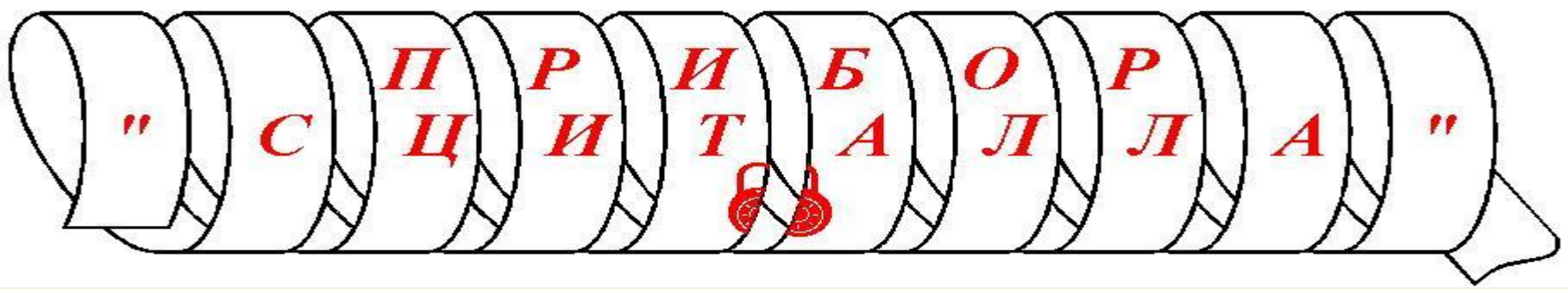
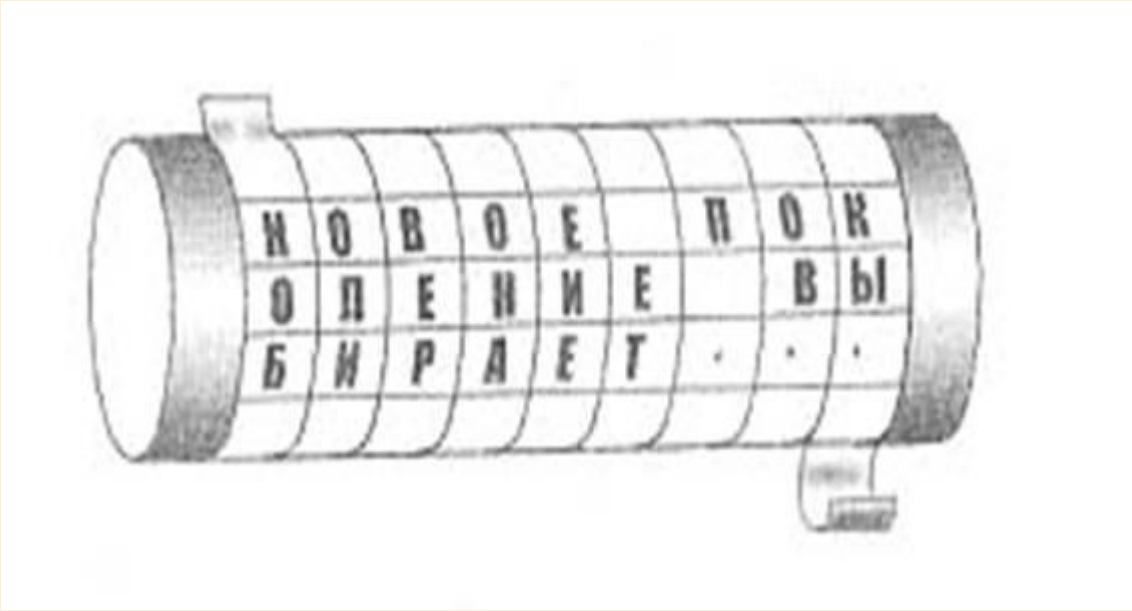
ШИФРЫ ПЕРЕСТАНОВКИ

ЮМАЕВА А.А.

ШИФРЫ ПЕРЕСТАНОВКИ

Шифрование перестановкой заключается в том, что символы открытого текста переставляются по определенному правилу в пределах некоторого блока этого текста.





