Шифр простой замены

Ласурия Данил Рустанбеевич

11 сентября, 2023, 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 [5]: s = 'CESAR'
        print(f'{s} : {cesar(s, 4)} : {dec_cesar(cesar(s, 4), 4)}')

        CESAR : GIWEV : CESAR
```

Figure 1: шифр Цезаря

Контрольный пример

```
    return res

In [9]: s = 'ATBASH'
        print (f'{s} : {atbash(s)} : {dec_atbash(atbash(s))}')

        ATBASH : ZGYZHS : ATBASH
```

Figure 2: шифр Атбаш

Выводы

Результаты выполнения лабораторной работы

Изучили алгоритмы шифрования Цезаря и Атбаш.