Защита лабораторной работы №8 Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Исаханян Эдуард Тигранович

2022 Sep 21th

RUDN University, Moscow, Russian Federation

Защита лабораторной работы №8

Цель работы

Цель работы

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

Задание

Задание

1. Написать программу, которая должна определять вид шифротекстов при известных открытых текстах и при известном ключе;
2. Также эта программа должна определить вид одного из текстов, зная вид другого открытого текста и зашифрованный вид обоих текстов (т.е. не нужно использовать ключ при дешифровке).

Функция, шифрующая данные

Ввод [2]:
```
import numpy as np
```

Ввод [17]:
```
def cypher(text1, text2):
    print('Open text: ', text1)
    arr1 = []
    for i in text1:
        arr1.append(i.encode('cp1251').hex())
    print("Open text in 16: ", *arr1)

    arr2 = []
    print('Open text: ', text2)
    for i in text2:
        arr2.append(i.encode('cp1251').hex())
    print("Open text in 16: ", *arr2)

    key = np.random.randint(0, 255, len(text1))
    key_16 = [hex(i)[2:] for i in key]
    print("key in 16: ", *key_16)

    crypt1 = []
    for i in range(len(arr1)):
        crypt1.append("{:02x}".format(int(arr1[i], 16) ^ int(key_16[i], 16)))
    print("cypher text in 16: ", *crypt1)

    crypt2 = []
    for i in range(len(arr2)):
        crypt2.append("{:02x}".format(int(arr2[i], 16) ^ int(key_16[i], 16)))
    print("cypher text in 16: ", *crypt2)

    found_text1 = bytearray.fromhex(''.join(crypt1)).decode('cp1251')
    print("cypher text: ", found_text1)

    found_text2 = bytearray.fromhex(''.join(crypt2)).decode('cp1251')
    print("cypher text: ", found_text2)

    return key_16, found_text1, found_text2
```

Figure 1: Функция, шифрующая данные

Результат работы функции, шифрующей данные

```
Ввод [19]: t1 = "ЭркюльПуаро"
           t2 = "АртурГастин"
           key, found_text1, found_text2 = cypher(t1, t2)

           Open text:  ЭркюльПуаро
           Open text in 16:  dd f0 ea fe eb fc cf f3 e0 f0 ee
           Open text:  АртурГастин
           Open text in 16:  c0 f0 f2 f3 f0 c3 e0 f1 f2 e8 ed
           key in 16:  2 17 e6 23 fe 37 9f ab b6 ea 66
           cypher text in 16:  df e7 0c dd 15 cb 50 58 56 1a 88
           cypher text in 16:  c2 e7 14 d0 0e f4 7f 5a 44 02 8b
           cypher text:  ЯзЭЛРХV€
           cypher text:  ВзРфZD‹
```

Figure 2: Результат работы функции, шифрующей данные

Функция, дешифрующая данные

Ввод [37]:

```
def foundtext2(crpher1, crpher2, text):
    print("open text: ", text)
    print("cypher text1: ", crpher1)
    print("cypher text2: ", crpher2)

    crpher1_16 = []
    for i in crpher1:
         crpher1_16.append(i.encode('cp1251').hex())
    print("crpher1 in 16: ", *crpher1_16)

    crpher2_16 = []
    for i in crpher2:
         crpher2_16.append(i.encode('cp1251').hex())
    print("crpher2 in 16: ", *crpher2_16)

    text_16 = []
    for i in text:
         text_16.append(i.encode('cp1251').hex())
    print("text in 16: ", *text_16)

    crpher1_2 = []
    text_16_2 = []
    for i in range(len(text_16)):
        crpher1_2.append("{:02x}".format(int(crpher1_16[i], 16) ^ int(crpher2_16[i], 16)))
        text_16_2.append("{:02x}".format(int(crpher1_2[i], 16) ^ int(text_16[i], 16)))

    print("Open text 2 in 16: ", *text_16_2)
    text_2 = bytearray.fromhex(''.join(text_16_2)).decode('cp1251')
    print("Open text 2: ", text_2)
    return text_2
```

Figure 3: Функция, дешифрующая данные

Результат работы функции, дешифрующей данные

```
Ввод [38]: text2 = foundtext2(found_text1, found_text2, t1)
           print("Open 2 text: ", text2)

open text:  ЭркюльПуаро
cypher text1:  ЯзЭЛРХV€
cypher text2:  ВзРфZD‹
crpher1 in 16:  df e7 0c dd 15 cb 50 58 56 1a 88
crpher2 in 16:  c2 e7 14 d0 0e f4 7f 5a 44 02 8b
text in 16:  dd f0 ea fe eb fc cf f3 e0 f0 ee
Open text 2 in 16:  c0 f0 f2 f3 f0 c3 e0 f1 f2 e8 ed
Open text 2:  АртурГастин
Open 2 text:  АртурГастин
```

Figure 4: Результат работы функции, дешифрующей данные

Результат работы функции, дешифрующей данные

```
Ввод [39]: text2 = foundtext2(found_text1, found_text2, t2)
           print("Open 2 text: ", text2)

open text:  АртурГастин
cypher text1:  ЯзЭЛРХV€
cypher text2:  ВзРфZD‹
crpher1 in 16:  df e7 0c dd 15 cb 50 58 56 1a 88
crpher2 in 16:  c2 e7 14 d0 0e f4 7f 5a 44 02 8b
text in 16:  c0 f0 f2 f3 f0 c3 e0 f1 f2 e8 ed
Open text 2 in 16:  dd f0 ea fe eb fc cf f3 e0 f0 ee
Open text 2:  ЭркюльПуаро
Open 2 text:  ЭркюльПуаро
```

Figure 5: Результат работы функции, дешифрующей данные

Вывод

Вывод

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