

Отчёт по лабораторной работе №1

Шифр простой замены

Семмар Вассим

Содержание

| | | |
|----------|---|-----------|
| 1 | Цель работы | 4 |
| 2 | Теоретические сведения | 5 |
| 2.1 | Шифр Цезаря | 5 |
| 2.2 | Шифр Атбаш | 6 |
| 3 | Выполнение работы | 7 |
| 3.1 | Реализация шифра Цезаря на языке Python | 7 |
| 3.2 | Реализация шифра Атбаш на языке Python | 8 |
| 3.3 | Контрольный пример | 9 |
| 4 | Выводы | 10 |
| | Список литературы | 11 |

List of Figures

| | | |
|-----|-----------------------------|---|
| 3.1 | Работа алгоритмов | 9 |
| 3.2 | Работа алгоритмов | 9 |

1 Цель работы

Изучение алгоритмов шифрования Цезаря и Атбаш

2 Теоретические сведения

2.1 Шифр Цезаря

Шифр Цезаря, также известный, как шифр сдвига, код Цезаря или сдвиг Цезаря — один из самых простых и наиболее широко известных методов шифрования.

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.

Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.

Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера, и все ещё имеет современное приложение в системе ROT13. Как и все моноалфавитные шифры, шифр Цезаря легко взламывается и не имеет практически никакого применения на практике.

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

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

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

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

С точки зрения математики шифр Цезаря является частным случаем аффинного шифра.

2.2 Шифр Атбаш

Атбаш — простой шифр подстановки, изначально придуманный для иврита. Правило шифрования состоит в замене i -й буквы алфавита буквой с номером $n - i + 1$, где n — число букв в алфавите.

3 Выполнение работы

3.1 Реализация шифра Цезаря на языке Python

Блок шифрования

```
# функция шифрования по алгоритму цезаря
def ceasar():
    letters = 'ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ'
    key_steps = 6
    text = input('Текст для шифровки ')
    result = ''
    for i in text:
        ind = letters.find(i)
        ind2 = ind + key_steps
        if i in letters:
            result += letters[ind2]
        else:
            result += i
    print(result)
```

Блок дешифровки

```
def ceasar_dec():
    letters = 'ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ'
    key_steps = 6
```

```

text = input('Текст для дешифровки: ')
result = ''
for i in text:
    ind = letters.find(i)
    ind2 = ind - key_steps
    if i in letters:
        result += letters[ind2]
    else:
        result += i
print(result)

```

3.2 Реализация шифра Атбаш на языке Python

Блок шифрования

```

def atbash():
    letters = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'
    letters_r = [x for x in letters]
    letters_r.reverse()

    text = input("Текст для шифровки")
    result = ""
    for i in text:
        for j,l in enumerate(letters):
            if i == l:
                result += letters_r[j]
    print(result)

```

Блок дешифровки

```

def atbash_dec():

```



```

letters = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'
letters_r = [x for x in letters]
letters_r.reverse()
text = input('Текст для дешифровки ')
result = ''
for i in text:
    for j, l in enumerate(letters_r):
        if i == l:
            result += letters[j]
print(result)

```

3.3 Контрольный пример

Entrée [8]: `ceasar()`

Текст для шифровки: THISISLABONE
ZNOYOYRGHUTK

Entrée [9]: `ceasar_dec()`

Текст для дешифровки: ZNOYOYRGHUTK
THISISLABONE

Figure 3.1: Работа алгоритмов

Entrée [11]: `atbash()`

Текст для шифровки: TEST
GVHG

Entrée [12]: `atbash_dec()`

Текст для дешифровки: GVHG
TEST

Figure 3.2: Работа алгоритмов

4 Выводы

Изучили алгоритмы шифрования Цезаря и Атбаш.

Список литературы

1. Шифр Цезаря
2. Шифр Атбаш