

Краевой конкурс творческих работ учащихся
«Прикладные и фундаментальные вопросы математики»

Прикладные вопросы математики

Шифры и математика

Верхоланцев Владислав Игоревич,
10 кл., МБОУ «СОШ №6», г.Пермь

Орлова Елена Валентиновна,
учитель математики МБОУ «СОШ №6»

Пермь. 2012.

Содержание

Введение	3
Шифры замены	4
Шифры и сравнения	5
Шифры и статистика	7
Шифры перестановки	8
Заключение	14
Список литературы	15
Приложение 1	16
Приложение 2	18
Приложение 3	19

Введение

Как только люди научились писать, у них сразу же появилось желание сделать написанное понятным не всем, а только узкому кругу. Даже в самых древних памятниках письменности учёные находят признаки намеренного искажения текстов: изменение знаков, нарушение порядка записи и т. д. Изменение текста с целью сделать его понятным только избранным дало начало науке криптографии (греч. «тайное письмо»). Процесс преобразования текста, написанного общедоступным языком, в текст, понятный только адресату, называют шифрованием, а сам способ такого преобразования называют шифром. Но если есть желающие скрыть смысл текста, то найдутся и желающие его прочесть. Методы чтения таких текстов изучает наука криптоанализ. Хотя сами методы криптографии и криптоанализа до недавнего времени были не очень тесно связаны с математикой, во все времена многие известные математики участвовали в расшифровке важных сообщений. И часто именно они добивались заметных успехов, ведь математики в своей работе постоянно имеют дело с разнообразными и сложными задачами, а каждый шифр — это серьёзная логическая задача. Постепенно роль математических методов в криптографии стала возрастать, и за последнее столетие они существенно изменили эту древнюю науку.

Цель работы: изучить применение основ математики в криптологии.

Задачи:

- изучить историю криптографии;
- познакомиться с разными видами шифров;
- рассмотреть способы шифрования, применяющие математику
- осуществить шифровку и дешифровку текста.

1. Шифры замены

С древнейших времен основная задача шифрования была связана с сохранением тайны переписки. Сообщение, попадавшее в руки постороннему человеку, должно было быть непонятно ему, а посвященный человек мог без труда расшифровать послание.³ Приемов тайнописи великое множество. Невозможно описать все известные шифры. Наиболее простейшими из криптографических шифров являются шифры замены или подстановки, когда одни символы сообщения заменяются другими символами, согласно некоторому правилу.⁴

Например, русские дипломаты XV—XVI веков применяли так называемую «**тарабарскую грамоту**», в которой все гласные буквы оставались неизменными, а согласные заменялись друг на друга по следующей схеме: (в первой строке согласные идут в обычном порядке, а во второй строке – в обратном)¹.

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

В рассказе А. Конан-Дойля «Пляшущие человечки» описан способ шифрования при помощи рисунков (буквы заменялись на изображения пляшущих человечков). Например, одна из шифровок, разгаданная неподражаемым Шерлоком Холмсом:

Фраза означала: «Никогда».



К шифрам замены относится и один из первых известных кодов в истории человечества – **код Цезаря** (Приложение 1), применявшийся в древнем Риме. Суть этого кода состояла в том, что буква алфавита заменялась другой с помощью сдвига по алфавиту на одно и то же число позиций³. Например, зашифруем слово ТАЙНОПИСЬ, используя сдвиг на одну букву вперед по алфавиту. Получим слово УБКОПРЙТЭ. Если будем для того же исходного слова применять сдвиг на две позиции назад, то получим РЮЗЛМНЖПЬ. Расшифровка таких записей очень проста даже при незнании сдвига. Для этого применяется метод полосок. На нескольких горизонтальных полосках записывается алфавит. Затем эти полоски прикладываются друг к другу так, чтобы по горизонтали получалось зашифрованное слово (непонятный набор символов). Остается в одной из строк найти осмысленное слово, которое и было зашифровано. Тогда определяется и сдвиг, и значение всех символов. Фрагмент расшифровки с помощью полосок

п	э	ж	к	л	м	ё	о	щ
р	ю	з	л	м	н	ж	п	ъ
с	я	и	м	н	о	з	р	ы
т	а	й	н	о	п	и	с	ь
у	б	к	о	п	р	й	т	э
ф	в	л	п	р	с	к	у	ю
х	г	м	р	с	т	л	ф	я

Таблица 1

содержится в таблице 1.

