# Лабораторная работа 1

## Шифры простой замены

Греков Максим Сергеевич

2022 Москва

RUDN University, Moscow, Russian Federation

# Цель работы

# Цель работы

Ознакомиться с шифрами простой замены.

Реализовать шифр Цезаря с произвольным ключом $k$.

Реализовать шифр Атбаш.

# Описание реализации

# Описание реализации

Для реализации алгоритмов использовались средства языка Python.

Был предложен функционал генерации алфавитов и их добавления. (рис. 1)

Были реализованы как шифраторы, так и дешифраторы рассматриваемых алгоритмов.

# Описание реализации

```python
def define_alphabet(c, alphabets):
    for alphabet in alphabets:
        if c in alphabet:
            return alphabet, alphabet.index(c)
    return None, None


def get_alphabets():
    en_low = [chr(c) for c in range(ord('a'), ord('z')+1)]
    en_up = [c.upper() for c in en_low]
    ru_low = [chr(c) for c in range(ord('а'), ord('е')+1)] + \
        ['ё'] + [chr(c) for c in range(ord('ж'), ord('я')+1)]
    ru_up = [c.upper() for c in ru_low]
    return en_low, en_up, ru_low, ru_up

```

**Figure 1:** Код генерации алфавитов

# Реализация

# Шифр Цезаря с произвольным ключом k

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. (рис. 2)

# Шифр Цезаря с произвольным ключом k

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики:

$$y = (x + k) mod (n)$$
$$x = (y - k) mod (n)$$

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

# Шифр Цезаря с произвольным ключом k

```python
def caesar_encode(string, alphabets, key):
    res = ''
    for c in string:
        alphabet, pos = define_alphabet(c, alphabets)
        res += c if alphabet is None else alphabet[(pos+key) % len(alphabet)]
    return res


def caesar_decode(string, alphabets, key):
    return caesar_encode(string, alphabets, -key)

```

**Figure 2:** Код Шифра Цезаря

# Шифр Атбаш

Шифр Атбаш — простой шифр подстановки для алфавитного письма. Правило шифрования состоит в замене $i$-й буквы алфавита буквой с номером $n - i + 1$, где $n$ — число букв в алфавите. (рис. 3)

# Шифр Атбаш

```python
def atbash_encode(string, alphabets):
    res = ''
    for c in string:
        alphabet, pos = define_alphabet(c, alphabets)
        res += c if alphabet is None else alphabet[len(alphabet)-pos-1]
    return res


def atbash_decode(string, alphabets):
    return atbash_encode(string, alphabets)
```

**Figure 3:** Код Шифра Атбаш

# Вывод

# Вывод

Ознакомились с шифрами простой замены.

Реализовали шифр Цезаря с произвольным ключом $k$.

Реализовали шифр Атбаш.