букв: ВП (2, 3 столбцы), ПС (3, 1 столбцы), ПВ (3, 2 столбцы). Перебрав их все, получаем наиболее вероятные сочетания биграмм по столбцам:

В	О	С	П	О
Л	Ь	З	У	Й
Т	Е	С	Ь	—
П	О	Д	С	К
А	З	К	О	Й

Получаем осмысленный текст:
ВОСПОЛЬЗУЙТЕСЬ_ПОДСКАЗКОЙ

Решите самостоятельно следующие аналогичные задачи:

Задача 7: НМВИАИ_НЕВЕ_СМСТУОРДИАНКМ;

Задача 8: ЕДСЗЬНДЕ_МУБД_УЭ_КРЗЕМНАЫ;

Задача 9: СОНРЧОУО_ХДТ_ИЕИ_ВЗКАТРРИ;

Задача 10: _ОНКА_БНЬЕЦВЛЕ_К_ТГОАНЕИР;

Задача 11: НЗМАЕЕАА_Г_НОТВОССОТЬЯАЛС.

ШИФР ДВОЙНОЙ ПЕРЕСТАНОВКИ

Задача 12 [16]: Дан шифротекст:

БЮЕЧТТОУ_СНСОРЧТРНАИДЬН_Е. Известно, что шифрование проводилось сначала по столбцам, а затем по строкам.

Решение: Запишем текст в квадратную матрицу 5x5. Расшифровывание следует проводить тем же способом, что и зашифровывание.

Ы	О	Е	Ч	Т
Т	О	У	_	С
Н	С	О	Р	Ч
Т	Р	Н	А	И
Д	Ь	Н	_	Е

Проводим анализ совместимости символов. Если в примере столбцовой перестановки можно было легко подобрать нужную комбинацию путем перебора, то здесь лучше воспользоваться таблицей частот букв русского языка (см. приложение). Для оптимизации скорости выполнения задания можно проверить все комбинации букв только в первой строке. Получаем ОЕ–15, ОЧ–12, ЕТ–33, ТЕ–31, ЧО–х, ЕО–7, ЧЫ–х, ОЫ–х, ТЫ–11, ТЧ–1, ЧЕ–23 (где х – запрещенная комбинация).

Из полученных результатов можно предположить следующую комбинацию замены столбцов **2 4 3 5 1**:

Таблица к задаче 12

О	Ч	Е	Т	Ы
О	—	У	С	Т
С	Р	О	Ч	Н
Р	А	Н	И	Т
Ь	—	Н	Е	Д

Теперь необходимо переставить строки в нужном порядке.

3 2 4 5 1:

С	Р	О	Ч	Н
О	—	У	С	Т
Р	А	Н	И	Т
Ь	—	Н	Е	Д
О	Ч	Е	Т	Ы

Получаем осмысленный текст:

СРОЧНО_УСТРАНИТЬ_НЕДОЧЕТЫ

Задачи для самостоятельного решения на криптоанализ шифра двойной перестановки:

Задача 13: СЯСЕ_ЛУНЫИАККННОГЯДУЧАТН;

Задача 14: МСЕЫ_ЛЫВЕНТОСАНТУЕИ_РЛПОБ;

Задача 15: АМНРИД_УЕБСЫ_ЕЙРСООКОТНВ_;

Задача 16: ОПЧУЛС_БООНЕВ_ОЖАЕОНЕЩЕИН;

Задача 17: ЕШИАНИРЛПГЕЧАВРВ_СЕЫНА_ЛО.

2. ШИФРЫ ЗАМЕНЫ

Шифр замены является простейшим, наиболее популярным шифром. Типичными примерами являются шифр Цезаря, «цифирная азбука» Петра Великого и «пляшущие человечки» А. Конан Дойла. Как видно из самого названия, шифр замены осуществляет преобразование замены букв или других «частей» открытого текста на аналогичные «части» шифрованного текста. Легко дать математическое описание шифра замены. Пусть X и Y – два алфавита (открытого и шифрованного текстов соответственно), состоящие из одинакового числа символов. Пусть также $g: X \rightarrow Y$ – взаимнооднозначное отображение X в Y . Тогда шифр замены действует так: открытый текст $x_1x_2\dots x_n$ преобразуется в шифрованный текст $g(x_1)g(x_2)\dots g(x_n)$.

Криптоанализ шифра простой замены основан на использовании статистических закономерностей языка. Приведем таблицы частот букв русского и английского языков, следуя [5].

Таблица 3

Частоты букв русского языка
(в 32-буквенном алфавите со знаком пробела)

– 0,175	О 0,090	Е,Ё 0,072	А 0,062
И 0,062	Т 0,053	Н 0,053	С 0,045
Р 0,040	В 0,038	Л 0,035	К 0,028
М 0,026	Д 0,025	П 0,023	У 0,021
Я 0,018	Ы 0,016	З 0,016	Ь,Ъ 0,014
Б 0,014	Г 0,013	Ч 0,012	Й 0,010
Х 0,009	Ж 0,007	Ю 0,006	Ш 0,006
Ц 0,004	Щ 0,003	Э 0,003	Ф 0,002

Полезной является диаграмма частот, см. ниже.

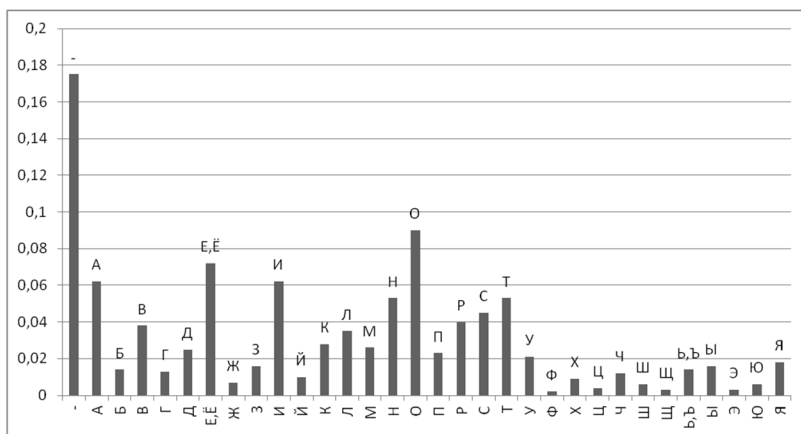


Рис. 2. Диаграмма частот букв русского языка

Для получения более точных сведений об открытых текстах можно строить и анализировать таблицы k -грамм при $k > 2$, однако для учебных целей вполне достаточно ограничиться биграммами. Неравновероятность k -грамм (и даже слов) тесно связана с характерной особенностью открытого текста – наличием в нем большого числа повторений отдельных фрагментов текста: корней, окончаний, суффиксов, слов и фраз. Так, для русского языка такими привычными фрагментами являются наиболее частые биграммы и триграммы:

СТ, НО, ЕН, ТО, НА, ОВ, НИ, РА, ВО, КО,
СТО, ЕНО, НОВ, ТОВ, ОВО, ОВА

Полезной является информация о сочетаемости букв, т. е. о предпочтительных связях букв друг с другом, которую легко извлечь из таблиц частот биграмм.

Имеется в виду таблица, в которой слева и справа от каждой буквы расположены наиболее предпочтительные "*sоседи*" (в порядке убывания частоты соответствующих биграмм). В таких таблицах обычно указывается также доля гласных и согласных

букв (в процентах), предшествующих (или следующих за) данной букве.

Таблица 4

Таблица частот биграмм русского языка

Часть 1

	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
А	2	12	35	8	14	7	6	15	7	7	19	27	19	45	3	11
Б	5					9	1		6			6		2	21	
В	35	1	5	3	3	32		2	17		7	10	3	9	58	6
Г	7				3	3			5		1	5		1	50	
Д	25		3	1	1	29	1	1	13		1	5	1	13	22	3
Е	2	9	18	11	27	7	5	10	6	15	13	35	24	63	7	16
Ж	5	1			6	12			5					6		
З	35	1	7	1	5	3			4		2	1	2	9	9	1
И	4	6	22	5	10	21	2	23	19	11	19	21	20	32	8	13
Й	1	1	4	1	3		1	2	4		5	1	2	7	9	7
К	24	1	4	1		4	1	1	26		1	4	1	2	66	2
Л	25	1	1	1	1	33	2	1	36		1	2	1	8	30	2
М	18	2	4	1	1	21	1	2	23		3	1	3	7	19	5
Н	54	1	2	3	3	34			58		3		1	24	67	2
О	1	28	84	32	47	15	7	18	12	29	19	41	38	30	9	18
П	7					15			4			9		1	46	

Часть 2

	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я
А	26	31	27	3	1	10	6	7	10	1			2	6	9
Б	8	1		6						1	11				2
В	6	19	6	7		1	1	2	4	1	18	1	2		3
Г	7			2											
Д	6	8	1	10			1	1	1		5	1			1
Е	39	37	33	3	1	8	3	7	3	3			1	1	2
Ж		1													
З	3	1		2							4				4
И	11	29	29	3	1	17	3	11	1	1			1	3	17
Й	3	10	2				1	3	2						

Продолжение таблицы 4

	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я
К	10	3	7	10			1								
Л		3	1	6		4		1			2	30		4	9
М	2	5	3	9	1			2			5	1	1		3
Н	1	9	9	7	1		5	2			36	3			5
О	43	50	39	3	2	5	2	12	4	3			2	3	2
П	41	1		6							2				2

Часть 3

	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
Р	55	1	4	4	3	37	3	1	24		3	1	3	7	56	2
С	8	1	7	1	2	25			6		40	13	3	9	27	11
Т	35	1	27	1	3	31		1	28		5	1	1	11	56	4
У	1	4	4	4	11	2	6	3	2		8	5	5	5	1	5
Ф	2					2			2						1	
Х	4	1	4	1	3	1		2	3		4	3	3	4	18	5
Ц	3					7			10		2				1	
Ч	12					23			13		2			6		
Ш	5					11			14		1	2		2	2	
Щ	3					8			6					1		
Ы		1	9	1	3	12		2	4	7	-3	6	6	3	2	10
Ь		2	4	1	1	2		2	2		6		3	13	2	4
Э											1			1		
Ю		2	1	2	1			3	1		1		1	1	1	3
Я	1	3	9	1	3	3	1	5	3	2	3	3	4	6	3	6

Часть 4

	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я
Р	1	5	9	16		1	1	1	2		8	3			5
С	4	11	82	6		1	1	2	2		1	8			17
Т	26	18	2	10				1			И	21			4
У	7	14	7			1		8	3	2				9	1
Ф	1	1													
Х	3	4	2	2	1			1							
Ц				1							1				
Ч			7	1					1			1			
Ш				1								1			

Продолжение таблицы 4

	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я
Щ				1											
Ы	3	9	4	1		16		1	2						
Ь	1	11	3					1	4				1	3	1
Э		1	9												
Ю	1	1	7				1	1		4					
Я	3	6	10			2	1	4	1	1			1	1	1

Пример криптоанализа шифра замены

Задача 18 [15]: Известно, что зашифровано стихотворение Р. Киплинга в переводе С. Я. Маршака. Шифрование заключалось в замене каждой буквы на двузначное число. Отдельные слова разделены несколькими пробелами, знаки препинания сохранены. Таблица частот букв русского языка приведена выше.

29 15 10 17 29 22 25 31 15 33 35 41 43 45 35 57 45 25 17 59
 15 10 25 41 25 69, 59 78 29 82 25 78 25 17 15 10 88 90 78 25
 62 25 22 10 57 73 79 35 67 78 90 88 29 45 35 29, 54 57 90 31 90 73
 22 88 15 88 29 15 17 69 41 25 15, 70 17 90 57 43 59 15 78 15 62 22
 25 17 57 25 69 88 15 82 17 25 88 29 45 35...

Решение: Подсчитаем частоты шифробозначений:

Обозначение	29	15	10	17	22	25	31	33	35	41	43	45	57
Количество	7	10	4	7	4	12	2	1	5	3	2	4	5
Обозначение	59	69	78	82	88	90	62	73	79	67	54	70	
Количество	3	3	4	2	6	5	1	2	1	1	1	1	

Из таблицы частот букв русского языка видно, что чаще всего встречается буква О, на втором месте Е. В нашем шифротексте чаще всего встречается обозначение 25 (12 раз), на втором месте идет обозначение 15 (10 раз), остальные обозначения им существенно уступают. Поэтому можем выдвинуть гипотезу: 25 = О, 15 = Е. Однако текст у нас не очень большой, поэтому закономерности русского языка проявляются в нем не обязательно в строгом соответствии с таблицей частот букв русского языка. Поэтому возможен и вариант: 25 = Е, 15 = О. Но тогда последнее слово в третьей строке имеет окончание ЕО, что возможно, но все же более вероятный вариант ОЕ. Итак, будем работать с текстом, считая, что 25 = О, 15 = Е.

Теперь нам поможет знак препинания: «29, ...». Крайне маловероятно, чтобы запятая стояла после согласной. Итак, 29 – гласная, причем вероятнее всего 29 = И или 29 = А, так как гласные Я, Ю, Э, У встречаются в осмысленных текстах на русском языке намного реже, чем И и А, что не противоречит таблице частот шифротекста.

В последней строке: 88 15, но 15 = Е, следовательно, 88 – согласная, причем наиболее вероятные значения – это Н и Т.

Итак, 25 = О, 15 = Е, 29 = А $\begin{pmatrix} A \\ И \end{pmatrix}$, 88 = $\begin{pmatrix} H \\ T \end{pmatrix}$. Теперь третье слово

в третьей строке имеет 4 варианта:

- 29 = И, 88 = Н: 22 Н Е Н И Е
- 29 = И, 88 = Т: 22 Т Е Т И Е
- 29 = А, 88 = Н: 22 Н Е Н А Е
- 29 = А, 88 = Т: 22 Т Е Т А Е

Из рассмотренных вариантов лишь один является осмысленным, и он позволяет найти значение 22. Имеем 22 = М и третье слово в третьей строке М Н Е Н И Е.

Теперь рассмотрим второе слово в первой строке. Е 10 17 И, причем 10 и 17 – согласные, и это не М и не Н. Наиболее вероятное слово Е С Л И, т. е. 10 = С, 17 = Л. Конечно, если мы, продолжая работать с текстом, вдруг получим «нечитаемое» слово, то

придется вернуться к этому этапу и рассмотреть другие варианты. Однако это маловероятно, поскольку вряд ли в стихотворении были слова наподобие Е Р Т И, Е В Л И и т. п.

Далее первое слово второй строки: 59 78 И, причем 59 и 78 – согласные, и это не С, не Л, не М и не Н. Так что это слово П Р И, т. е. 59 = П, 78 = Р. Тогда шестое слово первой строки 45 О Л П Е, что дает значение 45 = Т, и тогда при 57 = В получаем фрагмент «...В Т О Л П Е...». Также второе слово последней строки П Е Р Е 62 дает нам значение 62 = Д.

Далее рассмотрим начало второй строки: «П Р И 82 О Р О Л Е С Н 90 Р О Д О М ...». Из него следует, что 82 = К и 90 = А. Зная, что 82 = К, посмотрим на самое последнее слово К Л О Н И Т 35, откуда станет ясно, что 35 = Б.

Перед последней атакой выпишем текст, заменяя известные обозначения буквами.

И Е С Л И М О 31 Е 33 Ь 41 43 Т Ь В Т О Л П Е С О
41 О 69, П Р И К О Р О Л Е С Н А Р О Д О М С В 73 79 Ь 67
Р А Н И Т Ь И, 54 В А 31 А 73 М Н Е Н И Е Л 69 41 О Е, 70
Л А В 43 П Е Р Е Д М О Л В О 69 Н Е К Л О Н И Т Ь...

Из последней строки 69 = Ю, тогда слова Л Ю 41 О Е и С О 41 О Ю определяют так: 41: 41 = Б. Теперь из четвертого слова первой строки Б 43 Т Ь получаем, что 43 = Ы. А первое слово из последней строки 70 Л А В Ы – это Г Л А В Ы. Слово в первой строке М О 31 Е 33 Ь угадывается из контекста: М О Ж Е Ш Ь, т. е. 31 = Ж, 33 = Ш. Теперь второе слово в третьей строке запишется как 54 В А Ж А 73, откуда с учетом контекста: 54 = У, 73 = Я. После этого окончание второй строки имеет вид «... С В Я 79 Ь 67 Р А Н И Т Ь». Легко определяются буквы 79 = З, 67 = Х.

Ответ: И Е С Л И М О Ж Е Ш Ь Б Ы Т Ь В Т О Л П Е
С О Б О Ю, П Р И К О Р О Л Е С Н А Р О Д О М С В Я З Ь
Х Р А Н И Т Ь И, У В А Ж А Я М Н Е Н И Е Л Ю Б О Е,
Г Л А В Ы П Е Р Е Д М О Л В О Ю Н Е К Л О Н И Т Ь...

Решите самостоятельно аналогичные задачи, проверить решение можно по разделу «Ответы и указания».

Задача 19.1 [15]: Известно, что зашифровано стихотворение. Шифрование заключалось в замене каждой буквы двузначным числом. Отдельные слова разделены несколькими пробелами, знаки препинания сохранены. Найдите открытый текст.

29 35 87 41 29 58 43 44 31 58 31 68 95 58 31 25 63, 32 58 31
87 41 31 68 31 58 68 31 35 68 41 31 68 63 71 95 63 77 91
35 68 91 45 99 45 35 58 77 41 63 58,
29, 77 31 58 35 91 77 35 68 95 91 63 71 35 51 75 35, 25
31 61 35 71 75 87 51 31 68 45 – 82 35 17 77 91 35 61 51 29
19 87 29 41 – 68 31 17 31 82 51 31 68 29 58 75 87 68 31 29
58 91 63 54...

Задача 19.2: То же самое, шифротекст ниже.

56 67 92 18 58 39 99 27 87 67 56 25 56 80 67 10 17 92 39
62 25 56 27 24 95 56 31 95 46 27 73 56 31 17 58 39 58 67 95
58 92 56 95 40 24 40 17 92 39 62 69 39 40 17 56 67 58 –
56 18 99 92 46 67 56 87, 69 56 69 39 36 80 17 92 67 27 39 40
87 56 17 58 73 40. 25 56 39 73 56 10 17 92, 56 43 92 80 40 10,
95 56 23 80 40 23 17 40 24 40 25 46 92 69 14 95 67 27 73 95
73 58 87 67 56 73 58. 69 39 58 69 56 95 46 27 23 25 46 92 67
10 17 56 38 58 73 95 92 58 56 38 58 46 73 40 67 92 10. 25 46
92 18 56 46 56 69 92 25 27 17 62 73 56 69 24 80 58 39 62 18
14 17 56 25 46 58 69 58 17 92 95 56 58 87 67 56 43 58 39 73 69
56, 23 17 40 24 40 46 40 24 18 58 23 40 17 92 39 62. 56 80 67
40 95 56 18 17 40 23 56 80 40 46 10 73 58 87 43 58 80 69 27
87 67 58 80 58 17 10 87 73 46 58 67 92 46 56 69 56 95 67 40
87 40 95 58 73 58 92 73 14 39 10 38 58 95 46 40 73 67 56 25
56 69 73 56 46 58 67 67 14 87 67 40 39 73 40 69 17 58 67 92 10 87
92 67 39 73 46 27 95 73 56 46 40 56 67 92 39 56 69 58 46 99 58
67 67 56 73 56 38 67 56 24 67 40 17 92, 24 40 38 58 87 25
46 92 99 17 92. 25 56 67 10 73 92 10 67 58 92 87 58 17 92, 80
17 10 38 58 23 56 95 56 67 95 46 58 73 67 56 25 46 58 80 67 40
24 67 40 38 58 67 14 69 39 58 71 73 92 99 73 27 95 92 – 67
56 56 73 67 92 82 71 73 56 23 56 92 67 58 73 46 58 18 56
69 40 17 56 39 62.

