

# Шифр простой замены

---

Семмар Вассим

13 сентября, 2024, Москва, Россия

Российский Университет Дружбы Народов

# Цели и задачи

---

# Цель лабораторной работы

Изучение алгоритмов шифрования Цезаря и Атбаш

# **Выполнение лабораторной работы**

---

Шифрование – это такое преобразование исходного сообщения, которое не позволит всяким нехорошим людям прочесть данные, если они это сообщение перехватят. Делается это преобразование по специальным математическим и логическим алгоритмам.

Атбаш — простой шифр подстановки.

Правило шифрования состоит в замене  $i$ -й буквы алфавита буквой с номером  $n - i + 1$ , где  $n$  — число букв в алфавите.

# Шифр Цезаря

Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом 3 А была бы заменена на Г, Б станет Д, и так далее.

$$y = (x + k) \bmod n$$

$$x = (y - k + n) \bmod n$$

где  $x$  — символ открытого текста,  $y$  — символ шифрованного текста  $n$  — мощность алфавита  $k$  — ключ.

# Контрольный пример

Entrée [8]: `ceasar()`

Текст для шифровки: THISISLABONE  
ZNOYOYRGHUTK

Entrée [9]: `ceasar_dec()`

Текст для дешифровки: ZNOYOYRGHUTK  
THISISLABONE

**Figure 1:** Работа алгоритмов



# Контрольный пример

Entrée [11]: `atbash()`

Текст для шифровки: TEST  
GVHG

Entrée [12]: `atbash_dec()`

Текст для дешифровки: GVHG  
TEST

**Figure 2:** Работа алгоритмов

## **Выводы**

---

Изучили алгоритмы шифрования Цезаря и Атбаш.