Шифр простой замены

Алексей Бондарь

11 сентября, 2024, 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

```
    return res
```

In [2]:
```
s = 'HELLO RUDN'
print(f'{s} - {cesar(s, 4, 0)} - {cesar(cesar(s, 4, 0), 4, 1)}')
```

```
HELLO RUDN - LIPPS VYHR - HELLO RUDN
```

Figure 1: шифр Цезаря

Контрольный пример

```
    if w == 1:
        for i in text:
            for j,l in enumerate(liters_r):
                if i==l:
                    res += liters[j]
    return res
```

```
In [13]: s = 'HELLO RUDN'
         print(f'{s} - {atbash(s, 0)} - {atbash(atbash(s, 0), 1)}')
```

```
HELLO RUDN - TWPPMAJGXN - HELLO RUDN
```

Figure 2: шифр Атбаш

Выводы

Результаты выполнения лабораторной работы

Изучили алгоритмы шифрования Цезаря и Атбаш.