Златопольский Дмитрий Михайлович
Кандидат технических наук, доцент кафедры информатики и прикладной математики Московского городского педагогического университета.

Простейшие методы шифрования текста

В статье описан ряд простейших методов шифрования текста – его преобразования с целью невозможности чтения теми, кому текст не предназначен. Среди них – методы, основанные на замене символов, перестановочные шифры, шифрование с помощью таблиц и др.

Помните удивительную историю с пляшущими человечками, рассказанную знаменитым сыщиком Шерлоком Холмсом своему другу доктору Ватсону? Мы её пересказывать не будем, а только приведём странные записки, которые преступник посылал своей жертве, а потом напомним конец рассказа. Вот эти записки:

Рис. 1

Пляшущие человечки каждому могут показаться смешными: детские рисунки, глупая забава. А вот Шерлок Холмс, хорошо знакомый с различными видами тайнописи и даже написавший небольшую статью по этому вопросу, сразу определил, что перед ним шифр. Он понял: фигурки означают буквы, и начал искать ключ.

Вскоре ключ был найден, и знаменитый сыщик постепенно вытащил из небытия одну букву за другой.

Это позволило ему не только прочитать записки, но и самому послать преступнику строчку пляшу-

щих человечков, и... преступник попал в руки правосудия. Пляшущие фигурки означали слова: «Приходите сюда сейчас».

Существует много разных систем шифрования. К ним прибегают в военном деле, на дипломатической службе, вообще в тех случаях, когда нужно сохранить в тайне содержание переписки. Шифрование текста используется человечеством с того самого момента, как появилась первая секретная информация, т. е. такая, которая должна быть недоступна тем, кому она не предназначена.

1. Шифр Цезаря. Один из самых первых известных методов шифрования носит имя римского императора Юлия Цезаря (I век до н. э.), который если и не сам изобрёл его, то активно им пользовался. Этот метод основан на замене каждой буквы шифруемого текста на другую путём смещения в алфавите от исходной буквы на фиксированное количество символов, причём алфавит читается по кругу, т. е. после буквы *я* рассматривается *а*. Регистр символов не учитывается. Так, например, слово *байт* при смещении на два символа вправо кодируется словом *гвлф*.

1. Расшифруйте слово НУЛТХСЁУГЧЛВ, закодированное с помощью шифра Цезаря. Известно, что каждая буква исходного текста заменяется третьей после неё буквой.

2. Расшифруйте четверостишие Омара Хайяма:

РЛЗЬ ЁМЭЙЗ АВБЖУ ИЙЗАВЛУ, БЖЩЛУ ЖЩЭЗЬЖЗ ЖЮЁЩЕЗ,
ЫЩ ЫЩАЖФО ИЙЩЫВЕЩ БЩИЗЁЖВ ЭЕШ ЖЩРЩЕЩ:
ЛФ ЕМРСЮ ЪЗЕЗЭЩГ, РЮЁ РЛЗ ИЗИЩЕЗ ЮКЛУ
В ЕМРСЮ ЬМЭУ ЗЭВЖ, РЮЁ ЫЁЮКЛЮ К ДЮЁ ИЗИЩЕЗ.

Конкретный вариант шифрования методом Цезаря неизвестен.

2. Буратино и шифровка. Буратино обнаружил начальную строку зашифрованного послания, написанного неизвестным ему шифром:

ШЫР-ПИР Ю ПАПУЖГЫ
ЗЭЛЭМЪЫЙ ГЁСРЫГ...

Помогите Буратино расшифровать послание.

3. Машина для расшифровки из бумаги. Для шифра Цезаря имеется простой способ расшифровки текста, даже если направление и величина сдвига букв в алфавите неизвестны – так называемый «метод полосок». Берутся несколько полосок из бумаги, картона и т. п. и на каждую из них наносятся по порядку все буквы алфавита (см. рис. 2).

