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

Масолова Анна Олеговна, учебная группа: НФИмд-02-21
Преподаватель: Кулябов Дмитрий Сергеевич

14 ноября, 2021, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Изучение шифров простой замены.

Задачи лабораторной работы

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

Выполнение лабораторной работы

Шифры простой замены

Шифры простой замены — это наиболее часто используемые шифры. Они характеризуются тем, что какие-либо отдельные символы исходного текста заменяются другими символами. При этом замена осуществляется так, чтобы при расшифровке шифрограммы можно было однозначно восстановить исходное сообщение.

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

Шифр Атбаш

Данный шифр является шифром сдвига на всю длину алфавита:

$$m - n + 1,$$

где m – число букв в алфавите, n – порядковый номер заданного символа.

Полученные результаты

Шифр Цезаря

```
Введите:
1 - для работы с шифром Цезаря
2 - для работы с шифром Атбаш
0 - для выхода из программы
1

Введите:
1 - для зашифровки сообщения
2 - для дешифровки сообщения
1
Введите сообщение: banana12
Задайте сдвиг от 1 до 25: 7

Шифр Цезаря
Зашифрованное сообщение:
ihuhuh12

Введите:
1 - для работы с шифром Цезаря
2 - для работы с шифром Атбаш
0 - для выхода из программы
1

Введите:
1 - для зашифровки сообщения
2 - для дешифровки сообщения
2
Введите сообщение: ihuhuh12
Задайте сдвиг от 1 до 25: 7

Шифр Цезаря
Расшифрованное сообщение:
banana12
```

Рис. 1: Шифр Цезаря

Шифр Атбаш

```
Введите:
1 - для работы с шифром Цезаря
2 - для работы с шифром Атбаш
0 - для выхода из программы
2

Введите:
1 - для зашифровки сообщения
2 - для дешифровки сообщения
1
Введите сообщение: abcd!

Шифр Атбаш
Зашифрованное сообщение:
zyxw!

Введите:
1 - для работы с шифром Цезаря
2 - для работы с шифром Атбаш
0 - для выхода из программы
2

Введите:
1 - для зашифровки сообщения
2 - для дешифровки сообщения
2
Введите сообщение: zyxw!

Шифр Атбаш
Расшифрованное сообщение:
abcd!
```

Рис. 2: Шифр Атбаш

Выводы

Результаты выполнения лабораторной работы

Изучены шифры простой замены и реализованы шифры Цезаря и Атбаш.