Для расшифрования такого шифртекста нужно не только знать правило шифрования, но и обладать ключом в виде стержня определенного диаметра. Зная только вид шифра, но не имея ключа, расшифровать сообщение было непросто

ШИФРУЮЩИЕ ТАБЛИЦЫ

С начала эпохи Возрождения (конец XIV столетия) начала возрождаться и криптография. В разработанных шифрах перестановки того времени применяются шифрующие таблицы, которые, в сущности, задают правила перестановки букв в сообщении.

В качестве ключа в шифрующих таблицах используются:

1. размер таблицы;
2. слово или фраза, задающие перестановку;
3. особенности структуры таблицы.

	4	1	3	2
3	П	Р	И	Л
1	Е	Т	А	Ю
4	В	О	С	Ь
2	М	О	Г	О

Исходная таблица

	1	2	3	4
3	Р	Л	И	П
1	Т	Ю	А	Е
4	О	Ь	С	В
2	О	О	Г	М

Перестановка столбцов

	1	2	3	4
1	Т	Ю	А	Е
2	О	О	Г	М
3	Р	Л	И	П
4	О	Ь	С	В

Перестановка строк

При шифровании в такую таблицу вписывают исходное сообщение по определенному маршруту, а выписывают (получают шифрограмму) - по другому. Для данного шифра маршруты вписывания и выписывания, а также размеры таблицы являются ключом.

ШИФРУЮЩИЕ ТАБЛИЦЫ

Одним из самых примитивных табличных шифров перестановки является простая перестановка, для которой ключом служит размер таблицы. Этот метод шифрования сходен с шифром скитала. Например, сообщение "**ТЕРМИНАТОР ПРИБЫВАЕТ СЕДЬМОГО В ПОЛНОЧЬ**" записывается в таблицу поочередно по столбцам.

Т	Н	П	В	Е	Г	Л
Е	А	Р	А	Д	О	Н
Р	Т	И	Е	Ь	В	О
М	О	Б	Т	М	П	Ч
И	Р	Ы	С	О	О	Ь

После заполнения таблицы текстом сообщения по столбцам для формирования шифртекста считывают содержимое таблицы по строкам. Если шифртекст записывать группами по пять букв, получается такое шифрованное сообщение: "**ТНПВЕ ГЛЕАР АДОНР ТИЕЬВ ОМОБТ МПЧИР ЫСООЬ**".

ШИФРУЮЩИЕ ТАБЛИЦЫ

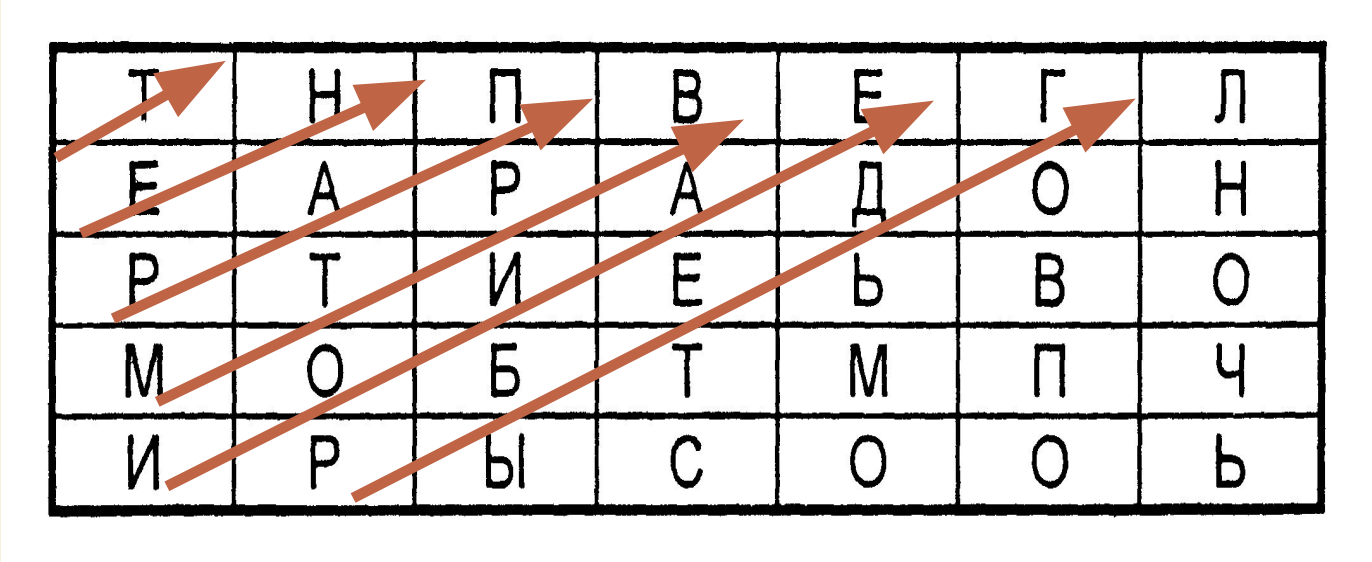
Т	Н	П	В	Е	Г	Л
Е	А	Р	А	Д	О	Н
Р	Т	И	Е	Ь	В	О
М	О	Б	Т	М	П	Ч
И	Р	Ы	С	О	О	Ь