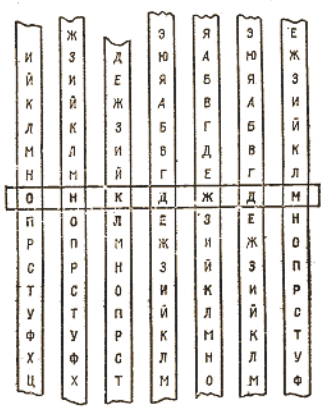


Рис. 2

В криптограмме (тексте, представляющем собой зашифрованное

сообщение) берётся некоторое слово, например, *онкдждм*. Полоски прикладываются друг к другу так, чтобы образовать данное слово (рис. 2). Двигаясь вдоль полосок, находим среди строк единственное осмысленное сочетание *полезен*, которое и служит расшифровкой данного слова. Одновременно можно найти величину сдвига.

В качестве упражнения предлагаю читателю расшифровать методом полосок следующую криптограмму, зашифрованную методом Цезаря:

ЕИФИРРЛМ ФЕИХОЮМ ЗИРЯ НОСРОФВ Н ЕИЫИУЦ РСКСЕЮИ ХЦЫНЛ ФХСВОЛ ЕЮФСНС Е ВФОСП РИДИ Л НГКГССЯ РИ ТОЮОЛ ПЛПС Г ЦШСЗЛОЛ Е ФГПЦБ ЖОЦДЯ ОГКЦУЛ.

Чтобы оценить преимущества описанной «машины», попробуйте также с её помощью расшифровать приведённое в п. 1 четверостишие Омара Хайяма.

4. «Тарабарская грамота». Найдите ключ к «тарабарской грамоте» – тайнописи, применявшейся ранее в России для дипломатической переписки:

Рис. 3

Пайцике тсюг т «камащамлтой чмароке» – кайпонили, нмирепяшвейля ш Моллии цся цинсоракигелтой неменилти.

Ключом в данном случае будем называть правила, по которым шифруется исходный текст.

5. Карл пишет Кларе. Клара получила от Карла письмо по электронной почте. Из-за неправильной настройки компьютера то ли у Карла, то ли у Клары текст письма выглядел так:

▲□♥▼♥♪ ⌂▶☻☺ ●☻■□♥♦♠☺
●▼☻┼☺■◀◙ ♦☺ ■♂☻◘♫ ◀♥Δ
Δ♥Δ ▶◀☻▼☻☺ ●♠■◙♂☻
●☻◀☺▼▌□☻■◙♣
♀◀●▼♥▶◙ ☺☼☻
●☻▶◀☻▼♦☻♣ ▲♥▼□♣

Рис. 4

Помогите Кларе прочитать послание. Клара знает, что Карл всегда правильно расставляет в письмах знаки препинания, а вместо буквы *ё* всегда пишет *е*.

6. Номера вместо букв. Если в некотором слове заменить буквы на номера этих букв в алфавите, то получится число 222122111121. Какое это слово?

7. Однажды в поезде. Когда-то давно, когда ещё существовала страна под названием СССР, автор статьи ехал в поезде и с удивлением обнаружил, что если в названиях пунктов отправления и назначения поезда заменить буквы их номерами в алфавите, то они (названия) записываются с помощью всего лишь двух цифр: 211221 и 21221.

Откуда и куда ехал автор?

8. Расшифровка текста. В рассмотренных ранее задачах шифрование текста было основано на принципе замены, при котором общепринятые буквы заменяются другими буквами, цифрами или какими-то символами. Но это, оказывается, не самый надёжный способ, и при известном навыке можно очень легко дойти до истинного смысла зашифрованного подобным образом текста, даже не зная того,

что мы называем таблицей кодировки, и в случае достаточно сложного шифра.

