Лабораторная работа №8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Рыбалко Элина[1]

2022, 22 October, 2022 Moscow, Russian Federation

[1]RUDN University, Moscow, Russian Federation

Прагматика выполнения лабораторной работы

- Приобретение практических навыков работы с кодированием различных исходных текстов одним ключом.

Цель выполнения лабораторной работы

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

Задачи выполнения лабораторной работы

- Подготовка лабораторного стенда.
- Написание программы.

Результаты выполнения лабораторной работы

```
[1]  import string
     import random

     def f_hkey(text):
       return ' '.join(hex(ord(i))[2:] for i in text)

     def f_key(size):
       return ''.join(random.choice(string.ascii_letters+string.digits) for _ in range(size))

     def encryption(text1, text2):
       txt1 = [ord(i) for i in text1]
       txt2 = [ord(i) for i in text2]
       return ''.join(chr(a^b) for a,b in zip (txt1, txt2))
```

Рис. 1: Фнкции программы

Результаты выполнения лабораторной работы

```
[5] P1 = 'НаВашисходящийот1204'
    P2 = 'ВСеверныйфилиалБанка'

    key = f_key(len(P1))
    print("Используемый ключ: ", key)

    hex_key = f_hkey(key)
    print("Ключ в шестнадцатиричносм виде: ", hex_key)

    C1 = encryption(P1,key)
    C2 = encryption(P2,key)
    print("Шифротекст: ", C1)
    print("Шифротекст: ", C2)

    decrypt = encryption(C1, C2)
    D1 = encryption(decrypt,P1)
    D2 = encryption(decrypt,P2)
    print("Расшифрованное сообщение ", D1)
    print("Расшифрованное сообщение ", D2)
```

```
Используемый ключ:  rBo7HxDlGyOs1zbI7t4e
Ключ в шестнадцатиричносм виде:  72 42 6f 37 48 78 44 6c 47 79 4f 73 31 7a 62 49 37 74 34 65
Шифротекст:  ѮѲѼЇЀpЅЩѩэЀкЉуќћ–F┘Q
Шифротекст:  ѠѢњЅѼиѩЧѾнѶшЉъљjЇщЎs
Расшифрованное сообщение  ВСеверныйфилиалБанка
Расшифрованное сообщение  НаВашисходящийот1204
```

Рис. 2: Основная программа

Вывод

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