Считывание по ГОРИОНТАЛИ, начиная с правого нижнего угла, двигаясь справа налево и слева направо

ЬООСЫРИМОБТМПЧОВЬЕИТ

РЕАРАДОНЛГЕВПНТ

ШИФРУЮЩИЕ ТАБЛИЦЫ

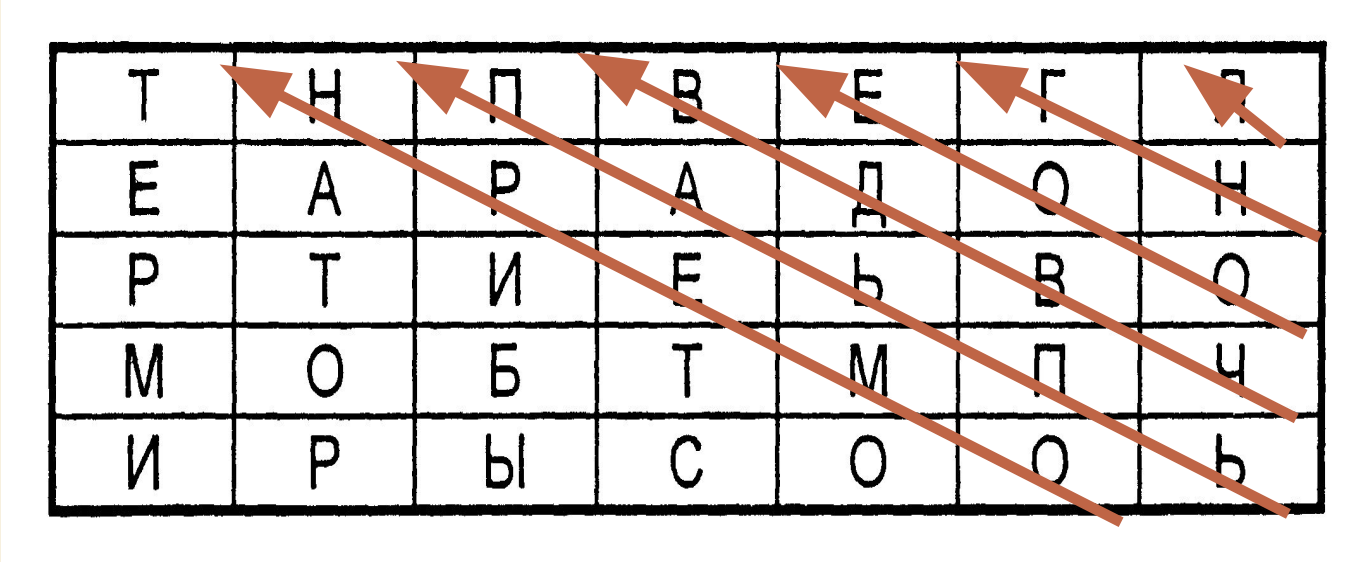


Т	Н	П	В	Е	Г	Л
Е	А	Р	А	Д	О	Н
Р	Т	И	Е	Ь	В	О
М	О	Б	Т	М	П	Ч
И	Р	Ы	С	О	О	Ь

Считывание по диагонали: слева направо, начиная с левого верхнего угла

Т Е Н Р А П М Т Р В И О И А Е Р Б Е Д Г Ы Т Ь О Л С М В Н О П О О Ч Ь

ШИФРУЮЩИЕ ТАБЛИЦЫ



Т	Н	П	В	Е	Г	Л
Е	А	Р	А	Д	О	Н
Р	Т	И	Е	Ь	В	О
М	О	Б	Т	М	П	Ч
И	Р	Ы	С	О	О	Ь

Считывание по диагонали: справа налево, начиная с правого верхнего угла

Л Н Г О О Е Ч В Д В Ь П Ь А П О М Е Р Н О Т И А Т С Б Т Е Ы О Р Р М И

ОДИНОЧНАЯ ПЕРЕСТАНОВКА ПО КЛЮЧУ

Этот метод отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы.

Применим в качестве ключа, например, слово "**ПЕЛИКАН**", а текст сообщения возьмем **ТЕРМИНАТОР ПРИБЫВАЕТ СЕДЬМОГО В ПОЛНОЧЬ**. На рисунке показаны две таблицы, заполненные текстом сообщения и ключевым словом, при этом левая таблица соответствует заполнению до перестановки, а правая таблица – заполнению после перестановки.

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. В правой таблице столбцы переставлены в соответствии с упорядоченными номерами букв ключа.

*При считывании содержимого правой таблицы по строкам и записи шифртекста группами по пять букв получим шифрованное сообщение: "**ГНВЕП ЛТООА ДРНЕВ ТЕЬИО РПОТМ БЧМОР СОЫЬИ**".*

ШИФРОВАНИЕ С ПОМОЩЬЮ МАГИЧЕСКИХ КВАДРАТОВ

Магическими квадратами называют квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число.

