# Шифрование с использованием метода шифрующих таблиц и метода магического квадрата

## Шифрующие таблицы

Идея метода простых шифрующих таблиц придумана задолго до появления современной цивилизации и предельно проста. Пусть известны величины m - число строк, эта цифра является ключом. Если длина открытого текста не кратна m, то придётся дополнить текст чем-нибудь, чтобы избавиться от этого свойства. Например, пробелами или не значащими буквами. Так, если входные данные состоят из 26 символов, m = 3, то добавляем 1 пробел или букву.   
Результат записываем по столбцам слева направо, для понятности пример: 3 строки текст "демократы"

|  |  |  |
| --- | --- | --- |
| Д | О | А |
| Е | К | Т |
| М | Р | Ы |

А теперь считываем по строкам сверху вниз. В нашем примере получим недемократичное слово "ДОАЕКТМРЫ". Таким способом шифруется весь текст, при этом пробелы не имеют никаких привилегий и считаются обычными символами.   
Результат объединяем в один текст - шифрованный.

Есть смысл стараться брать длину блока m такой, чтобы число m\*n (n- количество столбцов) имело как можно больше делителей. Это увеличивает количество вариантов шифрующих таблиц при известной длине блока. Например, 25 - плохая длина блока: есть только вариант 5\*5, 24 - получше - есть варианты 2\*12, 3\*8, 4\*6, 6\*4, 8\*3, 12\*2. Как видим, для небольших чисел m, n метод простых шифрующих таблиц легко вскрывается даже вручную. Хоть сколько-нибудь солидное количество вариантов ключа в методе простых шифрующих таблиц возможно только для очень длинных блоков.

## Магический квадрат

Магическими квадратами называются квадратные таблицы со вписанными в их клетки последовательными натуральными числами от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Подобные квадраты широко применялись для вписывания шифруемого текста по приведенной в них нумерации. Если потом выписать содержимое таблицы по строкам, то получалась шифровка перестановкой букв. На первый взгляд кажется, будто магических квадратов очень мало. Тем не менее, их число очень быстро возрастает с увеличением размера квадрата. Так, существует лишь один магический квадрат размером 3 х 3, если не принимать во внимание его повороты. Магических квадратов 4 х 4 насчитывается уже 880, а число магических квадратов размером 5 х 5 около 250000. Поэтому магические квадраты больших размеров могли быть хорошей основой для надежной системы шифрования того времени, потому что ручной перебор всех вариантов ключа для этого шифра был немыслим.

В квадрат размером 4 на 4 вписывались числа от 1 до 16. Его магия состояла в том, что сумма чисел по строкам, столбцам и полным диагоналям равнялась одному и тому же числу — 34. Впервые эти квадраты появились в Китае, где им и была приписана некоторая «магическая сила».

|  |  |  |  |
| --- | --- | --- | --- |
| 16 | 3 | 2 | 13 |
| 5 | 10 | 11 | 8 |
| 9 | 6 | 7 | 12 |
| 4 | 15 | 14 | 1 |

Шифрование по магическому квадрату производилось следующим образом. Например, требуется зашифровать фразу: «ПриезжаюСегодня.». Буквы этой фразы вписываются последовательно в квадрат согласно записанным в них числам: позиция буквы в предложении соответствует порядковому числу. В пустые клетки ставится точка.

|  |  |  |  |
| --- | --- | --- | --- |
| 16. | 3 и | 2 р | 13 д |
| 5 з | 10 е | 11 г | 8 ю |
| 9 С | 6 ж | 7 а | 12 о |
| 4 е | 15 я | 14 н | 1 П |

После этого шифрованный текст записывается в строку (считывание производится слева направо, построчно):  
.ирдзегюСжаоеянП

При расшифровывании текст вписывается в квадрат, и открытый текст читается в последовательности чисел «магического квадрата». Программа должна генерировать «магические квадраты» и по ключу выбирать необходимый. Размер квадрата больше чем 3х3.

# Шифрование с использованием: систем Цезаря и системы Трисемуса

## Система Цезаря

Шифр Цезаря — один из древнейших шифров. При шифровании каждый символ заменяется другим, отстоящим от него в алфавите на фиксированное число позиций. Шифр Цезаря можно классифицировать как шифр подстановки, при более узкой классификации — шифр простой замены.

Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки.

Математическая модель

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами:

http://kriptografea.narod.ru/13.png

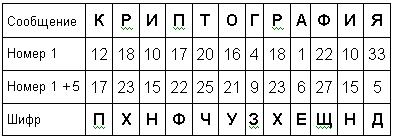
http://kriptografea.narod.ru/14.png

где x — символ открытого текста   
y — символ шифрованного текста   
n — мощность алфавита (кол-во символов)   
k — ключ. 

