Лабораторная работа №7

Филиппова Вероника Сергеевна- студентка группы НКНбд-01-18

11.12.2021

Элементы криптографии.

Однократное гаммирование

Цель выполнения лабораторной работы

Освоить на практике применение режима однократного гаммирования

Задачи выполнения работы

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!».

Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования.

Приложение должно:

1. Определить вид шифротекста при известном ключе и известном открытом тексте.

2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

Написала функцию шифрования, которая определяет вид шифротекста при известном ключе и известном открытом тексте "С Новы Годом, друзья'.

```
Ввод [1]: import numpy as np
```

```
Ввод [29]: def crypto(txt):
    print("Текст: ", txt)
    # Зададим массив для открытого текста в 16й системе счисления
    txt_arr=[]
    for i in txt:
        txt_arr.append(i.encode("cp1251").hex())
    print("\n Открытый текст в 16-м коде: ", *txt_arr)

    # Зададим случайно сгенерированный ключ в 16й системе счисления:
    keyDec = np.random.randint(0, 255, len(txt))
    keyHex = [hex(i)[2:] for i in keyDec]
    print("\nКлюч в 16й системе: ", *keyHex)

    #Зададим зашифрованный текст в 16й системе счисления:
    crypTxt = []
    for i in range(len(txt_arr)):
        crypTxt.append("{:02x}".format(int(txt_arr[i], 16) ^ int(keyHex[i], 16)))
    print("\nЗашифрованный текст в шестндцатеричном представлении: ", *crypTxt)

    res = bytearray.fromhex("".join(crypTxt)).decode("cp1251")
    print("\nЗашифрованный текст: ", res)

    return keyHex, res
```

```
Ввод [50]: #Решение
message="С Новым Годом,друзья!"
criprKey,crypTxt=crypto(message)

Текст:  С Новым Годом,друзья!

 Открытый текст в 16-м коде:  d1 20 cd ee e2 fb ec 20 c3 ee e4 ee ec 2c e4 f0 f3 e7 fc ff 21

Ключ в 16й системе:  76 34 46 2b 9f 30 fa 2e cc 0 43 6f 75 92 d 2f f5 fb 2a 47 52

Зашифрованный текст в шестндцатеричном представлении:  a7 14 8b c5 7d cb 16 0e 0f ee a7 81 99 be e9 df 06 1c d6 b8 73

Зашифрованный текст:  §<E}Л o§Ѓ™sйЯ цёs
```

Результаты выполнения лабораторной работы. Часть 2

Написала функцию дешифровки, которая определяет ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

Ввод [48]:
```
def decrypto(txt, res):
    print("Текст: ", txt)
    print("\nЗашифрованный текст: ", res)

    # Зададим массив из символов открытого текста в 16й системе:
    txtHex = []
    for i in txt:
        txtHex.append(i.encode("cp1251").hex())
    print("\nОткрый текст в 16 системе: ", *txtHex)

    # Массив из символов зашифрованного текста в 16й системек:
    resHex = []
    for i in res:
        resHex.append(i.encode("cp1251").hex())
    print("\n Зашифрованный текст в 16й системе: ", *resHex)

    # Поиск ключа:
    key = [hex(int(i, 16) ^ int(j, 16))[2:] for (i, j) in zip(txtHex, resHex)]
    print("\nКлюч в 16й системе: ", *key)
    return key
```

Ввод [47]:
```
key=decrypto(message, crypTxt)
```

```
Текст:  С Новым Годом,друзья!

Зашифрованный текст:  Шэ        З…ћh4жV}ъу O#
кґд

Открый текст в шестнадцатеричном представлении:  d1 20 cd ee e2 fb ec 20 c3 ee e4 ee ec 2c e4 f0 f3 e7 fc ff 21

Зашифрованный текст в 16й системе:  d8 fd 19 09 c7 85 80 68 34 e6 56 7d fa 79 05 4f 23 0a ea 81 e4

Ключ в 16й системе:  9 dd d4 e7 25 7e 6c 48 f7 8 b2 93 16 55 e1 bf d0 ed 16 7e c5
```

Выводы

Освоила на практике применение режима однократного гаммирования.