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

О	И	Р	М
Е	О	С	Ю
В	Т	А	Ь
Л	Г	О	П

Шифруемый текст вписывают в магические квадраты в соответствии с нумерацией их клеток. Если затем выписать содержимое такой таблицы по строкам, то получится шифртекст, сформированный благодаря перестановке букв исходного сообщения.

Пример магического квадрата и его заполнения сообщением "**ПРИЛЕТАЮ ВОСЬМОГО**" показан на рисунке

Шифртекст, получаемый при считывании содержимого правой таблицы по строкам, имеет вполне загадочный вид: "**ОИРМ ЕОСЮ ВТАЬ ЛГОП**".

ПРИМЕР ДЛЯ ЛР

Зашифровать слово ***УГОЛЬНИКОВ***

Матрица: 5*2 (5 строк, 2 столбца)

Маршрут вписывания: справа налево и слева направо, начиная с правого верхнего угла

Маршрут считывания:

- слева направо и справа налево, начиная с левого нижнего угла
- по диагонали слева направо начиная с левого верхнего угла
- по диагонали справа налево, начиная с правого нижнего угла
- перестановка строк в соответствии с ключом: 4 1 5 3 2

1. СТРОИМ МАТРИЦУ

Г	У
О	Л
Н	Ь
И	К
В	О

Матрица: 5*2 (5 строк, 2 столбца)

Маршрут вписывания: справа налево и слева направо, начиная с правого верхнего угла

2. ПРОИЗВОДИМ ШИФРОВАНИЕ

- слева направо и справа налево, начиная с левого нижнего угла

В О К И Н Ь Л О Г У

- по диагонали слева направо начиная с левого верхнего угла

Г О У Н Л И Ь В К О

- по диагонали справа налево, начиная с правого нижнего угла

О К В Ь И Л Н У О Г

- перестановка строк в соответствии с ключом: 4 1 5 3 2

И К Г У В О Н Ь О Л

1	Г	У
2	О	Л
3	Н	Ь
4	И	К
5	В	О