

Шифр гаммирования

Хитяев Евгений Анатольевич НПМмд-02-21

26 ноября, 2021, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Изучение алгоритма шифрования гаммированием

Выполнение лабораторной работы

Гаммирование – это наложение (снятие) на открытые (зашифрованные) данные криптографической гаммы, т.е. последовательности элементов данных, вырабатываемых с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

Наложение (или снятие) гаммы на блок сообщения в рассматриваемом нами стандарте реализуется с помощью операции побитного сложения по модулю 2 (XOR). То есть при шифровании сообщений каждый блок открытого сообщения XORится с блоком криптографической гаммы, длина которого должна соответствовать длине блоков открытого сообщения. При этом, если размер блока исходного текста меньше, чем размер блока гаммы, блок гаммы обрезается до размера блока исходного текста (выполняется процедура усечения гаммы).



Figure 1: Шифрование



Figure 2: Дешифровка

В аддитивных шифрах символы исходного сообщения заменяются числами, которые складываются по модулю с числами гаммы. Ключом шифра является гамма, символы которой последовательно повторяются. Перед шифрованием символы сообщения и гаммы заменяются их номерами в алфавите и само кодирование выполняется по формуле

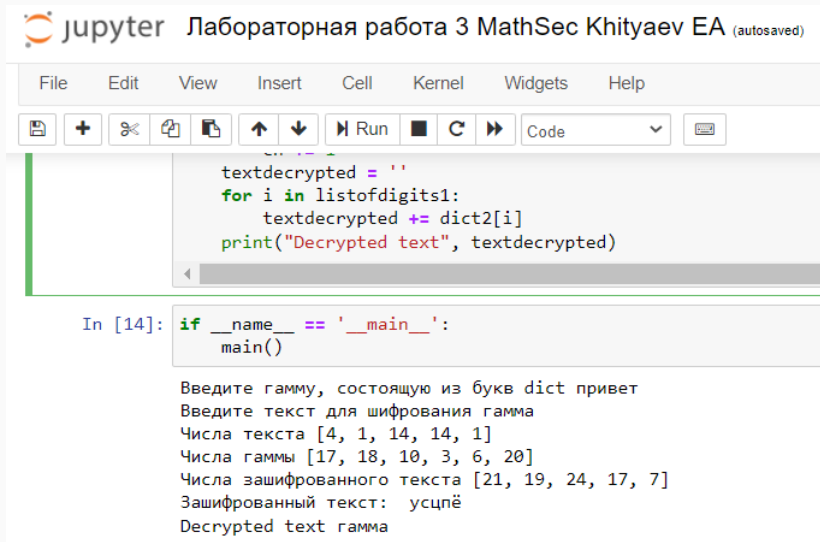
$$C_i = (T_i + G_i) \bmod N$$

Пример работы алгоритма

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------|----|----|----|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---|----|----|----|----|
| <i>T</i> | К | А | Ф | Е | Д | Р | А | | С | И | С | Т | Е | М | | И | Н | Ф | О | Р | М | А | Т | И | К | И |
| <i>G</i> | С | И | М | В | О | Л | С | И | М | В | О | Л | С | И | М | В | О | Л | С | И | М | В | О | Л | С | И |
| <i>T</i> | 12 | 1 | 22 | 6 | 5 | 18 | 1 | 34 | 19 | 10 | 19 | 20 | 6 | 14 | 34 | 10 | 15 | 22 | 16 | 18 | 14 | 1 | 20 | 10 | 12 | 10 |
| <i>G</i> | 19 | 10 | 14 | 3 | 16 | 13 | 19 | 10 | 14 | 3 | 16 | 13 | 19 | 10 | 14 | 3 | 16 | 13 | 19 | 10 | 14 | 3 | 16 | 13 | 19 | 10 |
| <i>T+G</i> | 31 | 11 | 36 | 9 | 21 | 31 | 20 | 44 | 33 | 13 | 35 | 33 | 25 | 24 | 48 | 13 | 31 | 35 | 35 | 28 | 28 | 4 | 36 | 23 | 31 | 20 |
| <i>mod N</i> | 31 | 11 | 36 | 9 | 21 | 31 | 20 | 0 | 33 | 13 | 35 | 33 | 25 | 24 | 4 | 13 | 31 | 35 | 35 | 28 | 28 | 4 | 36 | 23 | 31 | 20 |
| <i>0 → N</i> | 31 | 11 | 36 | 9 | 21 | 31 | 20 | 44 | 33 | 13 | 35 | 33 | 25 | 24 | 4 | 13 | 31 | 35 | 35 | 28 | 28 | 4 | 36 | 23 | 31 | 20 |
| <i>С</i> | Э | Й | 1 | З | У | Э | Т | 9 | Я | Л | 0 | Я | Ч | Ц | Г | Л | Э | 0 | 0 | Ъ | Ъ | Г | 1 | Х | Э | Т |

Figure 3: Работа алгоритма гаммирования

Пример работы программы



The screenshot shows a Jupyter Notebook window titled "jupyter Лабораторная работа 3 MathSec Khityaev EA (autosaved)". The interface includes a menu bar (File, Edit, View, Insert, Cell, Kernel, Widgets, Help) and a toolbar with icons for saving, adding cells, undo, redo, and running code. The code editor contains a Python function for decrypting a Vigenere cipher. Below the code editor, the output of the code is displayed, showing the input gamma, text, and the resulting decrypted text.

```
textdecrypted = ''
for i in listofdigits1:
    textdecrypted += dict2[i]
print("Decrypted text", textdecrypted)
```

```
In [14]: if __name__ == '__main__':
        main()
```

Введите гамму, состоящую из букв dict привет
Введите текст для шифрования гамма
Числа текста [4, 1, 14, 14, 1]
Числа гаммы [17, 18, 10, 3, 6, 20]
Числа зашифрованного текста [21, 19, 24, 17, 7]
Зашифрованный текст: усцпё
Decrypted text гамма

Figure 4: Пример работы алгоритма гаммирования

Выводы

Результаты выполнения лабораторной работы

В ходе выполнения работы мне удалось изучить алгоритмы шифрования на основе гаммирования и реализовать их на языке программирования Python.

Спасибо за внимание!