Лабораторная работа №1

Шифры простой замены

Хохлачева Яна Дмитриевна, НПМмд-02-22

17 сентября 2022

Российский университет дружбы народов, Москва, Россия

Цели и задачи

Цель лабораторной работы

Знакомство с шифрами простой замены: Цезаря и Атбаш.

Задачи лабораторной работы

- 1. Релизовать шифр Цезаря с произвольным ключом ${\bf k}.$
- 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.

Шифр Цезаря

Математически процедуру шифрования можно описать следующим образом:

$$T_m = T^j, j = 0, 1, ..., m - 1,$$

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

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,...,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 $(i+k)\ mod\ 26$.

Шифр Атбаш

Атбаш — простой шифр подстановки для алфавитного письма. Правило шифрования состоит в замене i-й буквы алфавита буквой с номером n-i+1, где n- число букв в алфавите. Данный шифр является шифром сдвига на всю длину алфавита.

Полученные результаты

Шифр Цезаря

Введите: Введите: 1 - для работы с шифром Цезаря 1 - для работы с шифром Цезаря 2 - для работы с шифром Атбаш 2 - для работы с шифром Атбаш 0 - для выхода из программы 0 - для выхода из программы Введите: Введите: 1 - для зашифровки сообщения 1 - для зашифровки сообщения 2 - для дешифровки сообщения 2 - для дешифровки сообщения Введите сообщение: rxt Введите сообщение: аwe Задайте сдвиг от 1 до 25: 1 Задайте сдвиг от 1 до 25: 1 Шифр Цезаря Шифр Цезаря Расшифрованное сообщение: Зашифрованное сообщение: rxf aws

Figure 1: Шифр Цезаря

Шифр Атбаш

Введите: Введите: 1 - для работы с шифром Цезаря 1 - для работы с шифром Цезаря 2 - для работы с шифром Атбаш 2 - для работы с шифром Атбаш 0 - для выхода из программы 0 - для выхода из программы 2 Введите: Введите: 1 - для зашифровки сообщения 1 - для зашифровки сообщения 2 - для дешифровки сообщения 2 - для дешифровки сообщения 1 Введите сообщение: idv Введите сообщение: awe Шифр Атбаш Шифр Атбаш Зашифрованное сообщение: Расшифрованное сообщение: idv awe

Figure 2: Шифр Атбаш



Результаты выполнения лабораторной работы

Таким образом в процессе лабораторной работы я была изучила теоретические основы шифров простой замены, а также программно реализовала шифр Цезаря с с произвольным ключом **k** и шифр Атбаш.