Пусть, например, в ваши руки попала следующая криптограмма, написанная по принципу замены букв числами (одинаковые буквы заменялись одинаковыми числами):

1, 2, 3 – 2, 3 – 4, 5, 6, 7, 4, 8 – 2, 3, 7 – 9, 10, 2, 8
11, 4, 12, 13, 14 – 1, 15, 16, 17 – 6 – 4, 9, 2 – 13, 9, 17, 14, 18, 2, 19, 20
21, 9, 13 – 18, 16, 4, 9, 11 – 22, 6, 23, 24 – 9, 13, 2, 9, 25, 11, 14, 18, 2, 19, 20
15, 16, 25, 13, 16, 3, 7, 4, 8 – 26, 22, 6, 25 – 1, 3, 2, 8

Слова в ней отделены друг от друга дефисом («-»), буквы – запятыми. Известно, что в самом зашифрованном тексте тире и дефисов нет и что буквы *е* и *ё* закодированы одним и тем же числом. Расшифруйте эту криптограмму. Не бойтесь попробовать – это можно сделать путём рассуждений.

9. Частотный анализ. Восстановить буквы текста, зашифрованного путём замены, с большой уверенностью можно, анализируя частоту появления тех или иных букв и их сочетаний. Этот метод (он так и называется – *частотный анализ*) основывается на том, что известно, как часто встречается та или иная буква в русском языке (или в английском языке – именно это учитывал герой рассказа Эдгара По «Золотой жук», расшифровывая найденный пергамент). Даже если в каких-то частях текста возникает неоднозначность, она легко устраняется по смыслу.

Относительные частоты букв русского языка указаны в табл. 1.

Таблица 1

№	Буква	Относит. частота	№	Буква	Относит. частота	№	Буква	Относит. частота
0	а	0,062	10	к	0,028	20	ф	0,002
1	б	0,014	11	л	0,035	21	х	0,009
2	в	0,038	12	м	0,026	22	ц	0,004
3	г	0,013	13	н	0,053	23	ч	0,012
4	д	0.025	14	о	0,090	24	ш	0,006
5	е, ё	0,072	15	п	0,023	25	щ	0,003
6	ж	0,007	16	р	0,040	26	ы	0,016
7	з	0,016	17	с	0,045	27	ь, ъ	0,014
8	и	0,062	18	т	0,053	28	э	0,003
9	и	0,010	19	у	0,021	29	ю	0,006
						30	я	0,018

Буквы *е* и *ё*, а также ъ, ъ кодируются обычно одинаково, поэтому в таблице они не различаются. Как явствует из таблицы, наиболее частая буква русского языка – *о*. Её относительная частота, равная 0,090, озна-

чает, что на 1 000 букв русского текста приходится в среднем 90 букв *о*. В таком же смысле понимаются относительные частоты и остальных букв. В табл. 1 не указан ещё один «символ» – промежуток между словами (пробел). Его относительная частота наибольшая и равна 0,175.

С помощью табл. 1 читатель сумеет, по-видимому, расшифровать такую криптограмму:

Цярснсмщи ямякзж онкджлм мд снкыйн гкю онгрсямнбнцмщф йпзоснвпялл мн б гптвзф ркткяюф нм ркнемдд.

10. Что такое «лягяня»? Расшифруйте следующий, текст:

Тядзгыщхоэь пэжо ч йчтэяшаь гэнэшюэь епяу дызысю, бэхыэь пыъ бэ лягяня чтгыщюпмчо ю ч ячпыхмшаью дызысыью, Ыщпяга.

Известно, что он зашифрован следующим образом. Гласные буквы

а, о, у, ы, я, е, ю, и, э, й

как-то разбиты на пары[1]. Согласные буквы

б, в, г, д, ж, з, к, л, м, н, п, р, с, т, ф, х, ц, ч, ш, щ, ъ, ь

также как-то разбиты на пары.

Каждая буква в тексте заменена на другую букву из той же пары. Зашифрованный текст записан по правилам русской пунктуации.

11. Шифр Вижинера. Шифр Вижинера представляет собой шифр Цезаря с переменной величиной сдвига. Величина сдвига задаётся некоторым ключевым словом. Например, ключевое слово ВАЗА означает следующую последовательность сдвигов букв исходного текста: 3 1 9 1 3 1 9 1 и т. д.

Используя ключевое слово ВАГОН, зашифруйте слова: АЛГОРИТМ, ПРАВИЛА, ИНФОРМАЦИЯ.

