
Шифр гаммирования

Милёхин Александр НПМмд-02-21

Цель лабораторной работы

Изучение алгоритма шифрования гаммированием

Гаммирование

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.

Гаммирование

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).

Алгоритм

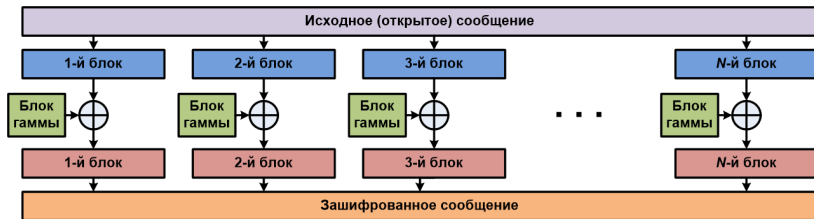


Figure 1: Шифрование

Алгоритм

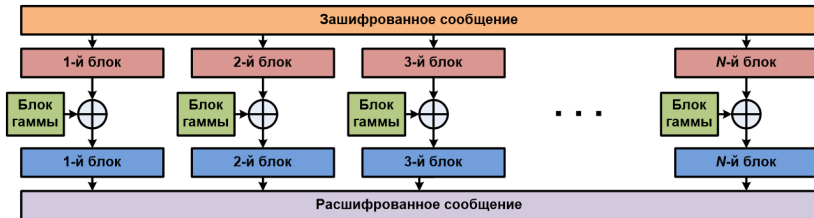


Figure 2: Дешифровка

Формула

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

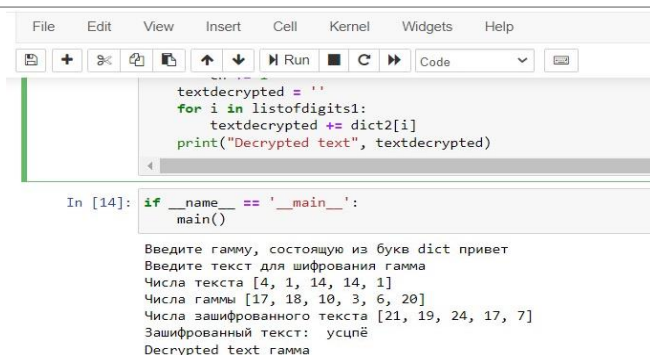
$$C_i = (T_i + G_i) \bmod N$$

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	О	Я	Ч	Ц	Г	Л	Э	О	О	Ъ	Ъ	Г	1	Х	Э	Т

Figure 3: Работа алгоритма гаммирования

Пример работы программы



The screenshot shows a Jupyter Notebook interface with a menu bar (File, Edit, View, Insert, Cell, Kernel, Widgets, Help) and a toolbar with icons for saving, adding, deleting, copying, pasting, and running code. The code is written in Python and demonstrates a gamma cipher algorithm. The code is as follows:

```
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

Результаты выполнения лабораторной работы

Я изучил алгоритмы шифрования на основе гаммирования и реализовал их на языке программирования Python.

Спасибо за внимание

A solid orange horizontal bar at the bottom of the slide.