

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 гаммирования.

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 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: оФрмь."тSд"н/с-шланиИс
```

Figure 1: Программа шифрования 1/2

Выполнение лабораторной работы

```

1  def f_key(text,f_text):
2      print('text: ', text)
3      print('f_text: ', f_text)
4      text_16=[]
5      for i in text:
6          text_16.append(i.encode('cp1251').hex())
7      print('text_16: ', *text_16)
8      f_text_16 = []
9      for i in f_text:
10         f_text_16.append(i.encode('cp1251').hex())
11     print('f_text_16: ', *f_text_16)
12     key = [hex(int(i,16)^ int(j, 16))[2:] for (i,j) in zip(text_16, f_text_16)]
13     print('key: ', *key)
14
15  f_key = f_key(text, f_text)
16
17  text:  С новым годом, друзья!
18  f_text:  0frh8*0tsg/h/c-mlaams
19  text_16:  d1 20 ed a0 e2 fb ec 20 e3 ee e4 ee c2 20 e4 f0 f3 e7 fc ff 21
20  f_text_16:  ee 40 72 de 8c 2e b0 86 bd c4 92 cd 2f 43 96 19 f8 cb 61 ab c8 73
21  key:  3f 66 9f 30 6e d5 5c a6 5e 2a 76 23 c3 6f b6 fd 8 38 86 57 37 52
22
23  [55]
24  if key == f_key:
25      print('key ok')
26  else:
27      print('key not ok')
28
29  key ok

```

Figure 2: Программа шифрования 2/2

Выводы

Я освоила на практике применение режима однократного гаммирования.