Информационная безопасность.

Лабораторная работа №7.

Филиппова Веорника Сергеевна.

Содержание

Цель работы

Освоить на практике применение режима однократного гаммирования

Задание

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.

Выполнение лабораторной работы

Написала функцию шифрования, которая определяет вид шифротекста при известном ключе и известном открытом тексте “С Новы Годом, друзья!” ‘crypto’.

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
```

Рисунок 1

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
```

Рисунок 2

Проверка работы функции шифрования на примере из лабораторной работы

Ввод [49]:
```
# Проверка
message="Штирлиц – Вы Герой!!"
criprKey,crypTxt=crypto(message)
```

```
Текст:  Штирлиц – Вы Герой!!

 Открытый текст в 16-м коде:  d8 f2 e8 f0 eb e8 f6 20 96 20 c2 fb 20 c3 e5 f0 ee e9 21 21

Ключ в 16й системе:  5a 16 f9 1d d0 27 75 a1 5f ca 5e 15 76 62 d 1f be a1 ad 6e

Зашифрованный текст в шестндцатеричном представлении:  82 e4 11 ed 3b cf 83 81 c9 ea 9c ee 56 a1 e8 ef 50 48 8c 4f

Зашифрованный текст:  ,д▯н;ПґЃЙкьоVЎипРНЊО
```

Рисунок 3

Результат функции шифрования.

```
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:  §□‹Е}Л□□□o§ѓ™sйЯ□□Цёs
```

Рисунок 4

Результат функции дешифрования.

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

```
Текст:  С Новым Годом,друзья!

Зашифрованный текст:  Шэ□       З…ЋЋ4жV}ъу□О#
кЃд

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
```

Рисунок 5

#Ответы на вопросы

1. Одократное гаммирование - выполнение операции XOR между элементами гаммы и элементами подлежащего сокрытию текста.
   Даже при раскрытии части последовательности гаммы нельзя получить информацию о всём скрываемом тексте.
2. Недостатки однократного гаммирования: Абсолютная стойкость шифра доказана только для случая, когда однократно используемый ключ, длиной, равной длине исходного сообщения, является фрагментом истинно случайной двоичной последовательности с равномерным законом распределения.
3. Преимущества однократного гаммирования: во-первых, такой способ симметричен, т.е. двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение; во-вторых, шифрование и расшифрование может быть выполнено одной и той же программой. Наконец, Криптоалгоритм не даёт никакой информации об открытом тексте: при известном зашифрованном сообщении C все различные ключевые последовательности K возможны и равновероятны, а значит, возможны и любые сообщения P.
4. Длина открытого текста должна совпадать с длиной ключа, т.к. если ключ короче текста, то операция XOR будет применена не ко всем элементам и конец сообщения будет не закодирован, а если ключ будет длиннее, то появится неоднозначность декодирования.
5. Операция XOR используется в режиме однократного гаммирования. Наложение гаммы по сути представляет собой выполнение побитовой операции сложения по модулю 2, т.е. мы должны сложить каждый элемент гаммы с соответствующим элементом ключа. Данная операция является симметричной, так как прибавление одной и той же величины по модулю 2 восстанавливает исходное значение.
6. Получение шифротекста по открытому тексту и ключу: $C_i = P_i \oplus K_i$

7. Получение ключа по окрытому тексту и шифротексту: $K_i = P_i \oplus C_i$
8. Необходимы и достаточные условия абсолютной стойкости шифра:
   - полная случайность ключа;
   - равенство длин ключа и открытого текста; однократное использование ключа.

Выводы

Освоила на практике применение режима однократного гаммирования.