67 58 25 46 56 99 17 56 92 87 92 67 27 73 14, 95 40 95
 56 67 27 69 92 80 58 17 51 58 17 62 92 82 67 58 17 58 23 95
 56 23 56 92 71 95 24 56 73 92 38 58 39 95 56 23 56 25 27 73 58
 99 58 39 73 69 92 10 - 73 46 92 25 27 17 62 73 40 25 56 25
 46 40 69 56 87 27 18 56 46 73 27, 27 39 14 25 40 67 67 14 58 38
 58 46 73 56 69 56 31 27 31 87 56 31 73 27 87 18 17 58 46 56 69,
 17 40 87 25 56 38 58 95, 25 58 46 58 95 17 36 38 40 73 58 17 58 31
 92 95 67 56 25 56 95. 73 46 92 69 14 25 27 95 17 14 82 71 95
 46 40 67 40 69 69 92 80 58 69 58 46 73 92 95 40 17 62 67 14 82
 25 46 10 87 56 27 23 56 17 62 67 92 95 56 69 – 56 67 92 39 40
 87 14 58, 67 92 95 40 95 56 31 56 99 92 18 95 92...

18 56 80 46 56 39 73 92 46 40 80 92, 56 67 25 56 69 73 56
 46 92 17 25 46 56 39 58 18 10 25 56 17 36 18 92 69 99 27 36 39
 10 51 92 73 40 73 27: “38 73 56 56 80 92 67 38 58 17 56 69
 58 95 25 56 39 73 46 56 92 17, 80 46 27 23 56 31 24 40 69 39
 58 23 80 40 46 40 24 17 56 87 40 73 62 39 87 56 43 58 73”. 92,
 25 56 82 17 56 25 40 69 25 56 25 17 58 38 27 39 73 46 40 99
 92 17 27 69 24 67 40 95 73 56 23 56, 38 73 56 67 40 25 40
 46 67 92 95 80 56 17 43 58 67 18 80 92 73 58 17 62 67 56 39 73
 56 10 73 62 67 40 99 27 82 58 46 58, 80 56 39 73 40 17 95 92
 67 43 40 17 92 24 25 46 92 99 92 73 14 82 67 40 80 95 56 17
 58 67 56 87 67 56 43 58 67.

Следующая задача посвящена криптоанализу текста на русском языке, зашифрованного двумя способами.

Задача 20: (Для этой задачи образцом послужила задача 6.3 [1], шифробозначения, текст мы заменили). Первый шифротекст получен из исходного текста перестановкой букв. Второй шифротекст получен из того же исходного текста заменой каждой буквы на другую букву так, что разные буквы заменены разными, а одинаковые – одинаковыми.

Восстановите исходный текст.

Первый шифротекст:

И Т Ш И Ъ О К Т С О Г М А О Ф О К Е Т А П С С Е О Н С
 С Ы А В М Ъ Ю З Т Ы Т А Ф О Ъ В В Б А С О Ж Е З Т С И Н Ы
 А Я Р Р Р Т О С Н М Я П Н Н О А Т Ш А О В О

Второй шифротекст:

Ф Я Р Ф Р У Ч Р Ф Ц Ы С А Б О В Я О Р Ц А Г Р Ф Ц Р Э Ц
Ы Г Ф И Г Р Х Н Р Ш Ч Д Н В Ц В Т В Н Ч В Ч И Ж Р Ч В Х Д Г
В И Ц Ф Э Ф Ц Р Л Т Р Ф Ц Ы М С А Б О В

Решение: Подсчитаем частоты букв первого шифротекста. Эти частоты будут частотами букв исходного текста, так как первый шифр-текст получен перестановкой букв из исходного текста. Одновременно подсчитаем частоты шифробозначений второго текста.

<i>Первый шифротекст</i>	<i>Второй шифротекст</i>
О – 11	Р – 11
Т, А, С – 8	Ц, Ф, В – 8
Н – 5	Ч – 5
В – 4	Г – 4
И, Ь, М, Е, Р – 3	Ы, А, О, И, Н – 3
Ш, К, Ф, П, Ы, З, Я – 2	Я, С, Б, Э, Х, Д, Т – 2
Й, Г, Ю, Б, Ж – 1	У, Ш, Ж, Л, М – 1

Сразу можно сделать вывод: шифробозначению Р соответствует буква О открытого текста, Ч – соответствует Н, а Г – В.

Будем постепенно «*проявлять*» текст. Запишем второй шифр-текст (в нем порядок следования букв не менялся), заменяя уже известные нам шифробозначения их значениями (прописные буквы – это буквы открытого текста, строчные – шифробозначения):

фяОфОуНОфцысабов...

Далее шифробозначение Ф скрывает одну из букв: Т, А, С. Шифробозначение Я скрывает либо букву Я, либо согласную. Предположим, что Я→Я, пробуем читать начало:

Ф→Т: ТЯТОТО...

Ф→А: АЯОАО...

Ф→С: СЯОСО...

Не читается. Вывод: Я скрывает согласную, причем одну из следующих: Ш, К, Ф, П, З (вариант Я→Ы мы отбросили сразу). Но если Ф→Т, то слово не читается. Проверим вариант Ф→С. Пробуем читать: СяОСОуНОСцы..., и из всех возможных замен

для Я подходит только П, тогда начало текста: СПОСОБНОСТЬ, и мы знаем теперь, что $Я \rightarrow П$, $У \rightarrow Б$, $Ц \rightarrow Т$, $Ы \rightarrow Ъ$.

Обратим внимание на фрагмент ...яорцагрфцрэцы... С учетом наших знаний это: ПоОТаВОСТОэТЬ, и мы находим еще соответствия: $О \rightarrow Р$, $А \rightarrow И$, $Э \rightarrow Я$. Кроме того, так как $Ф \rightarrow С$, $Ц \rightarrow Т$, то из таблицы: $В \rightarrow А$.

Теперь исследуем последний фрагмент текста: ...фцрлтрфцымсабов. Заменим обозначения их значениями: ...СТОлтОСТЬм... Обратимся к таблице. Обозначению Л соответствует одна из букв Й, Г, Ю, Б, Ж. Пробуем читать, получаем $Л \rightarrow Й$, и из таблицы: $Т \rightarrow К$. Но тогда $М \rightarrow Ю$, и слово получилось СТОЙКОСТЬЮ.

Теперь начало второй строки: ...АТАКАнНА..., ясно, что $Н \rightarrow М$. Далее записываем вторую строку:

...АТАКАМННанижОНАхдВАиТСЯСТОЙКОСТЬЮ...

И мы знаем: $И \rightarrow Е$, $Ж \rightarrow Г$, $Х \rightarrow З$, $Д \rightarrow Ы$.

Текст: «Способность шифра противостоять всевозможным атакам на него называется *стойкостью шифра*».

3. СОВЕТЫ ПО ВЫПОЛНЕНИЮ ЧАСТОТНОГО АНАЛИЗА АНГЛИЙСКИХ ТЕКСТОВ

(1) Начните с подсчета частоты появления каждой из букв шифротекста. Примерно пять букв должны появляться с частотой менее 1 %, и они, вероятно, представляют собой **j, k, q, x** и **z**. Одна из букв должна появляться с частотой более 10 %, и она, по-видимому, представляет собой **e**. Если шифротекст не подчиняется этому распределению частот, то, возможно, исходное сообщение написано не на английском языке. Вы можете определить, какой это язык, если проанализируете частотное распределение букв в шифротексте. К примеру, в итальянском языке есть три буквы с частотностью более 10 % и 9 букв с частотностью менее 1 %. В немецком языке буква **e** имеет чрезвычайно высокую частотность – 19 %, поэтому любой шифротекст, в котором одни из букв встречаются столь же часто, является, вполне возможно, немецким. После того, как вы определили язык, для выполнения частотного анализа вам следует воспользоваться соответствующей таблицей частотности букв для данного языка. Если у вас есть нужная таблица частотности букв, то нередко удастся дешифровать даже шифротексты на неизвестном языке.

(2) Если установлена взаимосвязь с английским языком, то, как часто и происходит, сразу же открытый текст не появляется, тогда обратите внимание на пары повторяющихся букв. В английском языке чаще всего повторяющимися буквами будут **ss, ee, tt, ff, ll, mm** и **oo**. Если в шифротексте имеются какие-либо повторяющиеся символы, то вы можете считать, что они представляют собой одну из этих пар.

(3) Если в шифротексте имеются пробелы между словами, то постарайтесь определить слова, состоящие из одной, двух или трех букв. Единственными словами в английском языке, состоящими из одной буквы, являются **a** и **I**. Чаще всего встречающимися двухбуквенными словами будут **of, to, in, it, is, be, as, at, so, we, he, by, or, on, do, if, me, my, up, an, go, no, us, am**. Наиболее часто появляющиеся трехбуквенные слова – **the** и **and**.

(4) Если удастся, подготовьте таблицу частотности букв для сообщения, которое вы стараетесь дешифровать. Например, в военных донесениях стремятся опускать местоимения и артикли, и отсутствие таких слов, как **I**, **he**, **a** и **the**, будет снижать частотность некоторых из чаще всего встречающихся букв.

Вышесказанное иллюстрируется задачами 23 и 24, см. ниже.

Если вы знаете, что работаете с военным донесением, вам следует использовать таблицу частотности букв, созданную на основе других военных донесений.

(5) Одно из самых полезных для криптоаналитика умений – это способность благодаря собственному опыту или чисто интуитивно – распознавать слова или даже целые фразы. Аль-Халил, один из первых арабских криптоаналитиков, продемонстрировал свои способности, когда взломал греческий шифр-текст. Он предположил, что шифр-текст начинается с приветствия «Во имя Бога». Установив, что эти буквы соответствуют определенному фрагменту шифр-текста, он смог использовать их в качестве лома и раскрыть остальной шифро-текст. Это получило название «*криб*».

(6) В некоторых случаях наиболее часто встречающейся буквой в шифро-тексте может быть **E**, следующей по частоте появления – **T** и т. д. Другими словами, частотность букв в шифро-тексте уже совпадает с частотностью букв в таблице. По-видимому, буква **E** в шифротексте является действительно **e**, и то же самое, похоже, справедливо и для других букв, и все же шифр-текст выглядит тарабарщиной. В этом случае вы столкнулись не с шифром замены, а с шифром перестановки. Все буквы остались теми же самими, но находятся они не на своих местах.

Таблица 5

Сочетаемость букв английского языка

Г	С	Слева		Справа	Г	С
19	81	l,c,d,m,n,s,w,t,r,e,h	A	n,t,s,r,l,d,c,m	6	94
55	45	y,b,n,t,u,d,o,s,a,e	B	e,l,u,o,a,y,b,r	70	30
61	39	u,o,s,n,a,i,l,e	C	h,o,e,a,i,t,r,l,k	59	41
52	48	r,i,l,a,n,e	D	e,i,t,a,o,u	54	46

Г	С	Слева		Справа	Г	С
8	92	c,b,e,m,v,d, s,l,n,t,r,h	E	r,d,s,n,a,t,m,e, c,o	21	79
69	31	s,n,f,d,a,i,e,o	F	t,o,e,i,a,r,f,u	52	48
36	64	o,d,u,r,i,e,a,n	G	e.h.o.r.a.t.f.w. i.s	42	58
7	93	g,e,w,s,c,t	H	e,a,i,o	90	10
13	87	f,m,w,e,n,l,d,s,r,h,t	I	n,t,s,o,c,r,e, m,a,l	17	83
28	72	y,w,t,s,n,e,c,b,a,c	J	u,o,a,e,m,w	88	12
53	47	y,u,i,n,a,r,o,c	K	e,i,n,a,t,s	68	32
52	48	m,p,t,i,b,u,o,e,l,a	L	e,i,y,o,a,d,u	65	35
69	31	s,d,m,r,i,a,o,e	M	e,a,o,i,p,m	71	29
89	11	u,e,o,a,i	N	d,t,g,e,a,s,o, i,c	32	68
21	79	o,d,l,p,h,n,e,c,f,s,i, r,t	O	n,f,r,u,t,m,l,s, w,o	18	82
47	53	r,l,t,n,i,p,m,a,o,u,e,s	P	o,e,a,r,l,u,p,t, i,s	59	41
20	80	o,n,l,e,d,r,s	Q	u	100	0
70	30	p,i,u,t,a,o,e	R	e,o,a,t,i,s,y	61	39
48	52	d,t,o,u,r,n,s,i,a,e	S	t,e,o,i,s,a,h,p, u	41	59
43	57	u,o,d,t,f,e,i,n,s,a	T	h,i,o,e,a,t,r	38	62
35	65	p,f,t,l,b,d,s,o	И	n,s,t,r,l,p,b,c	8	92
88	12	r,u,o,a,i,e	V	e,i,o,a	99	1
48	52	g,d,y,n,s,t,o,e	W	a,h,i,e,o,n	80	20
95	5	u,n,i,e	X	p,t,i,a,u,c,k,o	38	62
24	76	b,n,a,t,e,r,l	Y	a,o,s,t,w,h,i,e, d,m	38	62
88	12	o,n,a,i	Z	e,i,w	86	14

Таблица 6

Частоты биграмм английского языка

Часть 1

	A	B	C	D	E	F	G	H	I	J	K	L	M
A	4	20	28	52	2	11	28	4	32	4	6	62	23
B	13	0	0	0	55	0	0	0	8	2	0	22	0
C	32	0	7	1	69	0	0	33	17	0	10	9	1
D	40	16	9	5	65	18	3	9	56	0	1	4	15
E	84	20	55	125	51	40	19	16	50	1	4	55	54
F	19	3	5	1	19	21	1	3	30	2	0	11	1
G	20	4	3	2	35	1	3	15	18	0	0	5	1
H	101	1	3	0	270	5	1	6	57	0	0	0	3
I	40	7	51	23	25	9	11	3	0	0	2	38	25
J	3	0	0	0	5	0	0	0	1	0	0	0	0
K	1	0	0	0	11	0	0	0	13	0	0	0	0
L	44	2	5	12	62	7	5	2	42	1	1	53	2
M	52	14	1	0	64	0	0	3	37	0	0	0	7

Часть 2

	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	167	2	14	0	83	76	127	7	25	8	1	9	1
B	0	11	0	0	15	4	2	13	0	0	0	15	0
C	0	50	3	0	10	0	28	11	0	0	0	3	0
D	6	16	4	0	21	18	53	19	5	15	0	3	0
E	146	35	37	6	191	149	65	9	26	31	12	5	0
F	0	51	0	0	26	8	47	6	3	3	0	2	0
G	4	21	1	1	20	9	21	9	0	5	0	1	0
H	2	44	1	0	3	10	18	6	0	5	0	3	0
I	202	56	12	1	46	79	117	1	22	0	4	0	3

Продолжение табл. 6.

	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
J	0	4	0	0	0	0	0	3	0	0	0	0	0
K	2	2	0	0	0	6	2	1	0	2	0	1	0
L	2	25	1	1	2	16	23	9	0	1	0	33	0
M	1	17	18	1	2	12	3	8	0	1	0	2	0

Часть 3

	A	B	C	D	E	F	G	H	I	J	K	L	M
N	42	10	47	122	63	19	106	12	30	1	6	6	9
O	7	12	14	17	5	95	3	5	14	0	0	19	41
P	19	1	0	0	37	0	0	4	8	0	0	15	1
Q	0	0	0	0	0	0	0	0	0	0	0	0	0
R	83	8	16	23	169	4	8	8	77	1	10	5	26
S	65	9	17	9	73	13	1	47	75	3	0	7	11
T	57	22	7	1	76	5	2	330	126	1	0	14	10
U	11	5	9	6	9	1	6	0	9	0	1	19	5
V	7	0	0	0	72	0	0	0	28	0	0	0	0
W	36	1	1	0	38	0	0	33	36	0	0	4	1
X	1	0	2	0	0	1	0	0	3	0	0	0	0
Y	14	5	4	2	7	12	2	6	10	0	0	3	7
Z	1	0	0	0	4	0	0	0	0	0	0	0	0

Часть 4

	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
N	7	54	7	1	7	44	124	6	1	15	0	12	0
O	134	13	23	0	91	23	42	55	16	28	0	4	1
P	0	27	9	0	33	14	7	6	0	0	0	0	0
Q	0	0	0	0	0	0	0	17	0	0	0	0	0
R	16	60	4	0	24	37	55	6	11	4	0	28	0
S	12	56	17	6	9	48	116	35	1	28	0	4	0
T	6	79	7	0	49	50	56	21	2	27	0	24	0
U	31	1	15	0	47	39	31	0	3	0	0	0	0
V	0	5	0	0	0	0	0	0	0	0	0	3	0
W	8	15	0	0	0	4	2	0	0	1	0	0	0
X	0	1	5	0	0	0	3	0	0	1	0	0	0
Y	5	17	3	0	4	16	30	0	0	5	0	0	0
Z	0	0	0	0	0	0	0	0	0	0	0	0	0

4. ШИФР ВИЖЕНЕРА

Наиболее известными являются шифры замены или подстановки, особенностью которых является замена символов (или слов, или других частей сообщения) открытого текста соответствующими символами, принадлежащими алфавиту шифротекста. Различают *одноалфавитную* и *многоалфавитную* замену. Вскрытие одноалфавитных шифров основано на учете частоты появления отдельных букв или их сочетаний (биграмм, триграмм и т. п.) в данном языке. Классические примеры вскрытия таких шифров содержатся в рассказах Э. По "Золотой жук" и А. Конан Дойла "Пляшущие человечки".

Примером многоалфавитного шифра замены является так называемая *система Виженера*. Шифрование осуществляется по таблице, представляющей собой квадратную матрицу размерностью $n \times n$, где n – число символов используемого алфавита. На рис. 4 показана таблица Виженера для русского языка (алфавит Z_{32} – 32 буквы и пробел). Первая строка содержит все символы алфавита. Каждая следующая строка получается из предыдущей циклическим сдвигом последней на символ влево.

Выбирается ключ или ключевая фраза. После этого процесс зашифровывания осуществляется следующим образом. Под каждой буквой исходного сообщения последовательно записываются буквы ключа; если ключ оказался короче сообщения, его используют несколько раз. Каждая буква шифротекста находится на пересечении столбца таблицы, определяемого буквой открытого текста, и строки, определяемой буквой ключа. Пусть, например, требуется зашифровать сообщение:

ГРУЗИТЕ АПЕЛЬСИНЫ БОЧКАМИ ТЧК БРАТЬЯ
КАРАМАЗОВЫ ТЧК

[illegible]

Рис. 4. Таблица Виженера для алфавита Z_{32}

С помощью ключа ВЕНТИЛЬ запишем строку исходного текста с расположенной под ней строкой с циклически повторяемым ключом:

ГРУЗИТЕ АПЕЛЬСИНЫ БОЧКАМИ ТЧК БРАТЬЯ
КАРАМАЗОВЫ ТЧК

ВЕНТИЛЬВЕНТИЛЬВЕНТИЛЬВЕНТИЛЬВЕНТИЛЬВЕНТ
ИЛЬВЕНТИЛЬВЕ

В результате зашифрования, начальный этап которого показан на рис. 5, получим шифр-текст:

ЕХЩРЭАБЕЫЧУДККТИСЙЩРМЕЩЬЗЭРМДОБИЭУАД
ЧТШЛЕВМЪФГКЛЩП

ГРУЗИТЕ АПЕЛЬСИНЫ БОЧКАМИ

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

Рис. 5. Принцип шифрования по таблице Виженера

Расшифровывание осуществляется следующим образом. Под буквами шифротекста последовательно записываются буквы ключа; в строке таблицы, соответствующей очередной букве ключа, происходит поиск соответствующей буквы шифротекста. Находящаяся над ней в первой строке таблицы буква является соответствующей буквой исходного текста.

