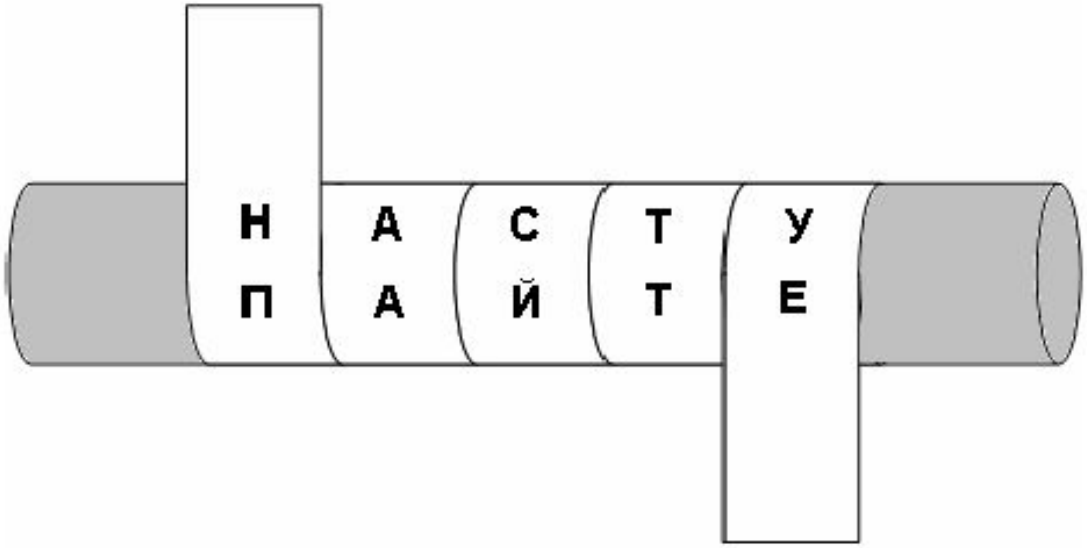
Тема: Шифры перестановки

Введение

В шифрах перестановки символы переставляются по определенному правилу в пределах всего текста или текст может разбиваться на блоки и перестановки происходят внутри каждого блока отдельно. При достаточной длине блока, в пределах которого осуществляется перестановка можно достигнуть приемлемой для простых практических приложений стойкости шифра. Шифры перестановки являются, вероятно, самыми древними шифрами.

Шифр перестановки «скитала»

Известно, что в V веке до нашей эры правители Спарты, наиболее воинственного из греческих государств, имели хорошо отработанную систему секретной военной связи и шифровали свои послания с помощью скитала, первого простейшего криптографического устройства, реализующего метод простой перестановки. Шифрование выполнялось следующим образом. На стержень цилиндрической формы, который назывался скитала, наматывали спиралью (виток к витку) полоску пергамента и писали на ней вдоль стержня несколько строк текста сообщения. Затем снимали со стержня полоску пергамента с написанным текстом. Буквы на этой полоске оказывались расположенными хаотично.



Сообщение ***наступайте*** при размещении его по окружности стержня по две буквы дает шифротекст ***нпаасйттуе***. Для расшифрования такого шифротекста 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. Шифр скитала многократно совершенствовался в последующие времена.

Шифрующие таблицы

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 из неё.

В качестве ключа в шифрующих таблицах используются:

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

Давайте с вами рассмотрим основные способы зашифровки сообщений с помощью шифрующих таблиц.

В первом варианте **используется прямоугольник, в который сообщение вписывается по строкам слева направо. Выписываться сообщение, будет по столбцам, начиная с последнего столбца.**

П	Р	И	В	Е	Т	К
А	К	Д	Е	Л	А	П
О	К	А	Н	Е	З	Н
А	Ю					

Зашифрованное сообщение:

КПН – ТАЗ – ЕЛЕ – ВЕН – ИДА – РККЮ – ПАОА

Во втором варианте **используется тоже прямоугольник, в который сообщение вписывается также по строкам слева направо. Выписывается сообщение по столбцам, которые пронумерованы в соответствии с ключом.**

Ключ: 3 – 4 – 1 – 2 – 5 – 7 – 6

3	4	1	2	5	7	6
П	Р	И	В	Е	Т	К
А	К	Д	Е	Л	А	П
О	К	А	Н	Е	З	Н
А	Ю					

Зашифрованный текст:

ИДА – ВЕН – ПАОА – РККЮ – ЕЛЕ – КПН – ТАЗ

Двойной метод шифрования

В этом случае перестановки определяются отдельно для столбцов и отдельно для строк. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При дешифрации порядок перестановок должен быть обратным. Используем для перестановки 2 ключа. Первый ключ используется для перестановки столбцов, второй для перестановки строк.

Ключ 1: **3 – 4 – 1 – 2 – 5 – 7 – 6**

Ключ 2: **4 – 2 – 3 – 1**

3	4	1	2	5	7	6
П	Р	И	В	Е	Т	К
А	К	Д	Е	Л	А	П
О	К	А	Н	Е	З	Н
А	Ю					

Выписали текст в соответствии с первым ключом:

Зашифрованный текст:

ИДА – ВЕН – ПАОА – РККЮ – ЕЛЕ – КПН – ТАЗ

Далее используя второй ключ (Ключ 2: **4 – 2 – 3 – 1**), получим:

4	И	Д	А	В	Е	Н	П
2	А	О	А	Р	К	К	Ю
3	Е	Л	Е	К	П	Н	Т
1	А	З					

Зашифрованный текст:

АЗ – АОАРККЮ – ЕЛЕКПНТ – ИДАВЕНП

Магические квадраты

В средние века для шифрования применялись магические квадраты. 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. Шифруемый текст вписывали в магические квадраты в соответствии с нумерацией их клеток. Если затем выписать содержимое такой таблицы по строкам, то получится шифротекст, сформированный благодаря перестановке букв исходного сообщения. В те времена считалось, что созданные с помощью магических квадратов шифротекст охраняет не только ключ, но и магическая сила.

Пример:

1) Сформируем магический квадрат
2) Впишем в квадрат сообщение: ***прилетаювосьмого*;**
3) Шифротекст, получаемый при считывании содержимого правой таблицы по строкам: ***оирмеосювтаьлгоп***

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

Число магических квадратов быстро возрастает с увеличением размера квадрата. Существует только один магический квадрат размером 3x3 если не учитывать его повороты. Количество магических квадратов 4x4 составляет уже 880, а количество магических квадратов 5x5 - около 250000.

Магические квадраты средних и больших размеров могли служить хорошей базой для обеспечения нужд шифрования того времени, поскольку практически нереально выполнить вручную перебор всех вариантов для такого шифра.