Обратите внимание на строки 2, 4 и 5. В них содержатся слово до шифровки и его шифры, уже знакомые нам.³

Легко дать математическое описание шифра замены. Пусть

$A = \{a_1, a_2, a_3, \dots, a_{35}\}$ – множество букв алфавита и знаков препинания, $B = \{b_1, b_2, b_3, \dots, b_{35}\}$ – множество знаков шифра. Пусть также $f: A \rightarrow B$ – взаимно-однозначное отображение A в B . Это значит, что каждой букве a_k алфавита A сопоставляется однозначно определенная буква b_k алфавита B , которую мы обозначаем символом $f(a_k)$, причем разным буквам сопоставляются разные буквы. Тогда шифр замены действует так: открытый текст $a_1 a_2 \dots a_k$ преобразуется в шифрованный текст $f(a_1) f(a_2) \dots f(a_k)$. Для русского языка можно обойтись 35 знаками; 31 буква (е, ё, и, б, ь не различаются), пробел, точка, запятая, тире. Если число знаков, используемых при шифровании, тоже равно 35, то каждый такой шифр задается взаимно-однозначным отображением одного множества из 35 элементов на другое такое же множество¹. Число таких отображений равно $1 \cdot 2 \cdot 3 \cdot \dots \cdot 35 = 35!$

Это настолько громадное число, что его трудно себе представить, оно примерно равно 10^{40} .

Иметь дело с произвольными отображениями f не слишком удобно: запомнить такое отображение трудно, а хранить при себе таблицу отображения – «ключ» шифра – нежелательно. Лучше иметь какое-нибудь простое правило, позволяющее по k найти $f(k)$. А такие правила дают методы математики.¹

2. Шифры и сравнения

Один из методов кодирования заключается в следующем. Разделим кольцо на 35 равных частей, занумеруем их и пометим каждую буквой или знаком препинания (см. рисунок 1). А теперь выберем какое-нибудь число s («ключевое число» шифра) и повернем кольцо вокруг центра по часовой стрелке так, чтобы каждая часть переместилась на s шагов. Это и задает шифр – отображение множества $A = \{a_1, a_2, a_3, \dots, a_{35}\}$ на множество знаков шифра $B = \{01, 02, 03, \dots, 35\}$ (перед однозначными числами надо писать 0, иначе неясно, что такое 15 — «пятнадцать» или «один», «пять»).

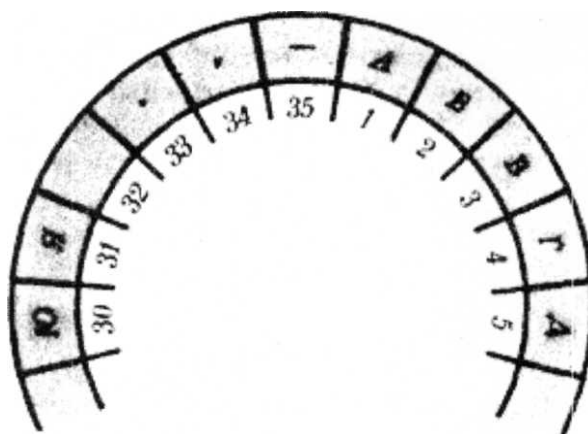


Рисунок 1

Например, если $s = 11$, то часть, помеченная числом 01, перейдет в часть, помеченную числом 12, а это значит, что букве «А» при кодировании отвечает число 12. Точно так же букве «В» отвечает число 14 и так далее.

В результате получается послание, в котором каждая буква или знак записаны двузначным числом. Адресату для расшифровки надо разбить полученную последовательность цифр на двузначные числа, вычесть из

каждого ключевое число и заменить полученное число k — номер знака a_k — на букву алфавита или знак препинания.

Впрочем, на самом деле правила кодирования и декодирования не столь просты — ведь если k больше, чем 24, то сумма $k + 11$ больше, чем 35, а в множестве B самое большое число равно 35. Но здесь надо вспомнить, что мы писали числа не на прямой, а на кольце, а, как известно, у кольца начала нет и нет конца — за числом 35 идет 1. Иными словами, после числа 35 все повторяется снова. Это значит, что, получив сумму, превосходящую 35, надо вычесть из нее 35. Полученная разность и покажет, в какое число переходит a_k .

Например, a_{27} (буква «ы») переходит не в число 38, а в 03, a_{32} («пробел») — в 08 и так далее. Таким образом,

$$f(a_k) = \begin{cases} k + 11, & \text{если } k \leq 24, \\ k - 24, & \text{если } 25 \leq k \leq 35. \end{cases}$$

А декодирование делается по следующим формулам:

$$g(n) = \begin{cases} a_{n-11}, & \text{если } 12 \leq n \leq 35, \\ a_{n+24}, & \text{если } 1 \leq n \leq 11. \end{cases}$$

Правило кодирования можно записать более компактно, если сложение понимать в особом смысле.

Разобьем все целые числа на классы, отнеся к одному классу числа, дающие одинаковые остатки при делении на 35. Например, в один и тот же класс попадут числа -32, 3, 38, 73, так как все они при делении на 35 дают в остатке 3. Общий вид чисел этого класса $3 + 35k$, где k — целое число. Обозначим через Z_{35} множество таких классов. Число различных классов равно 35 (при делении на 35 получаются остатки $0, 1, 2, \dots, 34$), и их можно обозначать теми же цифрами, что и соответствующие остатки, только писать сверху черточку. Например $\bar{5}$ означает не число 5, а класс, содержащий это число, то есть множество чисел $\{\dots, -30, 5, 40, 75, \dots\}$. В частности, $\bar{0}$ означает класс, содержащий число 35.