Для увеличения надежности шифра можно рекомендовать его использование после предварительной псевдослучайной перестановки букв в каждой строке таблицы. Возможны и другие модификации метода.

Теория криптоанализа шифра Виженера (изложение по [5]).

Рассмотрим шифр модульного гаммирования с уравнением

$$b_i = (a_i + y_i) \bmod n,$$

для которого гамма является периодической последовательностью знаков алфавита. Такая гамма обычно получается периодическим повторением некоторого ключевого слова. Например, ключевое слово КЕУ дает гамму КЕУКЕУКЕУ... . Рассмотрим задачу вскрытия такого шифра по тексту одной криптограммы достаточной длины.

Пусть μ – длина ключевого слова. Обычно криптоанализ шифра Виженера проводится в два этапа. На первом этапе определяется число μ , на втором этапе – само ключевое слово.

Для определения числа μ применяется так называемый *тест Казиски*, названный в честь Ф. Казиски, применившего его в 1863 г. Тест основан на простом наблюдении того, что два одинаковых отрезка открытого текста, отстоящих друг от друга на расстоянии, кратном μ , будут одинаково зашифрованы. В силу этого в шифротексте ищутся повторения длины, не меньшей трех и расстояния между ними. Обратим внимание на то, что случайно такие одинаковые отрезки могут появиться в тексте с достаточно малой вероятностью.

Пусть $d_1, d_2, \dots$ – найденные расстояния между повторениями и d – наибольший общий делитель этих чисел. Тогда μ должно делить d . Чем больше повторений имеет текст, тем более вероятно, что μ совпадает с d . Для уточнения значения μ , можно использовать так называемый «индекс совпадения», введенный в практику У. Фридманом в 1920 г.

Для строки $x = (x_1, \dots, x_m)$ длины m , составленной из букв алфавита A , индексом совпадения в x , обозначаемым $I_c(x)$ будем называть вероятность того, что две случайно выбранные буквы из x совпадают.

Пусть $A = \{a_1, \dots, a_n\}$. Будем отождествлять буквы алфавита с числами, так что

$$a_1 \equiv 0, \dots, a_{n-1} \equiv n-2, a_n \equiv n-1.$$

Теорема: Индекс совпадения в x вычисляется по формуле

$$I_c(x) = \frac{\sum_{i=0}^{n-1} f_i(f_i - 1)}{m(m-1)}, \quad (1)$$

где f_i – число вхождений буквы a_i в x , $i \in Z_n$.

Доказательство: Будем вычислять $I_c(x)$ как отношение числа благоприятных исходов к общему числу исходов. Благоприятным является исход, при котором на выбранных двух позициях в x расположены одинаковые буквы. Общее число исходов равно, очевидно, C_m^2 . Число благоприятных исходов есть

$$\sum_{i=0}^{m-1} C_{f_i}^2. \quad (2)$$

Переупорядочим буквы в x таким образом, чтобы сначала шли f_{a_1} букв a_1 , затем f_{a_2} букв a_2 и т. д.:

$$\underbrace{a_1, \dots, a_1}_{f_{a_1}} \dots \underbrace{a_n, \dots, a_n}_{f_{a_n}}. \quad (3)$$

Теперь заметим, что при случайном выборе мест (i и j) в строке x благоприятными являются следующие исходы:

$$\begin{aligned} (a_1) & \left\{ \begin{array}{l} 0 \dots i \dots j \dots m-1 \\ \dots a_1 \dots a_1 \dots \end{array} \right. \\ (a_2) & \left\{ \begin{array}{l} 0 \dots i \dots j \dots m-1 \\ \dots a_2 \dots a_2 \dots \end{array} \right. \\ \hline (a_n) & \left\{ \begin{array}{l} 0 \dots i \dots j \dots m-1 \\ \dots a_n \dots a_n \dots \end{array} \right. \end{aligned}$$

В случае (a_1) мы можем выбрать пару букв a_1 из набора (3) $C_{f_{a_1}}^2$ способами, в случае (a_2) пару букв a_2 из (3) – $C_{f_{a_2}}^2$ способами и т. д.

Таким образом, общее число благоприятных исходов выражается величиной (2), а индекс совпадения в x – формулой

$$I_c(x) = \frac{\sum_{i=0}^{m-1} C_{f_i}^2}{C_m^2}$$

и, следовательно, формулой (1).

Пусть x – строка осмысленного текста (например, английского). Допустим, как и ранее, что буквы в x появляются на любом месте текста с соответствующими вероятностями $p_0, \dots, p_{n-1}$ независимо друг от друга, где p_i – вероятность появления буквы i в осмысленном тексте, $i \in Z_n$. В такой модели открытого текста вероятность того, что две случайно выбранные буквы из x совпадают с $i \in Z_n$ равна p_i^2 следовательно,

$$I_c(x) \approx \sum_{i=0}^{n-1} p_i^2. \quad (4)$$

Взяв за основу значения вероятностей p_i для открытых текстов на английском языке, получаем приближение $\sum_{i=0}^{25} p_i^2 \approx 0,066$.

Тем самым для английских текстов x можно пользоваться следующим приближением для индекса совпадения:

$$I_c(x) \approx 0,066.$$

Аналогичные приближения можно получить и для других языков. Так, для русского языка получаем приближение:

$$I_c(x) \approx 0,053.$$

Приведем значения индексов совпадения для ряда европейских языков:

Таблица 7

Индексы совпадения европейских языков

Язык	Русский	Англ.	Франц.	Нем.	Итал.	Испан.
$I_c(x) \approx$	0,0529	0,0662	0,0778	0,0762	0,0738	0,0775

Рассуждения, использованные при выводе формулы (4), остаются, очевидно, справедливыми и в случае, когда x – результат зашифровывания некоторого открытого текста простой заменой. В этом случае вероятности p_i переставляются местами, но сумма $\sum_{i=0}^{n-1} p_i^2$ остается неизменной.

Предположим, что x – реализация независимых испытаний случайной величины, имеющей равномерное распределение на Z_n . Тогда индекс совпадения вычисляется по формуле

$$I_c(x) = \sum_{i=0}^{n-1} \frac{1}{n^2} = n \cdot \frac{1}{n^2} = \frac{1}{n}.$$

Вернемся к вопросу об определении числа μ .

Пусть $y = y_1 y_2 \dots y_n$ – данный шифротекст. Выпишем его с периодом μ :

$$\begin{array}{cccc} Y_1^\downarrow & Y_2^\downarrow & \dots & Y_\mu^\downarrow \\ \hline y_1 & y_2 & \dots & y_\mu \\ y_{\mu+1} & y_{\mu+2} & \dots & y_{2\mu} \\ y_{2\mu+1} & y_{2\mu+2} & \dots & y_{3\mu} \\ \dots & \dots & \dots & \dots \end{array},$$

и обозначим столбцы получившейся таблицы через $Y_1^\downarrow, \dots, Y_\mu^\downarrow$. Если μ – это истинная длина ключевого слова, то каждый столбец $Y_i^\downarrow, i \in 1, \dots, \mu$, представляет собой участок открытого текста, зашифрованный простой заменой, определяемой подстановкой

$$\begin{pmatrix} 0 & 1 & 2 & \dots & n-s & \dots & n \\ s & s+1 & s+2 & \dots & 0 & \dots & s-1 \end{pmatrix} \quad (5)$$

для некоторого $s \in 0, n-1$ (числа берутся по модулю n).

В силу сказанного выше (для английского языка) $I_c(Y_i^\downarrow) \approx 0,066$ при любом i . С другой стороны, если μ отлично от длины ключевого слова, то столбцы $Y_i^\downarrow$ будут более "случайными", поскольку они являются результатом зашифровывания фрагментов открытого текста некоторым многоалфавитным шифром. Тогда $I_c(Y_i^\downarrow)$ будет ближе (для английского языка) к числу $1/28 \approx 0,038$.

Заметная разница значений $I_c(x)$ для осмысленных открытых текстов и случайных последовательностей букв (для английского языка – 0,066 и 0,038, для русского языка – 0,053 и 0,030) позволяет в большинстве случаев установить точное значение μ .

Предположим, что на первом этапе мы нашли длину ключевого слова. Рассмотрим теперь вопрос о нахождении самого ключевого слова. Для его нахождения можно использовать так называемый *взаимный индекс совпадения*.

Пусть $x = (x_1, \dots, x_n), y = (y_1, \dots, y_m)$ – две строки букв алфавита A . Взаимным индексом совпадения x и y , обозначаемым $MI_c(x, y)$, называется вероятность того, что случайно выбранная буква из x совпадает со случайно выбранной буквой из y .

Пусть $f_0, f_1, \dots, f_n$ и $f^1_0, f^1_1, \dots, f^1_{n-1}$ – числа вхождений букв алфавита в x и y соответственно.

Теорема: *Взаимный индекс совпадения в x и y вычисляется по формуле* (эта теорема доказывается точно так же, как и предыдущая теорема.)

$$MI_c(x, y) = \frac{\sum_{i=0}^{n-1} f_i \cdot f^1_i}{m \cdot m'}. \quad (6)$$

Пусть $k = (k_1, \dots, k_r)$ – истинное ключевое слово. Попытаемся оценить индексы $MI_c(Y^{\downarrow}_i, Y^{\downarrow}_j)$.

Для этого напомним, что $Y^{\downarrow}_z$ является результатом зашифрования фрагмента открытого текста простой заменой, определяемой подстановкой (5) при некотором s . Вероятность того, что $Y^{\downarrow}_i$ и $Y^{\downarrow}_j$ – произвольная пара букв равна 0, имеет вид $p_{n-s_i} * p_{n-s_j}$ (где p_a – вероятность появления буквы a в открытом тексте); вероятность того, что обе буквы есть 1, равна $p_{n-s_i+1} * p_{n-s_j+1}$ и т. д. На основании этого получаем

$$MI_c(Y^{\downarrow}_i, Y^{\downarrow}_j) \approx \sum_{h=0}^{n-1} p_{h-s_i} \cdot p_{h-s_j} = \sum_{h=0}^{n-1} p_h \cdot p_{h+(s_i-s_j)}.$$

Заметим, что сумма в правой части последнего равенства зависит только от разности $(s_i - s_j) \bmod n$, которую назовем *относительным сдвигом* $Y^{\downarrow}_i$ и $Y^{\downarrow}_j$. Заметим также, что

$$\sum_{j=0}^{n-1} p_j \cdot p_{(j+s) \bmod n} = \sum_{j=0}^{n-1} p_j \cdot p_{(j-s) \bmod n}, \quad (7)$$

поэтому $Y_i^{\downarrow}$ и $Y_j^{\downarrow}$ с относительными сдвигами s и $n-s$ имеют одинаковые взаимные индексы совпадения. Приведем таблицу значений сумм (7) для английского языка:

Таблица 8

Взаимный индекс совпадения при сдвиге s

Сдвиг s	0	1	2	3	4	5	6
$MI_c(x, y) \approx$	0,066	0,039	0,032	0,034	0,044	0,033	0,036
Сдвиг s	7	8	9	10	11	12	13
$MI_c(x, y) \approx$	0,039	0,034	0,034	0,038	0,045	0,039	0,043

Обратим внимание на то, что ненулевые "сдвиги" дают взаимные индексы совпадения, изменяющиеся в пределах от 0,032 до 0,045, в то время как при нулевом сдвиге индекс $MI_c(x, y)$ близок к 0,066. Это наблюдение позволяет определить величины относительных сдвигов $s_i - s_j$ столбцов $Y_i^{\downarrow}$ и $Y_j^{\downarrow}$. Для этого заметим, что при некотором значении $s(i, j) \in 0, n-1$ столбец $Y^{s(i, j)\downarrow}_j$, полученный из $Y_j^{\downarrow}$ прибавлением к каждому его элементу числа $S(i, j)$ (по модулю n), имеет нулевой относительный сдвиг с $Y_i^{\downarrow}$.

Пусть $Y^{0\downarrow}_j, Y^{1\downarrow}_j, \dots, Y^{n-1\downarrow}_j$ – результаты зашифровывания $Y_j^{\downarrow}$ каждой из простых замен (5). Несложно вычислить взаимные индексы

$$MI_c(Y_i^{\downarrow}, Y_j^{\downarrow}), \quad 0 \leq s \leq n-1, \quad 1 \leq i < j \leq \mu,$$

(всего, таким образом, имеется $C^2 n$ значений). Для этого воспользуемся формулой, полученной из (6):

$$MI_c(Y_i^{\downarrow}, Y_j^{s\downarrow}) = \frac{\sum_{h=0}^{n-1} f_h \cdot f_{h-s}^1}{m \cdot m'}.$$

Если s равно $s_i - s_j$ (относительному сдвигу $Y_i^{\downarrow}$ и $Y_j^{\downarrow}$), то взаимный индекс впадения должен быть (для английского языка) близок к 0,066, так как относительный сдвиг $Y_i^{\downarrow}$ и $Y_j^{\downarrow}$ равен нулю. Если же s не равно $s_i - s_j$, то взаимный индекс совпадения должен колебаться в пределах 0,032 – 0,045.

Используя изложенный метод, мы сможем связать системой уравнений относительные сдвиги различных пар столбцов Y_i^l и Y_j^l . В результате останется 26 (для английского языка) вариантов для ключевого слова, из которых можно выбрать наиболее предпочтительный вариант (если ключевое слово является осмысленным).

Следует отметить, что предложенный метод будет эффективным для не слишком больших значений μ . Это объясняется тем, что для хороших сближений индексов совпадения требуются тексты достаточно большой длины.

Пример криптоанализа текста:

Задача 21 [16]: Дан текст, зашифрованный шифром Виженера, требуется определить ключевое слово и прочитать открытый текст.

Шифрованный текст:

Влцдугжбюцхърмшбрхцзооэцг**брь**цмйфктъьюмшсэяцпу-
нуяшцтаъдци**бь**гбрпачкъуцпъбьсэгкцъгуушарцёвърюуююэкааэ
брняфукабъарпябъкиъжяффнйояфывбнэнфуюг**брь**сшьжэтбэёч
юьюрьегофкбъчябашвъэуъьюаднчжчужцёвлрнчулбюпцурунь
ъшсэюъзкцхяррнрювяспэмасчкпэужъжыатуфуярюравртубурьп
эщлафоуфбюацмнубсюкйтаъэдийонооэгюожбгкбрънцэпотчмёод
зцвбцшщвщепчдчдрьююскасэгъппэгюкдойрсрэвоопчщоказръб
бнэугнялёкъсрбёуыэбдэулбюасшоуэтьшкрсдугэфлбубуъчнчтрт
пэгюкиугюэмэгюккъьпэгяпуфуэзьрадзьчнюрмфцхраююанчё
чюыхъьцомэфъцпоирькнщпэтэузуябашушбаыэйчдфрпэцърь
ыцъцпоилуфэдцойэдыттрачкубунфнтаъэдкцкрннцноабугюуу-
бурьпйюэъжтгюркуюощоуфъэгясуючщшцдцсфырэдщэуя-
фшёчцойршвахвмкршрпгюопэуцйттаъэдкци**брь**цыяжтюрбуэтэ-
бдущэубъибрювъагибргаббрымпуноцшяжцечкфод-
щоъчжшйуъцхчшвуэбдлдьэгясуахзцбдэульк-
нъщбжяцърьёдьвъювлрнуяфуоухфекыгцччгэъжтанопчынажпа
чкъуъмэкйрэфшцъьбудэндадьярьёюэлэтчоубъцэфэвлнё-
эгфдсэвъэкбсчоукгаутэьпубццкпэгю чсаъбэнэфъркацхёва-
етфяепьрювър жадфёжбъфующоявъьгупчршuiteачйчирам-
чюфчоуяюонкяжык гсцбръсшйотъжрщцл

Решение: Для определения числа букв в данном ключевом слове применяется так называемый *тест Казиски*. Тест основан на простом наблюдении того, что два одинаковых отрезка открытого текста, отстоящих друг от друга на расстоянии, кратном μ (количество букв в слове), будут одинаково зашифрованы. В силу этого в шифротексте ищутся повторения длины не меньшей трех, и расстояния между ними. Необходимо обратить внимание на то, что случайно такие одинаковые отрезки могут появиться в тексте с достаточно малой вероятностью.

В данном тексте обнаружено четырехкратное повторение буквосочетания «брь». Выясним расстояние между ними и найдем наибольший общий делитель этих расстояний.

В результате получаем 35, 85, 510, их НОД = 5.

Следовательно, с определенной долей вероятности можно заключить, что длина кодового слова равна 5.

Для подтверждения гипотезы воспользуемся математической статистикой для определения длины ключевого слова. Для этого запишем шифротекст в таблицу с 5 столбцами, предполагая, что длина ключевого слова равна 5.

Вычислим взаимные индексы совпадения $I_C(x)$ букв в каждом из столбцов таблицы, для достоверного установления длины ключевого слова. Для этого посчитаем частоту повторения букв в каждом столбце. Таблица состоит из 5 столбцов, так как на предыдущем этапе нами было установлено, что ключевое слово по НОД может состоять из 5 букв.