12. Послание будущим издателям. В одной книге, которая переводилась с английского языка, при переводе были сделаны ошибки. Тем, кто будет готовить новое издание книги, послали следующую шифровку:

ИВСЬПТРЕА СРТЫАЕ ОБШКИИ И ОАПТЕКЧИ И НЕ ДЙЕТЛЕА НЫОХВ!

Расшифруйте её.

13. Перестановочный шифр. При рассмотрении задач 8 и 9 уже отмечалась ненадёжность (сравнительная лёгкость расшифровки) подстановочных криптограмм, основанных на принципе замены. Потому были разработаны и другие методы шифрования. Среди них важное место занимают так называемые «перестановочные криптограммы». При их составлении весь текст разбивается на группы, состоящие из одинакового числа букв, и внутри каждой группы буквы некоторым образом переставляются. Если группа достаточно длинная (иногда это весь текст целиком), то число возможных перестановок очень велико, отсюда большое многообразие перестановочных криптограмм. Мы рассмотрим один тип перестановочной криптограммы, которая составляется при помощи так называемого «ключевого слова». Буквы текста, который должен быть передан в зашифрованном виде, первоначально записываются в клетки прямоугольной таблицы по её строчкам. Буквы ключевого слова пишутся над столбцами и указывают порядок (нумерацию) этих столбцов способом, объясняемым ниже. Чтобы получить закодированный текст, надо выписывать буквы по столбцам с учётом их нумерации. Пусть текст таков: «В связи с создавшимся положением отодвигаем сроки возвращения домой. Рамзай[2]». Используем для записи текста, в котором 65 букв, прямоугольную таблицу 11 × 6, в качестве ключевого возьмём слово из 6 букв

[1] Буква *й* условно причислена к гласным, а буквы ъ, ь – к согласным.

[2] Рамзай – псевдоним советского разведчика Рихарда Зорге.

запись, столбцы занумеруем в соответствии с положением букв ключевого слова в алфавите. В результате получится следующая шифровочная таблица (см. табл. 2).

Таблица 2

з	а	п	и	с	ь
2	**1**	**4**	**3**	**5**	**6**
в	с	в	я	з	и
с	с	о	з	д	а
в	ш	и	м	с	я
п	о	л	о	ж	е
н	и	е	м	о	т
о	д	в	и	г	а
е	м	с	р	о	к
и	в	о	з	в	р
а	щ	е	н	и	я
д	о	м	о	й	р
а	м	з	а	й	

Выписывая буквы из столбцов этой таблицы в порядке, соответствующем числам во второй строке (т. е. сначала из второго, затем из первого и т. д.), получаем такую шифровку:

Ссшоидмвщомвсвпноеиадаязмомирзноавоилевсемззсжогвийшаяетакряр.

Ключевое слово известно, конечно, и адресату, который поэтому без труда расшифрует это сообщение. Но для тех, кто этим ключом не владеет, восстановление исходного текста весьма проблематично (хотя в принципе и возможно). Частотный анализ здесь по вполне понятным причинам не решает задачи. В лучшем случае, поскольку частоты букв будут примерно такие, как в табл. 1, он позволяет предположить, что было применено перестановочное кодирование.

Использование ключевого слова, конечно, не обязательно, можно было указать нумерацию столбцов цифровым ключом, в данном случае числом 214356. Слово удобнее, если ключ надо хранить в памяти[1] (что немаловажно для конспирации).

Задания для самостоятельной работы

1. Подумайте, нужно ли получателю шифровки, кроме ключевого слова, знать количество строк в кодовой таблице, для того чтобы разбить шифрограмму на части, соответствующие столбцам таблицы.

2. Расшифруйте следующий текст:

метдллесньъсеенуютоислшмечсноя оячжфрпткгщоаменруоер - оелтоитеаеобпви,

если ключевое слово – *модель*.

3. Используя в качестве ключевого слово *пакет*, зашифруйте текст: «Подлинность документов полученных через агента Байтик подтверждаю Юстас».

14. Шифрование двумя цифрами.