Теперь уже можно написать, что $\bar{27} + 11 = \bar{3}$, то есть, прибавляя 11 к числам класса $\bar{27}$ мы получаем числа из класса $\bar{3}$. Значит, если номерами кодируемых букв и знаками шифра считать классы из Z_{35} , то формулы кодирования и декодирования можно записать так:

$$f(a_{\bar{k}}) = \bar{k} + 11,$$

$$g(n) = a_{\bar{n}-1}$$

Если уже известно, что шифр получен прибавлением одного и того же числа к номерам букв, то его можно разгадать, угадав значение хотя бы одной буквы, а еще лучше — нескольких букв. Например, если известно, что в письме речь идет о Москве и в нем часто встречается сочетание «УХШСЙЗ», то легко догадаться, что при шифровании номер каждой буквы увеличивали на 7.

Более сложный шифр получается, если заменить сложение умножением. Будем, например, умножать номера всех букв на 2. Конечно, если произведение окажется больше 35, надо заменять его остатком от деления на 35. Например, буква «Ч» получит при шифровке номер 13, так как номер буквы «Ч» равен 24, а при делении $24 \cdot 2 = 48$ на 35 получается остаток 13.¹

3. Шифры и статистика

Мы рассмотрели шифры, связанные с арифметическими операциями над номерами букв. У всех этих шифров есть один существенный недостаток — каждая буква переходит в один и тот же знак, где бы эта буква ни стояла в письме. Для расшифровки таких кодов можно применить методы математической статистики.¹ Одним из таких методов является частотный анализ.²⁴ Каждой букве русского алфавита и знаку пробела соответствует определенная частота, с которой они (в среднем) встречаются в длинных текстах:¹

пробел	0,175	р	0,040	я	0,018	у	0,009
о	0,090	в	0,038	ы	0,016	ж	0,007
е, ё	0,072	л	0,035	л	0,035	ю	0,006
а	0,062	к	0,028	ь, ъ	0,014	ш	0,006
и	0,062	м	0,026	б	0,014	ц	0,004
т	0,053	д	0,025	г	0,013	щ	0,003
н	0,053	п	0,023	ч	0,012	э	0,003
с	0,045	у	0,021	й	0,010	ф	0,002

Считаем, что при замене наиболее частые буквы переходят в наиболее частые. Поэтому можно взять расшифровываемое послание, подсчитать для каждого знака частоту, с которой он встречается, и на этом основании судить, что этот знак означает. Например, знак, попадающийся чаще всего, имеет много шансов оказаться пробелом.¹ Его относительная частота наибольшая и равна 0,175. Ну, а если не пробел, то, возможно, «о» (эта буква стоит на втором месте). Можно изучать и комбинации соседних знаков — чаще всего рядом с гласной буквой стоит согласная. Даже в не слишком длинном тексте можно без труда отделить знаки для согласных букв от знаков для гласных.¹ Хорошим подспорьем при дешифровке являются знаки препинания, поэтому в

шифрованных сообщениях они часто опускаются. Например, слова «что», «а», «но» часто следуют после запятой, а «потому», «тот», «там» — перед ней. Часто предложение, заканчивающееся вопросительным знаком, начинается с буквы «к».²⁴ Последовательно перебирая различные варианты, пытаемся либо прийти к противоречию с законами русского языка, либо получить читаемые куски сообщения. Далее по возможности продляем читаемые куски либо по смыслу, либо по законам русского языка⁴. Такие соображения облегчают разгадку кодов, основанных на простой замене букв знаками.

4. Шифры перестановки

Ненадежность подстановочных криптограмм (сравнительная легкость их расшифровки) была замечена уже давно, и поэтому в разное время предлагались различные другие методы шифрования. Среди них важное место занимают перестановочные криптограммы. При их составлении весь текст разбивается на группы, состоящие из одинакового числа букв, и внутри каждой группы буквы некоторым образом переставляются². Число различных преобразований шифра перестановки, предназначенного для зашифрования сообщения состоящего из n символов меньше либо равно $n!$ (заметим, что в это число входит и вариант преобразования, оставляющий все символы на своих местах)²³. Число возможных перестановок очень велико, отсюда большое разнообразие перестановочных криптограмм.

Типичным и древнейшим примером шифра перестановки является **шифр «Сциताल»** (Приложение 2). Для его реализации использовалась специальное шифрующее устройство. По описанию Плутарха (род. до 50 — ум. после 120 гг. н. э.), оно состояло из двух палок одинаковой длины и толщины. Одну оставляли себе, а другую отдавали отъезжающему. Эти палки называли сциталами. Когда правителям нужно было сообщить какую-нибудь важную тайну, они вырезали длинную и узкую, вроде ремня, полоску папируса, наматывали ее на свою сциталу, не оставляя на ней никакого промежутка, так чтобы вся поверхность палки была охвачена полосой. Затем, оставляя папирус на сцитале в том виде, как он есть, писали на нем все, что нужно, а написав, снимали полосу и без палки отправляли адресату. Так как буквы на ней разбросаны в беспорядке, то прочитать написанное он мог, только взяв свою сциталу и намотав на нее без пропусков эту полосу. Аристотелю (384 до н. э. — 322 до н. э.) принадлежит способ дешифрования этого шифра. Надо изготовить длинный конус и, начиная с основания, обертывать его лентой с зашифрованным сообщением, сдвигая ее к вершине. В какой-то момент начнут просматриваться куски сообщения.²² Шифр «Сцитала», реализует не более n перестановок (n — длина сообщения). Имеются еще и чисто физические ограничения, накладываемые реализацией шифра «Сцитала». Естественно предположить, что диаметр жезла не должен превосходить 10 сантиметров. При высоте строки в



