9. Классические методы шифрования. Шифрование методами перестановки: простая перестановка, одиночная перестановка по ключу, двойная перестановка, магический квадрат, шифр Кардано, шифр Ришелье

Простая перестановка

Одним из шифров, основанных на перестановке строк и столбцов в таблице с открытым текстом, является **шифр простой перестановки**. Создание криптограммы при использовании данного шифра следует начать с составления таблицы, в ячейки которой необходимо вписать по строкам буквы открытого текста. При этом количество строк и столбцов в такой шифровальной таблице выбирается произвольно. После заполнения таблицы буквы в криптограмму выписываются по столбцам, сначала из первого столбца, затем из второго и так далее.

В качестве примера зашифруем с помощью этого шифра открытый текст МЕСТО ВСТРЕЧИ ИЗМЕНИТЬ НЕВОЗМОЖНО. При выборе таблицы, состоящей из пяти строк и шести столбцов, ее ячейки будут заполнены следующим образом:

М	Е	С	Т	О	В
С	Т	Р	Е	Ч	И
И	З	М	Е	Н	И
Т	Ь	Н	Е	В	О
З	М	О	Ж	Н	О

Теперь для создания криптограммы достаточно последовательно выписать буквы из ячеек первого столбца, затем из ячеек второго столбца и так далее.

В окончательном виде криптограмма для открытого текста МЕСТО ВСТРЕЧИ ИЗМЕНИТЬ НЕВОЗМОЖНО будет выглядеть так:

МСИТЗ ЕТЗЬМ СРМНО ТЕЕЕЖ ОЧНВН ВИИОО

Если записать эту криптограмму без пробелов, то она примет следующий вид:

МСИТЗЕТЗЬИСРМНОТЕЕЕЖОЧНВНВИИОО

Для расшифровки такого шифрованного сообщения достаточно в таблицу аналогичных размеров по столбцам вписать буквы криптограммы, а затем по строкам прочитать открытый текст. Естественно, для этого получатель сообщения должен знать размер таблицы.

УСМАНОВА ИРИНА ОЛЕГОВНА

У	А	В	Р	А	Е	В
С	Н	А	И	О	Г	Н
М	О	И	Н	Л	О	А

УАВРАЕВСНАИОГНМОИНЛОА ТАБИЦА 3Х7

Метод шифрующих таблиц с одиночной перестановкой по ключу

Отличается от метода шифрующих таблиц, перестановкой столбцов таблицы по ключевому слову после заполнения таблицы исходным текстом. Длина ключевого слова, фразы или числа, задающего способ перестановки, должна быть равна числу столбцов таблицы. Столбцы переставляются в порядке следования в алфавите символов ключевого слова.

Пример 3. Зашифруем фразу «СИСТЕМНЫЙ ПАРОЛЬ ИЗМЕНЕН» с помощью таблицы размером 4х6 и ключевого слова «СКАНЕР».

Для записи заданной фразы достаточно одной таблицы. Сначала ее заполняют по столбцам исходной фразой (рис. 4а), затем переставляют столбцы по ключевому слову «СКАНЕР» и считывают символы по строкам (рис. 4б). В результате получаем шифрованное сообщение: «Й_ЕРЕС_ИМОНИПЗНЛЕСАМЫЬНТ».

а) исходная таблица б) после перестановки

Рис. 4. Реализация шифрующих таблиц с одиночной перестановкой по ключу

БОРЬБА ЕСТЬ УСЛОВИЕ ЖИЗНИ Ключ Слово Слово

С	Л	О	В	О
5	2	3	1	4
Б	А	Ь	О	Ж
О	-	-	В	И
Р	Е	У	И	З
Ь	С	С	Е	Н
Б	Т	Л	-	И

В	Л	О	О	С
1	2	3	4	5
О	А	Ь	Ж	Б
В	-	-	И	О
И	Е	У	З	Р
Е	С	С	Н	Ь
-	Т	Л	И	Б

ОАЬЖБВ—ИОИЕУЗРЕССНЬ-ТЛИБ

БОЯТЬСЯ НАДО НЕ СМЕРТИ, А ПУСТОЙ ЖИЗНИ.