Алфавит:



Пример:



Ответ: «Пхнфчузхещнд» Ключ: 5

## Система Трисемуса

Шифрующая система Трисемуса (Тритемия). В 1508 г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием «Полиграфия». В этой книге он впервые систематически описал применение модифицированного шифра Цезаря.

Здесь шаг смещения делается переменным, то есть зависящим от каких-либо дополнительных факторов. Например, можно задать закон смещения в виде линейной функции (уравнения зашифрования) позиции шифруемой буквы.

Сама функция должна гарантировать целочисленное значение. Прямая функция шифрования должна иметь обратную функцию шифрования, тоже целочисленную.

Уравнение зашифрования для шифра Тритемиуса имеет следующий вид:

Некоторые варианты вычисления шага смещения k:

,

,

где p — позиция буквы в сообщении; A, B, C — ключи.

Алгоритм шифрования с использованием системы Трисемуса:

1. Определяем порядковый номер шифруемой буквы в тексте.
2. Определяем код буквы в алфавите.
3. Вычисляем смещение k.
4. Находим код зашифрованной буквы, пользуясь нашим уравнением зашифрования.  
   Расшифрование
5. По коду L восстанавливаем очередную букву криптограммы.
6. Повторяем пункты 1..5 до окончания текста шифрограммы.

Для k=2p^2+5p+3 и алфавита:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я |  | , | . |
| 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 |

Оригинальный текст:

Съешь же ещё этих мягких французских булок, да выпей чаю.

Шифрованный текст:

ФБЩШЛГД Ч.ЪСЧДП ЕО,ЧЁЬЙЙЛЮЩЛ РЬА РЙХАКЕЛ,РЮШЮЭ,НТЩВ,ПЁФЦВ

# Реализация алгоритма шифрования Плейфера

Шифр Плейфера использует матрицу 5х5 (для латинского алфавита, для кириллического алфавита необходимо увеличить размер матрицы до 4х8), содержащую ключевое слово или фразу. Для создания матрицы и использования шифра достаточно запомнить ключевое слово и четыре простых правила. Чтобы составить ключевую матрицу, в первую очередь нужно заполнить пустые ячейки матрицы буквами ключевого слова (не записывая повторяющиеся символы), потом заполнить оставшиеся ячейки матрицы символами алфавита, не встречающимися в ключевом слове, по порядку (в английских текстах обычно опускается символ «Q», чтобы уменьшить алфавит, в других версиях «I» и «J» объединяются в одну ячейку). Ключевое слово может быть записано в верхней строке матрицы слева направо, либо по спирали из левого верхнего угла к центру. Ключевое слово, дополненное алфавитом, составляет матрицу 5х5 и является ключом шифра.

Для того чтобы зашифровать сообщение, необходимо разбить его на биграммы (группы из двух символов), например «Hello World» становится «HE LL OW OR LD», и отыскать эти биграммы в таблице. Два символа биграммы соответствуют углам прямоугольника в ключевой матрице. Определяем положения углов этого прямоугольника относительно друг друга. Затем, руководствуясь следующими 4 правилами, зашифровываем пары символов исходного текста:

1. Если два символа биграммы совпадают (или если остался один символ), добавляем после первого символа «Х», зашифровываем новую пару символов и продолжаем. В некоторых вариантах шифра Плейфера вместо «Х» используется «Q».

2. Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки.

3. Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящиеся непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца.

4. Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника.

Для расшифровки необходимо использовать инверсию этих четырёх правил, откидывая символы «Х» (или «Q»), если они не несут смысла в исходном сообщении.

Пример:

Используем ключ «playfair example», тогда матрица примет вид:

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

Зашифруем сообщение «Hide the gold in the tree stump»  
HI DE TH EG OL DI NT HE TR EX ES TU MP  
1. Биграмма HI формирует прямоугольник, заменяем её на BM.  
2. Биграмма DE расположена в одном столбце, заменяем её на ND.  
3. Биграмма TH формирует прямоугольник, заменяем её на ZB.  
4. Биграмма EG формирует прямоугольник, заменяем её на XD.  
5. Биграмма OL формирует прямоугольник, заменяем её на KY.  
6. Биграмма DI формирует прямоугольник, заменяем её на BE.  
7. Биграмма NT формирует прямоугольник, заменяем её на JV.  
8. Биграмма HE формирует прямоугольник, заменяем её на DM.  
9. Биграмма TR формирует прямоугольник, заменяем её на UI.  
10. Биграмма EX находится в одной строке, заменяем её на XM.  
11. Биграмма ES формирует прямоугольник, заменяем её на MN.  
12. Биграмма TU находится в одной строке, заменяем её на UV.  
13. Биграмма MP формирует прямоугольник, заменяем её на IF.  
Получаем зашифрованный текст «BM ND ZB XD KY BE JV DM UI XM MN UV IF»  
Таким образом сообщение «Hide the gold in the tree stump» преобразуется в «BMNDZBXDKYBEJVDMUIXMMNUVIF»

