

# Шифр простой замены

---

Эдвард Гогин

13 сентября, 2023, 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

```
22         res += 1
23     return res

In [6]: 1 s = 'я люблю рудн'
        2 print(f'{s} : {cesar(s, 5)} : {cesar_dec(cesar(s, 5), 5)}')
я люблю рудн : д ргёрг хшит : я люблю рудн
```

**Figure 1:** шифр Цезаря



# Контрольный пример

```
18         for j, l in enumerate(liters_1):
19             if i==1:
20                 res += liters[j]
21         return res

In [8]: 1 s = 'я люблю рудн'
        2 print(f'{s} : {atbash(s)} : {atbash_dec(atbash(s))}')

я люблю рудн : аубюуболыс : ялюблюрудн
```

**Figure 2:** шифр Атбаш

## **Выводы**

---

# Результаты выполнения лабораторной работы

Изучили алгоритмы шифрования Цезаря и Атбаш.