Информационная безопасность.

Лабораторная работа №8.

Филиппова Веорника Сергеевна.

Содержание

Цель работы

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

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).

Выполнение лабораторной работы

Написала функцию шифрования, которая определяет вид шифротекста при известном ключе и известных открытых текстах “НаВашисходящийот1204” и “ВСеверныйфилиалБанка”.

Ввод [12]:
```
import numpy as np
```

Ввод [13]:
```
def encryption(text1, text2):
    print("Открытый текст №1: ", text1)
    # Массив из символов открытого 1го текста в 16 системе:
    text_array1 = []
    for i in text1:
        text_array1.append(i.encode("cp1251").hex())
    print("\nОткрый  текст в 16 системе: ", *text_array1)

    print("\nОткрытый текст №2: ", text2)
    # Задам массив из символов открытого 2го текста в 16 системе:
    text_array2 = []
    for i in text2:
        text_array2.append(i.encode("cp1251").hex())
    print("\nОткрый текст №2 в 16 системе: ", *text_array2)

    # Задам случайно сгенерированный ключ в 16 системе:
    key_dec = np.random.randint(0, 255, len(text1))
    key_hex = [hex(i)[2:] for i in key_dec]
    print("\nКлюч в 16 системе: ", *key_hex)

    # Задам зашифрованный 1ый текст в 16 системе:
    crypt_text1 = []
    for i in range(len(text_array1)):
        crypt_text1.append("{:02x}".format(int(text_array1[i], 16) ^ int(key_hex[i], 16)))
    print("\nЗашифрованный текст №1 в 16 системе: ", *crypt_text1)

    # Задам зашифрованный 2ой текст в 16 системе:
    crypt_text2 = []
    for i in range(len(text_array2)):
        crypt_text2.append("{:02x}".format(int(text_array2[i], 16) ^ int(key_hex[i], 16)))
    print("\nЗашифрованный текст №2 в 16 системе: ", *crypt_text2)

    # Задам зашифрованный 1ый текст :
    final_text1 = bytearray.fromhex("".join(crypt_text1)).decode("cp1251")
    print("\nЗашифрованный текст №1: ", final_text1)

    # Задам зашифрованный 2ой текст :
    final_text2 = bytearray.fromhex("".join(crypt_text2)).decode("cp1251")
    print("\nЗашифрованный текст №2: ", final_text2)

    return key_hex, final_text1, final_text2
```

Рисунок 1

Написала функцию дешифровки, которая определяет вид одного из текстов, зная вид другого открытого текста и зашифрованный вид обоих текстов

Ввод [14]:
```
def decryption(cr_text1, cr_text2, op_text1):
    print("\nЗашифрованный текст №1 : ", cr_text1)
    print("\nЗашифрованный текст №2: ", cr_text2)
    print("Открытый текст №1: ", op_text1)

    cr_text_hex1 = []
    for i in cr_text1:
        cr_text_hex1.append(i.encode("cp1251").hex())
    print("\nЗашифрованный текст №1 в 16 системе: ", *cr_text_hex1)

    cr_text_hex2 = []
    for i in cr_text2:
        cr_text_hex2.append(i.encode("cp1251").hex())
    print("\nЗашифрованный текст №2 в 16 системе: ", *cr_text_hex2)

    op_text_hex1 = []
    for i in op_text1:
        op_text_hex1.append(i.encode("cp1251").hex())
    print("\nОткрытый текст №1 в 16 системе: ", *op_text_hex1)

    cr1_cr2 = []
    op_text_hex2 = []
    for i in range(len(op_text1)):
        cr1_cr2.append("{:02x}".format(int(cr_text_hex1[i],16) ^ int(cr_text_hex2[i],16)))
        op_text_hex2.append("{:02x}".format(int(cr1_cr2[i], 16) ^ int(op_text_hex1[i], 16)))

    print("Открытый текст №2 в 16 системе: ", *op_text_hex2)
    op_text2 = bytearray.fromhex("".join(op_text_hex2)).decode("cp1251")
    print("Откртый текст№2: ", op_text2)
    return op_text2
```

Рисунок 2

Результат функции шифрования.

```
Ввод [15]: p1 = "НаВашисходящийот1204"
           p2 = "ВСеверныйфилиалБанка"
           key, res1, res2 = encryption(p1, p2)

           Открытый текст №1:  НаВашисходящийот1204

           Открый  текст в 16 системе:  cd e0 c2 e0 f8 e8 f1 f5 ee e4 ff f9 e8 e9 ee f2 31 32 30 34

           Открытый текст №2:  ВСеверныйфилиалБанка

           Открый текст №2 в 16 системе:  c2 d1 e5 e2 e5 f0 ed fb e9 f4 e8 eb e8 e0 eb c1 e0 ed ea e0

           Ключ в 16 системе:  33 aa aa d7 7e b4 c1 27 3a 80 9 ed 28 54 51 df f1 33 9b b1

           Зашифрованный текст №1 в 16 системе:  fe 4a 68 37 86 5c 30 d2 d4 64 f6 14 c0 bd bf 2d c0 01 ab 85

           Зашифрованный текст №2 в 16 системе:  f1 7b 4f 35 9b 44 2c dc d3 74 e1 06 c0 b4 ba 1e 11 de 71 51

           Зашифрованный текст №1:  юJh7†\0TΦdцAS╕-A«…

           Зашифрованный текст №2:  c{O5›D,bYt6Ar€ЮqQ
```

