

# Элементы криптографии. Однократное гаммирование

---

Жижченко Валерия Викторовна

Российский Университет Дружбы Народов

# Цель лабораторной работы

---

# Цель лабораторной работы

Освоить на практике применение режима однократного гаммирования

# Выполнение работы

---

Разработали приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение обладает следующим функционалом:

# Выполнение работы

1. Определяет вид шифротекста при известном ключе и известном открытом тексте.

```
Message: С Новым Годом, Друзья!  
Encrypted Message: 00G2w/r{[]00 %U0~          9F04$~  
  
Message hex:  
0xd0    0xa1    0x20    0xd0    0x9d  
0xd0    0xbe    0xd0    0xb2    0xd1  
0x8b    0xd0    0xbc    0x20    0xd0  
0x93    0xd0    0xbe    0xd0    0xb4  
0xd0    0xbe    0xd0    0xbc    0x2c  
0x20    0xd0    0x94    0xd1    0x80  
0xd1    0x83    0xd0    0xb7    0xd1  
0x8c    0xd1    0x8f    0x21    0  
  
Encrypted Message hex:  
0x9     0xdb    0xbd    0x30    0x47  
0x32    0xb2    0x77    0x2f    0xa7  
0x72    0xc0    0x7b    0x5d    0x2  
0x91    0xe5    0x80    0x8a    0x25  
0x55    0x1d    0x7e    0x84    0xe4  
0x9     0x39    0xbb    0x46    0xe3  
0xa4    0xf3    0xe     0xa4    0x81  
0x34    0x24    0xd3    0x7e    0x92
```

## Выполнение работы

2. Определяет ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

Key1:

0xd9	0x7a	0x9d	0xe0	0xda
0xe2	0xc	0xa7	0x9d	0x76
0xf9	0x10	0xc7	0x7d	0xd2
0x2	0x35	0x3e	0x5a	0x91
0x85	0xa3	0xae	0x38	0xc8
0x29	0xe9	0x2f	0x97	0x63
0x75	0x70	0xde	0x13	0x50
0xb8	0xf5	0x5c	0x5f	0x92

Key2:

0xd9	0x7a	0x9d	0xe0	0xda
0xe2	0xc	0xa7	0x9d	0x76
0xf9	0x10	0xc7	0x7d	0xd2

## **Ответы на контрольные вопросы**

---



### 1. Поясните смысл однократного гаммирования.

Гаммирование – выполнение операции XOR между элементами гаммы и элементами подлежащего сокрытию текста. Если в методе шифрования используется однократная вероятностная гамма (однократное гаммирование) той же длины, что и подлежащий сокрытию текст, то текст нельзя раскрыть. Даже при раскрытии части последовательности гаммы нельзя получить информацию о всём скрываемом тексте.

2. Перечислите недостатки однократного гаммирования.

Абсолютная стойкость шифра доказана только для случая, когда однократно используемый ключ, длиной, равной длине исходного сообщения, является фрагментом истинно случайной двоичной последовательности с равномерным законом распределения.

### 3. Перечислите преимущества однократного гаммирования.

Во-первых, такой способ симметричен, т.е. двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение. Во-вторых, шифрование и расшифрование может быть выполнено одной и той же программой. Наконец, Криптоалгоритм не даёт никакой информации об открытом тексте: при известном зашифрованном сообщении  $C$  все различные ключевые последовательности  $K$  возможны и равновероятны, а значит, возможны и любые сообщения  $P$ .

4. Почему длина открытого текста должна совпадать с длиной ключа?

Если ключ короче текста, то операция XOR будет применена не ко всем элементам и конец сообщения будет не закодирован. Если ключ будет длиннее, то появится неоднозначность декодирования.

5. Какая операция используется в режиме однократного гаммирования, назовите её особенности?

Наложение гаммы по сути представляет собой выполнение побитовой операции сложения по модулю 2, т.е. мы должны сложить каждый элемент гаммы с соответствующим элементом ключа. Данная операция является симметричной, так как прибавление одной и той же величины по модулю 2 восстанавливает исходное значение.

6. Как по открытому тексту и ключу получить шифротекст?

В таком случае задача сводится к правилу:

$$C_i = P_i \oplus K_i$$

т.е. мы поэлементно получаем символы зашифрованного сообщения, применяя операцию исключающего или к соответствующим элементам ключа и открытого текста.

7. Как по открытому тексту и шифротексту получить ключ?

Подобная задача решается путем применения операции исключающего или к последовательностям символов зашифрованного и открытого сообщений:

$$K_i = P_i \oplus C_i.$$

8. В чем заключаются необходимые и достаточные условия абсолютной стойкости шифра?

Необходимые и достаточные условия абсолютной стойкости шифра:

- полная случайность ключа;
- равенство длин ключа и открытого текста;
- однократное использование ключа.



## Вывод

---

Освоили на практике применение режима однократного гаммирования