Таблица к задаче 21

Y1	Y2	Y3	Y4	Y5
В	л	ц	д	у
Т	ж	б	ю	ц
Х	ъ	я	р	р
М	ш	б	р	х
Ц	э	о	о	э
Ц	г	б	р	ь
Ц	м	й	ф	к
Т	ъ	ъ	ю	ь
М	ш	э	с	я

Продолжение табл. к задаче 21

Y1	Y2	Y3	Y4	Y5
Ц	п	у	н	у
Я	щ	э	й	т
А	ь	э	д	к
Ц	и	б	р	ь
Ц	г	б	р	п
А	ч	к	ъ	у
Ц	п	ъ	б	ь
С	э	г	к	ц
Ъ	г	у	у	щ
А	р	ц	ё	э
В	ъ	р	ю	у
О	ю	э	к	а
А	э	б	р	н
Я	ф	у	к	а
Б	ъ	а	р	п
Я	ъ	а	ф	к
Ъ	и	ь	ж	я
Ф	ф	н	й	о
Я	ф	ы	в	б
Н	э	н	ф	у
Ю	г	б	р	ь
С	ш	Ь	ж	э
Т	б	э	ё	ч
Ю	ъ	ю	р	ъ
Е	г	о	ф	к
Б	ь	ч	я	б
А	ш	в	ё	э
У	ъ	ъ	ю	а
Д	н	ч	ж	ч
У	ж	ц	ё	э
В	л	р	н	ч
У	л	б	ю	п
Ц	у	р	у	н
Ь	ъ	Ш	с	э
Ю	ъ	З	к	ц
Х	ъ	Я	р	р
Н	р	Ю	в	я

Продолжение табл. к задаче 21

Y1	Y2	Y3	Y4	Y5
С	п	Э	м	а
С	ч	К	п	э
У	ж	Ь	ж	ы
А	т	У	ф	у
Я	р	Ю	р	а
В	р	Т	у	б
У	р	Ь	п	э
Щ	л	А	ф	о
У	ф	Б	ю	а
Ц	м	Н	у	б
С	ю	К	й	т
А	ь	Э	д	й
Ю	н	О	о	э
Г	ю	О	ж	б
Г	к	Б	р	ъ
Н	ц	Э	п	о
Т	ч	М	ё	о
Д	з	Ц	в	б
Ц	ш	Щ	в	щ
Е	п	Ч	д	ч
Д	р	Ъ	ю	ь
С	к	А	с	э
Г	ъ	П	п	э
Г	ю	К	д	о
Й	р	С	р	э
В	о	О	п	ч
Щ	ш	О	к	а
З	р	Ъ	б	б
Н	э	У	г	н
Я	л	Ё	к	ь
С	р	Б	ё	у
Ы	э	Б	д	э
У	л	Б	ю	а
С	ш	О	у	э
Т	ъ	Ш	к	р
С	д	У	г	э

Продолжение табл. к задаче 21

Y1	Y2	Y3	Y4	Y5
Ф	л	Б	у	б
У	ъ	Ч	н	ч
Т	р	Т	п	э
Г	ю	К	и	у
Г	ю	Э	м	э
Г	ю	К	к	ъ
Ъ	п	Э	г	я
А	п	У	ф	у
Э	з	Ь	р	а
Д	з	Ь	ж	ч
Ю	р	М	ф	ц
Х	р	А	ю	ю
А	н	Ч	ё	ч
Ю	ъ	Ы	х	ь
Ъ	ц	О	м	э
Ф	ъ	Ц	п	о
И	р	Ь	к	н
Щ	п	Э	т	э
У	з	У	я	б
А	щ	У	щ	б
А	ы	Э	й	ч
Д	ф	Р	п	э
Ц	ъ	Ь	р	ь
Ц	ъ	Ц	п	о
И	л	У	ф	э
Д	ц	О	й	э
Д	я	Т	р	р
А	ч	К	у	б
У	ф	Н	й	т
А	ь	Э	д	к
Ц	к	Р	н	н
Ц	ю	А	б	у
Г	ю	У	у	б
У	р	Ь	п	й
Ю	э	Ъ	ж	т
Г	ю	Р	к	у

Продолжение табл. к задаче 21

Y1	Y2	Y3	Y4	Y5
Ю	щ	О	ъ	у
Ф	ъ	Э	г	я
С	у	О	и	ч
Щ	щ	Ч	д	ц
С	ф	Ы	р	э
Д	щ	Э	ъ	у
Я	ф	Ш	ё	ч
Ц	ю	Й	р	щ
В	я	Х	в	м
К	р	Ш	р	п
Г	ю	О	п	э
У	ц	Ч	й	т
А	ь	Э	д	к
Ц	и	Б	р	ь
Ц	ы	Я	ж	т
Ю	р	Б	у	э
Т	э	Б	д	у
Я	щ	Э	у	б
Ъ	и	Б	р	ю
В	ъ	Е	ж	а
Г	и	Б	р	б
А	г	Б	р	ы
М	п	У	н	о
Ц	ш	Я	ж	ц
Е	ч	К	ф	о
Д	щ	О	ъ	ч
Ж	ш	Й	у	ъ
Ц	х	Ч	щ	в
У	э	Б	д	л
Д	ъ	Э	г	я
С	у	А	х	з
Ц	э	Б	д	э
У	л	Ь	к	н
Ъ	щ	Б	ж	я
Ц	э	Ь	р	ё
Д	ъ	Ь	в	ю

Продолжение табл. к задаче 21

Y1	Y2	Y3	Y4	Y5
В	л	Р	н	у
Я	ф	У	о	у
Х	ф	Е	к	ь
Г	ц	Ч	ч	ч
Г	э	Ъ	ж	т
А	н	О	п	ч
Ы	н	А	ж	п
А	ч	К	ъ	у
Ъ	м	Э	н	к
Й	р	Э	ф	щ
Э	ь	Ь	б	у
Д	э	Н	д	а
Д	ь	Я	р	ь
Е	ю	Э	л	э
Т	ч	О	у	б
Ъ	ц	Э	ф	э
В	л	Н	ё	э
Г	ф	Д	с	э
В	э	Ё	к	б
С	ч	О	у	к
Г	а	У	т	э
Ы	п	У	б	б
Ц	ч	К	п	э
Г	ю	Ч	с	а
Ъ	б	Э	н	э
Ф	ь	Р	к	а
Ц	х	Ё	в	а
Е	т	У	ф	я
Е	п	Ь	р	ю
В	ь	Р	ж	а
Д	ф	Ё	ж	б
Ь	ф	У	т	о
Щ	о	Я	в	ь
Ъ	г	У	п	ч
Р	ш	У	и	т
Е	а	Ч	й	ч

Продолжение табл. к задаче 21

Y1	Y2	Y3	Y4	Y5
И	р	А	м	ч
Ю	ф	Ч	о	у
Я	ю	О	н	к
Я	ж	Ы	к	г
С	ц	Б	р	я
С	ш	Ч	й	о
Т	ъ	Ъ	ж	р
С	щ	Ч	л	

Частота повторения букв в столбцах: 1-й столбец (общее количество букв $m = 198$).

Обозначение	а	б	в	г	д	е	ё	ж	з	и	й	к	л
Количество	17	2	10	16	14	7	0	1	1	3	2	1	0
Обозначение	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш
Количество	3	4	1	0	1	16	9	14	5	5	23	0	0
Обозначение	щ	ъ	ы	ь	э	ю	я						
Количество	5	10	3	2	2	10	11						

$$I_c(x) = \frac{\sum_{i=0}^{n-1} f_i(f_i - 1)}{m(m-1)} = \frac{272 + 2 + 90 + 240 + 182 + 42 + 6 + 2 + 6 + 12 + 240 + 72 + 182 + 20 + 20 + 506 + 20 + 90 + 6 + 2 + 2 + 90 + 110}{198 * 197} = 0,05676 ;$$

2-й столбец (общее количество букв $m = 198$)

Обозначение	а	б	в	г	д	Е	ё	ж	з	и	й	к	л
Количество	2	2	0	7	1	0	0	4	4	5	0	3	11
Обозначение	м	н	о	п	р	С	т	у	ф	х	ц	ч	ш
Количество	3	5	2	10	18	0	2	3	14	2	7	9	11
Обозначение	щ	ъ	ы	ь	э	Ю	я						
Количество	9	26	2	5	14	15	2						

3-й столбец (общее количество букв $m = 198$)

Обозначение	а	б	в	г	д	Е	ё	ж	з	и	й	к	л
Количество	9	24	1	1	1	2	4	0	1	0	3	10	0
Обозначение	м	н	о	п	р	С	т	у	ф	х	ц	ч	ш
Количество	2	6	17	1	9	1	3	19	0	1	6	14	4
Обозначение	щ	ъ	ы	ь	э	Ю	я						
Количество	1	8	4	14	23	3	6						

$$I_C(x) = \frac{\sum_{i=0}^{n-1} f_i(f_i - 1)}{m(m-1)} = \frac{72+552+2+12+6+90+2+30+272+72+6+342+30+182+12+56+12+182+506+6+30}{198 \cdot 197} = 0,0634$$

4-й столбец (общее количество букв $m = 198$)

Обозначение	а	б	в	г	д	Е	ё	ж	з	и	й	к	л
Количество	0	5	8	5	13	0	9	16	0	3	9	15	2
Обозначение	м	н	о	п	р	С	т	у	ф	х	ц	ч	ш
Количество	4	9	4	14	27	5	3	13	13	2	0	1	0
Обозначение	щ	ъ	ы	ь	э	Ю	я						
Количество	2	5	0	0	0	9	2						

$$I_C(x) = \frac{\sum_{i=0}^{n-1} f_i(f_i - 1)}{m(m-1)} = \frac{20+56+20+156+72+240+2+12+72+12+182+702+20+6+156+156+2+2+20+72+2}{198*197} = 0,0584$$

5-й столбец (общее количество букв $m = 197$)

Обозначение	а	б	в	г	д	Е	ё	ж	з	и	й	к	л
Количество	15	18	1	1	0	0	1	0	1	0	2	9	1
Обозначение	м	н	о	п	р	С	т	у	ф	х	ц	ч	ш
Количество	1	6	11	5	5	0	8	19	0	1	6	17	0
Обозначение	щ	ъ	ы	ь	э	Ю	я						
Количество	4	4	2	13	33	4	9						

$$I_C(x) = \frac{\sum_{i=0}^{n-1} f_i(f_i - 1)}{m(m-1)} = \frac{210 + 306 + 2 + 72 + 30 + 110 + 20 + 20 + 56 + 342 + 30 + 272 + 12 + 12 + 2 + 156 + 1056 + 12 + 72}{197 * 196} = 0,0723.$$

По полученным индексам совпадения можно сказать, что длина ключевого слова выбрана верно и равна 5.

После того, как мы нашли длину ключевого слова, проведем поиск его истинного значения. Для его нахождения можно использовать так называемый взаимный индекс совпадения

$$MI_c(x, y) = \frac{\sum_{i=0}^{n-1} f_i \cdot f_i^1}{m \cdot m'},$$

где f_i, f_i^1 – частота буквы i в столбцах Y_i, Y_i^1 соответственно;

m, m' – число букв в столбцах Y_i, Y_i^1 соответственно;

Так как каждый из столбцов таблицы является результатом зашифровывания фрагмента открытого текста простой заменой, определяемой подстановкой, то попытаемся оценить взаимные индексы совпадения.

Взаимный индекс совпадения значения ключевого слова для русского языка должен находиться в пределах 0,053–0,07. И для его вычисления предварительно необходимо определить относительный сдвиг всех столбцов относительно первого.

Сдвиг 2-го столбца на 6-й позиций

Обозначение	а	б	в	г	д	Е	ё	ж	з	и	й	к	л
Количество	26	2	5	14	15	2	2	2	0	7	1	0	0
Обозначение	м	н	о	п	р	С	т	у	ф	х	ц	ч	ш
Количество	4	4	5	0	3	11	3	5	2	10	18	0	2
Обозначение	щ	ъ	ы	ь	э	Ю	я						
Количество	3	14	2	7	9	11	9						

$$MI_c(Y1, Y2^6) = 0,05494$$

Сдвиг 3-го столбца на 3-й позиции

Обозначение	а	б	в	г	Д	е	ё	ж	з	и	й	к	л
Количество	23	3	6	9	24	1	1	1	2	4	0	1	0
Обозначение	м	н	о	п	Р	с	т	у	ф	х	ц	ч	ш
Количество	3	10	0	2	6	17	1	9	1	3	19	0	1
Обозначение	щ	ъ	ы	ь	Э	ю	я						
Количество	6	14	4	1	8	4	14						

$$MI_c(Y1, Y3^3) = 0,5798$$

Сдвиг 4-го столбца на 16 позиций

Обозначение	а	б	в	г	д	Е	ё	ж	з	и	й	к	л
Количество	27	5	3	13	13	2	0	1	0	2	5	0	0
Обозначение	м	н	о	п	р	С	т	у	ф	х	ц	ч	ш
Количество	0	9	2	0	5	8	5	13	0	9	16	0	3
Обозначение	щ	ъ	ы	ь	э	Ю	я						
Количество	9	15	2	4	9	4	14						

$$MI_c(Y1, Y4^{16}) = 0,06068.$$

Сдвиг 5-го столбца на 3-й позиции

Обозначение	а	б	в	г	д	Е	ё	ж	з	и	й	к	л
Количество	33	4	9	15	18	1	1	0	0	1	0	1	0
Обозначение	м	н	о	п	р	С	т	у	ф	х	ц	ч	ш
Количество	2	9	1	1	6	11	5	5	0	8	19	0	1
Обозначение	щ	ъ	ы	ь	э	Ю	я						
Количество	6	17	0	4	4	2	13						

$$MI_c(Y1, Y5^3) = 0,106045.$$

По взаимным индексам совпадения можно судить, что сдвиги между столбцами выбраны верно.

Составим уравнения для определения ключевого слова:

$$\begin{array}{lll}
 g[1]-g[2]=6 & g[1]=g[2] + 6 & g[2]=g[1] - 6 \\
 g[1]-g[3]=3 & g[1]=g[3] + 3 & g[3]=g[1] - 3 \\
 g[1]-g[4]=16 & g[1]=g[4] + 16 & g[4]=g[1] - 16 \\
 g[1]-g[5]=3 & g[1]=g[5] + 3 & g[5]=g[1] - 3
 \end{array}$$

Теперь только необходимо вычислить значение $g[1]$

$$\begin{array}{lll}
 g[1]=1: \text{быносю} & g[1]=2: \text{вьятя} & g[1]=3: \text{гэауа} \\
 g[1]=4: \text{дюбфб} & g[1]=5: \text{еявхв} & g[1]=6: \text{ёагцг} \\
 g[1]=7: \text{жбдчд} & g[1]=8: \text{звеше} & g[1]=9: \text{игёщё} \\
 g[1]=10: \text{йджъж} & g[1]=11: \text{кезыз} & g[1]=12: \text{лёйиы} \\
 g[1]=13: \text{мжйэй} & g[1]=14: \text{нзкюк} & g[1]=15: \text{оилаял} \\
 g[1]=16: \text{пйамм} & g[1]=17: \text{ркнбн} & g[1]=18: \text{«слово»} \\
 g[1]=19: \text{тмпгп} & g[1]=20: \text{унрдр} & g[1]=21: \text{фосес} \\
 g[1]=22: \text{хптёт} & g[1]=23: \text{цружу} & g[1]=24: \text{чсфзф} \\
 g[1]=25: \text{штхих} & g[1]=26: \text{щуцйц} & g[1]=27: \text{ъфчкч} \\
 g[1]=28: \text{ыхшлш} & g[1]=29: \text{ыцщмщ} & g[1]=30: \text{эчънъ} \\
 g[1]=31: \text{юшыоы} & g[1]=32: \text{ящъпъ} &
 \end{array}$$

Найдено одно ключевое слово «СЛОВО».

Расшифруем зашифрованный текст:

Разве быть здоровым то же самое что не быть больным? Определить, что такое здоровье, что такое болезнь, для нас физическое здоровье это состоит из способности и энергии заниматься тем, что нам необходимо, получать при этом удовольствие и не вызывать без всякой помощи из здоровья парадоксально, вы не можете непосредственно заставить себя стать здоровым, вам остается только наблюдать, затем как удивительная способность вашего организма исцелять себя, начинает действовать сама собой, и ваше богатство или бедность, жестокость или доброта, деятельность не имеют здесь по видимому, никакого значения, здоровье это нечто позитивное, оно не означает отказа от удовольствия, здоровье является естественным следствием нашего образа жизни, взаимоотношений, диеты, окружающей обстановки, здоровье это не предмет собственности, это процесс, это то, что мы делаем, результат наших мыслей и чувств, это образ существования, интересно, что на направление медицинских исследований все больше и больше отклоняется в сторону той области, которая досих пор считалась сферой деятельности психологов, сейчас уже трудно провести четкие границы, сближения между физическими и ментальными факторами заболеваний.

Ключевое слово верное, текст читается.

Замечание: Криптоанализ шифра Виженера является трудоемкой задачей для решения без использования программ. Лабораторный практикум, подготовленный авторами, содержит задачи, аналогичные представленной, для успешного решения этих задач предлагается программный инструментарий. Использование этого инструментария позволяет решать такие задачи за сравнительно короткое время.

5. РАЗНЫЕ ЗАДАЧИ

Как отмечалось ранее, при решении задач криптоанализа часто бывает необходимо учитывать особенности языка, на котором составлен открытый текст. Полезным является и знание способа перевода буквенного открытого текста в цифровую форму перед шифрованием. Следующие задачи, на наш взгляд, помогут развитию криптоаналитической интуиции:

а) задачи, которые условно можно назвать *лингвистическими*.

Задача 22 (Составлена по образцу задач 11.3, 12.2, 16.3 из [1]). Используется русский алфавит, Е и Ё не различаются. Буквы алфавита кодируются следующим образом: каждой букве ставится в соответствие двоичная запись её номера, начиная с нуля. Таким образом, А соответствует 00000, Б соответствует 00001, В соответствует 00010, ..., Ю – > 11110, Я – >11111. Для передачи используется пять проводов. По каждому передается соответствующий разряд пятизначного двоичного числа. При монтаже 5 проводов были перепутаны, и теперь мы не знаем, по какому проводу приходит цифра старшего разряда и т. д. Перед вами полученный текст. Известно, что исходный текст был осмысленным. Восстановите его.

Полученный текст: ЫАДАФЭС

Решение: Перепутывание проводов не могло изменить количество единиц в двоичной записи буквы. Поэтому вторая и четвертая буквы исходного текста находятся сразу, это буквы А, так как А кодируется как 00000. Первая буква полученного текста Ы. Её код 11011, количество единиц четыре. Запишем буквы с четырьмя единицами в двоичной записи: П, Ч, Э, Ю. Варианты начала слова: ЫА, ПА, ЧА, ЭА, ЮА. Третья буква полученного текста – Д. Её двоичная запись 00100, найдём буквы, имеющие, как и Д, одну единицу в двоичной записи. Это буквы: Б, В, И, Р. Вариант начала ЫА отбросим как невозможный, имеем следующие варианты для первых четырех букв:

$$\begin{array}{cccc}
 \text{ПА} \begin{pmatrix} \frac{B}{I} \\ \frac{B}{I} \\ \frac{P}{P} \end{pmatrix} A, & \text{ЧА} \begin{pmatrix} \frac{B}{I} \\ \frac{B}{I} \\ \frac{P}{P} \end{pmatrix} A, & \text{ЭА} \begin{pmatrix} \frac{B}{I} \\ \frac{B}{I} \\ \frac{P}{P} \end{pmatrix} A, & \text{ЮА} \begin{pmatrix} \frac{B}{I} \\ \frac{B}{I} \\ \frac{P}{P} \end{pmatrix} A.
 \end{array}$$

Шестая буква полученного текста Э, её код 11101, и есть следующие буквы, коды которых содержат те же четыре единицы: П, Ч, Ы, Ю. Учёт осмысленности исходного текста вариантов для 5 и 7 букв позволяют прочитать: ПАРАШЮТ.

Задача 23 [17]: Ниже записаны в зашифрованном виде: слева английские слова, справа – их переводы (иногда несколько переводов, но не обязательно все) на русский язык. Английские слова зашифрованы таким образом, что одной и той же букве латинского алфавита соответствует одно и то же число, записанное арабскими цифрами, разным буквам – разные числа. Аналогичным образом, но совершенно независимо, русские слова зашифрованы при помощи последовательности чисел, записанных римскими цифрами.

Буквы одного и того же слова отделены друг от друга запятыми, слова в заданиях – точками с запятой, фразы в заданиях – точками.

Надстрочные знаки и апострофы не учитываются, но **и** и **й** считаются разными буквами, а **е** и **ё** – не различаются.

1 – I

2, 3 – II, III, IV или II, III, I или II, III, V

4, 5, 6 – V, V

7, 8, 9 – VI или VII

8, 10 – VIII, V, IX

3, 10, 11 – IX, X или XI, X

7, 12 – XII

2, 10, 12, 4, 5, 6 – II, VII, IX, XIII

13, 6, 1, 5, 8, 9, 14 – XIV, XV, XII, XVI, XIII, I

Переведите следующие зашифрованные русские слова и фразы в английские:

1) XI, III, IX; XIV, XI, V, XV, XIII; XIV, III, II, VII;

2) VI, XVI; II, III, XV, I;

- 3) XIV, V, XV, V, XI, XIII, I;
4) II, V, VIII, I; XVI, III, XI, XII, IX; IX, III, II.