Рисунок 3

Результат функции дешифрования.

```
Ввод [18]: text1 = decryption(res2, res1, p2)
           print("\nОткрытый текст №1: ", text1)

           Зашифрованный текст №1 :  c{O5›D,bYt6Ar€ЮqQ

           Зашифрованный текст №2:  юJh7†\0TΦdцAS╕-A«…
           Открытый текст №1:  ВСеверныйфилиалБанка

           Зашифрованный текст №1 в 16 системе:  f1 7b 4f 35 9b 44 2c dc d3 74 e1 06 c0 b4 ba 1e 11 de 71 51

           Зашифрованный текст №2 в 16 системе:  fe 4a 68 37 86 5c 30 d2 d4 64 f6 14 c0 bd bf 2d c0 01 ab 85

           Открытый текст №1 в 16 системе:  c2 d1 e5 e2 e5 f0 ed fb e9 f4 e8 eb e8 e0 eb c1 e0 ed ea e0
           Открытый текст №2 в 16 системе:  cd e0 c2 e0 f8 e8 f1 f5 ee e4 ff f9 e8 e9 ee f2 31 32 30 34
           Откртый текст№2:  НаВашисходящийот1204

           Открытый текст №1:  НаВашисходящийот1204
```

Рисунок 4

```
Ввод [19]: text2 = decryption(res1, res2, p1)
           print("\nОткрытый текст №2: ", text2)

           Зашифрованный текст №1 :  c{O5›D,bYt6Ar€ЮqQ

           Зашифрованный текст №2:  юJh7†\0TΦdцAS╕-A«…
           Открытый текст №1:  ВСеверныйфилиалБанка

           Зашифрованный текст №1 в 16 системе:  f1 7b 4f 35 9b 44 2c dc d3 74 e1 06 c0 b4 ba 1e 11 de 71 51

           Зашифрованный текст №2 в 16 системе:  fe 4a 68 37 86 5c 30 d2 d4 64 f6 14 c0 bd bf 2d c0 01 ab 85

           Открытый текст №1 в 16 системе:  c2 d1 e5 e2 e5 f0 ed fb e9 f4 e8 eb e8 e0 eb c1 e0 ed ea e0
           Открытый текст №2 в 16 системе:  cd e0 c2 e0 f8 e8 f1 f5 ee e4 ff f9 e8 e9 ee f2 31 32 30 34
           Откртый текст№2:  НаВашисходящийот1204

           Открытый текст №1:  НаВашисходящийот1204

           Зашифрованный текст №1 :  юJh7†\0TΦdцAS╕-A«…

           Зашифрованный текст №2:  c{O5›D,bYt6Ar€ЮqQ
           Открытый текст №1:  НаВашисходящийот1204

           Зашифрованный текст №1 в 16 системе:  fe 4a 68 37 86 5c 30 d2 d4 64 f6 14 c0 bd bf 2d c0 01 ab 85

           Зашифрованный текст №2 в 16 системе:  f1 7b 4f 35 9b 44 2c dc d3 74 e1 06 c0 b4 ba 1e 11 de 71 51

           Открытый текст №1 в 16 системе:  cd e0 c2 e0 f8 e8 f1 f5 ee e4 ff f9 e8 e9 ee f2 31 32 30 34
           Открытый текст №2 в 16 системе:  c2 d1 e5 e2 e5 f0 ed fb e9 f4 e8 eb e8 e0 eb c1 e0 ed ea e0
           Откртый текст№2:  ВСеверныйфилиалБанка

           Открытый текст №2:  ВСеверныйфилиалБанка
```

Рисунок 5

Ответы на вопросы

1. Не зная ключа, для определения одного из текстов, зная другой, необходимо воспользоваться формулой: $C_1 \oplus C_2 \oplus +P_1 = P_1 \oplus P_2 \oplus +P_1 = P_2$, где C_1 и C_2 - шифротексты.
2. При повторном использовании ключа при шифровании текста получим исходное сообщение
3. Режим шифрования однократного гаммирования одним ключом двух открытых текстов реализуется по формуле:

$$C_1 = P_1 \oplus +K$$
$$C_2 = P_2 \oplus +K,$$

4. где C_i - шифротексты, P_i - открытые тексты, K - единый ключ шифровки
5. Недостатки шифрования одним ключом двух открытых текстов:
   - Если одно из сообщений доступно в открытом виде и есть оба шифротекста, можно расшифровать каждое сообщение, не зная ключа.
   - Зная шаблон сообщений, есть возможность определить те символы сообщения P_2, которые находятся на позициях известного шаблона сообщения P_1.
6. Преимущества шифрования одним ключом двух открытых текстов:
   - Данный подход помогает упростить процесс шифрования и дешифровки.
   - При отправке сообщений между двумя компьютерами, удобнее пользоваться одним общим ключом для передаваемых данных

Выводы

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