

Шифр простой замены

Хайдара Абдульджалиль Мухаммад Махди

3 января, 2024, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

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 — 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.

```
In [6]: 1 if __name__ == "__main__":  
        2     main()
```

```
Цезарь - шифрование :)HELLO  
MJQQT  
Цезарь - дешифровкаMJQQT  
HELLO  
Атбаш - шифрованиеHELLO  
SV00L  
Атбаш - дешифровкаSV00L  
HELLO
```

Рис. 1: Работа алгоритмов

Выводы

Изучили алгоритмы шифрования Цезаря и Атбаш.