Шифр простой замены

Милёхин Александр НПМмд-02-21

Цели и задачи

Цели и задачи

Изучение шифрования методом простой замены

Криптография

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) mod n
x = (y - k + n) mod n
```

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

Шифр Атбаш

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 с 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

Результаты выполнения лабораторной работы

Я освоил шифрование методом простой замены и реализовать программу для шифрования на языке Python.

Спасибо за внимание