

# Шифр простой замены

---

Шевляков Илья Николаевич НФИмд-01-21

13 ноября, 2021, Москва, Россия

Российский Университет Дружбы Народов

# Цели и задачи

---

# Цель лабораторной работы

Изучение алгоритмов шифрования Цезаря и Атбаш

# **Выполнение лабораторной работы**

---

Шифрование – это обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней. Главным образом, шифрование служит задачей соблюдения конфиденциальности передаваемой информации. Важной особенностью любого алгоритма шифрования является использование ключа, который утверждает выбор конкретного преобразования из совокупности возможных для данного алгоритма

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

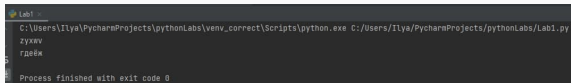
Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом 3 А была бы заменена на Г, Б станет Д, и так далее.

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

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

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

# Контрольный пример



The image shows a terminal window titled 'Lab1'. The command prompt shows the execution of a Python script: `C:\Users\Ilya\PycharmProjects\pythonLabs\venv_correct\Scripts\python.exe C:/Users/Ilya/PycharmProjects/pythonLabs/Lab1.py`. The script outputs the text 'зуххв' and 'гдеж' on two separate lines. At the bottom of the terminal, it states 'Process finished with exit code 0'.

```
Lab1 >  
C:\Users\Ilya\PycharmProjects\pythonLabs\venv_correct\Scripts\python.exe C:/Users/Ilya/PycharmProjects/pythonLabs/Lab1.py  
зуххв  
гдеж  
Process finished with exit code 0
```

**Figure 1:** Работа алгоритмов



## **Выводы**

---

## Результаты выполнения лабораторной работы

Во время выполнения данной лабораторной работы были изучили алгоритмы шифрования Цезаря и Атбаш.