1 сантиметр на одном витке такого жезла уместится не более 32 букв ($10\pi < 32$). Таким образом, число перестановок, реализуемых «Считалой», вряд ли превосходит 32.²³

Рассмотрим способ **шифрования с помощью кодового (ключевого) слова**. Выбирается слово, все буквы которого различны. Его буквы нумеруются по порядку появления их в алфавите. Затем в таблицу помещается кодовое слово, под ним - номера букв, а текст вписывается по горизонтали (как в таблице 2). Для зашифровки текст из столбцов по порядку номеров записывается в строку.

ц	е	з	а	р	ь
5	2	3	1	4	6
м	а	т	е	м	а
т	и	к	а	-	ц
а	р	и	ц	а	в
с	е	х	н	а	у
к	,	а	р	и	ф
м	е	т	и	к	а
-	ц	а	р	и	ц
а	м	а	т	е	м
а	т	и	к	и	а

Таблица 2

Например, возьмём в качестве кодового слово ЦЕЗАРЬ. Зашифруем текст «МАТЕМАТИКА-ЦАРИЦА ВСЕХ НАУК, АРИФМЕТИКА – ЦАРИЦА МАТЕМАТИКИ» В последней строчке остались свободные места, заполним их буквами. Выпишем текст по столбцам в строку. Получим шифровку: ЕАЦНРИРТКАИРЕ,

ЕЦМТТКИХАТААИМ- ААИКИЕИМТАСК-АААЦВУФАЦМ

Зная кодовое слово, легко расшифровать текст, производя операции в обратном порядке.³

Книжный шифр, является еще одним примером шифра перестановки. Этот шифр изобрел Эней (4-ое столетие до н.э), и описал его в сочинении «Об обороне укрепленных мест». Эней предложил прокалывать малозаметные дырки в книге или в другом документе над буквами секретного сообщения. Интересно отметить, что в первой мировой войне германские шпионы использовали аналогичный шифр, заменив дырки на точки, наносимые

симпатическими чернилами на буквы газетного текста. Книжный шифр в современном варианте имеет несколько другой вид. Суть этого шифра состоит в замене букв на номер строки и номер этой буквы в строке в заранее оговоренной странице некоторой книги. Ключом такого шифра является книга и используемая страница в ней. Положим ключом к шифру будет отрывок из стихотворения А.С.Пушкина: «Цыганы».

Предстоит зашифровать слово: «Криптография». Первая буква слова – «К», мы её обозначаем 1/5, где числителем будет

*Птичка божья не знает
Ни заботы, ни труда,
Хлопотливо не свивает
Долговечного гнезда.
Вдолгу ночь на ветке дремлет;
Солнце красное взойдет,
Птичка гласу бога внимлет,
Встрепенется и поет.*

А.С. Пушкин "Цыганы"

строка, знаменателем – порядок букв в этой строке. Рекомендовалось вносить побольше разнообразия, заимствуя букву из разных мест ключа, чтобы затруднить для посторонних специалистов расшифрование написанного. Тогда шифром слова "Гимназия" будет такой текст: "1/5, 8/4, 2/1, 3/4, 7/2, 6/2, 4/3, 2/6, 4/4, 7/3, 8/12".²⁶

Книжный шифр оказался «долгожителем» и применялся даже во времена второй мировой войны²⁵.

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

к	р	а	с	н
а	п	т	и	ц
а	п	е	р	ь
е	м	,	а	ч
е	л	о	в	е
к	у	ч	е	н
ь	е	м	а	б

же сообщение будем по другому маршруту: по вертикали, начиная с верхнего правого угла и двигаясь поочередно сверху вниз и снизу вверх.⁵ Зашифруем, например, указанным способом фразу:

КРАСНА ПТИЦА ПЕРЬЕМ, А ЧЕЛОВЕК УЧЕНЬЕМ
размера пять на семь :

Зашифрованная фраза выглядит так:

НЦЬЧЕНБСИРАВЕААТЕ,ОЧМРППМЛУЕКААЕЕКЪ

Теоретически маршруты могут быть значительно более изощренными, однако запутанность маршрутов усложняет использование таких шифров.²⁵

Шифр «Поворотная решетка» или «Решетка Кардано»

(Приложение 3). Для использования шифра, называемого поворотной решеткой, изготавливается трафарет из прямоугольного листа клетчатой бумаги размера $2m \times 2k$ клеток. В трафарете вырезано mk клеток так, что при

его последовательном использовании (поворачивании) каждая клетка лежащего под ним листа окажется занятой. Трафарет сначала поворачивают вдоль вертикальной оси симметрии на 180° , а затем вдоль горизонтальной оси также на 180° . И вновь повторяют ту же процедуру.¹⁸ Буквы сообщения последовательно вписываются в вырезы трафарета (по строкам, в каждой строке слева направо) при каждом из четырех его возможных положений в заранее установленном порядке.²³ Если решетка Кардано - квадрат, то возможен второй вариант самосовмещений фигуры, а именно, последовательные повороты вокруг центра квадрата на 90° .¹⁸

Поясним процесс шифрования на примере. Пусть в качестве ключа используется решетка 6×10 , приведенная на рисунке 2.

