

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 – 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 [4]: `sesar()`

Текст для шифровки RUDN
WZIS

In [5]: `sesar_dec()`

Текст для дешифровки: WZIS
RUDN

Figure 1: Работа алгоритмов


```
In [16]: atbash()
```

```
Текст для шифровки RUDN  
IFWM
```

```
In [17]: atbash_dec()
```

```
Текст для дешифровки IFWM  
RUDN
```

Figure 2: Работа алгоритмов

Выводы

Результаты выполнения лабораторной работы

Изучили алгоритмы шифрования Цезаря и Атбаш.