Лабораторная работа №8

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

Лёшьен Стефани

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 учусь в РУДН"
print(len(p1))
p2="на оржиникдзе!"
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)
```

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

     text1:  я учусь в РУДН
     text1 in 16:  ['ff', '20', 'f3', 'f7', 'f3', 'f1', 'fc', '20', 'e2', '20', 'd0', 'd3', 'c4', 'cd']
     text2:  на оржиникдзе!
     text2 in 16:  ['ed', 'e0', '20', 'ee', 'f0', 'e6', 'e8', 'ed', 'e8', 'ea', 'e4', 'e7', 'e5', '21']
     key in 16:  ['66', '90', 'fb', 'dd', '91', '62', '24', 'f6', '24', '4a', '17', '85', '16', '0']
     cypher text1 in 16:  ['99', 'b0', '08', '2a', '62', '93', 'd8', 'd6', 'c6', '6a', 'c7', '56', 'd2', 'cd']
     cypher text1:  ™*b“ШЦЖj3VTH
     cypher text2 in 16:  ['8b', '70', 'db', '33', '61', '84', 'cc', '1b', 'cc', 'a0', 'f3', '62', 'f3', '21']
     cypher text2:  ‹рЫ3а„M℗M yby!
```

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)
```

```
decrypt(et2, et1, p1)

cypher text1:  ‹рЫ3а„М?М yby!
cypher text1 in 16:  ['8b', '70', 'db', '33', '61', '84', 'cc', '1b', 'cc', 'a0', 'f3', '62', 'f3', '21']
cypher text2:  ™*b“ШЦЖj3VTH
cypher text2 in 16:  ['99', 'b0', '08', '2a', '62', '93', 'd8', 'd6', 'c6', '6a', 'c7', '56', 'd2', 'cd']
open text1:  я учусь в РУДН
open text1 in 16:  ['ff', '20', 'f3', 'f7', 'f3', 'f1', 'fc', '20', 'e2', '20', 'd0', 'd3', 'c4', 'cd']
open text2 in 16:  ['ed', 'e0', '20', 'ee', 'f0', 'e6', 'e8', 'ed', 'e8', 'ea', 'e4', 'e7', 'e5', '21']
open text2:  на оржиникдзе!
('я учусь в РУДН', 'на оржиникдзе!')
```

Figure 3: Результат выполнения функции decrypt.

Итоги

Итоги

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