Зашифруем с ее помощью текст

ШИФРРЕШЕТКАЯВЛЯЕТСЯЧАСТНЫМСЛУЧАЕМ

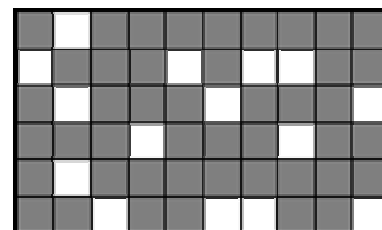


Рисунок 2

ШИФРАМАРШРУТНОЙ ПЕРЕСТАНОВКИ

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

Рисунок 3

Наложив решетку на лист бумаги, вписываем первые 15 (по числу вырезов) букв сообщения: ШИФРРЕШЕТКАЯВЛЯ.... Сняв решетку, мы увидим текст, представленный на рис. 3. Поворачиваем решетку на 180° . В окошечках появятся новые, еще не заполненные клетки. Вписываем в них следующие 15 букв. Получится запись, приведенная на рис. 4. Затем переворачиваем решетку на другую сторону и зашифровываем остаток текста аналогичным образом (рис. 5,6).

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

Рисунок 4

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

Рисунок 5

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

Рисунок 6

Получатель сообщения, имеющий точно такую же решетку, без труда прочтет исходный текст, наложив решетку на шифртекст по порядку четырьмя способами. Число возможных трафаретов, то есть количество ключей шифра ``решетка'', составляет $T = 4^{mk}$. Этот шифр предназначен для сообщений

длины $n=4mk$. Число всех перестановок в тексте такой длины составит $(4mk)!$, что во много раз больше числа T . Однако, уже при размере трафарета 8×8 число возможных решеток превосходит 4 миллиарда.²³

Далее возникает вопрос: “А как запомнить уже составленную, изготовленную решетку, ведь если ее носить с собой постоянно, то и тайны никакой не будет. Кто хочет, тот сможет, повертев решетку на тексте записки, прочесть ее?”

Есть несколько путей решения вопроса.

Например, запомнить таблицу, в которой отмечены числа (см. табл.) в каждой строке (см. рис. 7).

Первая строка	2, 4, 5
Вторая строка	14
Третья строка	9, 11, 7
Четвертая строка	16
Пятая строка	8, 15
Шестая строка	3, 12
Седьмая строка	10, 6
Восьмая строка	13, 1

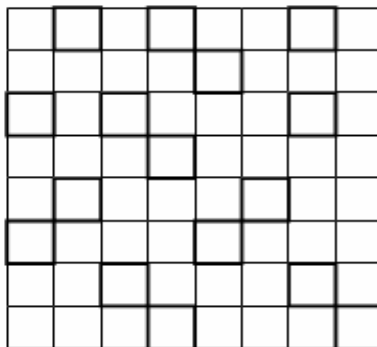


Рисунок 7

Но это очень трудно. Есть другой способ. Записать окошки в двоичной системе, где окошко – 1.

0	1	0	1	0	0	1	0
0	0	0	0	1	0	0	0
1	0	1	0	0	0	1	0
0	0	0	1	0	0	0	0
0	1	0	0	0	1	0	0
1	0	0	0	1	0	0	0
0	0	1	0	0	0	1	0
0	0	0	1	0	0	0	1

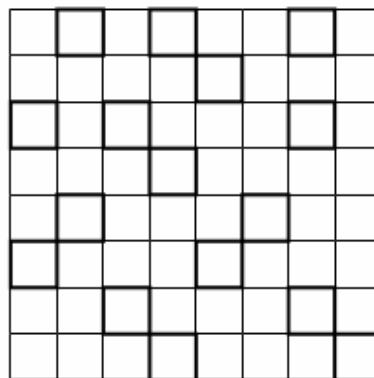


Рис. 23

Но числа в двоичной системе запомнить еще сложнее, а вот перевести их в десятичную систему – очень просто.

$$\begin{aligned}
 01010010 &= 1010010_2 = 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + \\
 &+ 0 \cdot 2^0 = 64_{10} + 16_{10} + 2_{10} = 82_{10}; \\
 00001000_2 &= 1000_2 = 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0 = 8; \\
 10100010_2 &= 162_{10}; \\
 00010000_2 &= 16_{10}; \\
 01000100_2 &= 68_{10}; \\
 10001000_2 &= 136_{10}; \\
 00100010_2 &= 34_{10}; \\
 00010001_2 &= 17_{10}.
 \end{aligned}$$

Таким образом, можно заполнить решетку, если знать числа 82, 8, 162, 16, 68, 136, 34, 17.

