Шифр простой замены

Хайретдинов Линар Ринатович

5 сентября, 2025, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Изучение алгоритмов шифрования Цезаря и Атбаш

Выполнение лабораторной работы

Шифрование

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

Шифр Атбаш

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

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

Контрольный пример

In [18]:
```
def cesar(text, step, p=0):
    liters = 'абвгдеёжзийклмнопрстуфхцчшщъыьэюяабвгдеёжзийклмнопрстуфхцчшщъыьэюя'
    res = ''
    if p==1:
        for i in text:
            index = liters.find(i)
            new_index = index + step
            if i in liters:
                res += liters[new_index]
            else:
                res += i
    if p == 0:
        for i in text:
            index = liters.find(i)
            new_index = index - step
            if i in liters:
                res += liters[new_index]
            else:
                res += i

    return res
```

In [19]:
```
t = 'физмат сила'
```

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

```
физмат сила - члкпгх флог - физмат сила
```

Рис. 1: шифр Цезаря

Контрольный пример

In [23]:
```
def atbash(text, p=0):
    liters = 'абвгдеёжзийклмнопрстуфхцчшщъыьэюя '
    liters_r = [i for i in liters]
    liters_r.reverse()
    res=''
    if p==1:
        for i in text:
            for j,l in enumerate(liters):
                if i==l:
                    res += liters_r[j]
    if p==0:
        for i in text:
            for j,l in enumerate(liters_r):
                if i==l:
                    res += liters[j]

    return res
```

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

```
физмат сила - лчшу наочф  - физмат сила
```

Рис. 2: шифр Атбаш

Выводы

Результаты выполнения лабораторной работы

Изучили алгоритмы шифрования Цезаря и Атбаш.