

# Лабораторная работа №1

## Шифры простой замены

---

Баулин Егор Александрович, НФИмд-02-22

17 сентября 2022

Российский университет дружбы народов, Москва, Россия

## Цели и задачи

---

Знакомство с шифрами простой замены: Цезаря и Атбаш.

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

## Выполнение лабораторной работы

---

Шифры простой замены — это наиболее часто используемые шифры. Они характеризуются тем, что какие-либо отдельные символы исходного текста заменяются другими символами.

Математически процедуру шифрования можно описать следующим образом:

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

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

где  $(a + j) \bmod m$  — операция нахождения остатка от целочисленного деления  $a + j$  на  $m$ ;  $T_m$  — циклическая подгруппа. Пронумеруем буквы латинского алфавита от 0 до 25:  $a = 0, b = 1, c = 2, \dots, z = 25$ . 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  $(i + 3) \bmod 26$ . Возможно и обобщение шифра Цезаря на случай произвольного ключа  $k$ : символ с номером  $i$  заменится на символ с номером  $(i + k) \bmod 26$ .

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

---

Введите:

1 - шифр Цезаря

2 - шифр Атбаш

0 - для выхода

1

Введите:

1 - шифрование

2 - расшифровка

1

Введите сообщение: abc

Введите сдвиг 1

Шифр Цезаря

Зашифрованное сообщение:

bcd

Введите:

1 - шифр Цезаря

2 - шифр Атбаш

0 - для выхода

1

Введите:

1 - шифрование

2 - расшифровка

2

Введите сообщение: bcd

Введите сдвиг 1

Шифр Цезаря

Расшифрованное сообщение:

abc

Введите:

1 - шифр Цезаря

2 - шифр Атбаш

0 - для выхода

2

Введите:

1 - шифрование

2 - расшифровка

1

Введите сообщение: abc

Шифр Атбаш

Расшифрованное сообщение:

zux

Введите:

1 - шифр Цезаря

2 - шифр Атбаш

0 - для выхода

2

Введите:

1 - шифрование

2 - расшифровка

2

Введите сообщение: zux

Шифр Атбаш

Расшифрованное сообщение:

abc

Figure 2: Шифр Атбаш

## Выводы

---

Таким образом в процессе лабораторной работы была изучена теоретическая основа шифров простой замены, а также программно реализован шифр Цезаря с произвольным ключом  $k$  и шифр Атбаш.