А для того чтобы восстановить ее, надо перевести эти числа из десятичной в двоичную систему, затем в соответствии с полученными числами сделать

решетку. Если при переводе в двоичную систему получается число, не содержащее 8 знаков, то слева приписывают нужное количество нулей.

Как осуществить перевод из десятичной в двоичную систему?

Можно это сделать с помощью деления.

Число делят на 2. Запоминают остаток от деления; неполное частное тоже делят на 2, запоминают остаток и т. д. Процесс продолжают до тех пор, как неполное частное не станет 0. Записывают остатки, начиная с последнего. В данном случае получим число 1010010. Чтобы оно стало восьмизначным, припишем слева 0, получим 01010010, что будет соответствовать первой строке решетки (рис. 8).

$$\begin{array}{r}
 82 \overline{) 2} \\
 \underline{82} 41 \overline{) 2} \\
 40 \overline{) 20} \overline{) 2} \\
 1 20 \overline{) 10} \overline{) 2} \\
 0 10 \overline{) 5} \overline{) 2} \\
 0 4 \overline{) 2} \overline{) 2} \\
 1 2 \overline{) 1} \overline{) 2} \\
 0 0 \overline{) 0} \\
 1
 \end{array}$$

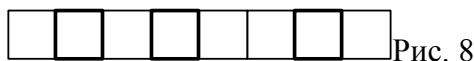


Рис. 8

Есть второй способ перевода в двоичную систему. Надо помнить степени числа 2 до $n = 7$. $2^1 = 2$; $2^2 = 4$; $2^3 = 8$; $2^4 = 16$; $2^5 = 32$; $2^6 = 64$; $2^7 = 128$. А затем подбирать, прикидывая, сколько каких степеней содержится в числе, которое надо перевести из десятичной системы в двоичную.

Например, число 82.

128 в этом числе не будет, а 64 – точно, значит $82 = 64 \cdot 1 + 18$.

В числе 18 содержится из степеней двойки число 16. То есть $18 = 16 + 2$

и 2 – это тоже степень двойки. Значит $82 = 1 \cdot 64 + 1 \cdot 16 +$

$+ 2 = 1 \cdot 2^6 + 1 \cdot 2^4 + 1 \cdot 2^1$. Добавим остальные степени, умножив их на 0, так как они в числе 82 не содержатся.

$$82_{10} = 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$$

Запишем коэффициенты перед степенями двойки в качестве цифр числа в двоичной системе:²⁰

$$82_{10} = 1010010_2$$

Заключение

Под шифром понимается совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных. Самое важное составляющее любого шифра – это общее правило (ключ), по которому преобразуется исходный текст.



Наука, занимающаяся методами шифрования и дешифрования информации – криптология – немыслима без абстрактного мышления, без анализа и синтеза, без сравнения и аналогии, а это значит, что математика белее всего подходит к решению проблем этой науки. Знания математики, с точки зрения рассматриваемых вопросов, нужны для того, чтобы:

- Найти простую, но надежную систему кодирования, недоступную для расшифровки посторонним лицам.
- Найти способы декодирования чужой системы тайнописи, чужих кодов.

В работе рассмотрены шифры подстановки (простой замены) и шифры перестановки при работе с которыми не обойтись без математических методов (поиск закономерностей, сравнения, частотный анализ, комбинаторика).

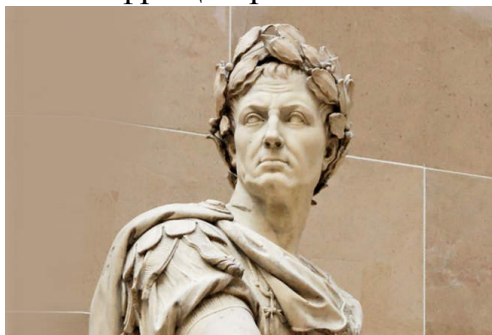
В наше время потребность в кодировании информации не менее актуальна, чем в былые времена. Шифруется дипломатическая и экономическая корреспонденция, военные сообщения и медицинские диагнозы, сенсационные сообщения прессы и информация биржевых маклеров. Поэтому тема «Математика и шифры» интересна, современна и актуальна.

