

Презентация по лабораторной работе №7.

Основы информационной безопасности.

Рогожина Н.А.

9 мая 2024

Российский университет дружбы народов, Москва, Россия

Информация

- Рогожина Надежда Александровна
- Студентка 2го курса, НКАбд-02-22
- Компьютерные и информационные науки
- Российский университет дружбы народов
- Github

Вводная часть

Освоить на практике применение режима однократного гаммирования.

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно:

1. Определить вид шифротекста при известном ключе и известном открытом тексте.
2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

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.

В соответствии с теорией криптоанализа, 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. Наложение гаммы по сути представляет собой выполнение операции сложения по модулю 2 (XOR) (обозначаемая знаком \oplus) между элементами гаммы и элементами подлежащего сокрытию текста.

Такой метод шифрования является симметричным, так как двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение, а шифрование и расшифрование выполняется одной и той же программой.

Выполнение

```
def gen_key(string):  
    k = np.random.randint(0, 255, len(string))  
    key = [hex(i)[2:] for i in k]  
    return key
```

```
def gamma(string, key):  
    print(f'Изначальный текст: {string}')
```

hex_str = []

```
    for i in string:  
        hex_str.append(i.encode('cp1251').hex().upper())  
    print(f'Изначальный текст в 16-ой системе: ',*hex_str)
```

```
hex_key = []  
    for i in key:  
        hex_key.append(i.upper())  
print(f'Ключ шифрования: ', *hex_key)
```

```
gamma = []
for i in range(len(hex_str)):
    gamma.append('{:02x}'.format(int(hex_str[i], 16)^int(hex_key[i], 16)))
print(f'Gamma текст: ', *gamma)
cr_str = bytearray.fromhex(''.join(gamma)).decode('cp1251')
print(f'Зашифрованный текст: ', cr_str)
return cr_str
```

Результат работы программы

```
In [131]: string = 'С Новым Годом, друзья!'
          key = gen_key(string)
```

```
In [134]: crypt = gamma(string, key)
```

Изначальный текст: С Новым Годом, друзья!

Изначальный текст в 16-ой системе: D1 20 CD EE E2 FB EC 20 C3 EE E4 EE EC 2C 20 E4 F0 F3 E7 FC FF 21

Ключ шифрования: 8C BC E4 5D FD 7E CC EF B8 D7 8 F9 43 ED 47 6D 22 77 37 7 8 7 82

Gamma текст: 5d 9c 29 b3 1f 85 20 cf 7b 39 ec 17 af c1 67 89 d2 84 d0 fb 78 a3

Зашифрованный текст:]ъ)i@... П{9м@ЇБ&T,,РыхJ

```
In [135]: dectypr = gamma(crypt, key)
```

Изначальный текст:]ъ)i@... П{9м@ЇБ&T,,РыхJ

Изначальный текст в 16-ой системе: 5D 9C 29 B3 1F 85 20 CF 7B 39 EC 17 AF C1 67 89 D2 84 D0 FB 78 A3

Ключ шифрования: 8C BC E4 5D FD 7E CC EF B8 D7 8 F9 43 ED 47 6D 22 77 37 7 8 7 82

Gamma текст: d1 20 cd ee e2 fb ec 20 c3 ee e4 ee ec 2c 20 e4 f0 f3 e7 fc ff 21

Зашифрованный текст: С Новым Годом, друзья!

Рис. 1: С Новый Годом, друзья!

Выводы

В ходе лабораторной работы мы написали код для шифрации и дешифрации фразы “С Новым Годом, друзья!”, а также освоили основные принципы однократного гаммирования.

Спасибо за внимание
