

Шифр простой замены

Казюлина Анна

16 сентября, 2023, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Изучение алгоритмов шифрования Цезаря и Атбаш

Выполнение лабораторной работы

Шифрование – это такое преобразование исходного сообщения, которое не позволит всяким нехорошим людям прочесть данные, если они это сообщение перехватят. Делается это преобразование по специальным математическим и логическим алгоритмам.

Атбаш — простой шифр подстановки.

Правило шифрования состоит в замене i -й буквы алфавита буквой с номером $n - i + 1$, где n — число букв в алфавите.

Шифр Цезаря

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.

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

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

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

Контрольный пример

```
In [18]: 1 def cesar(text, step, p=0):
2         letters = 'абвгдеёзийклмнопрстуфхцчщъыэюяабгдейклмнопрстуфхцчщъыэя'
3         res = ''
4         if p==1:
5             for i in text:
6                 index = letters.find(i)
7                 new_index = index + step
8                 if i in letters:
9                     res += letters[new_index]
10                else:
11                    res += i
12            if p == 0:
13                for i in text:
14                    index = letters.find(i)
15                    new_index = index - step
16                    if i in letters:
17                        res += letters[new_index]
18                    else:
19                        res += i
20            return res
21
```

```
In [19]: 1 t = 'физмат сила'
```

```
In [20]: 1 print(f'{t} - {cesar(t, 3, 1)} - {cesar(cesar(t, 3, 1), 3, 0)}')
```

физмат сила - чклпгх флог - физмат сила

Figure 1: шифр Цезаря

Контрольный пример

```
In [23]: 1 def atbash(text, p=0):
2         liters = 'абггдеёжзийклмнопрстуфхцчщъыьэюя '
3         liters_r = [i for i in liters]
4         liters_r.reverse()
5         res=''
6         if p==1:
7             for i in text:
8                 for j,l in enumerate(liters):
9                     if i==l:
10                        res += liters_r[j]
11         if p==0:
12             for i in text:
13                 for j,l in enumerate(liters_r):
14                     if i==l:
15                        res += liters[j]
16
17         return res

In [24]: 1 print(f'{t} - {atbash(t, 1)} - {atbash(atbash(t, 1), 0)}')
        физмат сила - лчшу наочф - физмат сила
```

Figure 2: шифр Атбаш

Выводы

Результаты выполнения лабораторной работы

Изучили алгоритмы шифрования Цезаря и Атбаш.