

# Шифр простой замены

---

Елисеева Ирина Михайловна

12 сентября, 2025, 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 — 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

```
In [2]: s = 'HELLO WORLD'
print(f'{s} : {sesar(s, 7)} : {dec_sesar(sesar(s, 7), 7)}')
```

HELLO WORLD : OLSSV DVYSK : HELLO WORLD

**Рис. 1:** Работа алгоритмов



```
return res

In [12]: s = 'HELLO WORLD'
print(f'{s} : {atbash(s)} : {dec_atbash(atbash(s))}')

HELLO WORLD : TWPPMAEMJPX : HELLO WORLD
```

**Рис. 2:** Работа алгоритмов

## **Выводы**

---

# Результаты выполнения лабораторной работы

Изучили алгоритмы шифрования Цезаря и Атбаш.