Шифр можно ещё более усложнить, если дополнительно к этому каждую букву заменять не одним, а двумя или несколькими символами (буквами или числами). Вот пример. Расположим буквы русского алфавита в квадратной таблице 6 × 6 произвольным образом, например так, как в табл. 3.

Таблица 3

	0	*1*	*2*	*3*	*4*	*5*
0		з	и	ы	р	с
1	а	т	у	й	ь	э
2		б	в	ф	к	л
3	м	ю	я	г	х	ц
4	ч	н	о		д	е
5	ж	ш	щ	п		

Каждую букву шифруем парой цифр: первая цифра – это номер строки, в которой стоит данная буква, вторая – номер столбца. Например, букве *б* соответствует обозначение 21, а слову *шифр* – обозначение 51022304.

[1] Своей, а не компьютера – ☺.

Задания для самостоятельной работы

1. Расшифруйте следующий текст, зашифрованный с использованием табл. 2:

220511044540105345044541420502
110532411041454253044544452545414
1031305044224

2. Используя табл. 2, зашифруйте текст: «Срочно приезжай Ангел».

15. Шифр Тритемиуса. Ещё бóльшие трудности для криптоанализа (расшифровки) представляет шифр, связываемый с именем учёного аббата из Вюрцбурга Тритемиуса, которого к занятиям криптографией побуждало, быть может, не только монастырское уединение, но и потребность сохранять от огласки некоторые духовные тайны. Этот шифр является развитием описанного ранее шифра Цезаря и состоит в следующем. Буквы алфавита нумеруются по порядку числами 0, 1, ..., 30 (см. табл. 1). При шифровании некоторое ключевое слово (или номера его букв) подписывается под сообщением с повторениями, как показано ниже[1]:

всвязиссоздавшимсяположениемотодвигаемсрокивозвращениядомойра
записьзаписьзаписьзаписьзаписьзаписьзаписьзаписьзаписьзаписьзаписьз
мзай
апис

Каждая буква сообщения «сдвигается» вдоль алфавита по следующему правилу: буква с номером m в табл. 1, под которой стоит буква ключевого слова с номером k, заменяется на букву с номером $l = m + k$ (если $m + k < 31$) или букву с номером $l = m + k - 31$ (если $m + k > 31$). Например, первая буква *в* сдвигается на 7 букв и заменяется буквой *и*, следующая буква *с* остаётся без изменения и т. д. Таким образом, номер l кодирующей буквы вычисляется по формуле:

$$l = (m + k) \bmod 31,$$

где mod – операция определения остатка.

В цифровых обозначениях исходное сообщение и повторяемое ключевое слово запишутся в следующем виде (см. табл. 4).

Таблица 4

Сообщение	2	17	2	30	7	8	17	17	14	7	4	0	2
Ключ	7	0	15	8	17	27	7	0	15	8	17	27	7
Сообщение	24	8	12	17	30	15	14	11	14	6	5	13	8
Ключ	0	15	8	17	27	7	0	15	8	17	27	7	0
Сообщение	5	12	14	18	14	4	2	8	3	0	5	12	17
Ключ	15	8	17	27	7	0	15	8	17	27	7	0	15
Сообщение	16	14	10	8	2	14	7	2	16	0	25	5	13
Ключ	8	17	27	7	0	15	8	17	27	7	0	15	8
Сообщение	8	30	4	14	12	14	9	16	0	12	7	0	9
Ключ	17	27	7	0	15	8	17	27	7	0	15	8	17

После суммирования верхней и нижней строки по модулю 31 получаем последовательность чисел:
9.17.17.7.24.4.24.17.29.15.21.27.9.24.23.20.3.
26.22.14.26.22.23.1.20.8.20.20.0.14.21.4.17.
16.20.27.12.12.1.24.0.6.15.2.29.15.19.12.7.25.
20.21.25.26.11.14.27.22.26.12.7.12.22.8.26.

Наконец, заменяя числа на буквы,

[1] К сожалению, возможности типографского набора не позволяют разместить буквы строго одна под другой.

приходим к закодированному тексту:
йссшдшсюпхъйшчфгыцоыцчббфи ффаохдсрфьммбшажпвюпумзщфхщ ылоъцымзмцицы.

