Лабораторная работа № 8

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

Абдуллаев Сайидазизхон Шухратович

Цель работы

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

Ход работы

Импорт библиотек и два текста одинаковой длины

In [1]:
```
import numpy as np
import operator as op
import sys
```

In [2]:
```
p1 = "Первый текст"
p2 = "Второй текст"
print(len(p1), len(p2))
```

```
12 12
```

Функция определяющая вид шифротекстов C1 и C2 при известном ключе

In [10]:
```
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 key:
        newkey.append(i.encode("cp1251").hex().upper())
    print("key in 16: ", key)
    xortext1=[]
    for i in range(len(newtext1)):
        xortext1.append("{:02x}".format(int(key[i], 16) ^ int(newtext1[i],16)))
    print("cypher text1 in 16: ", xortext1)
    en_text1=bytearray.fromhex("".join(xortext1)).decode("cp1251")
    print("cypher text1: ", en_text1)
    xortext2=[]
    for i in range(len(newtext2)):
        xortext2.append("{:02x}".format(int(key[i], 16) ^ int(newtext2[i],16)))
    print("cypher text2 in 16: ", xortext2)
    en_text2=bytearray.fromhex("".join(xortext2)).decode("cp1251")
    print("cypher text2: ", en_text2)
    return key, xortext1, en_text1, xortext2, en_text2
```

Вывод функции:

```
In [11]: k, t1, et1, t2, et2=encrypt(p1,p2)

text1:  Первый текст
text1 in 16: ['cf', 'e5', 'f0', 'e2', 'fb', 'e9', '20', 'f2', 'e5', 'ea', 'f1', 'f2']
text2:  Второй текст
text2 in 16: ['c2', 'f2', 'ee', 'f0', 'ee', 'e9', '20', 'f2', 'e5', 'ea', 'f1', 'f2']
key in 16:  ['b7', '5', '4c', '1e', '54', 'f', 'c2', '2e', 'e9', '6a', '7f', '75']
cypher text1 in 16:  ['78', 'e0', 'bc', 'fc', 'af', 'e6', 'e2', 'dc', '0c', '80', '8e', '87']
cypher text1:  хаjьЇжвьЂЋ‡
cypher text2 in 16:  ['75', 'f7', 'a2', 'ee', 'ba', 'e6', 'e2', 'dc', '0c', '80', '8e', '87']
cypher text2:  цчўоєжвьЂЋ‡
```

Новая функция:

Написал функцию, которая при известных двух шифротекстах и одном открытом тексте находит вид второго открытого текста без ключа.

In [20]:
```
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())
    print("open text1 in 16: ", newp1)
    xortmp=[]
    sp2=[]
    for i in range(len(p1)):
        xortmp.append("{:02x}".format(int(newc1[i],16) ^ int(newc2[i], 16)))
        sp2.append("{:02x}".format(int(xortmp[i],16) ^ int(newp1[i], 16)))
    print("open text2 in 16: ", sp2)
    p2=bytearray.fromhex("".join(sp2)).decode("cp1251")
    print("open text2: ", p2)
    return p1, p2
```

Вывод функции:

```
In [21]: decrypt(et1, et2, p1)

         cypher text1:  xajьЇжвьЂЋ‡
         cypher text1 in 16:  ['78', 'e0', 'bc', 'fc', 'af', 'e6', 'e2', 'dc', '0c', '80', '8e', '87']
         cypher text2:  uчўoєжвьЂЋ†
         cypher text2 in 16:  ['75', 'f7', 'a2', 'ee', 'ba', 'e6', 'e2', 'dc', '0c', '80', '8e', '87']
         open text1:  Первый текст
         open text1 in 16:  ['cf', 'e5', 'f0', 'e2', 'fb', 'e9', '20', 'f2', 'e5', 'ea', 'f1', 'f2']
         open text2 in 16:  ['c2', 'f2', 'ee', 'f0', 'ee', 'e9', '20', 'f2', 'e5', 'ea', 'f1', 'f2']
         open text2:  Второй текст

Out[21]: ('Первый текст', 'Второй текст')

In [22]: decrypt(et2, et1, p2)

         cypher text1:  uчўoєжвьЂЋ†
         cypher text1 in 16:  ['75', 'f7', 'a2', 'ee', 'ba', 'e6', 'e2', 'dc', '0c', '80', '8e', '87']
         cypher text2:  xajьЇжвьЂЋ‡
         cypher text2 in 16:  ['78', 'e0', 'bc', 'fc', 'af', 'e6', 'e2', 'dc', '0c', '80', '8e', '87']
         open text1:  Второй текст
         open text1 in 16:  ['c2', 'f2', 'ee', 'f0', 'ee', 'e9', '20', 'f2', 'e5', 'ea', 'f1', 'f2']
         open text2 in 16:  ['cf', 'e5', 'f0', 'e2', 'fb', 'e9', '20', 'f2', 'e5', 'ea', 'f1', 'f2']
         open text2:  Первый текст

Out[22]: ('Второй текст', 'Первый текст')
```

Вывод

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