Лабораторная работа №7

Валиева Найля Разимовна, студентка группы НКНбд-01-18

09.12.2021

Элементы криптографии.

Однократное гаммирование

Прагматика выполнения

- Криптография - наука о методах шифрования. Знание однократного гаммирования и его особенностей является необходимым для дальнейшего знакомства с криптографией.

Цель выполнения лабораторной работы

- Освоить на практике применение режима однократного гаммирования

Задачи выолнения работы

- Написать программу, которая должна определить вид шифротекста при известном ключе и известном открытом тексте
- Также эта программа должна определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста

Результаты выполнения лабораторной работы

- Написала программу, которая определяет вид шифротекста при известном ключе и известном открытом тексте (рис - @fig:001, рис - @fig:002)

In [2]:
```
import numpy as np
```

In [3]:
```
def encryption(text):
    print("Open text", text)

    text_array = []
    for i in text:
        text_array.append(i.encode("cp1251").hex())
    print("\nOpen text of 16th format", *text_array)


    key_dec = np.random.randint(0, 255, len(text))
    key_hex = [hex(i)[2:] for i in key_dec]
    print("\nKey of 16th format", *key_hex)

    crypt_text = []
    for i in range(len(text_array)):
        crypt_text.append("{:2x}".format(int(text_array[i], 16) ^ int(key_hex[i], 16)))
    print("\nEncrypted text of 16th format", *crypt_text)

    final_text = bytearray.fromhex("".join(crypt_text)).decode("cp1251")
    print("\nEncrypted text", final_text)
    return key_hex, final_text
```

Рис. 1: Функция, шифрующая данные

```
In [5]: a = "С Новым годом, друзья!"

        crypt_key, crypt_text = encryption(a)

        Open text С Новым годом, друзья!

        Open text of 16th format d1 20 cd ee e2 fb ec 20 e3 ee e4 ee ec 2c 20 e4 f0 f3 e7 fc ff 21

        Key of 16th format 65 61 f6 40 ca 4b 94 3 f6 3d 24 15 5d 3b 12 f9 6e b9 42 bf 7f fc

        Encrypted text of 16th format b4 41 3b ae 28 b0 78 23 15 d3 c0 fb b1 17 32 1d 9e 4a a5 43 80 dd

        Encrypted text rA;®(°x#▨УАы±▨2▨ЋЈЃСЋЭ
```

Рис. 2: Результат работы функции, шифрующей данные

- Написанная мною программа определяет ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста (рис - @fig:003, рис - @fig:004)

```
In [4]: def decryption(text, final_text):
            print("Open text", text)
            print("\nEncrypted text", final_text)

            text_hex = []
            for i in text:
                text_hex.append(i.encode("cp1251").hex())
            print("\nOpen text of 16th format", *text_hex)

            final_text_hex = []
            for i in final_text:
                final_text_hex.append(i.encode("cp1251").hex())
            print("\nEncrypted text of 16th format", *final_text_hex)

            key = [hex(int(i, 16) ^ int(j, 16))[2:] for (i,j) in zip(text_hex, final_text_hex)]
            print("\nKey we needed with 16th format", *key)
            return key
```

Рис. 3: Функция, дешифрующая данные

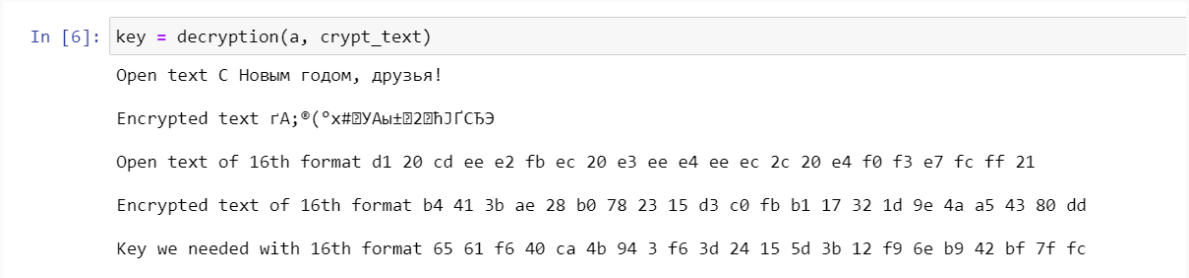

Рис. 4: Результат работы функции, дешифрующей данные

```
In [7]: print("Answer is right!") if crypt_key == key else print("Answer isnt right")
        Answer is right!
```

Рис. 5: Сравнение ключей

Таким образом, я освоила на практике применение режима однократного гаммирования.