И	Г	Р	А
З	2	4	1
Б	О	И	Й
О	-	,	-
Я	Н	-	Ж
Т	Е	А	И
Ь	-	-	З
Я	С	П	Н
-	М	У	И
Н	Е	С	.
А	Р	Т	1
Д	Т	О	1

А	Г	И	Р
1	2	3	4
Й	О	Б	И
-	-	О	,
Ж	Н	Я	-
И	Е	Т	А
З	-	Ь	-
Н	С	Я	П
И	М	-	У
.	Е	Н	С

1	Р	А	Т
1	Т	Д	О

ЙОБИ—О,ЖНЯ-ИЕТАЗ-Ь-НСЯПИМ-У.ЕНС1РАТ1ТДО

А	Г	И	Р
1	2	3	4
Й	О	Б	И
-	-	О	,
Ж	Н	Я	-
И	Е	Т	А
З	-	Ь	-
Н	С	Я	П
И	М	-	У
.	Е	Н	С
1	Р	А	Т
1	Т	Д	О

Шифрующие таблицы с двойной перестановкой по ключу

Используют для повышения скрытности шифра. В данном методе используются два ключевых слова. Первое слово определяет перестановку столбцов, второе – перестановку строк таблицы. Перестановки производятся согласно порядку следования в алфавите символов ключевых слов.

На первом этапе исходный текст (или его фрагмент) построчно записывается в таблицу. Далее перестанавливаются столбцы исходной таблицы по первому ключевому слову. Затем переставляются строки полученной таблицы по второму ключевому слову. На последнем этапе из итоговой таблицы считывается шифртекст по столбцам.

Пример 4. Зашифруем фразу из третьего примера с помощью таблицы размером 4х6 и ключевых слов «СКАНЕР» и «4123».

После заполнения исходной таблицы по строкам (рис. 5а) переставляем столбцы по порядку следования в алфавите букв слова «СКАНЕР» (рис. 5б). Затем переставляем строки. Порядковый номер строки определяет цифра второго ключевого слова «4123» (рис. 5в). На этом перестановки в таблице заканчиваются. Шифртекст считываем по столбцам и получаем: «ЙЛЕСП_ЕЕЫОМИ_ЬНТАИНМНРЗС»

	С	К	А	Н	Е	Р
	6	3	1	4	2	5
4	С	И	С	Т	Е	М
1	Н	Ы	Й		П	А
2	Р	О	Л	Ь		И
3	З	М	Е	Н	Е	Н

а) исходная таблица

	А	Е	К	Н	Р	С
	1	2	3	4	5	6
4	С	Е	И	Т	М	С
1	Й	П	Ы		А	Н
2	Л		О	Ь	И	Р
3	Е	Е	М	Н	Н	З

б) перестановка столбцов

	А	Е	К	Н	Р	С
	1	2	3	4	5	6
1	Й	П	Ы		А	Н
2	Л		О	Ь	И	Р
3	Е	Е	М	Н	Н	З
4	С	Е	И	Т	М	С

в) перестановка строк

Рис. 5. Пример шифрования методом двойной перестановки

Шифрование по методу 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, строке и диагонали одно и то же число.

При шифровании буквы открытого текста необходимо вписать в магический квадрат в соответствии с нумерацией его клеток. Для получения шифртекста считывают содержимое заполненной таблицы по строкам.

Пример 5. Зашифруем фразу «МАГИЧЕСКАЯ СИЛА» с помощью магического квадрата размером 4х4. Для этого выберем один из 880 вариантов магических квадратов заданного размера (рис. 6а). Затем вписываем каждую букву сообщения в отдельную ячейку таблицы с

номером, соответствующим порядковому номеру буквы в исходной фразе (рис. 6б). При считывании заполненной таблицы по строкам получаем шифртекст: «_ГАИАЕССЧЯ_КИАЛМ».

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

а) магический квадрат

	Г	А	И
А	Е	С	С
Ч	Я		К
И	А	Л	М

б) квадрат с сообщением

Рис. 6. Пример шифрования с помощью магических квадратов