Если ключевое слово известно, то дешифровка производится безо всякого труда на основе равенства:

$$m = (l - k) \bmod 31.$$

Расшифровать подобный текст, если ключ неизвестен, чрезвычайно трудно, хотя в истории криптографии были случаи, когда такие тексты разгадывались.

Задания для самостоятельной работы

1. Расшифруйте следующий текст, зашифрованный шифром Тритемиуса, если ключевое слово – *Бейсик*:

5.19.19.5.20.15.14.23.4.31.22.21.20.28.17.28.23.26.15.25.14.33.25.24.17.

2. Используя ключевое слово *байт*, зашифруйте шифром Тритемиуса текст: «Срочно приезжай Ангел».

16. Три письма. Разведчик-резидент направил своему агенту три письма. В первом письме был листочек с квадратной таблицей (см. рис. 5):

Э	А	П	Я	Т	З
Р	О	Е	Т	Ы	О
В	Ш	В	О	Ш	Е
А	Р	И	Т	Е	Ф
Р	К	О	Т	Т	С
А	Н	Я	Н		А

Рис. 5

в третьем (см. рис. 6) – с таблицей:

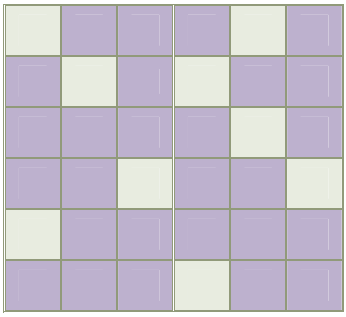


Рис. 6

Второе письмо, содержавшее пояснения по использованию этих таблиц, потерялось. Помогите агенту прочитать послание шефа.

17. Шифрование текста с помощью табличек. Если вас заинтересовал способ шифрования текста, использованный в предыдущей задаче, то давайте обсудим вопрос о том, как изготовить вспомогательную табличку, в частности, как сделать так, чтобы при поворотах окошечко не попадало повторно на уже прочитанную клетку и все клетки зашифрованного сообщения были просмотрены?

Например, необходимо зашифровать текст, содержащий k букв. Пусть $\sqrt{k} = m$. Заменим m на ближайшее к нему целое чётное число, не меньшее $\sqrt{k}$. Возьмём квадратную таблицу порядка m (m строк, m столбцов), в которой по определённому правилу будем вырезать квадраты-окошки.

В качестве примера зашифруем фразу «Тарабарская грамота – несложный шифр». В ней 31 буква, $\sqrt{31} \approx 5{,}6$. Значит, $m = 6$, т. е. наша таблица будет содержать 6 строк и 6 столбцов.

Разделим квадратную таблицу на четыре равных квадрата, обозначим их **A**, **B**, **C**, **D** .

A	B
C	D

При этом каждый из квадратов содержит $m/2$ строк. Заполним квадрат **A** последовательно числами от 1 до $(m/2)^2$. Для $m = 6$ получим:

1	2	3
4	5	6
7	8	9

При повороте квадрата **A** на 90° по часовой стрелке мы получим квадрат **B**, при этом числа квадрата **A** тоже повернутся:

7	4	1
8	5	2
9	6	3

Точно так же заполним числами квадраты **C** и **D**. Таким образом, таблица принимает вид:

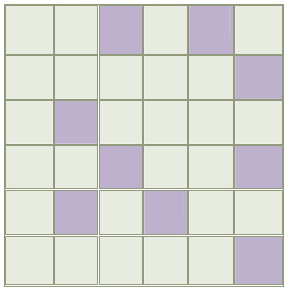
1	2	3	7	4	1
4	5	6	8	5	2
7	8	9	9	6	3
3	6	9	9	8	7
2	5	8	6	5	4
1	4	7	3	2	1

Теперь остаётся вырезать 9 «окошек» (всего клеток $6 \times 6 = 36$; поворотов – 4, значит, окошек должно быть $36/4 = 9$).

