ЛАБОРАТОРНАЯ РАБОТА №1

Шифры простой замены

1. Шифр Цезаря.

В основе функционирования шифров простой замены лежит следующий принцип: для получения шифртекста отдельные символы или группы символов исходного алфавита заменяются символами или группами символов шифроалфавита.

Шифр Цезаря (также он является шифром простой замены) – это моноалфавитная подстановка, т.е. каждой букве открытого текста ставится в соответствие одна буква шифртекста. На практике при создании шифра простой замены в качестве шифроалфавита берется исходный алфавит, но с нарушенным порядком букв (*алфавитная перестановка*). Для запоминания нового порядка букв перемешивание алфавита осуществляется с помощью пароля. В качестве пароля могут выступать слово или несколько слов с неповторяющимися буквами. Шифровальная таблица состоит из двух строк: в первой записывается стандартный алфавит открытого текста, во второй – начиная с некоторой позиции размещается пароль (пробелы опускаются), а далее идут в алфавитном порядке оставшиеся буквы, не вошедшие в пароль. В случае несовпадения начала пароля с началом строки процесс после ее завершения циклически продолжается с первой позиции. Ключом шифра служит пароль вместе с числом, указывающим положение начальной буквы пароля. Таблица шифрования на ключе *4 пароль* будет иметь вид:

а б в г д е ж з и й к л м н о п р с т у ф х ц ч ш щ ъ ы ь э ю я

ы э ю я **п а р о л ь** б в г д е ж з и й к м н с т у ф х ц ч ш щ ъ

В процессе шифрования каждая буква открытого текста заменяется на стоящую под ней букву.

В 1 в. н.э. Ю. Цезарь во время войны с галлами, переписываясь со своими друзьями в Риме, заменял в сообщении первую букву латинского алфавита (A) на четвертую (D), вторую (B) – на пятую (E), наконец, последнюю – на третью:

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

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

Донесение Ю. Цезаря Сенату об одержанной им победе над Понтийским царем выглядело так:

YHQL YLGL YLFL ("Veni, vidi, vici" – лат. "Пришел, увидел, победил").

Император Август (1 в. н. э.) в своей переписке заменял первую букву на вторую, вторую – на третью и т. д., наконец, последнюю – на первую:

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

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

Любимое изречение императора Августа выглядело так:

GFTUJOB MFOUF ("Festina lente" – лат. "Торопись медленно").

Из примеров видно, что изменяя величину сдвига, можно получить несколько разных криптограмм для одного исходного текста.

Математически процедуру шифрования можно описать следующим образом:

$$T_m = \{T^j\}, j = 0,1, \dots, m-1,$$

$$T^j(a) = (a+j) mod\ m,$$

где $(a+j) mod\ m$ – операция нахождения остатка от целочисленного деления $a+j$ на m; T_m – циклическая подгруппа. Пронумеруем буквы латинского алфавита от 0 до 25: $a = 0, b = 1, c = 3, \dots, z = 25$. В латинском алфавите 26 букв и поэтому примем $m = 26$. Тогда операцию шифрования запишем в виде: буква с номером i заменяется на букву с номером $(i+3)\ mod\ 26$. Возможно и обобщение шифра Цезаря на случай произвольного ключа k: символ с номером i заменится на символ с номером $(i+k) mod\ 26$.

Таким образом, открытый текст $a_0, a_1, \dots, a_{N-1}$ преобразуется в криптограмму $T^j(a_0), T^j(a_1), \dots, T^j(a_{N-1})$. При использовании для шифрования подстановки T^j символ a открытого текста заменяется символом $a+j$

шифрованного текста. Цезарь обычно для шифрования использовал подстановку T^3.

Взлом такого шифра осуществляется путем анализа частотных характеристик языка открытых текстов. Например, в русском тексте длиной 10000 символов буква О встречается в среднем 1047 раз, Е – 836, А – 808, Н – 723 и т.д. Поэтому, если в достаточно длинной криптограмме какой-то символ встречается чаще остальных, то есть все основания полагать, что это буква О.

2. Шифр Атбаш.

Данный шифр является шифром сдвига на всю длину алфавита. Для алфавита, состоящего только из русских букв и пробела, таблица шифрования будет иметь следующий вид:

а б в г д е ж з и й к л м н о п р с т у ф х ц ч ш щ ъ ы ь э ю я ␣

␣ я ю э ь ы ъ щ ш ч ц х ф у т с р п о н м л к й и з ж е д г в б а

При программной реализации шифра Атбаш на языке Pascal целесообразно использовать таблицу ASCII и функции работы с ней (ord и char). Далее показана функция перевода символа открытого текста в шифр путем зеркального отражения по таблице ASCII.

```
Function Atbash(openchar:char):char;
 Begin
  Atbash := 255 – ord(openchar);
End.
```

Задания к лабораторной работе

1. Реализовать шифр Цезаря с произвольным ключом k.
2. Реализовать шифр Атбаш.