Математические основы защиты информации и информационной безопасности. Лабораторная работа №1. Шифр простой замены

Лесков Данила Валерьевич, учебная группа: НФИмд-02-21
Преподаватель: Кулябов Дмитрий Сергеевич

14 ноября, 2021, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Ознакомиться с шифрами простой замены на примере шифра Цезаря и Атбаш.

Задачи лабораторной работы

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

Выполнение лабораторной работы

Шифры простой замены

При шифровании заменой (подстановкой) символы шифруемого текста заменяются символами того же или другого алфавита по заранее установленным правилам замены. В шифре простой замены каждый символ исходного текста заменяется символами того же алфавита одинаково на всем протяжении текста

Шифр Цезаря

Данный шифр замены позволяет зашифровать сообщение путем сдвига каждого символа сообщения на произвольный ключ `j`. Таким образом, можно вывести соотношение:

$$T_m = T^j, j = 0, 1, ..., m - 1,$$
$$T^j(a) = (a + j) mod\, m,$$

где T_m — циклическая подгруппа; $(a + j) mod\, m$ - операция нахождения остатка от целочисленного деления $a + j$ на m.

Шифр Атбаш

Шифрование Атбаш - шифрование, правило замены которого строится из следующего соотношения:

$$m - n + 1,$$

где переменная m - число букв в алфавите; n - порядковый номер заданного символа. Говоря по простому метод сдвига на порядковый номер буквы в алфавите.

Полученные результаты

Шифр Цезаря

```
Нажмите:
    1 - для работы с шифром цезаря;
    2 - для работы с шифром атбаш;
    0 - для выхода из программы.
1
Введите сообщение: this is the 1st message!
Задайте сдвиг (от 1 до 25): 4

Зашифрованное сообщение (Шифр Цезаря):
xlmw mw xli 1wx qiwweki!
```

Рис. 1: Шифр Цезаря

Шифр Атбаш

```
Нажмите:
    1 - для работы с шифром цезаря;
    2 - для работы с шифром атбаш;
    0 - для выхода из программы.
2
Введите сообщение: and this is the 2nd sentence!?

Зашифрованное сообщение (Шифр Атбаш):
zmw gsrh rh gsv 2mw hvmgvmxv!?
```

Рис. 2: Шифр Атбаш

Выводы

Результаты выполнения лабораторной работы

В ходе выполнения данной лабораторной работы было выполнено ознакомление с шифрами простой замены на примере шиффров Цезаря и Атбаш.
В результате проделанной работы были реализованы методы шифрования Цезаря и Атбаш. Также были получены навыки работы с функциями преобразования строковых символов в таблицу ASCII.
Как итог, поставленные цели и задачи были успешно достигнуты.