Решение: Единственное английское слово, состоящее из одной буквы, которое переводится русским словом тоже из одной буквы, – это ‘я’ (1 = I; I = я). Единственное русское слово из двух идентичных букв – это ее (её) (4 = h, 5 = e, 6 = r; V = e). Единственное английское слово из трёх букв, переводящееся одним из двух русских слов, каждое из которых состоит из одной буквы, – это and (7 = a, 8 = n, 9 = d; VI = (a или и), VII = (и или a)). Последнее английское слово: 13, r, i, e, n, d, 14, переведённое как XIV, XV, XII, XVI, XIII, я, должно быть friends ‘друзья’ (13 = f, 14 = s; XII = y, XIII = ь, XIV = д, XV = p, XVI = з). Слово a, 12, переведённое как у, должно быть тогда at (12 = t). Слово 2, 10, t, h, e, r, переведённое как II, и/a, IX, ь, – это мать (2 = m, 10 = o; II = m, VI = и, VII = a, IX = т).

Слова m, III, IV; m, III, я; m, III, e являются переводами одного и того же слова m, 3, которое, очевидно, является словом my (3 = y; III = o, IV = й).

И, наконец, 8, 10 = no, a 3, 10, 11 = you (11 = u; VIII = n, X = ы, XI = в).

Русские слова и фразы, которые нужно перевести, – это:

- 1) Вот дверь дома;
- 2) из моря;
- 3) деревья;
- 4) Меня зовут Том.

Их переводы на английский язык не представляют никаких трудностей.

Задача 24 [15]: Английский язык. Открытый текст на английском языке (различие между строчной и прописной буквой не делается) кодируется, т. е. переводится в числовую форму, по правилу: букве A присваивается номер 0, букве B – номер 1, букве Z – номер 25, пробелу соответствует номер 26. Затем текст шифруется по следующему алгоритму: вычисляется число $aP + b$, где P – номер буквы открытого текста, а числа a и b – ключ шифрования (неизвестный вам). Вычисленное число заменяется

остатком от деления на 27, полученному числу соответствует буква шифрованного текста. Вам известен алгоритм, неизвестен ключ.

Перед вами перехваченный шифрованный текст. Этих данных недостаточно для расшифровки. Однако из агентурных сведений стало известно – первый символ открытого текста – буква Q. Теперь данных достаточно. Прочитайте открытый текст.

Шифр-текст: IQTNX

Решение: Известно, что в английском языке после буквы Q следует буква U. Таким образом, нам известны 2 буквы открытого текста. Буква Q кодируется числом 16, далее шифруется по формуле $a \cdot 16 + b = 8 + 27 \cdot p$, p – некоторое целое.

Аналогично получаем ещё одно условие:

$20 \cdot a + b = 16 + 27 \cdot q$. Вычитая первое уравнение из второго, получим $4 \cdot a = 8 + 27 \cdot (q - p)$, т. е. число $4a$ делится на 27 с остатком 8. Итак, $a = 2$, тогда $b = 3$.

Имеем уравнения для нахождения номеров букв открытого текста:

$$\begin{cases} 2 \cdot x + 3 = 19 + 27 \cdot r \\ 2 \cdot y + 3 = 7 + 27 \cdot s \\ 2 \cdot z + 3 = 23 + 27 \cdot t, \end{cases}$$

где x, y, z – номера 3, 4, 5 букв, а r, s, t – некоторые целые числа. Легко видеть, что $x = 8, y = 2, z = 10$ удовлетворяют условиям. Но 8 – это код буквы I, 2 – код C, 10 – код K.

Ответ: открытый текст QUICK

Задача 25 (О. Н. Жданов). **Сравнения:** Используется русский алфавит из 31 буквы: буквы Е и Ё не различаются, буквы И и Й не различаются. Каждой букве такого алфавита поставлено в соответствие число: А соответствует 0, Б – 1, В – 2, ..., Ю – 29, Я – 30. Известен алгоритм зашифровывания: номер буквы открытого текста умножается на число a , к результату прибавляется число b , находится остаток от деления полученного числа на 31. Этот остаток определяет номер буквы в шифрованном тексте.

Пробелы и знаки препинания сохранены. Ключом является пара чисел (a, b) . Итак, алгоритм известен, ключ Вам неизвестен. При зашифровывании противник не учел особенности русского языка, которые позволяют Вам и без знания ключа расшифровать текст. Шифрованный текст:

**ВЯТЖХШИАВБ – АНЯЯЖЬГМ, НН ЯИЕЖ
ЫИЦВЦИГМ.**

Решение: Слову из двух одинаковых букв НН может соответствовать в открытом тексте только слово ЕЁ (напомним, Е и Ё при шифровании не различались). Итак, при расшифровывании нужно Н заменить на Е (Ё).

И у нас есть информация о ключе зашифрования: число $a \cdot 5 + b$ дает остаток 12 при делении на 31.

Напомним определение: числа, дающие при делении на m одинаковые остатки, называются сравнимыми по модулю m . Обозначение: $x \equiv y \pmod{m}$. В данной задаче $m = 31$. Итак, $5a + b \equiv 12 \pmod{31}$.

Обратим внимание на третью и четвертую буквы второго слова. Заметим, что наиболее вероятной буквой после Е является Н, биграмма ЕН встречается в русских осмысленных текстах примерно в два раза чаще, чем следующие по частоте биграммы с буквой Е: ЕР, ЕС, ЕЛ (см. таблицу на с....). С учетом удвоения буквы тем более вероятно, что символу Я шифрованного текста соответствует буква Н открытого текста.

Конечно, исследуемый текст может оказаться особенным, исключительным. И наша гипотеза может оказаться неверной. В таком случае мы придем к противоречию, к неосмысленному тексту и нам придется вернуться к началу задачи и проверять другие гипотезы. Однако мы начнем с проверки наиболее вероятной гипотезы: Н→Я. На языке сравнений наша гипотеза записывается так: $12a + b \equiv 30 \pmod{31}$.

Вычитая из второго сравнения первое, получаем: $7a \equiv 18 \pmod{31}$. Из этого сравнения найдем a . Воспользуемся расширенным алгоритмом Евклида.

$$31 = 4 \cdot 7 + 3 \quad 7 = 2 \cdot 3 + 1.$$

Из последнего равенства: $1 = 7 - 2 \cdot 3$, из первого равенства $3 = 31 - 4 \cdot 7$, и $1 = 7 - 2 \cdot (31 - 4 \cdot 7) = -2 \cdot 31 + 9 \cdot 7$. Следовательно,

$\text{mod } 31 = 9$ и $a = 9 \cdot 18 \text{ mod } 31 = 7$. Теперь $b = 12 - 5a = 12 - 5 \cdot 7 = -23 = 8$ (напомним, все вычисления ведутся по модулю 31). Мы нашли ключ шифрования. Чтобы расшифровать сообщение, зашифрованное применением отображения $C \equiv aP + b \pmod{31}$, нужно выразить P через C : $P \equiv sC + t \pmod{31}$, где $s = a^{-1}$ есть обратное к a по модулю 31 число, а t равно $-a^{-1}b$. Так как 31 число простое, то s и t однозначно находятся. Легко видеть, что ключ расшифровывания следующий: $s = 9, t = 21$.

Теперь мы можем проводить расшифровывание. Букве И соответствует номер 8, и $9 \cdot 8 + 21 = 93 = 0$, так что букве И в шифр-тексте соответствует буква А в открытом тексте. Подведем итог предыдущим рассуждениям. Символы шифр-текста запишем строчными буквами, а уже найденные буквы открытого текста – прописными. Вот что мы знаем:

вНтжхшАавб-аЕННжъгм, ЕЕ НАеж ыАцвцАгм.

Продолжим вычисления. Буква е имеет номер 5, и $9 \cdot 5 + 21 = 66 = 4$, а 4 – это номер буквы Д. Буква ж имеет номер 6, $9 \cdot 6 + 21 = 75 = 13$, а это номер буквы О. И мы знаем третье слово полностью: НАДО. Вычисляем букву открытого текста, зашифрованную символом ц: это Щ. Запишем результаты:

вНтОхшАавб-аЕННОъгм, ЕЕ НАДО ыАЩцвЩАгм.

Тактически правильно будет найти буквы открытого текста, зашифрованные символами г и м. Вычисления дают: $г \rightarrow Т, м \rightarrow Ь$. И мы можем «проявить» еще часть текста:

вНтОхшАавб-аЕННОъТЬ, ЕЕ НАДО ыАЩцвЩАТЬ.

Теперь уже последнее слово легко и угадать. Но все же вычислим еще две буквы. Действительно, $ы \rightarrow З, в \rightarrow И$, последнее слово ЗАЩИЩАТЬ. Кроме того, мы узнали еще часть первого слова. Итог этого этапа:

ИНтОхшАаИБ-аЕННОъТЬ, ЕЕ НАДО ЗАЩИЩАТЬ.

Далее $а \rightarrow Ц, ь \rightarrow С$, что позволяет записать второе слово: ЦЕННОСТЬ. Легко вычислить и остальные буквы.

Ответ:

ИНФОРМАЦИЯ – ЦЕННОСТЬ, ЕЕ НАДО ЗАЩИЩАТЬ.

б) Разные задачи.

Задача 26: Предлагалась на Санкт-Петербургской математической олимпиаде 1997 г. для 6 классов [7. С. 83]. **Логика.** Два мудреца написали на семи карточках числа от 5 до 11. После этого они перемешали карточки, первый мудрец взял себе три карточки, второй взял две, а две оставшиеся карточки они, не глядя, спрятали в мешок. Изучив свои карточки, первый мудрец сказал второму: «Я знаю, что сумма чисел на твоих карточках четная!».

Какие числа написаны на карточках первого мудреца? Единственный ли ответ в задаче?

Решение: Первый мудрец знает числа, написанные на тех четырех карточках, которые находятся не у него, но не знает, какие именно из них достались второму. Поэтому он может сделать своё заявление только в том случае, если для *любых* двух находящихся не у него карточек сумма написанных на них чисел четна. Для этого необходимо, чтобы числа на этих четырех карточках были все одинаковой четности, то есть были либо все четными, либо все нечетными. Четными они быть не могут, так как карточек с четными числами всего три. Поэтому они все нечетны, а три карточки с четными числами должны быть у первого мудреца.

Задача 27: (Заимствована из [9]). **Логика.** Известно, что A , B , C , D говорят правду лишь в одном случае из трех (независимо друг от друга). A утверждает, что B отрицает, что C говорит, будто D солгал. Какова вероятность, что D сказал правду? (см. «Ответы и указания»).

Задача 28: Задача олимпиады Москвы 1961 г. [4. С. 187]. **Количество вопросов.** Играют двое, один загадывает набор из целых однозначных чисел $(x_1, x_2, \dots, x_n)$ как положительных, так и отрицательных. Второму разрешается спрашивать, чему равна сумма $a_1x_1 + a_2x_2 + \dots + a_nx_n$, где $(a_1, a_2, \dots, a_n)$ – любой набор чисел.

Каково наименьшее число вопросов, за которое отгадывающий узнает задуманный набор?

Решение: Покажем, что задуманный набор можно определить, задав всего один вопрос. Именно достаточно взять $a_1 = 100$, $a_2 = 100^2$, ..., $a_n = 100^n$.

$$\text{Теперь, } \frac{s^1}{100^n} = \frac{100 \cdot x_1 + 100^2 \cdot x_2 + \dots + 100^{n-1} \cdot x_{n-1}}{100^n} + x_n,$$

$$\text{покажем, что } \left| \frac{100 \cdot x_1 + 100^2 \cdot x_2 + \dots + 100^{n-1} \cdot x_{n-1}}{100^n} \right| < \frac{1}{10}.$$

Действительно,

$$|100 x_1 + 100^2 x_2 + \dots + 100^{n-1} x_{n-1}| \leq 100 |x_1| + 100^2 |x_2| + \dots, \text{ так как } x_1, \\ + 100^{n-1} |x_{n-1}| \leq 9 (100 + 100^2 + \dots + 100^{n-1})$$

$x_2, \dots, x_{n-1}$ — однозначные числа. Число $9 \cdot (100 + 100^2 + \dots + 100^{n-1})$ имеет $2n - 1$ десятичных знаков и состоит из нулей и девяток, т. е. оно меньше, чем $\underbrace{9 \dots 9}_{2n-1}$, и тем более меньше, чем 10^{2n-1} . Таким

образом, интересующая нас дробь меньше, чем

$$\frac{10^{2n-1}}{100^n} = \frac{10^{2n} \cdot \frac{1}{10}}{10^{2n}} = \frac{1}{10}.$$

Итак, $\frac{s_1}{100^n}$ отличается от целого числа x_n меньше, чем на $\frac{1}{10}$.

Это позволяет однозначно определить x_n . Зная x_n , мы можем найти $s_2 = s_1 - 100^n \cdot x_n$ и по ней найти x_{n-1} и т. д.

Задача 29 (Журнал «Квант»). **Количество вопросов:** Двое играют в такую игру. Первый загадывает два числа от 1 до 25, а второй должен их угадать. Он может назвать любые два числа от 1 до 25 и узнать у первого, сколько из названных им чисел — 0, 1 или 2 — совпадают с загаданными. За какое минимальное число вопросов он сможет наверняка определить загаданные числа?

Задача 30 (Журнал «Квант»). **Карты:** Из колоды выбрали 7 карт, показали всем, перетасовали и раздали двум игрокам по 3 карты, а оставшиеся отдали постороннему наблюдателю.

Игроки могут по очереди сообщать **ВСЛУХ ОТКРЫТЫМ ТЕКСТОМ** любую информацию о своих картах. Могут ли они

сообщить друг другу свои карты так, чтобы при этом посторонний наблюдатель не смог вычислить местонахождение ни одной из карт, которых он не видит?

Задача 31[8]: Алфавит состоит из n букв. Какова максимальная длина слова, если выполнены два условия:

- а) в нем две рядом стоящие буквы всегда различны;
- б) из него нельзя получить вычеркиванием букв слова вида $abab$, где a и b – различные буквы?

Решение: Если буква встречается только один раз, назовем ее буквой первого рода. В противном случае – буквой второго рода. Буквы, стоящие рядом с буквой второго рода, различны, это следует из свойства «б».

Если слово содержит хотя бы два вида букв, то оно содержит хотя бы одну букву первого рода. В противном случае мы можем получить из него слово вида $abab$, что противоречит условию. Вычеркнув все буквы второго рода, совпадающие с некоторой, получим слово из $n - 1$ различных букв. Вычеркивая буквы второго рода и далее, придем к слову, состоящему только из букв первого рода.

Докажем методом математической индукции, что слово имеет длину не более $2n - 1$ буквы. Для $n = 1$ утверждение верно. Предположим теперь, что оно верно для $n = k$ букв и докажем его для $n = k + 1$.

Пусть слово содержит $k + 1$ различную букву, α – буква первого рода, а β – соседняя с ней буква. Если β – первого рода, то при вычеркивании β возникает слово из k различных букв, максимальная длина которого не превышает $2k - 1$ букв (по предположению индукции), а само исходное слово имеет длину не более $2k$. Если β – второго рода, то обе соседние буквы пары α, β или различны, или имеется только одна соседняя буква, т. е. пара α, β стоит с краю. Поэтому пару α, β можно вычеркнуть, оставшееся слово удовлетворяет условию «а» задачи. Длина оставшегося слова $2k - 1$ букв, а первоначального – $2k - 1 + 2 = 2(k + 1) - 1$. Утверждение доказано. Итак, слово имеет длину не более $2n - 1$ букв.

Приведем пример слова, имеющего длину в точности $2n - 1$ букв. Из алфавита $a_1, a_2, \dots, a_n$ можно составить слово $a_1 a_2 \dots a_n a_{n-1} a_{n-2} \dots a_1$.

Задача 32 [17]: Даны пять правил подстановки:

1. $D \rightarrow AB$;
2. $A \rightarrow CD$;
3. $B \rightarrow b$;
4. $C \rightarrow c$;
5. $D \rightarrow d$.

Правила означают следующее: если в какой-либо последовательности букв можно отыскать левую часть какого-либо из пяти правил, то её разрешается заменить правой частью этого правила и переписать последовательность в новом виде, не меня остальных букв. После этого можно опять постараться применить какое-либо правило и т. д.

а) Какие из следующих последовательностей можно получить из буквы D применением какого-либо числа раз правил 1–5: $bb, bbc, bbcd, bbcd, bd, cbd, bdc, b, cdb, cb, cc, ccd, ccdbb, ccccd$?

б) Охарактеризуйте все последовательности строчных букв, которые могут получиться из буквы D путём применения правил 1–5 и к которым уже нельзя применить ни одного из этих правил.

Решение: Если применить каждое из пяти правил по одному разу, то получится последовательность cdb . Но вместо того, чтобы использовать правило 5, мы всегда можем снова использовать правило 1, и тогда вместо d появится опять cdb . Это означает, что мы можем получать только следующие циклические последовательности: $cdb, ccdbb, cccdbbb$ и т. д.; каждая такая последовательность описывается следующим образом: c может повторяться сколько угодно раз, потом идёт одно d и столько же раз b , сколько было c .

Задача 33 [17]: Будем рассматривать последовательности, состоящие только из букв А и В (например, ААВ АВВ, АА, В и т. п.). Разрешается преобразовывать каждую из последовательностей следующим образом:

- если в последовательности есть группа ВА (подряд и именно в этом порядке), то её можно заменить на АВВВ;
- АВВВ можно заменить (при тех же условиях) на ВА;
- можно вычеркнуть подряд идущую группу АА или ВВВВ;
- между любыми двумя стоящими рядом буквами последовательности, или левее всех букв, или правее всех букв можно написать группу АА или ВВВВ.

К каждой последовательности можно применить любое из этих преобразований, к полученной последовательности – снова любое из этих преобразований и т. д.

а) Какую цепочку преобразований нужно применить к последовательности АВ, чтобы получить из неё последовательность ВВВА (известно, что это можно сделать)?

б) Какую цепочку преобразований нужно применить к последовательности АВ, чтобы получить последовательность АВ АВ АВ?

в) Можно ли путём указанных преобразований из последовательности АВ получить последовательность АВ АВ?

г) Докажите, что нельзя путём разрешённых преобразований получить из последовательности АВ последовательность ВА.

Решение:

а) $AB \rightarrow BBVBAV \rightarrow BBVABVVV \rightarrow BBVA$

(сначала слева приписана последовательность ВВВВ, затем образовавшийся фрагмент ВА заменён на АВВВ, затем фрагмент ВВВВ в конце образовавшейся последовательности вычеркнут);

б) $AB \rightarrow ABA \rightarrow ABAABVVV \rightarrow AVABAV$

(справа приписана последовательность АА, затем справа приписана последовательность ВВВВ, затем фрагмент АВВВ заменён на ВА);

в) Нельзя, так как преобразования сохраняют чётность количества А (а также В) в группе букв;

г) Рассмотрим пару произвольных чисел $(x; y)$, причём $x \neq 0$ и $y \neq 0$.