# Шифрование с использованием системы Вижинера и шифра «двойной квадрат» Уитстона

**Цель работы: изучить и закрепить умение шифровать информацию системой Вижинера и с помощью двойного квадрата Уитстона.**

**Теоретические сведенья:**

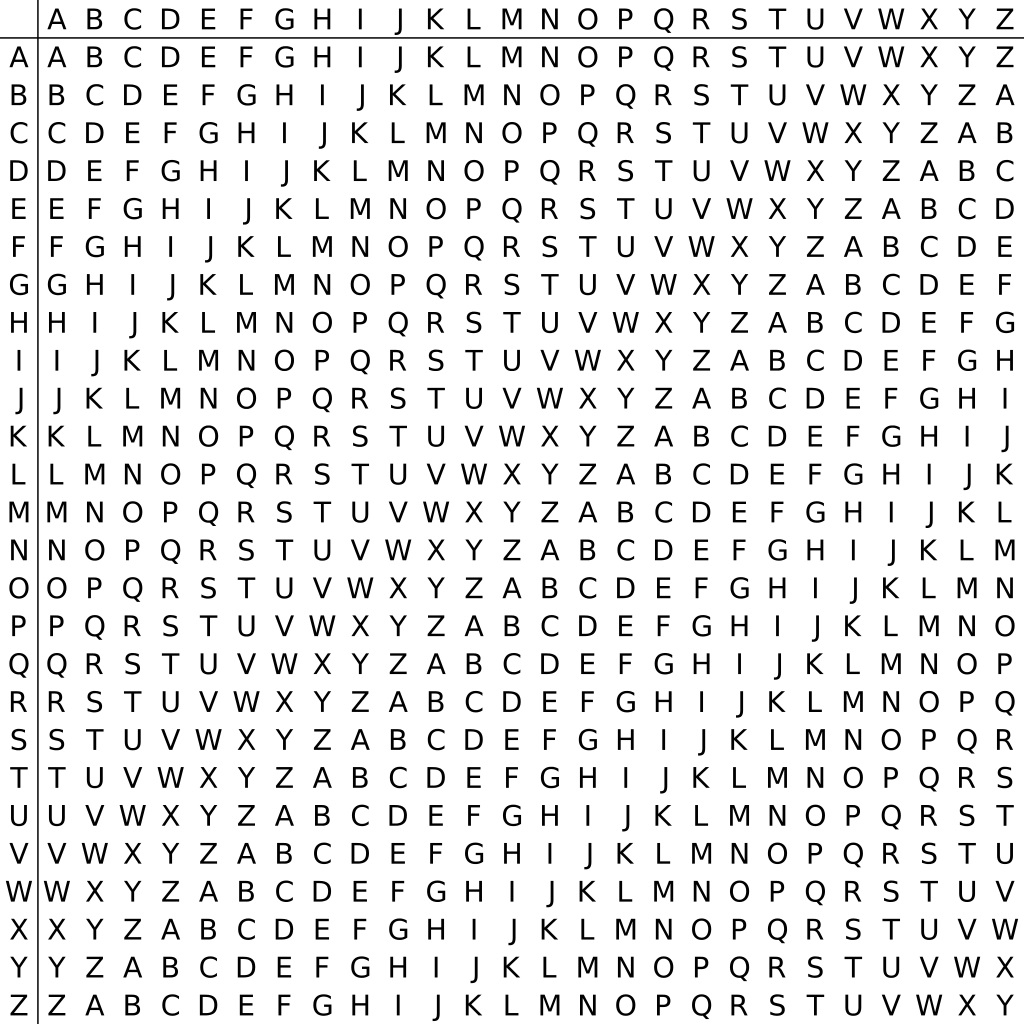
## **Система Вижинера**

В [шифре Цезаря](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A6%D0%B5%D0%B7%D0%B0%D1%80%D1%8F) каждая буква алфавита сдвигается на несколько строк; например в шифре Цезаря при сдвиге +3, A стало бы D, B стало бы E и так далее. Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая tabula recta или квадрат (таблица) Виженера. Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова. Например, предположим, что исходный текст имеет вид:

ATTACKATDOWN

Человек, посылающий сообщение, записывает ключевое слово («LEMON») циклически до тех пор, пока его длина не будет соответствовать длине исходного текста:

LEMONLEMONLE



Первый символ исходного текста A зашифрован последовательностью L, которая является первым символом ключа. Первый символ L шифрованного текста находится на пересечении строки L и столбца A в таблице Виженера. Точно так же для второго символа исходного текста используется второй символ ключа; то есть второй символ шифрованного текста X получается на пересечении строки E и столбца T. Остальная часть исходного текста шифруется подобным способом.

