

Шифр гаммирования

Альсид Мона НФИбд-03-18¹

11 декабря 2021 г. Москва, Россия

¹российский Университет Дружбы Народов

Цели и задачи

Изучение алгоритма шифрования гаммированием

Выполнения 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).

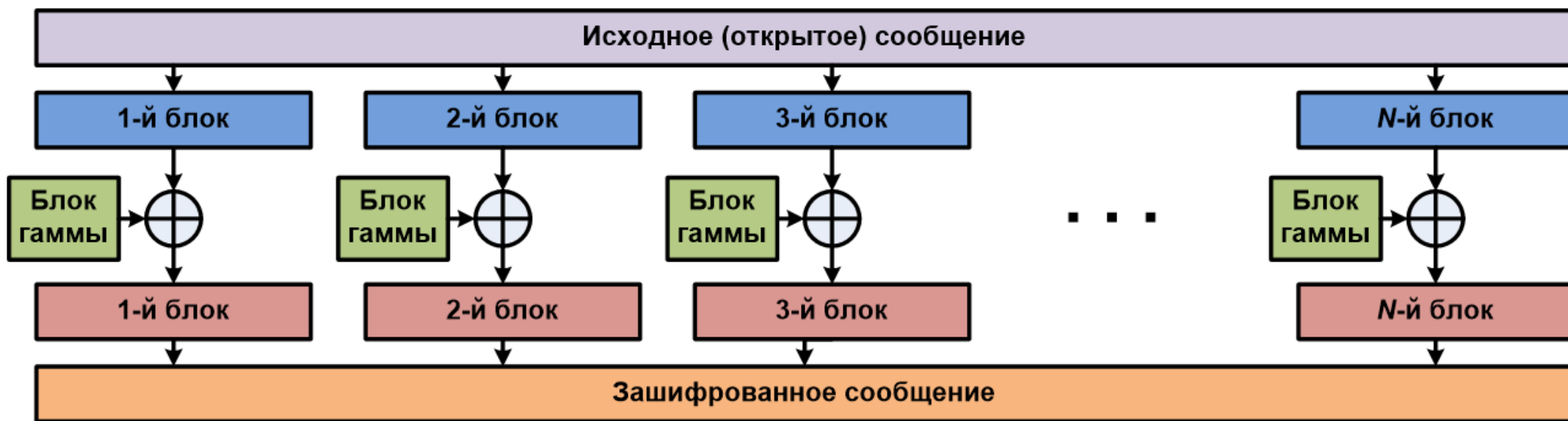


Figure 1: Шифрование

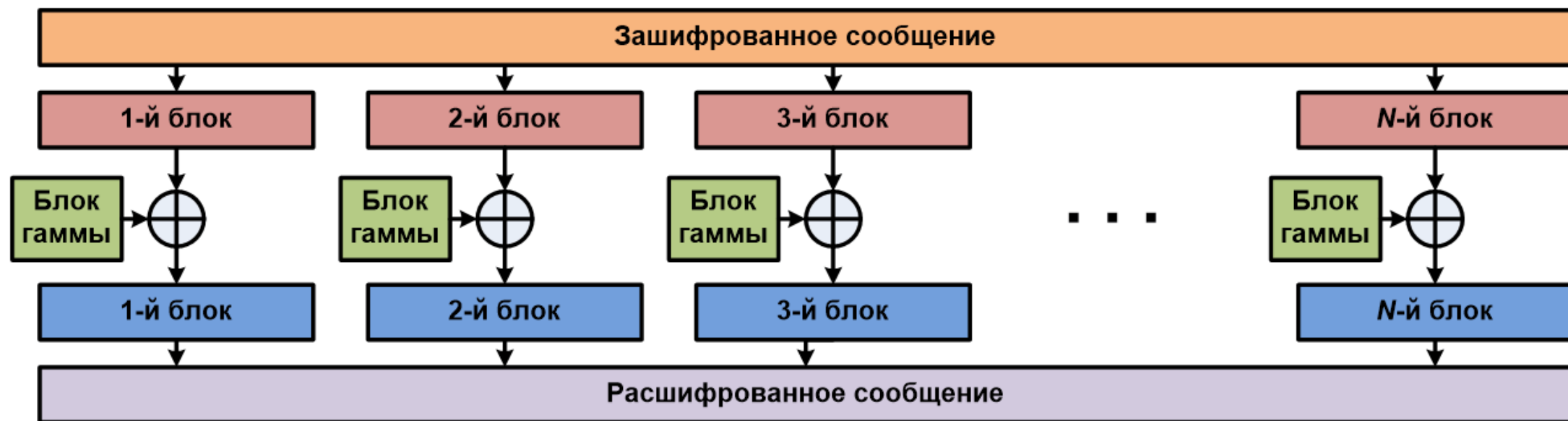
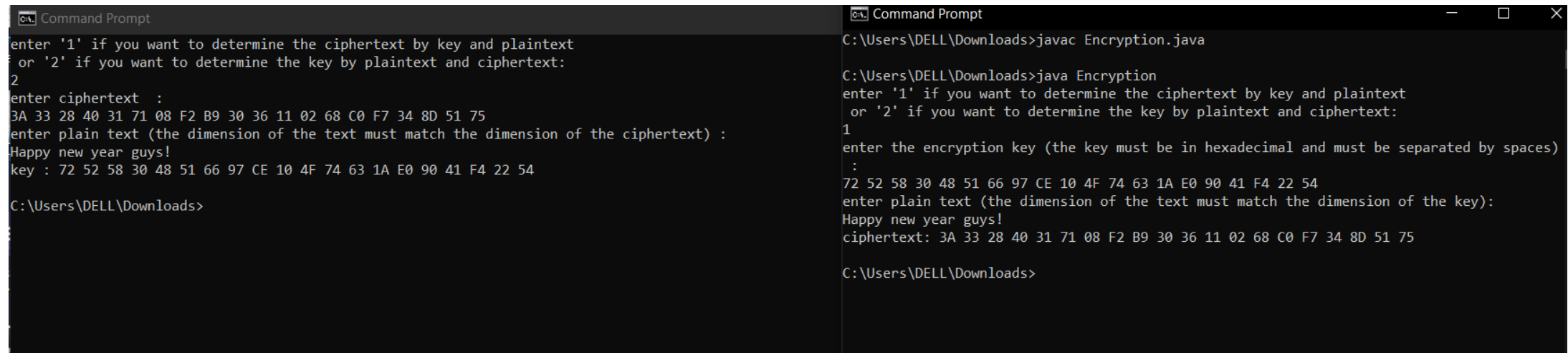


Figure 2: Дешифровка



```
C:\Users\DELL\Downloads>java Encryption
enter '1' if you want to determine the ciphertext by key and plaintext
or '2' if you want to determine the key by plaintext and ciphertext:
2
enter ciphertext :
3A 33 28 40 31 71 08 F2 B9 30 36 11 02 68 C0 F7 34 8D 51 75
enter plain text (the dimension of the text must match the dimension of the ciphertext) :
Happy new year guys!
key : 72 52 58 30 48 51 66 97 CE 10 4F 74 63 1A E0 90 41 F4 22 54

C:\Users\DELL\Downloads>

C:\Users\DELL\Downloads>javac Encryption.java

C:\Users\DELL\Downloads>java Encryption
enter '1' if you want to determine the ciphertext by key and plaintext
or '2' if you want to determine the key by plaintext and ciphertext:
1
enter the encryption key (the key must be in hexadecimal and must be separated by spaces)
:
72 52 58 30 48 51 66 97 CE 10 4F 74 63 1A E0 90 41 F4 22 54
enter plain text (the dimension of the text must match the dimension of the key):
Happy new year guys!
ciphertext: 3A 33 28 40 31 71 08 F2 B9 30 36 11 02 68 C0 F7 34 8D 51 75

C:\Users\DELL\Downloads>
```

Figure 3: Работа алгоритма гаммирования

Выводы

Изучили алгоритм шифрования с помощью гаммирования.