Придадим буквам А и В смысл операций с парами чисел:

А – «заменить знак первого числа на противоположный, второе число оставить без изменений», т. е. $(x; y) A \rightarrow (-x; y)$;

В – «поменять числа местами, после чего у числа, оказавшегося на втором месте, поменять знак на противоположный», т. е. $(x; y) B \rightarrow (y; -x)$.

Последовательность из букв А и В будем рассматривать как последовательность выполнения заданных этими буквами операций (в том порядке, как эти буквы записаны).

Очевидно, что последовательности операций АА и ВВВВ не меняют исходную пару чисел.

$$(x; y) A \rightarrow (-x; y) A \rightarrow (x; y)$$

$$(x; y) B \rightarrow (y; -x) B \rightarrow (-x; -y) B \rightarrow (-y; x) B \rightarrow (x; y)$$

Поэтому их можно добавлять или вычёркивать в любом месте последовательности операций, результат от этого не поменяется.

Также легко убедиться, что ВА и АВВВ всегда приводят к одному и тому же результату, т. е. являются взаимозаменяемыми.

$$(x; y) B \rightarrow (y; -x) A \rightarrow (-y; -x)$$

$$(x; y) A \rightarrow (-x; y) B \rightarrow (y; x) B \rightarrow (x; -y) B \rightarrow (-y; -x).$$

То есть, выполняя только разрешённые в условии задачи замены в любой последовательности букв А и В, мы всегда будем получать последовательности операций, в итоге приводящих к одному и тому же результату.

А последовательности операций АВ и ВА приводят к различным результатам.

$$(x; y) A \rightarrow (-x; y) B \rightarrow (y; x)$$

$$(x; y) B \rightarrow (y; -x) A \rightarrow (-y; -x)$$

Поэтому с помощью разрешённых в условии замен получить из последовательности АВ последовательность ВА невозможно.

• Дополнение.

Пару чисел $(x; y)$ можно рассматривать как координаты некоторой точки в декартовой прямоугольной системе координат. В этом случае операция А – это осевая симметрия относительно координатной оси Оу, а операция В – это поворот относительно начала координат на 90° по часовой стрелке.

Задача 34 (Задача 2.3 [1. С. 41]): Рассмотрим преобразование цифрового текста, в котором каждая цифра заменяется остатком от деления значения многочлена $F(x) = b \cdot (x^3 + 7x^2 + 3x + a)$ на число 10, где a, b – фиксированные натуральные числа.

Выясните, при каких значениях a, b указанное преобразование может быть шифр-преобразованием, т. е. допускает однозначное расшифровывание.

Решение: Пусть $f(x)$ – остаток от деления значения $F(x)$ на 10. Для однозначного расшифровывания необходимо и достаточно, чтобы разным значениям x соответствовали разные значения $f(x)$. Поэтому $f(0), f(1), \dots, f(9)$ принимают все значения от 0 до 9. Найдем эти значения. Для удобства записи обозначим $r_{10}(t)$ – остаток от деления t на 10. Имеем:

$$\begin{aligned} f(0) &= r_{10}(ab) & f(5) &= r_{10}((a+5)b) \\ f(1) &= r_{10}((a+1)b) & f(6) &= r_{10}((a+6)b) \\ f(2) &= r_{10}((a+2)b) & f(7) &= r_{10}((a+7)b) \\ f(3) &= r_{10}((a+3)b) & f(8) &= r_{10}((a+8)b) \\ f(4) &= r_{10}((a+4)b) & f(9) &= r_{10}((a+9)b) \end{aligned}$$

Теперь заметим, что b должно быть нечетным, иначе все значения $f(x)$ будут четными. Далее, b не должно делиться на 5, иначе $f(x)$ будут только 0 и 5. Поэтому число b может быть одним из чисел вида: 1) $5p + 1$, p – четно; 2) $5p + 2$, p – нечетно; 3) $5p + 3$, p – четно; 4) $5p + 4$, p – нечетно. Легко заметить, что числа эти имеют запись соответственно: $10k + 1$, $10k + 7$, $10k + 3$, $10k + 9$, k – целое. В первом случае имеем:

$$\begin{aligned} f(0) &= r_{10}(a) & f(5) &= r_{10}(a+5) \\ f(1) &= r_{10}(a+1) & f(6) &= r_{10}(a+6) \\ f(2) &= r_{10}(a+2) & f(7) &= r_{10}(a+7) \\ f(3) &= r_{10}(a+3) & f(8) &= r_{10}(a+4) \\ f(4) &= r_{10}(a+4) & f(9) &= r_{10}(a+5) \end{aligned}$$

При любом значении a эти числа различны. Непосредственной проверкой убеждаемся, что и для $b = 10k + 7$, $b = 10k + 3$, $b = 10k + 9$ все числа $f(x)$, $x = 0, 1, \dots, 9$ будут различными при любом a .

Ответ: a – любое, b имеет вид $10k + m$, где m – одно из чисел 1, 3, 7,

Задача 35: Цифры заменены буквами, разные цифры – разными буквами, одинаковые – одинаковыми. В фразе

И ВСЕ ЖЕ ОН НЕ ПРАВ

Каждое слово является квадратом некоторого натурального числа. Найдите соответствие между цифрами и буквами.

(Задача из второй заочной олимпиады по криптографии Саратовского Государственного Университета).

Задача 36 (составлена по аналогии с задачей 6.4 из [1]):

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

На зубцах второй и третьей 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.

Зашифровывание производится вращением первой шестеренки против часовой стрелки до первого попадания шифруемой буквы под стрелку. В этот момент последовательно выписываются цифры, на которые указывают вторая и третья стрелки. В начале шифрования стрелка 1-го колеса указывала на букву А, а стрелки 2-го и 3-го колес – на цифру 0.

Расшифруйте сообщение **948593312255334486**.

Решение: Очевидно, что если начать вращение первой шестерёнки ПРОТИВ часовой стрелки, то вторая начнёт вращаться ПО часовой стрелке, а третья ПРОТИВ часовой стрелки. Шифровалась первая буква. При этом цифра 0 на второй шестерёнке заменена на 9. Замена 0 на 9 могла произойти при повороте второй шестерёнки на 1 позицию или на 11 или на 21, 31. На третьей шестерёнке цифра 0 оказалась заменена на 4. Это могло произойти при повороте на 4 позиции или на 11 или 18 или 25 позиций. Из возможных вариантов для сдвига шестерёнок лишь число 11 является общим. Итак, при шифровании первой буквы произошёл сдвиг на 11 позиций на каждой шестерёнке, в том числе на первой. Таким образом, место под стрелкой заняла буква, отстоящая от А на 11 позиций. Сдвиг на одну позицию заменяет А на Б, сдвиг на две позиции заменит А на В и т. д. Сдвиг на 11 позиций заменит А на К. Следовательно, первая буква открытого текста – это буква К.

Далее пара цифр 94 при шифровании второй буквы перешла в 85. Цифра 9 на второй шестерёнке переходит в 8 при повороте на 1 позицию, а также на 11, 21, 31. А цифра 4 на третьей шестерёнке переходит в 5 при повороте на 1, 8, 15, 22, 29. Мы видим, что общим для вариантов сдвига на двух шестерёнках является число 1, и только оно. Вывод: при шифровании второй буквы первая шестерёнка вращалась так, что буква К была заменена на отстоящую от неё на ОДНУ ПОЗИЦИЮ, а это буква Л. И мы знаем первые две буквы открытого текста: КЛ, продолжая рассуждать описанным способом, находим (вычисляем!) все буквы.

Ответ: КЛЮЧШИФРА.

6. АУТЕНТИФИКАЦИЯ

Наряду с конфиденциальностью не менее важной задачей является аутентификация.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности. Иными словами, это процедура определения того, действительно ли пользователь или иной субъект передачи информации (приемопередающее оборудование, узел локальной сети и т. д.) по каналу связи является тем, за кого он себя выдает.

На сегодняшний день механизмы аутентификации широко применяются практически во всех компьютерных системах хранения, передачи и обработки информации, прежде всего, для обеспечения работы систем разграничения доступа и авторизации пользователей системы.

Все механизмы аутентификации основаны на предъявлении пользователем системе специальной информации, на основании которой модуль аутентификации выносит решение о том, считать ли данного пользователя легитимным или признать, что произошла попытка (возможно, неумышленная) подмены пользователя.

Базовая классификация типов систем аутентификации основывается на различии видов информации, используемой в качестве аутентификационной:

1. Последовательность информационных символов, которую пользователь предъявляет системе для успешного прохождения аутентификации. Простейший пример – парольная аутентификация на ПЭВМ, для которой пользователю достаточно ввести в систему свой идентификатор и пароль.

2. Уникальное содержимое или характеристики предмета. В этом качестве могут выступать, как правило, любые внешние носители информации: смарт-карты, электронные таблетки iButton, USB-токены и т. д. Реже для удаленной аутентификации узла сети могут использоваться уникальные данные о его аппаратном обеспечении.

3. Биометрическая информация человека, которая неотъемлема от него и уникальна для каждого индивида. Это может быть

отпечаток пальца, рисунок радужной оболочки глаза, форма лица, параметры голоса и т. д.

Используются также комбинированные схемы, основанные на нескольких видах информации, передаваемой системе аутентификации. Типичный пример: аутентификационная информация пользователя для входа в программную систему хранится на смарт-карте, для доступа к которой нужно ввести пароль (PIN-код). Такая аутентификация называется *двухфакторной*. Намного реже встречаются системы с трехфакторной аутентификацией.

В ряде случаев требуется и взаимная аутентификация – когда оба участника информационного обмена проверяют подлинность идентификаторов друг друга. Например, перед передачей удаленному серверу каких-либо данных пользователь должен убедиться, что это именно тот сервер, который ему необходим.

Помимо этого, существует естественное деление механизмов аутентификации на локальную (в рамках локализованной информационной системы) и удаленную (при передаче информации по каналу связи).

В случае удаленной аутентификации существует проблема передачи аутентификационной информации по недоверенным (ненадежным) каналам связи, так как возникает угроза перехвата аутентификационной информации злоумышленником (противником) с целью дальнейшего использования для атаки на систему защиты.

Рассмотрим несколько задач, моделирующих в упрощенном виде реальную работу системы парольной аутентификации в средствах защиты информации от несанкционированного доступа.

Задача 37 (см.[10]). Разделение секрета: Сейф с документами открывается, если набрано секретное число M . Для разделения секрета используется многочлен $F(x) = ax^2 + bx + M$, где a , b – целые числа. Каждый из трех членов комиссии получил свою долю секрета. Именно: первый знает, что $F(2)$ делится на 13 с остатком 3, второй знает: $F(3)$ делится на 13 с остатком 7, третий знает: $F(5)$ делится на 13 с остатком 5.

Докажите, что объединив свои знания, эти трое смогут открыть сейф (и найдите число M), а любые двое из них не смогут (числа a и b члены комиссии не знают).

Решение: Нужно найти M из условий:

$$\begin{cases} 4a + 2b + M = 3 + 13p, \\ 9a + 3b + M = 7 + 13q, \\ 12a + 5b + M = 5 + 13t, \end{cases}$$

где p, q, t – некоторые целые числа.

Складывая первое равенство со вторым и вычитая из их суммы третье, получим $a + M = 5 + 13p'$, где p' – некоторое целое. Вычитая первое из второго, получим $5a + b = 4 + 13q'$.

Теперь подставим $a = 5 - M + 13p'$, $b = 4 - 5a + 13q' = 4 - 5 \cdot (5 - M + 13p') + 13q'$ в первое уравнение. Получим $M = 11 + 13u$, u – целое число. Так как каждое число заменяется его остатком от деления на 13, то $M = 11$.

Поскольку a, b, M неизвестны, то любые двое, объединившись, получат систему из двух уравнений относительно трех неизвестных.

Задача 38 (Журнал «Квант»). **Пароль:** Семизначный код, состоящий из семи различных цифр, назовём хорошим. Известно, что сейф откроется, если введён хороший код и на каком-нибудь месте цифра кода совпала с соответствующей цифрой пароля. За какое наименьшее количество попыток можно с гарантией открыть сейф?

Ответ: за 6 попыток.

Приведём пример, в котором сейф с гарантией открывается за 6 попыток:

1234560,
2345610,
3456120,
4561230,
5612340,
6123450.

Среди первых 6 цифр пароля есть цифра от 1 до 6. Поскольку мы каждую из 6 цифр по разу набрали на каждом из первых 6 мест, значит, в одном из случаев она совпадает с соответствующей цифрой пароля.

Теперь докажем, что пяти попыток недостаточно. Пусть сделано пять попыток. Обозначим через M_1 множество цифр, которые не набирались в качестве первой цифры в этих попытках. Аналогично определим множества $M_2, M_3, \dots, M_7$. Так как всего было 5 попыток, то $|M_1| \geq 10 - 5 = 5$ (здесь через $|X|$ обозначаем количество элементов во множестве X). Так как каждая из цифр 0, 1, ..., 9 набирались не более одного раза в каждой попытке, то она содержится не менее чем в двух из семи множеств M_i . Покажем, что найдётся пароль $a_1, a_2, \dots, a_7$, где a_i – цифра из M_i ; это и будет означать, что в случае такого пароля сейф не откроется.

1-й случай: Пусть в двух из множеств M_i не менее семи цифр, скажем, $|M_6| \geq 7$ и $|M_7| \geq 7$. Тогда можно выбрать в M_1 любую цифру a_1 , в M_2 – цифру a_2 , отличную от a_1 , и т. д., в M_7 – цифру a_7 , отличную от $a_1, a_2, \dots, a_6$.

2-й случай: Пусть хотя бы в шести из множеств M_i не более 6 цифр. Тогда найдётся цифра x , которая не принадлежит двум из этих подмножеств, скажем, x не принадлежит M_4 и M_5 . Также выберем ещё одну цифру $y \neq x$, не принадлежащую M_5 . Цифра y принадлежит хотя бы одному подмножеству $M_i, i \neq 4$, скажем, $y \in M_6$. Цифра x принадлежит хотя бы одному подмножеству $M_i, i \neq 6$, скажем, $x \in M_7$. Положим $a_6 = y, a_7 = x$. Вычеркнув цифры x и y из подмножеств $M_1, \dots, M_5$, мы приходим к подмножествам $M'_1, \dots, M'_5$, для которых $|M'_1| \geq 3, |M'_2| \geq 3, |M'_3| \geq 3, |M'_4| \geq 4, |M'_5| \geq 5$ ($M'_5 = M_5$). Далее рассуждаем аналогично случаю 1: можно выбрать в M'_1 любую цифру a_1 , в M'_2 – цифру a_2 , отличную от a_1 , и т. д., в M'_5 – цифру a_5 , отличную от a_1, a_2, a_3, a_4 .

Замечание: Можно рассмотреть общую задачу про n -значный код в алфавите из $m \neq n$ символов (в нашем случае $n = 7, m = 10$) и доказать, что минимальное число попыток при $n \leq m/2$ будет равно $m + 1 - n$, а при $n < m/2$ оно равно $\left\lceil \frac{m}{2} \right\rceil + 1$.

Задача 39 (фольклор): А теперь Вы по заданию Центра должны проникнуть на сервер противника. Для этого Вам предстоит подобрать пароль к серверу методом «грубой силы» (последовательного перебора). Известно, что пароль назначается компьютером, регулярно меняется, а предыдущие пароли выглядели следующим образом (все буквы – латинские):

abStwdRd
pVtrKRLp
iryzhToz
URbhhbEH
OJEXHZmJ
pzTDXJrZ

Какие выводы надо сделать, чтобы ускорить процесс подбора пароля? (Время имеет значение!).

Решение: Нетрудно заметить, что каждый из паролей является строкой из 8 латинских символов в верхнем и нижнем регистрах. Таким образом, пространство перебора имеет вид $\{a \dots z \cup A \dots Z\}^8$. Мощность парольного пространства равна $52^8 \approx 5,3 \cdot 10^{13}$.

Для ускорения процесса подбора пароля необходимо обнаружить какие-либо закономерности в последовательности известных паролей, чтобы сократить пространство перебора.

Из приведенных в условии задачи паролей видно, что в каждом из них есть хотя бы одна буква в нижнем регистре и хотя бы одна – в верхнем. Можно предположить, что генератор парольных последовательностей исключает возможность генерации пароля, состоящего только из строчных или только из заглавных букв. Это предположение естественно, так как это является одним из классических критериев стойкости пароля к подбору.

Таким образом, из подбора следует исключить строки, состоящие только из строчных или только из заглавных букв. Это позволит уменьшить пространство перебора на $2 \cdot 26^8 \approx 4,1 \cdot 10^{11}$ попыток подбора.

Задача 40: Специалист по защите информации А разработал собственную систему авторизации на компьютере. Пользователь вводит пароль – трехзначное натуральное число. Компьютер делит это число на 31, полученный при этом остаток М умножает на 2 и получает число К. После этого число К делит на 23 и полученный остаток А сохраняет на жестком диске. Например, если $N = 123$, то $M = 30$, соответственно, $K = 60$ и $A = 14$. Если пользователь ввел пароль Р, и после указанных вычислений получилось число, совпадающее с числом, хранящимся в памяти компьютера, то он получает доступ.

Пользователь Б решил использовать на своем компьютере такую же систему. Но чтобы А не подал на него в суд за кражу интеллектуальной собственности, решил поменять местами числа 23 и 31, т. е. сначала стал делить на 23, а потом на 31.

Известно, что в компьютере А и в компьютере Б хранится число $A = 5$. Злоумышленник не знает паролей А и Б и поэтому перебирает их все подряд в случайном порядке. Чей компьютер он взломает быстрее?

Решение: Всего различных паролей 900 ($100 \leq N \leq 999$). Вычислим, сколько из них дают в итоге число 5 по схеме пользователя А. Остаток 5 от деления на 23 дают натуральные числа 5, 28, 51. Больших чисел быть не может, так как $K < 62 = 31 \cdot 2$. Так как 5 и 51 – нечетные числа, то $K = 2M = 28$, значит, $M = 14$. Числа N, дающие остаток от деления на 31, равный 14, имеют вид $N = 14 + 31s$. Так как $100 \leq N \leq 999$, то $s = 3, 4, 5, \dots, 31$. В итоге получаем $31 - 2 = 29$ допустимых паролей (из 900 возможных).

Если те же вычисления провести по схеме Б, то получим следующие претенденты для числа К : 5, 36. Следовательно, $M = 18$ и $N = 18 + 23s$, где $s = 4, 5, 6, \dots, 42$. Итого 39 допустимых паролей.

Итак, вероятность взлома системы Б выше в $39/29 \approx 1,34$ раза, чем у А.

Задача 41: Для подтверждения своих полномочий в компьютерной системе пользователь должен ввести свое имя и пароль, состоящий из 10 букв русского алфавита с исключенными Ё и Ъ.

Файл с паролями пользователей хранится на сервере в зашифрованном виде. Для их зашифровывания использовался следующий способ. Буквам алфавита поставлены в соответствие числа от 0 до 30: А – 0, Б – 1, ..., Я – 30. При зашифровывании пароля каждую его букву заменяют остатком от деления на 31 значения выражения $(6a^3 + 5a^2 + 6a + 20)$, где a – число, соответствующее заменяемой букве. В начале каждого сеанса работы введенный пользователем пароль зашифровывается и сравнивается с соответствующей записью в файле. При совпадении сеанс продолжается, а при расхождении пароль запрашивается снова. Злоумышленник хочет войти в систему под чужим именем, а соответствующий этому имени пароль не знает. Он написал программу, которая в случайном порядке перебирает пароли. Какой из двух паролей – «ШИФРОВАНИЕ» или «КРИПТОГРАФ» – устойчивее к действию этой программы?

