Лабораторная работа №8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Victoria M. Shutenko

29 October, 2022, Moscow, Russian Federation

RUDN University, Moscow, Russian Federation

Цель выполнения лабораторной работы

Цель выполнения лабораторной работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Подключение библиотек

```
import numpy as np
import operator as op
import sys

p1 = "Я устала и хочу спать."
p2 = "Спокойной ночи, друг!!"
print(len(p1))
print(len(p2))
```

Функция encrypt

```
def encrypt(text1, text2):
    print("text1: ", text1)
    newtext1=[]
    for i in text1:
        newtext1.append(i.encode("cp1251").hex())
    print("text1 in 16: ", newtext1)
    print("text2: ", text2)
    newtext2=[]
    for i in text2:
        newtext2.append(i.encode("cp1251").hex())
    print("text2 in 16: ", newtext2)
    r=np.random.randint(0,255, len(text1))
    key=[hex(i)[2:] for i in r]
    newkey=[]
    for i in newkey:
```

Вывод encrypt

```
k, t1, et1, t2, et2 = encrypt(p1,p2)
```

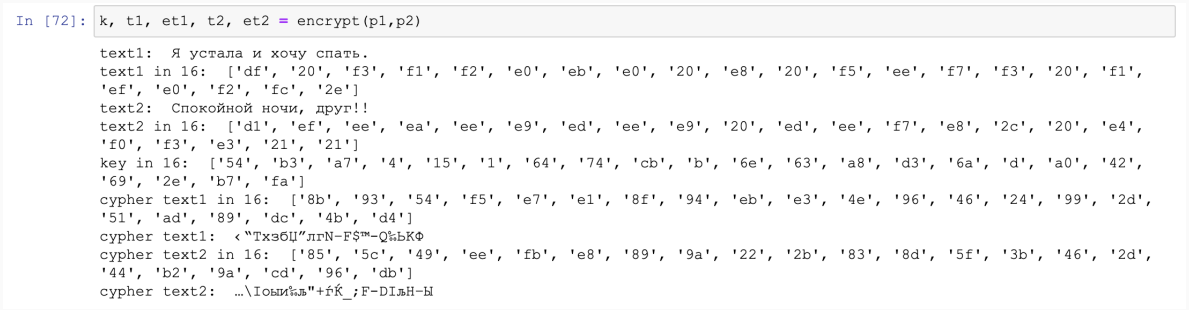

Figure 1: Результат выполнения функции encrypt.

Функция decrypt

```
def decrypt(c1, c2, p1):
    print("cypher text1: ", c1)
    newc1=[]
    for i in c1:
        newc1.append(i.encode("cp1251").hex())
    print("cypher text1 in 16: ", newc1)
    print("cypher text2: ", c2)
    newc2=[]
    for i in c2:
        newc2.append(i.encode("cp1251").hex())
    print("cypher text2 in 16: ", newc2)
    print("open text1: ", p1)
    newp1=[]
    for i in p1:
        newp1.append(i.encode("cp1251").hex())
```

Вывод decrypt

```
decrypt(et1, et2, p1)
```

```
In [74]: decrypt(et1, et2, p1)

         cypher text1:  ‹"ТхэбЦ"лгN-F$™-Q%ЬКФ
         cypher text1 in 16:  ['8b', '93', '54', 'f5', 'e7', 'e1', '8f', '94', 'eb', 'e3', '4e', '96', '46', '24', '99', '2d',
         '51', 'ad', '89', 'dc', '4b', 'd4']
         cypher text2:  …\Iоыи‰ль"+ѓЌ_;F-DIљН-Ы
         cypher text2 in 16:  ['85', '5c', '49', 'ee', 'fb', 'e8', '89', '9a', '22', '2b', '83', '8d', '5f', '3b', '46', '2d',
         '44', 'b2', '9a', 'cd', '96', 'db']
         open text1:  Я устала и хочу спать.
         open text1 in 16:  ['df', '20', 'f3', 'f1', 'f2', 'e0', 'eb', 'e0', '20', 'e8', '20', 'f5', 'ee', 'f7', 'f3', '20',
         'f1', 'ef', 'e0', 'f2', 'fc', '2e']
         open text2 in 16:  ['d1', 'ef', 'ee', 'ea', 'ee', 'e9', 'ed', 'ee', 'e9', '20', 'ed', 'ee', 'f7', 'e8', '2c', '20',
         'e4', 'f0', 'f3', 'e3', '21', '21']
         open text2:  Спокойной ночи, друг!!

Out[74]: ('Я устала и хочу спать.', 'Спокойной ночи, друг!!')
```

Figure 3: Результат выполнения функции decrypt.

Итоги

Итоги

- изучили шифрование в режиме гаммирования
- написали код из 2-х функций для решения задачи