Список литературы

1. Виленкин Н.Я. Математика и шифры. – Квант, № 8, 1997.
2. Аршинов М.Н., Садовский Л.Е. Коды и математика. – М.: Наука, 1983.
3. Гонина Е.Е. Шифры, коды, тайны. – Живая математика, № 1, 2008.
4. Дориченко С.А., Ященко В.В. 25 этюдов о шифрах: Популярно о современной криптографии — М.: Теис, 1994.
5. Ященко В.В., ред. Введение в криптографию. – М: МЦНМО, 2000.
6. К. Шеннон. Работы по теории информации и кибернетике. – М., ИЛ, 1963.
7. Жельников В. Криптография от папируса до компьютера. - М.: "ABF", 1996 -335с.
8. А.Н. Лебедев. Криптография с «открытым ключом» и возможности ее практического применения. «Защита информации», выпуск 2, 1992.
9. У.Болл, Г.Коксетер Математические эссе и развлечения - М.:Мир,1986
- 10.Фелкон Тэвис, Джуди Хиндлей, Рут Томисон, Хизер Эмери. Краткий курс юного шпиона Авт. лит. обработки Анна Данковцева.- М.: Педагогика, 1985.
11. Г. Фролов. Тайны тайнописи. - М., 1992.
12. М. Гарднер. От мозаик Пенроуза к надежным шифрам. - М.; Мир, 1993.
13. М. Масленников. Практическая криптография. Санкт-Петербург: БХВ - Петербург, 2003.
14. Виноградов И. М. Основы теории чисел. М.: Наука. 1972.
15. Серов Е., Волгин В. Тайны военной разведки (1918 -1945). // Армия. - М., 1994 - № 7 - с. 52 -55.
16. Виленкин Н.Я., Депман И.Я. За страницами учебника математики – М.: Просвещение, 1986.
17. Баранова Т., Кочетков, К., Семенов А. Школьный интеллектуальный марафон. Математика// Прил. К газете «Первое сентября», № 5, 33,1995. №35, 1999., №34, 2004.
- 18.Зельманзон М., Хлобыстова Л. Самосовмещение квадрата и тайнопись - «Квант», № 12, 1980.
- 19.Коробова, Л. Математические загадки детективного сюжета - «Математика» // Прил. к газете «Первое сентября», №19,1998 г.
- 20.Алгебра, геометрия, информатика. Элективные курсы – Волгоград: Учитель,2008.(CD)
21. Гатчин Ю.А., Коробейников А.Г. Основы криптографических алгоритмов. Учебное пособие. - СПб.: СПбГИТМО(ТУ), 2002.
- 22.Коробейников А. Г. Математические основы криптографии. Учебное пособие. – СПб: СПб ГИТМО (ТУ), 2002.
23. citforum.ru/security/cryptography/yaschenko/78.html
24. сайт: students.uni-vologda.ac.ru
25. [http://ru.science.wikia.com/wiki/Шифр перестановки](http://ru.science.wikia.com/wiki/Шифр_перестановки)
26. Википедия
27. wiki: [saripkru.ru/index.php/Из истории криптографии](http://saripkru.ru/index.php/Из_истории_криптографии)

Приложение 1

Шифр Цезаря



Шифр Цезаря называют в честь Юлия Цезаря, который согласно «Жизни двенадцати цезарей» Светония использовал его со сдвигом 3, чтобы защищать военные сообщения. **Гай Юлий Цезарь** (100 или 102 до н. э. – 44 до н. э.) – древнеримский государственный и политический деятель, диктатор, полководец, писатель. Хотя Цезарь был первым зафиксированным человеком использующим эту схему, другие шифры

подстановки, как известно, использовались и ранее. Его племянник, Август, также использовал этот шифр, но со сдвигом вправо на один, и он не повторялся к началу алфавита. Есть доказательства, что Юлий Цезарь использовал также и более сложные схемы.

Часто для удобства использования шифра Цезаря используют два диска разного диаметра с нарисованными по краям дисков алфавитами, насаженных на общую ось. Изначально диски поворачиваются так, чтобы напротив каждой буквы алфавита внешнего диска находилась также буква алфавита малого диска. Если теперь повернуть внутренний диск на несколько символов, то мы получим соответствие между символами внешнего диска и внутреннего - шифр Цезаря. Получившийся диск можно использовать как для шифрования, так и для расшифровки. Например, если внутреннее колесо повернуть так, чтобы символу А внешнего диска соответствовал символ D внутреннего диска, то мы получим шифр со сдвигом 3 влево.²⁶



Естественным развитием шифра Цезаря стал **шифр Виженера**. Этот шифр удобнее всего представлять себе как шифр Цезаря с переменной величиной сдвига. Чтобы знать, насколько сдвигать очередную букву открытого текста, заранее договариваются о способе запоминания сдвигов. Сам Виженер предлагал запоминать ключевое слово, каждая буква которого своим номером в алфавите указывает величину сдвига. Ключевое слово повторяется столько раз, сколько нужно для замены всех букв открытого текста. Например, ключевое слово ВАЗА означает следующую последовательность сдвигов букв открытого текста: 3191319131913191... Например, открытый текст КРИПТОГРАФИЯ при таком способе шифрования преобразуется в шифртекст НССРХПЛСГХСА.⁴



Блез де Виженер (1523-1596) был французским

дипломатом и криптографом. Вижнер родился в деревне Saint-Pourçain (англ.). В возрасте 17 лет он поступил младшим секретарем на дипломатическую службу к Вормсский эдикт. В возрасте 24 он поступил на службу к герцогу Невер. В 1954 и 1966 он посетил Рим с двухгодичной дипломатической миссии. В этих поездках, он познакомился с книгами о криптографии и и самой криптографией. Умер в 1596 от рака горла.