*Исходный текст: ATTACKATDAWN*

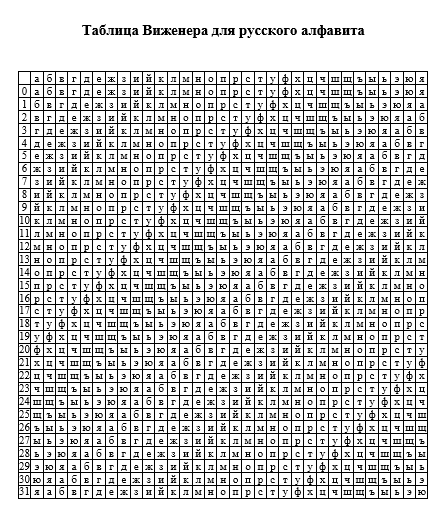
*Ключ: LEMONLEMONLE*

*Зашифрованный текст: LXFOPVEFRNHR*

Расшифровывание производится следующим образом: находим в таблице Виженера строку, соответствующую первому символу ключевого слова; в данной строке находим первый символ зашифрованного текста. Столбец, в котором находится данный символ, соответствует первому символу исходного текста. Следующие символы зашифрованного текста расшифровываются подобным образом.

Если буквы A—Z соответствуют числам 0—25, то шифрование Виженера можно записать в виде формулы:

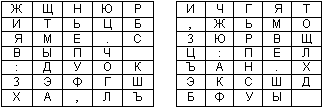
Расшифровка:



## **Шифр «двойной квадрат» Уитстона**

В 1854 г. англичанин Чарльз Уитстон разработал новый метод шифрования биграммами, который называют "двойным квадратом". Свое название этот шифр получил по аналогии с по-либианским квадратом. Шифр Уитстона открыл новый этап в истории развития криптографии. В отличие от полибианского шифр "двойной квадрат" использует сразу две таблицы, размещенные по одной горизонтали, а шифрование идет биграммами, как в шифре Плейфейра. Эти не столь сложные модификации привели к появлению на свет качественно новой криптографической системы ручного шифрования. Шифр "двойной квадрат" оказался очень надежным и удобным и применялся Германией даже в годы второй мировой войны.

Поясним процедуру шифрования этим шифром на примере. Пусть имеются две таблицы со случайно расположенными в них русскими алфавитами. Перед шифрованием исходное сообщение разбивают на биграммы. Каждая биграмма шифруется отдельно. Первую букву биграммы находят в левой таблице, а вторую букву - в правой таблице. Затем мысленно строят прямоугольник так, чтобы буквы биграммы лежали в его противоположных вершинах. Другие две вершины этого прямоугольника дают буквы биграммы шифртекста.



Две таблицы со случайно расположенными символами русского алфавита для шифра "двойной квадрат"

Предположим, что шифруется биграмма исходного текста ИЛ. Буква И находится в столбце 1 и строке 2 левой таблицы. Буква Л находится в столбце 5 и строке 4 правой таблицы. Это означает, что прямоугольник образован строками 2 и 4, а также столбцами 1 левой таблицы и 5 правой таблицы. Следовательно, в биграмму шифртекста входят буква О, расположенная в столбце 5 и строке 2 правой таблицы, и буква В, расположенная в столбце 1 и строке 4 левой таблицы, т.е. получаем биграмму шифртекста 0В.

Если обе буквы биграммы сообщения лежат в одной строке, то и буквы шифртекста берут из этой же строки. Первую букву биграммы шифртекста берут из левой таблицы в столбце, соответствующем второй букве биграммы сообщения. Вторая же буква биграммы шифртекста берется из правой таблицы в столбце, соответствующем первой букве биграммы сообщения. Поэтому биграмма сообщения ТО превращается в биграмму шифртекста ЖБ. Аналогичным образом шифруются все биграммы сообщения:

Сообщение ПР ИЛ ЕТ АЮ \_Ш ЕС ТО ГО

Шифртекст ПЕ 0В ЩН ФМ ЕШ РФ БЖ ДЦ

Шифрование методом "двойного квадрата" дает весьма устойчивый к вскрытию и простой в применении шифр. Взламывание шифртекста "двойного квадрата" требует больших усилий, при этом длина сообщения должна быть не менее тридцати строк.