Лабораторная работа №8

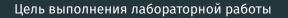
Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Лёшьен Стефани

29 October, 2022, Moscow, Russian Federation

RUDN University, Moscow, Russian Federation

Цель выполнения лабораторной работы



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))
    kev=[hex(i)[2:] for i in r]
    newkev=[]
    for i in newkey:
```

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

```
[] k, tl, etl, t2, et2-encrypt(pl.p2)

texti: a y-y-c a FyBH
texti in 1c, ['ff', '2a', 'f2', 'f2', 'f2', 'f2', 'fc', '2a', 'e2', '2a', 'ea', 'ea', 'ea', 'ca', 'ca']
text2: sa opnomonant
text2 in 1c, ['ea', 'ea', '7a', '7a', 'fa', 'fa', 'ea', 'ea'
```

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())
```

decrypt(et1, et2, p1)

O decrypt(et2, et1, p1)

D cypher text1: (p81a,)@kytyl'
cypher text2: ""b"mulg37H;
cypher text2: ""b", 'e8', 'e8',

Figure 3: Результат выполнения функции decrypt.

Итоги

Итоги

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