Лабораторная работа № 5

Методы защиты информации. Шифр Цезаря.

Цель работы: Освоить технологию шифрования и дешифрования информации с использованием шифра Цезаря.

Теоретическая часть

Шифр Цезаря является частным случаем шифра простой замены (одноалфавитной подстановки). Свое название этот шифр получил по имени римского императора Гая Юлия Цезаря, который использовал этот шифр при переписке.

При шифровании исходного текста каждая буква заменяется другой буквой того же алфавита по следующему правилу. Заменяющая буква определяется путем смещения по алфавиту к концу от исходной буквы на ***k*** букв. При достижении конца алфавита выполняется циклический переход к его началу.

Например: пусть **A** – используемый алфавит:

$\mathbf{A}=\{a_1, a_2,\ldots,a_m,\ldots,a_N\}$,

где $a_1, a_2,\ldots,a_m,\ldots,a_N$ – символы алфавита**; N** ширина алфавита.

Пусть ***k*** – число позиций сдвига символов алфавита при шифровании,

$0<\boldsymbol{k}<\mathbf{N}$. При шифровании каждый символ алфавита с номером ***m*** из кодируемого текста заменяется на символ этого же алфавита с номером $\boldsymbol{m}+\boldsymbol{k}$. Если $\boldsymbol{m}+\boldsymbol{k}>\mathbf{N}$, номер символа в алфавите **A** определяется как $\boldsymbol{m}+\boldsymbol{k}-\mathbf{N}$.

Для дешифрования текстовой информации номер позиции символа восстанавливаемого текста определяется как $\boldsymbol{m}-\boldsymbol{k}$. Если $\boldsymbol{m}-\boldsymbol{k}<0$, то вычисление этого номера производится как $\boldsymbol{m}-\boldsymbol{k}+\mathbf{N}$.

Пример: Алфавит A = { _, А, Л, М, Р, У, Ы} Ключ k = 1

Открытый текст «МАМА МЫЛА РАМУ»

Шифртекст «РЛРЛАР МЛАУЛРЫ»

Достоинством этой системы является простота шифрования и дешифрования. К недостаткам системы Цезаря следует отнести:

- подстановки, выполняемые в соответствии с системой Цезаря, не маскируют частот появления различных букв исходного и отрытого текста;

- сохраняется алфавитный порядок в последовательности заменяющих букв; при изменении значения ***k*** изменяются только начальные позиции такой последовательности;

- число возможных ключей ***k*** мало;

- шифр Цезаря легко вскрывается на основе анализа частот появления букв в шифре.

Порядок выполнения лабораторной работы

1. Выписать исходное сообщение и составить алфавит открытого текста.
2. Составить таблицу замен символов открытого текста символами шифртекста.
3. Составить шифртекст.
4. Рассчитать частоту появления отдельных символов в открытотм тексте и шифртексте.

Варианты заданий для шифра Цезаря

1. БАРАН КАРАБКАЛСЯ С КАРАБИНОМ (k=4)
2. ТАРАКАН ПОПАЛ В КАПКАН (k=2)
3. БАРАБАНЩИК БИЛ В ЯЩИК (k=6)
4. КОЛОКОЛ ИЗ ВОЛОКОЛАМСКА (k=3)
5. ПОЛОТЕНЦЕ ПОПАЛО В БОЛОТО (k=5)
6. КОЛОБОК ПОЛОТЕНЦЕ УВОЛОК (k=7)
7. ХЕРЕС ПОПАЛ НА ПЕРЕВЯЗЬ (k=3)
8. МЕЛ ЕМЕЛЯ МЕЛ В МЕЛЬНИЦЕ (k=4)
9. НА ЛАПУ УПАЛА КАПЛЯ ПАКЛИ (k=7)
10. НЕ ПЕЙ ПЕНУ У РЕПЕЙНИКА (k=6)
11. КОЛЕСИЛ СОКОЛ ОКОЛО ОКОЛИЦЫ (k=5)
12. КАК ЛОМ САМ ПОЛОМАЛСЯ ПОПОЛАМ (k=2)

Содержание отчета о лабораторной работе:

- номер группы, ФИО, дата выполнения работы;
- исходная фраза и ключ;
- алфавит открытого текста;
- таблица замен сиволов
- шифртекст;
- сравнение частот появления символов открытого текста и шифртекста.

Пример отчета

Исходное сообщение: "МАМА МЫЛА РАМУ", ключ: k = 1

Алфавит: А = { " ", А, Л, М, Р, У, Ы }

Таблица замен символов:

Символ	Замена
" "	А
А	Л
Л	М
М	Р
Р	У
У	Ы
Ы	" "

Шифртекст: «РЛРЛАР МЛАУЛРЫ»

Сравнение частот символов в открытом тексте и шифртексте:

Открытый текст

Символ	Частота
" "	2
А	4
Л	1
М	4
Р	1
У	1
Ы	1

Шифртекст

Символ	Частота
" "	1
А	2
Л	4
М	1
Р	4
У	1
Ы	1

Вывод: частоты появления символов в открытом тексте и шифртексте позволяют установить величину сдвига, то есть ключ шифра.