

Шифр простой замены

Хитяев Евгений НПМмд-02-21

15 ноября, 2021, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Изучение шифрования методом простой замены

Выполнение лабораторной работы

Криптография (от греч. *тайное письмо*) — наука о математических методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.

В древности криптография вызывала огромный интерес, так как позволяла безопасно передавать информацию.

Шифр Цезаря

Шифр Цезаря — один из самых простых и наиболее широко известных методов шифрования.

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики:

$$y = (x + k) \bmod n$$

$$x = (y - k + n) \bmod n$$

где: x — символ открытого текста, y — символ зашифрованного текста, n — мощность алфавита, k — ключ.

Ключ к расшифровке шифра Атбаш прост: первая буква алфавита должна быть заменена на последнюю, вторая – на предпоследнюю и так до последней буквы, которая станет первой. На языке математики эту замену можно представить в такой формуле: $i = n - j + 1$, где j – это номер символа, который мы хотим зашифровать, а n – количество всех символов алфавита.

Контрольный пример

```
In [19]: if __name__ == "__main__":  
         main()
```

Цезарь:

Зашифровка: Abcd

Результат: Fghi

Дешифровка: Fghi

Результат: Abcd

Атбаш:

Зашифровка: Abcd

Результат: X765

Дешифровка: X765

Результат: Abcd

Figure 1: Работа алгоритмов

Выводы

Результаты выполнения лабораторной работы

В ходе выполнения работы, мне удалось освоить шифрование методом простой замены и реализовать программу для шифрования на языке Python.