Решение: В данной задаче необходимо вычислить все значения многочлена $(6a^3 + 5a^2 + 6a + 20)$ по модулю 31 для всех чисел от 0 до 30. Результаты вычисления представлены в следующей таблице:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
20	6	7	28	12	26	13	9	19	17	8	28	20	20	2	2

16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я
25	14	5	3	13	9	27	10	25	15	16	2	9	11	13

Таким образом, слово «ШИФРОВАНИЕ» зашифруется строкой чисел «25, 19, 13, 25, 2, 7, 20, 20, 19, 26». Перечисленные числа в качестве шифр-символов встречаются соответственно 2, 1, 3, 2, 3, 1, 3, 3, 1 и 1 раза в таблице. Следовательно, число различных паролей, в зашифрованном виде имеющих вид «25, 19, 13, 25, 2, 7, 20, 20, 19, 26» будет равно $3^4 \cdot 2^2 = 324$.

Для слова «КРИПТОГРАФ» мы после шифрования получаем последовательность «8, 25, 19, 2, 5, 2, 28, 25, 20, 13». Аналогичный подсчет дает число различных паролей, зашифровывающихся такой же последовательностью, равное $3^4 \cdot 2^3 = 648$.

Пароль «ШИФРОВАНИЕ» в 2 раза надежнее, чем «КРИПТОГРАФ».

Ответы и указания к задачам для самостоятельного решения

Задача 2: В первом тексте 30 шифрообозначений, а во втором – 35. Следовательно, второй текст зашифрован с ошибками, а про первый ничего сказать не можем.

Задача 19.1: Составим таблицу частот шифрообозначений:

Обозначение	29	35	87	41	58	43	44	31	68	95	25	63	32
Количество	7	11	5	5	10	1	1	15	11	2	2	6	1
Обозначение	71	77	91	45	99	51	75	61	82	17	19	54	
Количество	3	5	6	3	1	4	3	2	2	2	1	1	

Сравнение таблицы частот букв русского языка с таблицей частот шифр-обозначений позволяет выдвинуть гипотезу: 31= О. И есть три «кандидата» на букву Е, это обозначения 68, 35, 58.

Посмотрим на третье слово в первой строке. Если 58 = Е, то получим 44 О Е О 68, что нехарактерно для русского языка. Если 68 = Е, то последнее слово первой строки имеет вид 87 41 О Е О – снова маловероятное сочетание букв. Поэтому будем считать, что 35 = Е. Конечно, если в процессе работы над текстом мы придем к противоречию, то придется вернуться к началу и пробовать другие варианты.

Обратим внимание на начало второй строки 58 68 О Е. Можем сделать вывод, что 58 и 68 – согласные. В тексте эти обозначения встречаются часто, уступая лишь 31. Из таблицы частот видно, что наиболее распространенные согласные – это Т и Н.

Если 58 = Н, то слово Н 68 О Е трудно прочитать: подставляя вместо 68 различные буквы, всякий раз получаем сочетание, не имеющее смысла. Итак, $58 \neq Н$.

Если 58 = Т, то слово Т 68 О Е читается: Т В О Е, и 68 = В.

Запишем первую строку: «29 Е 87 41 29 Т 43 44 О Т О В 95 Т О 25 63, 32 Т О 87 41 О В О...». Теперь 32 = Ч или 32 = К. Кроме того, 43 = Ы. Два слова «...Т Ы 44 О Т О В...» позволяет найти значение 44: ясно, что 44 = Г. Фрагмент «...Т Ы Г О Т О В 95 Т О 25 63, 32 Т О...» позволяет уверенно считать, что 95 = К, 32 = Ч, 25 = М, 63 = У.

Обратим теперь внимание на запятую в начале третьей строки. Слово из одной буквы и запятая – ясно, что это не согласная. Варианты для 29: Ы, У, Ю, Э отбросим, О уже используется, О = 31. Возможные варианты для 29 – это Я, А, И.

Вернемся к первой строке. С учетом уже прочитанных обозначений получаем: « $\begin{pmatrix} Я \\ А \\ И \end{pmatrix}$ Е 87 41 $\begin{pmatrix} Я \\ А \\ И \end{pmatrix}$ Т Ы Г О Т О В

К Т О М У, Ч Т О...». Единственный осмысленный вариант теперь: 29 = И. Тогда второе слово Е С Л И, и мы знаем еще два значения: 87 = С, 41 = Л.

Запишем текст, заменяя шифрообозначения на их известные значения.

И ЕСЛИ ТЫ ГОТОВ К ТОМУ, ЧТО СЛОВО
ТВОЕ В ЛОВУ 71 КУ 77 91 Е В 91 45 99 45 Е Т 77 Л У Т,
И, 77 О Т Е 91 77 Е В К 91 У 71 Е 51 75 Е, М О 61 Е 71 75
С 51 О В 45 – 82 Е 17 77 91 Е 61 51 И 19 С И Л –
В О 17 О 82 51 О В И Т 75 С В О И Т 91 У 54...

Последнее слово второй строки сразу позволяет угадать: 77 = П. Тогда второе слово третьей строки П О Т Е 91 П Е В, и 91 = Р. Четвертое слово второй строки: П Р Е В Р 45 99 45 Е Т = П Р Е В Р А Щ А Е Т, и мы знаем, что 45 = А, 99 = Щ. Конец

третьей строки: С 51 О В А = С Н О В А, 51 = Н. Кроме того, третье слово второй строки позволяет найти 71 = Ш.

Запишем две последние строки.

И, ПОТЕРПЕВ КРУШЕН 75 Е, МО 61 Е Ш 75
С Н О В А – 82 Е 17 П Р Е 61 Н И 19 С И Л –
ВО 17 О 82 Н О В И Т 75 С В О И Т Р У 54...

Отсюда следует, что 75 = Ъ, но тогда 17 = З, 82 = Б, 61 = Ж.

Теперь последняя строка: «Б Е З П Р Е Ж Н И 19 С И Л –
В О З О Б Н О В И Т Ь С В О И Т Р У 54...». Второе слово позволяет понять, что 19 = Х. Учтем, что И и Й не различаются в данном алфавите. Тогда последние слова С В О Й Т Р У Д.

Ответ:

И ЕСЛИ ТЫ ГОТОВ К ТОМУ, ЧТО СЛОВО
ТВОЕ В ЛОВУШКУ ПРЕВРАЩАЕТ ПЛУТ, И,
ПОТЕРПЕВ КРУШЕНИЕ, МОЖЕШЬ СНОВА –
БЕЗ ПРЕЖНИХ СИЛ – ВОЗОБНОВИТЬ СВОЙ
ТРУД...

Задача 19.2:

Ключ:

Бук ва	Чис ло	Бук ва	Чис ло	Бук ва	Чис ло	Бук ва	Чис ло	Бук ва	Чис ло
а	40	ж	43	м	87	т	73	ы	14
б	18	з	24	н	67	у	27	ь	92
в	69	и	92	о	56	х	82	э	71
г	23	й	31	п	25	ц	51	ю	36
д	80	к	95	р	46	ч	38	я	10
е	58	л	17	с	39	ш	99		

Ответ:

ОНИ БЕСШУМНО ПОДНЯЛИСЬ ПО УЗ
КОЙ КРУТОЙ ЛЕСЕНКЕ И ОКАЗАЛИСЬ
В САЛОНЕ – ОБШИРНОМ, ВО ВСЮ ДЛИ
НУ САМОЛЕТА. ПОСТОЯЛИ, ОЖИДАЯ, К
ОГДА ГЛАЗА ПРИВЫКНУТ К ТЕМНОТЕ.
ВСЕ ВОКРУГ ПРИНЯЛО ЧЕТКИЕ ОЧЕРТА
НИЯ. ПРИБОРОВ И ПУЛЬТОВ ЗДЕСЬ БЫ

ЛО ПРЕВЕЛИКОЕ МНОЖЕСТВО, ГЛАЗА РАЗБЕГАЛИСЬ. ОДНАКО БЛАГОДАРЯ ТЕМ ЖЕ ДВУМ НЕДЕЛЯМ ТРЕНИРОВОК НА МАКЕТЕ И ТЫСЯЧЕКРАТНО ПОВТОРЕННЫМ НАСТАВЛЕНИЯМ ИНСТРУКТОРА ОНИ СОВЕРШЕННО ТОЧНО ЗНАЛИ, ЗА ЧЕМ ПРИШЛИ. ПОНЯТИЯ НЕ ИМЕЛИ, ДЛЯ ЧЕГО КОНКРЕТНО ПРЕДНАЗНАЧЕНЫ ВСЕ ЭТИ ШТУКИ – НО ОТ НИХ ЭТОГО И НЕ ТРЕБОВАЛОСЬ.

НЕ ПРОШЛО И МИНУТЫ, КАК ОН УВИДЕЛ ЦЕЛЬ ИХ НЕЛЕГКОГО И ЭКЗОТИЧЕСКОГО ПУТЕШЕСТВИЯ – ТРИ ПУЛЬТА ПО ПРАВОМУ БОРТУ, УСЫПАННЫЕ ЧЕРТОВОЙ УЙМОЙ ТУМБЛЕРОВ, ЛАМПОЧЕК, ПЕРЕКЛЮЧАТЕЛЕЙ И КНОПОК. ТРИ ВЫПУКЛЫХ ЭКРАНА В ВИДЕ ВЕРТИКАЛЬНЫХ ПРЯМОУГОЛЬНИКОВ – ОНИ САМЫЕ, НИКАКОЙ ОШИБКИ...

БОДРОСТИ РАДИ, ОН ПОВТОРИЛ ПРО СЕБЯ ПОЛЮБИВШУЮСЯ ЦИТАТУ: “ЧТО ОДИН ЧЕЛОВЕК ПОСТРОИЛ, ДРУГОЙ ЗА ВСЕГДА РАЗЛОМАТЬ СМОЖЕТ”. И, ПОХЛОПАВ ПО ПЛЕЧУ СТРАШИЛУ В ЗНАК ТОГО, ЧТО НАПАРНИК ДОЛЖЕН БДИТЕЛЬНО СТОЯТЬ НА ШУХЕРЕ, ДОСТАЛ КИНЖАЛ ИЗ ПРИШИТЫХ НАД КОЛЕНОМ НОЖЕН.

Задача 27: Обозначим логические значения высказываний: И = «истина», Л = «ложь». С высказыванием «*A утверждает, что B отрицает, что C говорит, будто D солгал*» совместимы некоторые комбинации истины и лжи. Выясним, какие именно. Итак, начнем заполнять таблицу истинности, начиная с D. Нас интересует случай, когда D сказал истину.

Начало таблицы: $\begin{pmatrix} A & B & C & D \\ ? & ? & И & И \end{pmatrix}$ и $\begin{pmatrix} A & B & C & D \\ ? & ? & Л & И \end{pmatrix}$.

Если D сказал истину и C – тоже, то C НЕ говорил, будто D солгал. В этом случае, если B говорит истину, то и A может сообщать только истину. Если в случае $\begin{pmatrix} C & D \\ \dots & И & И \end{pmatrix}$ высказывание

B ложно, т. е. B НЕ отрицал, что C говорил, будто D солгал, то A, утверждая, что B отрицает и т. д., лжет. Итак, если D сказал истину и C сказал истину, то обязательно либо и A, и B говорят истину, либо оба лгут. Другими словами, из $\begin{pmatrix} C & D \\ \dots & И & И \end{pmatrix}$ следует, что

возможны два варианта: $\begin{pmatrix} A & B & C & D \\ И & И & И & И \end{pmatrix}$ и $\begin{pmatrix} A & B & C & D \\ Л & Л & И & И \end{pmatrix}$.

Рассмотрим случай $\begin{pmatrix} C & D \\ \dots & Л & И \end{pmatrix}$, т. е. D сказал правду, а C говорит, будто D солгал. Если B говорит истину, то он НЕ отрицает, что C говорит, будто D солгал, но тогда A лжет. Если же B лжет, то он отрицает, что C сказал, что D солгал. Тогда A, утверждая, что B отрицает, и т. д., говорит правду.

Вывод: из $\begin{pmatrix} C & D \\ \dots & Л & И \end{pmatrix}$ следует, что либо A лжет, а B говорит правду, либо наоборот.

Подведем предварительный итог. Непротиворечивы следующие варианты, и только они: $\begin{pmatrix} A & B & C & D \\ И & И & И & И \end{pmatrix}$, $\begin{pmatrix} A & B & C & D \\ Л & Л & И & И \end{pmatrix}$, $\begin{pmatrix} A & B & C & D \\ Л & И & Л & И \end{pmatrix}$, $\begin{pmatrix} A & B & C & D \\ И & Л & Л & И \end{pmatrix}$.

Поскольку каждый из высказывающихся говорит правду в одном случае из трех и делает это независимо от других, то таблица всех возможных случаев имеет $3^4 = 81$ строку.

Комбинацию $\begin{pmatrix} A & B & C & D \\ И & И & И & И \end{pmatrix}$ можно получить лишь одним способом (1 строка в таблице), а каждую из комбинаций $\begin{pmatrix} A & B & C & D \\ Л & Л & И & И \end{pmatrix}$, $\begin{pmatrix} A & B & C & D \\ Л & И & Л & И \end{pmatrix}$, $\begin{pmatrix} A & B & C & D \\ И & Л & Л & И \end{pmatrix}$ – четырьмя способами (на каждое ложное высказывание одного приходится два ложных высказывания другого).

Понимая вероятность как отношение числа исходов, благоприятных наступлению события, к общему числу исходов, получаем $P = \frac{1+4+4+4}{81} = \frac{13}{81}$.

Задача 29: Покажем, что всегда можно определить загаданные числа не более чем за 13 вопросов.

Называя пары (1, 2), (3, 4), ..., (21, 22), мы используем 11 вопросов; при этом возможны следующие 4 случая:

- а) после какого-то вопроса получен ответ «2»;
- б) на все вопросы получены ответы «0»;
- в) на какие-то два вопроса – i -й и j -й – получены ответы «1»;
- г) только на один i -й вопрос получен ответ «1», на остальные вопросы – «0» (без рассмотрения этого случая можно сделать неправильный вывод, что нельзя гарантировать определение загаданных чисел за 13 вопросов).

Укажем дальнейшие действия отгадывающего в каждом из этих случаев.

- а) После ответа «2» загаданные числа определены.
- б) Загаданы два числа из чисел 23, 24, 25. Задаём вопрос (23, 24). Если ответ «2», то эти числа и загаданы, если ответ «1», то вопросом (23, 22) определим, какое из чисел – 23 или 24 – загадано наряду с числом 25.
- в) Числа в i -й паре $(2i-1)$ и $2i$, в j -й паре – $(2j-1)$ и $2j$. Задаём вопросы $(25, 2i)$, $(25, 2j)$.

Ответ «1» на первый (двенадцатый) вопрос означает, что в i -й паре загадано число $2i$; ответ «0» указывает на число $(2i-1)$. Аналогично со вторым (тринадцатым) вопросом.

г) Вопросы $(2i, 23)$, $(2i, 24)$ при всех возможных ответах определяют загаданные числа. В самом деле, ответ «2» на первый или второй вопрос не требует пояснений. Для других комбинаций ответов на эти два вопроса мы сообщаем загаданные числа (легко проверяется, что другого мнения о том, какие числа загаданы, не может быть) – см. таблицу.

Ответ	Загаданные числа
1, 1	$2i$, 25
1, 0	$2i-1$, 23
0, 1	$2i-1$, 24
0, 0	$2i-1$, 25

Итак, мы показали, что за 13 вопросов всегда можно определить загаданные числа; естественно, как следует из решения, иногда хватает и меньшего количества вопросов.

Для завершения решения докажем, что нельзя гарантировать определение загаданных чисел за 12 вопросов. После 11 вопросов все ответы могут быть «0»; при этом всегда существуют три числа, не включённые в вопросы. Если двенадцатый вопрос не содержит ни одного из этих трёх чисел, то ответ «0» позволит любым двум из них быть загаданными. Если же в двенадцатый вопрос входит одно или два из этих двух чисел, то после ответа «1» также нельзя однозначно указать загаданные числа.

Задача 30: Назовем игроков Первый и Второй. Занумеруем карты числами от 0 до 6. Пусть Первый и Второй по очереди назовут остатки от деления суммы номеров своих карт на 7. Тогда они узнают расклад: каждый из них должен лишь прибавить к своей сумме сумму другого и найти остаток, противоположный этой общей сумме по модулю 7 (т. е. такой, который при прибавлении к этой сумме даст число, делящееся на 7). Это и будет номер карты Наблюдателя. После этого восстановление расклада не составляет труда. Проверим, что Наблюдатель ничего не узнал. Рассмотрим карту с номером s . Покажем, что она могла попасть к Первому, если он назвал сумму a . Для этого надо дополнить эту карту двумя другими с суммой номеров $a-s$. Легко видеть, что существует три различные пары номеров, дающих в сумме $a-s$. Из них две, возможно, испорчены тем, что туда входит карта с номером s или карта, оставшаяся у Наблюдателя. Но как минимум одна пара остается. Ею мы и дополним набор Первого. Такие же рассуждения показывают, что любая карта могла оказаться и у Второго.

Приведем пример. Пусть Первый сообщает открыто число 3, а Второй – число 4. Теперь они, сложив 3 и 4 и поделив сумму

с остатком на 7, получают 0. И они знают карту Наблюдателя: это карта с номером 0. Ясно, что после этого каждый из них знает весь расклад. Наблюдатель, видя свою карту с номером 0, услышав число 3, делает вывод: у Первого сумма номеров карт равна 10. Услышав число 4, Наблюдатель делает вывод: у Второго сумма номеров карт равна 11. Но сумма 10 может быть получена сложением чисел: 1, 3, 6, т. е. возможен расклад: у Первого 1, 3, 6; у Второго 2, 4, 5. Но возможен и такой расклад: у Первого 1, 4, 5; у Второго 2, 3, 6. И еще такой: у Первого 2, 3, 5; у Второго 1, 4, 6. И мы видим, что карта с любым номером могла оказаться как у Первого, так и у Второго. И Наблюдатель не узнал местонахождение ни одной карты.

Задача 35: Заметим, что в этой задаче буквы Е и Ё не различаются, иначе цифр было бы 11. Двухзначные числа, являющиеся квадратами: 16, 25, 36, 49, 64, 81. Запишем варианты для слов ЖЕ, ОН и НЕ:

ЖЕ	ОН	НЕ
16	16	16
25	25	25
36	36	36
49	49	49
64	64	64
81	81	81

Вторая цифра числа из первого столбца должна совпадать со второй цифрой числа из третьего столбца, а первые цифры должны быть разными. Следовательно, либо ЖЕ = 16, НЕ = 36, либо ЖЕ = 36, НЕ = 16. Но первая цифра числа из третьего столбца совпадает со второй цифрой числа из второго столбца, поэтому остался единственный вариант: НЕ = 16, ОН = 81, ЖЕ = 36. Теперь обратим внимание на слово ВСЕ. Этому слову соответствует число, последняя цифра которого 6. Квадрат двухзначного числа оканчивается цифрой 6, следовательно, это двухзначное число может иметь вторую цифру либо 4, либо 6. Такие числа: 14, 16, 24, 26. Но $14^2 = 196$, а букве В не может соответ-

ствовать 1. Далее $16^2 = 256$, но тогда $B = 2$, и слову ПРАВ соответствует число, оканчивающееся цифрой 2, что невозможно: квадрат натурального числа не может иметь последнюю цифру 2. Проверяем число 26, получаем $26^2 = 676$, но тогда $B = 6$, т. е. $B = E$ – противоречие. Вычисляем $24^2 = 576$, и это единственный вариант для слова ВСЕ, не противоречащий условиям задачи. Итак, $B = 5$. Значит, число, квадрат которого соответствует слову ПРАВ, оканчивается цифрой 5, но тогда последние две цифры числа, соответствующего ПРАВ, это 25, т. е. $A = 2$. Двухзначное число, вторая цифра которого 5 и квадрат которого состоит из различных цифр, только одно, это 95, так что ПРАВ = 9025. И для буквы И остался единственный вариант, это 4.

