## Лабораторная работа №1

Шифры простой замены

Доборщук В.В.

17 сентября 2022

Российский университет дружбы народов, Москва, Россия



#### Докладчик

- Доборщук Владимир Владимирович
- студент группы НФИмд-02-22, студ. билет 1132223451
- учебный ассистент кафедры прикладной информатики и теории вероятностей
- Российский университет дружбы народов
- · 1132223451@rudn.ru



Цели и задачи

## Цели и задачи

**Цель работы** — изучить и программно реализовать шифры простой замены.

Задачами являются:

- $\cdot$  Реализовать шифр Цезаря с произвольным ключом k;
- Реализовать шифр Атбаш.

# Теоретическое введение

#### Теоретическое введение

В основе функционирования шифров простой замены лежит следующий принцип: для получения шифртекста отдельные символы или группы символов исходного алфавита заменяются символами или группами символов шифроалфавита.

## Шифр Цезаря

**Шифр Цезаря** является моноалфавитной подстановкой, т.е. каждой букве открытого текста ставится в соответствие одна буква шифротекста.

Математическая процедура шифрования описывается как

$$T_m = \{T^j\}, j = 0, 1, \cdots, m - 1,$$

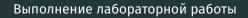
$$T^j(a) = (a+j) \mod m,$$

Сам же Цезарь обычно использовал подстановку  $T^3$ .

## Шифр Атбаш

**Шифр Атбаш** является сдвигом на всю длину алфавита. Правило шифрования состоит в замене i-й буквы алфавита буквой с номером n-i+1, где n- число букв в алфавите.

Выполнение лабораторной работы



Для реализации шифров мы будем использовать Python, так как его синтаксис позволяет быстро реализовать необходимые нам алгоритмы.

# Реализация шифра Цезаря с произвольным ключом $k^{\parallel}$

return t letter

```
# --- Ceasar's Cipher ---
def ceasar(letter: chr. kev: int. alphabet: list):
    def ceasar(letter: chr. kev: int):
        return alphabet.index(letter) + kev
    if letter.lower() not in alphabet:
        return letter
    t letter = alphabet[ceasar(letter.lower(), key) % len(alphabet)]
    if letter.isupper():
        t letter = t letter.upper()
```

```
# --- Atbash's Cipher ---
def atbash(letter: chr, alphabet: list):
    if letter.lower() not in alphabet:
        return letter
    t_letter = alphabet[len(alphabet) - alphabet.index(letter.lower()) - 1]
    if letter.isupper():
        t letter = t letter.upper()
    return t_letter
```

Для тестирования мы создали следующие функции:

```
# --- Tests ---
def test ceasar(message: str. key: int. alphabet: list):
    ciphered message = list(map(
      lambda letter: ceasar(letter, key, alphabet), message)
    return "".join(ciphered_message)
def test atbash(message: str, alphabet: list):
    ciphered message = list(map(
      lambda letter: atbash(letter, alphabet), message)
    return "".join(ciphered message)
```

```
CRASAL'S CIPHER TEST 1

Original: Veni, vidi, vidi.
CIPHER TEST 2

Original: Many with vidi.
CIPHER TEST 2

Original: Many with vidi.
CIPHER TEST 2

Original: Many New Yars, my dailing friend!
CipHered: Many New Yars, my dailing friend!
Original: Many New Yars, my dailing friend!
Original: Original: Many New Yars, my dailing friend!
Original: Many New Yars, my dailing friend!
Original: Original: Many New Yars, my dailing friend!
Original: Many New Yars, my d
```

Рис. 1: Вывод программы с реализованными шифрами простой замены

```
Для шифра Цезаря с ключом k=3 получаем следующий результат:
```

```
CEASAR'S CIPHER TEST 1
```

-----

Original: Veni, vidi, vici Ciphered: Yhql, ylgl, ylfl

-----

Дополнительно проверим механизм шифрования, передав другую строку из букв латинского алфавита:

#### CEASAR'S CIPHER TEST 2

-----

Original: Happy New Year, my darling friend! Ciphered: Kdssb Qhz Bhdu, pb gduolqj iulhqg!

-----

Шифр Атбаш мы проверяем на кириллическом алфавите, содержащим также в себе символ пробела. Для проверки, передадим в него также весь русский алфавит с пробелом в виде одной строки:

#### ATBASH'S CIPHER TEST STRING OUTPUT

-----

Original: абвгдежзийклмнопрстуфхцчшщъыьэюя

Ciphered: яюэьыъщшчцхфутсрпонмлкйизжедгвба

-----

Выведем полученный результат в формате спсика, где сможем рассмотреть каждый обработанный символ отдельно:

#### ATBASH'S CIPHER TEST LIST OUTPUT

15/16





В рамках выполненной лабораторной работы мы изучили и реализовали следующие шифры простой замены: шифр Цезаря (с произвольным ключом k) и шифр Атбаш.