Выделяем числа от 1 до 9 из любого квадрата, например, такие:

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

Итак, окончательный вид вспомогательной таблицы-трафарета:



Вписываем в окошки построчно текст без пробелов, поворачивая вспомогательную таблицу по мере заполнения. Так как букв во фразе всего 31, а клеток – 36, то 5 оставшихся клеток заполним последовательными буквами алфавита: *а, б, в, г, д*.

н	ш	т	и	а	ф
р	а	е	я	с	р
л	а	г	о	а	р
б	а	б	в	ж	а
н	р	г	с	а	м
о	ы	т	й	а	к

Для расшифровки получателю послания необходимо воспользоваться такой же точно вспомогательной таблицей, четырежды повернуть её и прочитать текст.

Вариантов вспомогательных таблиц размера 6×6 очень много. В нашем примере окно под номером 1 мы взяли из квадрата **C**, хотя возможных вариантов – 4 (из квадрата **A**, **B**, **C** или **D**). Точно так же число 2 можно взять не из квадрата **B**, а из любого из четырех. Значит, существует $4 \times 4 = 4^2 = 16$ способов выбрать два окна. Рассуждая таким образом, приходим к выводу, что существует $4^9 = 262\,144$ различных комбинаций для таблицы размера 6×6. Так что вероятность подобрать таблицу для расшифровки крайне мала.

Как только что говорилось, для последующей расшифровки второй участник секретной переписки должен иметь точно такую же вспомогательную таблицу, то есть вместе с сообщением необходимо передавать и матрицу, что не всегда удобно. Если бы можно было и её закодировать! Один из вариантов решения этой задачи заключается в том, чтобы «окошечки» обозначить единицей, а «невырезанные» клетки – нулём. Тогда каждой строке таблицы можно поставить в соответствие

некоторое двоичное число. Далее следует перевести полученные двоичные числа в десятичные. В результате такого шифрования в приведённой чуть выше вспомогательной матрице будут записаны числа:

– 1-я строка: $001010_2 = 1010_2 = 10_{10}$,
– 2-я строка: $000001_2 = 1_2 = 1_{10}$,
– 3-я строка: $010000_2 = 10000_2 = 16_{10}$,
– 4-я строка: $001001_2 = 1001_2 = 9_{10}$,
– 5-я строка: $010100_2 = 10100_2 = 20_{10}$,
– 6-я строка: $000001_2 = 1_2 = 1_{10}$.

Теперь достаточно передать вместе с зашифрованным сообщением только полученные числа (в нашем случае это 10, 1, 16, 9, 20, 1). Количество чисел задаёт размер матрицы. После перевода десятичных чисел в двоичные таблица определяется однозначно.

Задания для самостоятельной работы

1. Расшифруйте сообщение: А Ь И Л П П П Т И О О С О З С Д Ь Ь П Р М Г О В Р А А Р М О В М Л У Р Я Е Ю О Т Ч И Е Т Т Д А А П К Р Ц Т Б А Ь Е В У К И Д Р Ю 2, 69, 16, 66, 149, 32, 4, 164.

2. Зашифруйте рассмотренным методом текст: ВСЁИДЕТПОПЛАНУ.

Литература

1. *Аршинов М.Н., Садовский Л.Е.* Коды и математика. – М.: Наука, 1983.
2. «Квант»: научно-популярный физико-математический журнал, 1970 – 1995.
3. *Кобринский Н.Е., Пекелис В.Д.* Быстрее мысли. – М.: Молодая гвардия, 1963.
4. *Кордемский Б.А.* Математическая смекалка. – М.: Юнисам, МДС, 1994.
5. *Перельман Я.И.* Занимательная математика. – М.: Издательство Русанова, 1994.

Калейдоскоп Калейдоскоп Калейдоскоп

Ньютон о «просторах науки»

Не знаю, чем я могу казаться миру, но сам себе я кажусь мальчиком, играющим на морском берегу и развлекающимся тем, что до поры до времени отыскиваю камешек более цветистый, чем обыкновенный, или красивую раковину, в то время как великий океан истины расстилается передо мной неисследованным.