

Шифр гаммирования

Шемякин Алексей НФИбд-02-18

11 декабря, 2021, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Освоить на практике применение режима однократного гаммирования

Выполнение лабораторной работы

Гаммирование представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Иными словами, наложение гаммы — это сложение её элементов с элементами открытого (закрытого) текста по некоторому фиксированному модулю, значение которого представляет собой известную часть алгоритма шифрования.

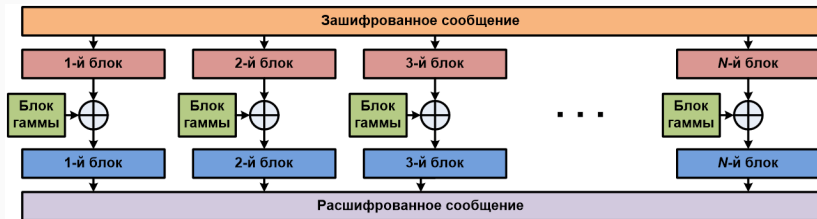


Figure 1: Шифрование

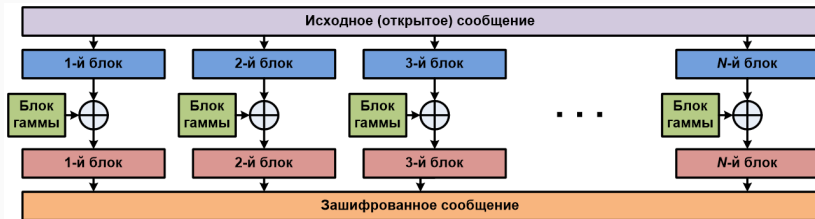


Figure 2: Дешифровка

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>C</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

```
"C:\Program Files\Java\jdk-11.0.11\bin\java.exe" "-javaagent:C:\Program Files\JetBrains\IntelliJ IDEA 2020.2.3\lib\jbr\bin\java.exe" -jar C:\Program Files\JetBrains\IntelliJ IDEA 2020.2.3\lib\jbr\bin\java.exe
Введите:
'1' если хотите определить шифротекст по ключу и открытому тексту
'2' если хотите определить ключ по открытому тексту и шифротексту:
1
Введите ключ шифрования (ключ должен быть в шестнадцатеричной системе счисления и должен быть разделен пробелами):
05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 0B B2 70 54 0E 4E 37
Введите открытый текст (размерность текста должна совпадать с размерностью ключа):
Happy New Year Friends!
Шифротекст : 4D 6D 67 0F 77 6E 79 87 E3 30 50 4B 43 25 0F 8E 79 DB 15 3A 6A 3D 16

Process finished with exit code 0
```

Figure 4: Работа алгоритма гаммирования

Пример работы программы 2

```
"C:\Program Files\Java\jdk-11.0.11\bin\java.exe" "-javaagent:C:\Program Files\JetBrains\I  
Введите:  
'1' если хотите определить шифротекст по ключу и открытому тексту  
'2' если хотите определить ключ по открытому тексту и шифротексту:  
2  
Введите шифротекст :  
4D 6D 67 0F 77 6E 79 B7 E3 30 50 4B 43 25 DF 8E 79 DB 15 3A 6A 3D 16  
Введите открытый текст (размерность текста должна совпадать с размерностью шифротекста):  
Happy New Year Friends!  
Ключ : 05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 0B B2 70 54 0E 4E 37  
  
Process finished with exit code 0
```

Figure 5: Работа алгоритма гаммирования

Выводы

Освоил на практике применение режима однократного гаммирования