Шифргаммирования

Назармамадов Умед Джамшедович

22 апреля, 2025, Москва, Россия

РоссийскийУниверситетДружбы Народов

Целиизадачи

Изучение алгоритма шифрования гаммированием

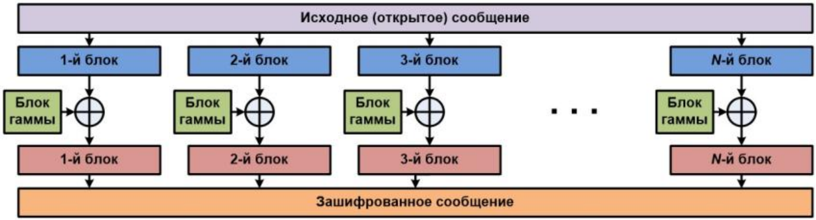
Выполнениелабораторной работы

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.

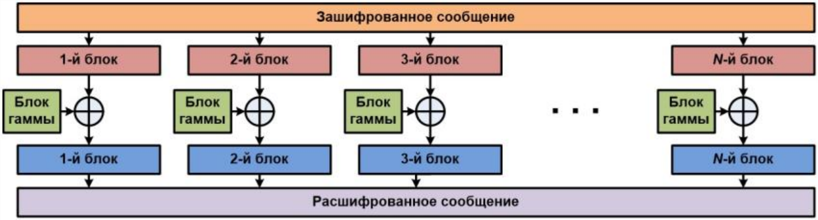
Наложение (или снятие) гаммы на блок сообщения в рассматриваемом нами стандарте реализуется с помощью операции побитного сложения по модулю 2 (XOR). То есть при шифровании сообщений каждый блок открытого сообщения ксорится с блоком криптографической гаммы, длина которого должна соответствовать длине 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).



Исходное (открытое) сообщение
1-й блок
2-й блок
3-й блок
N-й блок
Блок гаммы
Блок гаммы
Блок гаммы
Блок гаммы
1-й блок
2-й блок
3-й блок
N-й блок
Зашифрованное сообщение

Рис. 1: Шифрование



Зашифрованное сообщение

1-й блок

2-й блок

3-й блок

N-й блок

Блок гаммы

1-й блок

2-й блок

3-й блок

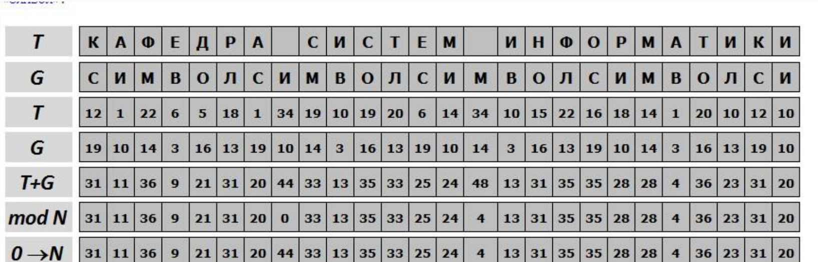
N-й блок

Расшифрованное сообщение

Рис. 2: Дешифровка

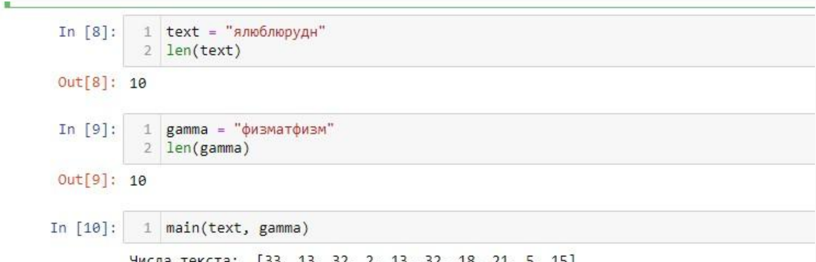
В аддитивных шифрах символы исходного сообщения заменяются числами, которые складываются по модулю с числами гаммы. Ключом шифра является гамма, символы которой последовательно повторяются. Перед шифрованием символы сообщения и гаммы заменяются их номерами в алфавите и само кодирование выполняется по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

$$Ci = (Ti+Gi) mod N$$



T	К	А	Ф	Е	Д	Р	А		С	И	С	Т	Е	М		И	Н	Ф	О	Р	М	А	Т	И	К	И
G	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
T	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
G	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
T+G	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
mod N	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
0 → N	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

Рис. 3: Работа алгоритма гаммирования



```
In [8]:  text = "ялюблюрудн"
         len(text)

Out[8]:  10

In [9]:  gamma = "физматфизм"
         len(gamma)

Out[9]:  10

In [10]: main(text, gamma)

         Числа текста:  [33, 13, 32, 2, 13, 32, 18, 21, 5, 15]
```

Рис. 4: Работа алгоритма гаммирования

Выводы

Изучили алгоритм шифрования с помощью гаммирования