Шифр простой замены

Михаил Пименов НФИмд-02-23

9 сентября, 2022, 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, у - символ шифрованного текста n- мощность алфавита $\mathbf{k}-$ ключ.

Контрольный пример

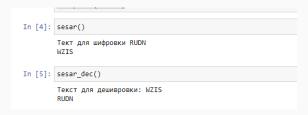


Figure 1: Работа алгоритмов

Контрольный пример

```
In [16]: atbash()

Тект для шифровкиRUDN

IFWM

In [17]: atbash_dec()

Тект для дешифровки IFWM

RUDN
```

Figure 2: Работа алгоритмов

Выводы

Результаты выполнения лабораторной работы

Изучили алгоритмы шифрования Цезаря и Атбаш.