Элементы криптографии. Однократное гаммирование

Акопян Изабелла Арменовна НБИбд 01-20

21 октября, 2023, Москва, Россия

Российский Университет Дружбы Народов

Цель работы

Освоить на практике применение режима однократного гаммирования.

1. Создана программа, шифрующая сообщение по ключу.

2. Создана программа, определяющая ключ по шифру и исходному тексту.

3. Программа проверена на данных из пособия

Цель лабораторной работы

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммиро 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 собо возможных вариантов прочтения открытого текста

Выполнение лабораторной работы

Выполнение лабораторной работы

```
[49] import numpy as np

     def code(text):
         array = []
         for i in text:
             array.append(i.encode('cp1251').hex())
         print('text 16: ', *array)

         key = np.random.randint(0, 255, len(text))
         key_16 = [hex(i)[2:] for i in key]
         print("key 16: ", *key_16)
         cr = []
         for i in range(len(array)):
             cr.append("{:02x}".format(int(array[i], 16) ^ int(key_16[i], 16)))
         print("text in 16: ", *cr)

         f_text = bytearray.fromhex(''.join(cr)).decode('cp1251')
         print('text: ', f_text)
         return key_16, f_text

     text = "С новым годом, друзья!"
     key, f_text = code(text)

     text 16:  d1 20 ed ee e2 fb ec 20 e3 ee e4 ee ec 2c 20 e4 f0 f3 e7 fc ff 21
     key 16:  3f 66 9f 30 6e d5 5c a6 5e 2a 76 23 c3 6f b6 fd 8 38 86 57 37 52
     text in 16:  ee 46 72 de 8c 2e b0 86 bd c4 92 cd 2f 43 96 19 f8 cb 61 ab c8 73
     text:  оFrЮь.°†SД’Н/С–ЂшЛа«Иs
```

Figure 1: Программа шифрования 1/2

Выполнение лабораторной работы

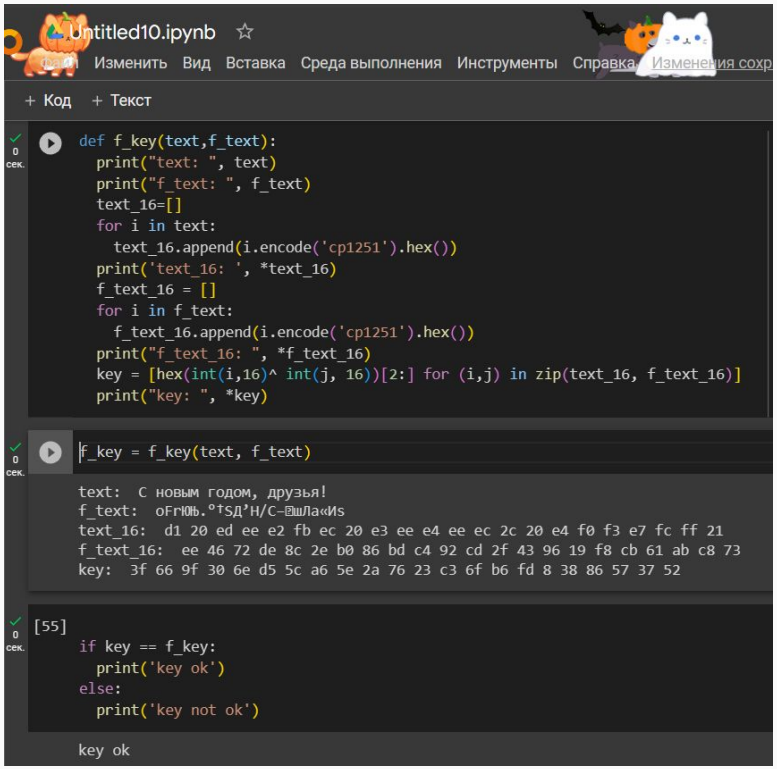

Figure 2: Программа шифрования 2/2

Выводы

Результаты выполнения лабораторной работы

Я освоила на практике применение режима однократного гаммирования.