Ответ: 4 576 36 81 16 9025.

Краткий исторический очерк развития криптографии

Наукой не установлен точный исторический период, когда появилась криптография, каковы были ее первоначальные формы и кто был ее создателем. Однако считается, что криптография старше египетских пирамид. Уже в исторических документах древних цивилизаций — Индии, Египта, Месопотамии — имеются сведения о системах и способах составления шифрованного письма. Сохранились достоверные сведения о системах шифров, применявшихся в Древней Греции. Свой след в истории криптографии оставили многие хорошо известные исторические личности.

В истории криптографии условно можно выделить четыре этапа:

- I. Наивный;**
- II. Формальный;**
- III. Научный;**
- IV. Компьютерный.**

Рассмотрим кратко каждый из этапов.

I. Для *наивной криптографии* (до начала XVI в.) характерно использование любых, обычно примитивных, способов запутывания противника относительно содержания шифруемых тек-

стов. На начальном этапе для защиты информации использовались методы кодирования и стеганографии, которые родственны, но не тождественны криптографии.

Большинство из используемых шифров сводились к перестановке или моноалфавитной подстановке.

Первые сведения об использовании шифров в военном деле связаны с именем спартанского полководца Лисандра, разработавшего шифр «Считала». Этот шифр известен со времен войны Спарты против Афин в V веке до н.э. Для его реализации использовалась считала – жезл, имеющий форму цилиндра. На считалу виток к витку наматывалась узкая папирусная лента (без просветов и нахлестов), а затем на этой ленте вдоль оси считалы записывался текст. Лента разматывалась, и получалось (для непосвященных), что поперек ленты в беспорядке написаны какие-то буквы. Затем лента отправлялась адресату. Адресат брал такую же считалу, таким же образом наматывал на неё полученную ленту и читал сообщение вдоль оси считалы. В этом шифре преобразование открытого текста в зашифрованный заключается в определенной перестановке букв открытого текста. Поэтому класс шифров, к которым относится и шифр «Считала», называется *шифрами перестановки*.

Считается, что автором способа взлома шифра считалы является Аристотель, который наматывал ленту на конусообразную палку до тех пор, пока не появлялись читаемые куски текста.

С именем Энея Тактика, полководца IV века до н.э., связывают несколько техник шифрования и тайнописи.

Диск Энея представлял собой диск диаметром 10–15 см с отверстиями по числу букв алфавита. Для записи сообщения нитка протягивалась через отверстия в диске, соответствующим буквам сообщения. При чтении получатель вытягивал нитку, и получал буквы, правда, в обратном порядке. Хотя недоброжелатель мог прочесть сообщение, если перехватит диск, Эней предусмотрел способ быстрого уничтожения сообщения – для этого было достаточно выдернуть нить, закреплённую на катушке в центре диска.

Первым действительно криптографическим инструментом можно назвать линейку Энея, реализующей шифр замены. Вместо диска использовалась линейка с отверстиями по числу букв алфавита, катушкой и прорезью. Для шифрования нить протягивалась через прорезь и отверстие, после чего на нити завязывался очередной узел. Для дешифрования необходимо было иметь саму нить и линейку с аналогичным расположением отверстий. Таким образом, даже зная алгоритм шифрования, но, не имея ключа (линейки), прочитать сообщение было невозможно.

В своём сочинении «О перенесении осады» Эней описывает ещё одну технику тайнописи, позже названную «*книжный шифр*». Он предложил делать малозаметные дырки рядом с буквами в книге или другом документе.

Эта система применялась даже в середине XX века, во время Второй мировой войны.

Во II веке до н.э. в Древней Греции был изобретён Квадрат Полибия. В нём буквы алфавита записывались в квадрат 5 на 5 (при использовании греческого алфавита одна ячейка оставалась пустой), после чего с помощью оптического телеграфа передавались номер строки и столбца, соответствующие символу исходного текста (на каждую букву приходилось два сигнала: число факелов обозначало разряд буквы по горизонтали и вертикали).

Некоторые исследователи полагают, что это можно рассматривать как первую систему, уменьшавшую (сжимавшую) исходный алфавит, и, в некотором смысле, как прообраз современной системы двоичной передачи данных.

Постепенно, по мере распространения техники частотного криптоанализа, шифры усложняются, что приводит к появлению шифров омофонической замены, а затем и полиалфавитных шифров.

Первые попытки систематизации и обобщения накопленного за века опыта были предприняты в арабских странах. Арабского происхождения и само слово «*шифр*».

Арабский филолог Халиль аль-Фарахида первым обратил внимание на возможность использования стандартных фраз открытого текста для дешифрования. Он предположил, что первыми словами в письме на греческом языке византийскому императору будут «Во имя Аллаха», что позволило ему прочитать

оставшуюся часть сообщения. Позже он написал книгу с описанием данного метода – «Китаб аль-Маумма» («Книга тайного языка»).

Первая книга, специально посвященная описанию и сравнению разных систем шифрования, появилась в 855 году. Это «Книга о большом стремлении человека разгадать загадки древней письменности» арабского учёного Абу Бакр Ахмед бен-Али бен-Вахшия ан-Набати, содержала описания нескольких шифров, в том числе с применением нескольких алфавитов. Также к IX в. относится первое известное упоминание о частотном криптоанализе – в книге Ал-Кинди «Манускрипт о дешифровке криптографических сообщений».

В книге X в. «Адаб аль-Куттаб» («Руководство для секретарей») ал-Сули есть инструкции по шифрованию записей о налогах, что подтверждает распространение криптографии в обычной, гражданской жизни.

В 1412 г. выходит 14-томная энциклопедия Шехаба ал-Кашканди «Шауба ал-Аша», один из разделов которой «Относительно сокрытия в буквах тайных сообщений» содержал описание семи шифров замены и перестановки, частотного метода криптоанализа, а также таблицы частотности букв в арабском языке.

II. Этап *формальной криптографии* (конец XV – начало XX вв.) связан с появлением формализованных и относительно стойких к ручному криптоанализу шифров. В европейских странах это произошло в эпоху Возрождения, когда развитие науки и торговли вызвало спрос на надежные способы защиты информации. Важная роль на этом этапе принадлежит Леону Батисте Альберти, итальянскому архитектору, который одним из первых предложил многоалфавитную подстановку. Данный шифр, получивший имя дипломата XVI в. Блеза Вижинера, состоял в последовательном "*сложении*" букв исходного текста с ключом (процедуру можно облегчить с помощью специальной таблицы). Его работа "Трактат о шифре" считается первой научной работой по криптологии. Одной из первых печатных работ, в которой обобщены и сформулированы известные на тот момент алгоритмы шифрования, является труд "Полиграфия" немецкого аббата Иоганна Трисемуса. Ему принадлежат два небольших, но важных открытия:

способ заполнения полибианского квадрата (первые позиции заполняются с помощью легко запоминаемого ключевого слова, остальные – оставшимися буквами алфавита) и шифрование пар букв (биграмм). Простым, но стойким способом многоалфавитной замены (подстановки биграмм) является шифр Плейфера, который был открыт в начале XIX в. Чарльзом Уитстоном. Уитстону принадлежит и важное усовершенствование – шифрование *"двойным квадратом"*. Шифры Плейфера и Уитстона использовались вплоть до первой мировой войны, так как с трудом поддавались ручному криптоанализу. В XIX в. голландец Керкхофф сформулировал главное требование к криптографическим системам, которое остается актуальным и поныне: секретность шифров должна быть основана на секретности ключа, но не алгоритма.

Известно, что крупные политические и военные акции Ивана Грозного оказали влияние и на развитие тайнописного дела. И традиции были продолжены. Так, в наказе царя Федора Иоанновича (1557–1589) – сына Ивана Грозного, данном в 1589 г. послу Николаю Воркачу, ему поручалось «писать письма мудрою азбукою, чтоб оприч Царского величества никто не разумел». С конца XVI в. русские посланники за рубежом получают шифры в виде таблиц. И все же первым из российских государей, который предельно ясно осознавал важность развития шифровального дела для обеспечения безопасности государства, был Петр Великий. Государственные шифры того времени были шифрами простой замены. В российские шифры с начала XVIII в., как правило, вводятся «пустышки» – шифрообозначения, которым не соответствует никакого знака открытого текста. Хотя обычно для этого использовалось всего пять–восемь шифровеличин в качестве пустышек, очевидно, что введение их в шифротекст отражает стремление создателей шифров осмыслить процесс дешифрования. Эти пустышки разбивают структурные лингвистические связи открытого текста и изменяют статистические характеристики, т. е. именно те особенности текста, которые используют в первую очередь при атаке на шифр простой за-

мены. Кроме того, они изменяют длину передаваемого сообщения. Поэтому, видимо, не случайно, первый такой русский шифр был раскрыт англичанами лишь в 1725 г.

Наконец, последним словом в донаучной криптографии, которое обеспечило еще более высокую криптостойкость, а также позволило автоматизировать процесс шифрования стали роторные криптосистемы.

Одной из первых подобных систем стала изобретенная в 1790 г. Томасом Джефферсоном механическая машина. Многоалфавитная подстановка с помощью роторной машины реализуется вариацией взаимного положения вращающихся роторов, каждый из которых осуществляет «*прошитую*» в нем подстановку.

Практическое распространение роторные машины получили только в начале XX века. Одной из первых практически используемых машин, стала немецкая Enigma, разработанная в 1917 г. Эдвардом Хеберном и усовершенствованная Артуром Кирхом. Роторные машины активно использовались во время второй мировой войны. Помимо немецкой машины Enigma использовались также устройства Sigaba (США), Typex (Великобритания), Red, Orange и Purple (Япония). Роторные системы – вершина формальной криптографии, так как относительно просто реализовывали очень стойкие шифры. Успешные криптоатаки на роторные системы стали возможны только с появлением ЭВМ в начале 40-х годов.

И первая, и вторая мировые войны дали много примеров применения математики к анализу шифров. Криптографы воюющих стран напряженно работали, совершенствуя свои алгоритмы шифрования и "*взламывая*" шифры противника. И во второй половине XX в. ведущие державы мира уделяли большое внимание развитию криптографии.

III. Главная отличительная черта *научной криптографии* (1930–1960-е гг.) – появление криптосистем со строгим математическим обоснованием криптостойкости. К началу 30-х гг. окончательно сформировались разделы математики, являющиеся научной основой криптологии: теория вероятностей и математическая статистика, общая алгебра, теория чисел, начали активно развиваться теория алгоритмов, теория информации, кибернетика.

Своеобразным водоразделом стала работа Клода Шеннона «Теория связи в секретных системах», которая подвела научную базу под криптографию и криптоанализ. С этого времени стали говорить о криптологии (от греческого «*kryptos*» – «тайный» и «*logos*» – «общение») – науке о преобразовании информации для обеспечения ее секретности. Этап развития криптографии и криптоанализа до 1949 г. стали называть *донаучной криптологией*.

Шеннон ввел понятия «*рассеивание*» и «*перемешивание*», обосновал возможность создания сколь угодно стойких криптосистем. В 1960-х гг. ведущие криптографические школы подошли к созданию блочных шифров, еще более стойких по сравнению с роторными криптосистемами, однако допускающих практическую реализацию только в виде цифровых электронных устройств.

IV. *Компьютерная криптография* (с 1970-х гг.) обязана своим появлением вычислительным средствам с производительностью, достаточной для реализации криптосистем, обеспечивающих при большой скорости шифрования на несколько порядков более высокую криптостойкость, чем «*ручные*» и «*механические*» шифры.

Первым классом криптосистем, практическое применение которых стало возможно с появлением мощных и компактных вычислительных средств, стали блочные шифры. В 70-е гг. был разработан американский стандарт шифрования DES. Один из его авторов, Хорст Фейстель описал модель блочных шифров, на основе которой были построены другие, более стойкие симметричные криптосистемы, в том числе отечественный стандарт шифрования ГОСТ 28147–89.

С появлением DES обогатился и криптоанализ, для атак на американский алгоритм был создано несколько новых видов криптоанализа (линейный, дифференциальный и т.д.), практическая реализация которых опять же была возможна только с появлением мощных вычислительных систем.

В середине 70-х гг. XX столетия произошел настоящий прорыв в современной криптографии – появление асимметричных криптосистем, которые не требовали передачи секретного ключа между сторонами. Здесь отправной точкой принято считать ра-

боту, опубликованную Уитфилдом Диффи и Мартином Хеллманом в 1976 г. под названием «Новые направления в современной криптографии». В ней впервые сформулированы принципы обмена шифрованной информацией без обмена секретным ключом. Независимо к идее асимметричных криптосистем подошел Ральф Меркли. Несколькими годами позже Рон Ривест, Ади Шамир и Леонард Адлеман открыли систему RSA, первую практическую асимметричную криптосистему, стойкость которой была основана на проблеме факторизации больших простых чисел. Асимметричная криптография открыла сразу несколько новых практических направлений, в частности системы электронной цифровой подписи (ЭЦП) и электронных денег.

В 1980–90-е гг. появились совершенно новые направления криптографии: вероятностное шифрование, квантовая криптография и другие. Актуальной остается и задача совершенствования симметричных криптосистем. В этот же период были разработаны нефеистелевские шифры (SAFER, RC6 и др.), а в 2000 г. после открытого международного конкурса был принят новый национальный стандарт шифрования США – AES.

Теоретические вопросы

1. Каково максимальное число простых замен, из которых может состоять многоалфавитный шифр?
2. Алгоритмы сжатия данных хорошо подходят для совместного использования с криптографическими алгоритмами. Какой из двух вариантов предпочтительнее: сжать файл до того, как он будет зашифрован или сначала зашифровать, потом сжать?
3. В алгоритме DES таблицы замен одинаковы для всех пользователей и открыто опубликованы, секретным является только ключ. В российском алгоритме ГОСТ 28147–89 таблицы (а не только ключ) секретны и выбираются пользователем. Перечислите достоинства и недостатки этих двух подходов.
4. Перечислите причины, по которым криптостойкость алгоритма шифрования со временем изменяется.
5. Попробуйте назвать как можно большее количество причин ненадежности криптосистем.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Зубов А. Ю., Зязин А. В., Овчинников В. Н., Рамоданов С. М.* Олимпиады по криптографии и математике для школьников – М.: МЦНМО, 2006. – 136 с.: ил.
2. *Морозова Е. А., Петраков И. С., Скворцов В. А.* Международные математические олимпиады. Задачи, решения, итоги: пособие для учащихся. – 4-е изд., испр. и доп. – М.: Просвещение, 1976. – 288 с.: ил.
3. *Страшевич С., Бровкин Е.*; предисл. *Пелчинского А. и Шинцеля А.* Польские математические олимпиады / Пер. с польск. *Ю. А. Данилова* / Под ред. *В. М. Алексеева*. – М.: Мир, 1978. – 338 с.: ил.
4. *Леман А. А.* Сборник задач московских математических олимпиад : пособие для внеклассной работы по математике / Под ред. *В. Г. Болтянского*. – М.: Просвещение, 1965. – 298 с.: ил.
5. *Алфёров А. П., Зубов А. Ю., Кузьмин А. С., Черёмушкин А. В.* Основы криптографии: Учеб. пособие. – М. : Гелиос АРВ, 2001. – 480 с.: ил.
6. *Овсянников Э. Ф.* От «А» до «Я»: словесные игры. – Минск: Полымя, 1994. – 233 с.: ил.
7. *Берлов С. Л., Иванов С. В., Кохась К. П.* Петербургские математические олимпиады. – СПб.: Лань, 1998. – 448 с.
8. *Конягин С. В., Тоноян Г. А., Шарыгин И. Ф. и др.* Зарубежные математические олимпиады/Под ред. *И.Н. Сергеева*. – М.: Наука, 1987. – 416 с. – (Б-ка мат. кружка).
9. Избранные задачи по математике из журнала «American Mathematical Monthly»: Учеб. пособие. / Пер. с англ. / Под ред. и с предисл. *В. М. Алексеева*. – 3-е изд. – М.: Либроком, 2009. – 600 с.
10. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си – М.: Триумф, 2003. – 816 с.: ил.
11. Введение в криптографию / Под общ. ред. *В. В. Яценко*. – М.: Моск. центр непрерыв. мат. образования, 2000. – 288 с.
12. *Жданов О. Н., Золотарев В. В.* Методы и средства криптографической защиты информации: Учеб. пособие.– Красноярск: Сиб. гос. аэрокосмич. ун-т, 2007. – 253 с.

13. *W. Diffie and M.E. Hellman.* «New Directions in Cryptography», IEEE Transactions on Information Theory. – V. IT-22, n.6, Nov 1976. – PP. 644–654.

14. *Adleman L. M., Rivest R. L., Shamir A.* A method for obtaining digital signatures and public-key cryptosystems. – Comm. – V. 21, ACM, 1978. – P.120–126.

15. КРИПТОГРАФИЯ. Сборник задач краевых олимпиад 2007–2011 гг. с решениями и комментариями / Под ред. *О. Н. Жданова.* – Красноярск: СибГАУ, 2011. – 98 с.

16. *Жданов О. Н., Куденкова И. А.* Криптоанализ классических шифров. – Красноярск: СибГАУ, 2007.

17. Задачи лингвистических олимпиад. 1965–1975 / Ред.-состав. *В. И. Беликов, Е. В. Муравенко, М. Е. Алексеев.* / – М.: МЦНМО, 2006. – 570 с.

СОДЕРЖАНИЕ

Введение.....	3
1 Шифры перестановки.....	7
2 Шифры замены.....	17
3 Советы по выполнению частотного анализа английских текстов.....	28
4 Шифр Виженера.....	33
5 Разные задачи.....	56
6 Аутентификация.....	71
Библиографический список.....	94

Учебное издание

Жданов Олег Николаевич
Елемесов Куат Каирович

НАЧАЛА КРИПТОГРАФИИ
В ЗАДАЧАХ И УПРАЖНЕНИЯХ

Учебное пособие

Нач. РО УИЦ

Редактор

Компьютерная верстка

З. А. Губайдулина

З. А. Губайдулина

Л. Т. Касжанова

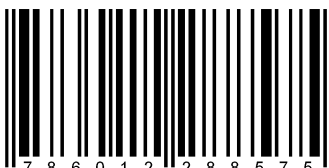
Подписано в печать 08.02.2016 г.

Тираж 300 экз. Формат 60х84х 1/16. Бумага типогр. № 1.
Уч.-изд.л. 6,0. Усл. п.л. 5,58. Заказ № 666. Цена договорная.

Издание Казахского национального исследовательского
технического университета имени К. И. Сатпаева

Учебно-издательский центр КазНITU имени К. И. Сатпаева,
г. Алматы, ул. Сатпаева, 22

ISBN 978-601-228-857-5



9

7 8 6 0 1 2 2 8 8 5 7 5