Шифрование методами перестановки

Этот метод заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов. Рассмотрим некоторые наиболее часто встречающиеся разновидности этого метода, которые могут быть использованы в автоматизированных системах.

Самая простая перестановка - написать исходный текст задом наперед и одновременно разбить шифрограмму на пятерки букв. Например, из фразы:

ПУСТЬ БУДЕТ ТАК, КАК МЫ ХОТЕЛИ,

получится такой шифртекст:

ИЛЕТО ХЫМКА ККАТТ ЕДУБЬ ТСУП

В последней группе (пятерке) не хватает одной буквы. Значит, прежде чем шифровать исходное выражение, его следует дополнить незначащей буквой (например, О) до числа, кратного пяти:

ПУСТЬ-БУДЕТ-ТАККА-КМЫХО-ТЕЛИО.

Тогда шифрограмма, несмотря на столь незначительное изменение, будет выглядеть по-другому:

ОИЛЕТ ОХЫМК АККАТ ТЕДУБ ЬТСУП

Кажется ничего сложного, но при расшифровке возникнут серьезные неудобства.

Во время Гражданской войны в США использовался был такой шифр: исходную фразу писали в несколько строк. Например, по пятнадцать букв в каждой (с заполнением последней строки ничего не значащими буквами).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** |
| П | У | С | Т | ь | Б | У | Д | Е | Т | т | А | К | К | А |
| К | М | Ы | х | О | Т | Е | Л | И | к | л | М | н | О | П |

После этого вертикальные столбцы по порядку писали в строку с разбивкой на пятерки букв:

ПКУМС ЫТХЬО БТУЕД ЛЕИТК ТЛАМК НКОАП

Вариант этого шифра: сначала исходную фразу записать в столбики:

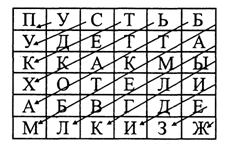
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** |
| П | С | ь | У | Е | Т | К | А | М | х | т | Л | А | В | Д |
| У | Т | Б | Д | Т | А | К | К | ы | О | Е | И | Б | Г | Е |

Потом разбить строки на пятерки букв:

ПСЬУЕ ТКАМХ ТЛАВД УТБДТ АККЫО ЕИБГЕ

Если строки укоротить, а их количество увеличить, то получится *прямоугольник-решетка,* в который можно записывать исходный текст. Но тут уже требуются предварительные договоренности между адресатом и отправителем посланий, поскольку сама решетка может быть различной длины-высоты, записывать в нее можно по строкам, по столбцам, по спирали туда или по спирали - обратно, можно писать и по диагоналям, а для шифрования можно брать тоже различные направления. В общем, вариантов масса.

Для примера возьмем решетку 6х6 (причем количество строк может увеличиваться или уменьшаться в зависимости от длины исходного сообщения) и заполним ее по строкам:



Если шифровать по стрелкам (диагоналям) сверху вниз с левого верхнего угла, то в итоге получится такая шифрограмма:

П УУ СДК ТЕКХ ЬТАОА БТКТБМ АМЕВЛ ЫЛГК ИДИ ЕЗ Ж

Для окончательного оформления шифртекст может быть разбит на группы по 6 символов:

ПУУСДК ТЕКХЬТ АОАБТК ТБМАМЕ ВЛЫЛГК ИДИЕЗЖ

Очень часто используют перестановки с ключом. Тогда правила заполнения решетки и шифрования из нее упрощаются, становятся стандартными. Единственное, что надо помнить и знать - это ключ, которым может быть любое слово, например, РАДИАТОР. В соответствии с расположением букв в алфавите, буква А получает номер 1, вторая буква А - 2, следующая по алфавиту буква Д - 3, потом И - 4, О – 5; первая буква Р - 6, вторая Р - 7 и буква Т - 8. Заполняем решетку:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Р** | **А** | **Д** | **и** | **А** | **т** | **О** | **Р** |
| 6 | 1 | 3 | 4 | 2 | 8 | 5 | 7 |
| П | У | с | Т | Ь | Б | У | Д |
| Е | Т | т | А | К | К | А | К |
| М | Ы | х | О | Т | Е | Л | и |
| О |  |  |  |  |  |  |  |

Записываем столбики в соответствии с номерами букв ключа:

УТЫ ЬКТ СТХ ТАО УАЛ ПЕМО ДКИ БКЕ

Затем последовательность опять разбивается на пятерки:

УТЫЬК ТСТХТ АОУАЛ ПЕМОД КИБКЕ

Таким шифром простой перестановки колонок пользовались немецкие секретные агенты во время Второй мировой войны. В качестве ключа они использовали первые буквы строк на определенной странице какой-нибудь обыкновенной книги.

Развитием этого шифра является шифр перестановки колонок с пропусками, которые располагаются в решетке тоже в соответствии с ключом (в нашем случае через 6-1-3-4-2-8-5-7 ... символов):

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Р** | **А** | **Д** | **И** | **А** | **Т** | **О** | **Р** |
| 6 | 1 | 3 | 4 | 2 | 8 | 5 | 7 |
| П | У | с | Т | Ь | Б | = | У |
| = | Д | Е | Т | = | Т | А | К |
| К | = | Х | О | = | Т | Е | Л |
| и | к | Л | М | = | О | П | Р |

Шифрограмма будет такой:

УДК Ь СЕХЛ ТТОМ АЕП ПКИ УКЛР БТТО

Из рассмотренных примеров видно, что все процедуры шифрования и расшифрования по методу перестановок являются в достаточной степени формальными и могут быть реализованы алгоритмически.

Задание. Зашифровать следующие фразы:

Моя любимая пора года \_\_ (дописать вашу).

Метод перестановки.

Защита компьютерной информации.

Я хочу сдать зимнюю сессию.

Спортсмен должен быть здоровым.