

Лабораторная работа 1

Шифры простой замены

Пологов Владислав Александрович

2022 Москва

RUDN University, Moscow, Russian Federation

Цель работы

Цель работы

Реализовать шифр Цезаря с произвольным ключом k .

Реализовать шифр Атбаш.

Описание реализации

Для реализации алгоритмов использовались средства языка Python.

Сгенерированы английский и русские алфавиты. (рис. 1)

Были реализованы как шифраторы, так и дешифраторы рассматриваемых алгоритмов.

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

def get_alphabet():
    en = [chr(c) for c in range(ord('a'), ord('z')+1)]
    EN = [c.upper() for c in en]
    ru = [chr(c) for c in range(ord('a'), ord('я')+1)]
    RU = [c.upper() for c in ru]
    return en, EN, ru, RU
```

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:

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

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

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

Шифр Цезаря с произвольным ключом k

```
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 — 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)

```
17 def atbash_encode(string, alphabets):
18     res = ''
19     for c in string:
20         alphabet, pos = define_alphabet(c, alphabets)
21         res += c if alphabet is None else alphabet[len(alphabet)-pos-1]
22     return res
23
24
25 def atbash_decode(string, alphabets):
26     return atbash_encode(string, alphabets)
```

Figure 3: Код Шифра Атбаш

Вывод

Реализовали шифр Цезаря с произвольным ключом k .

Реализовали шифр Атбаш.

