Отчёт по лабораторной работе №1

Шифр простой замены

Кодже Лемонго Арман

Содержание

Список иллюстраций

Цель работы

Целью данной является изучение алгоритмов шифрования Цезаря и Атбаш

Теоретические сведения

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 разновидность шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите.

```
y = (x + k) mod n
x = (y - k + n) mod 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.

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.

Выполнение работы

Реализация шифра Цезаря на языке Python

Блок шифрования

```
# функция шифрования по алгоритму цезаря
def cesar(text, step):
    alph = 'ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ'
    res = ''
    for i in text:
        index = alph.find(i)
        n_index = index + step
        if i in alph:
            res += alph[n_index]
        else:
            res += i
    return res
```

Блок дешифровки

```
def dec_cesar(text, step):
    alph = 'ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ'
    res = ''
    for i in text:
        index = alph.find(i)
```

```
        n_index = index - step
        if i in alph:
            res += alph[n_index]
        else:
            res += i
    return res
```

Реализация шифра Атбаш на языке Python

Блок шифрования

```
def atbash(text):
    alph = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'
    alph_r = [x for x in alph]
    alph_r.reverse()
    res =''
    for i in text:
        for j,l in enumerate(alph):
            if i == l:
                res += alph_r[j]
    return res
```

Блок дешифровки

```
def dec_atbash(text):
    alph = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'
    alph_r = [x for x in alph]
    alph_r.reverse()
    res = ''
    for i in text:
        for j,l in enumerate(alph_r):
```

```
            if i == l:
                res += alph[j]
    return res
```

Контрольный пример

```
[20]: s = 'CESAR'
      print (f'{s} : {cesar(s, 4)} : {dec_cesar(cesar(s, 4), 4)}')

      CESAR : GIWEV : CESAR

[37]: s = 'WELCOME'
      print (f'{s} : {cesar(s, 4)} : {dec_cesar(cesar(s, 4), 4)}')

      WELCOME : AIPGSQI : WELCOME
```

Рис. 1: шифр Цезаря

```
[33]: s = 'ATBASH'
      print (f'{s} : {atbash(s)} : {dec_atbash(atbash(s))}')

      ATBASH : ZGYZHS : ATBASH

[36]: s = 'WELCOME'
      print (f'{s} : {atbash(s)} : {dec_atbash(atbash(s))}')

      WELCOME : DVOXLNV : WELCOME
```

Рис. 2: шифр Атбаш

Выводы

в конце нашего лабораторная работа, я изучил алгоритмы шифрования Цезаря и Атбаш.

Список литературы

1. Шифр Цезаря
2. Шифр Атбаш