Первое точное документированное описание многоалфавитного шифра было сформулировано Леоном Баттиста Альберти в 1467 году.



Для переключения между алфавитами использовался металлический шифровальный диск. Система Альберти переключает алфавиты после нескольких зашифрованных слов. Позднее, в 1518 году, Иоганн Трисемус в своей работе «Полиграфия» изобрел *tabula recta* — центральный компонент шифра Виженера.

То, что сейчас известно под шифром Виженера, впервые описал Джованни Баттиста Беллазо в своей книге *La cifra del. Sig. Giovan Battista Bellaso*. Он использовал идею Трисемуса, но добавил ключ для переключения алфавитов шифра через каждую букву.

Блез Вижнер представил своё описание простого, но стойкого шифра перед комиссией Генриха III во Франции в 1586 году, и позднее изобретение шифра было присвоено именно ему. Давид Кан в своей книге «Взломщики кодов» отозвался об этом осуждающе, написав, что история «проигнорировала важный факт и назвала шифр именем Виженера, несмотря на то, что он ничего не сделал для его создания».

Шифр Виженера имел репутацию исключительно стойкого к «ручному» взлому. Известный писатель и математик Чарльз Лютвидж Доджсон (Льюис Кэрролл) назвал шифр Виженера невзламываемым в своей статье «Алфавитный шифр», опубликованной в детском журнале в 1868 году. Это представление было опровергнуто после того, как Казиски полностью взломал шифр в XIX веке, хотя известны случаи взлома этого шифра некоторыми опытными криптоаналитиками ещё в XVI веке.²⁶

Приложение 2

Шифр «Считаль»

Этот шифр известен со времен войны Спарты и Персии против Афин. Спартанский полководец Лисандр подозревал персов в возможной измене, но не знал их тайных планов. Его агент в стане персов прислал зашифрованное



сообщение, которое позволило Лисандру опередить персов и разгромить их. Зашифрованное сообщение было написано на поясе официального гонца от персов следующим образом: агент намотал пояс на считаль (деревянный цилиндр определенного диаметра) и написал на поясе сообщение вдоль считалья; потом он разматал пояс, и получилось, что поперек пояса в беспорядке написаны буквы. Гонца не догадывался, что узор на его красивом поясе на самом деле содержит зашифрованную информацию.

Лисандр взял считаль такого же диаметра, аккуратно намотал на него пояс и вдоль считалья прочитал сообщение от своего агента. Например, если роль считалья выполняет карандаш с шестью гранями, то открытый текст КРИПТОГРАФИЯ может быть преобразован в шифртекст РПОРФЯКИТГАИ. Шифртекст может быть и другим, так как он зависит не только от диаметра карандаша.²⁷

Приложение 3

Джероламо Кардано (24 сентября 1501 – 21 сентября 1576) — итальянский математик, механик, астролог, философ и медик, побочный сын Фацио Кардано.



Учился в университетах Павии и Падуи. Занимался сначала исключительно медициной, а с 1534 был профессором математики в Милане и Болонье; однако для увеличения скромных доходов профессоров того времени продолжал заниматься врачеванием, а также составлял альманахи.

Кардано внёс значительный вклад в развитие алгебры: его имя носит формула Кардано для нахождения корней кубического неполного уравнения вида $x^3 + ax + b = 0$. Он же первым в Европе стал использовать отрицательные корни уравнений. Кардано также занимался механикой: изобретенные им карданный подвес и карданная передача до сих пор широко применяются в технике.

В 1550 году предложил простую решётку для шифрования сообщений. Он планировал маскировать сообщения под обычное послание, так что в целом они не были полностью похожи на зашифрованные. Такое замаскированное сообщение считается примером стеганографии (не путать с криптографией). Но имя Кардано относилось к решёткам, которые могли и не быть изобретением Кардано, тем не менее, шифры, реализованные с использованием картонных решеток, принято называть решётками Кардано. Известно, что Кардинал Ришелье (1585—1642) был приверженцем решётки Кардано и использовал её в личной и деловой переписке. Образованные жители Европы XVII века были знакомы с игрой слов в литературе, в том числе с акrostихом, анаграммой и шифрами. К концу XVII века первые решётки Кардано уже почти не использовались, но иногда они всё же появлялись в виде зашифрованных посланий и в качестве литературных диковинок. Например, Джордж Гордон Байрон пользовался решёткой Кардано, но скорее для демонстрации литературных навыков, чем для серьёзного шифрования.

Из сочинений Кардано интересны: «*Ars magna, sive de regulis Algebrae*»; «*Ars magna Arithmeticae*»; «*Exaereton mathematicorum*», «*De subtilitate*» и «*De varietate rerum*». Им оставлена также любопытная автобиография под заглавием «*De vita propria*». Несмотря на многочисленность сочинений Кардано, в науке сохранились лишь формулы, данные им для решения уравнений третьей степени и носящие имя Кардано.

Занимаясь составлением гороскопов Кардано, помимо прочего, предсказал день своей смерти и, как говорит предание, чтобы оправдать своё предсказание, сам уморил себя голодом.