Лабораторная работа №5

“Низамова Альфия Айдаровна. НФИбд-01-20”[1]

23 сентября, 2023, Москва, Россия

[1]Российский Университет Дружбы Народов

Цель работы

Цель работы:

Освоить на практике применение режима однократного гаммирования

Задание

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. 3.

Ход лабораторной работы.

Импортируем необходимые библиотеки (рис.1)

```
import numpy as np
import pandas as pd
import sys
```

Рис. 1: Рис. 1

2

Мы написали функцию *func( )*, определяющую вид шифротекста при известном ключе и известном открытом тексте (рис.2)

```
def func(a):
    text = []

    for i in a:
        text.append(i.encode("cp1251").hex())

    k = np.random.randint(0, 255, len(a))
    key = [hex(i)[2:] for i in k]
    newkey = []
    for i in key:
        newkey.append(i.encode("cp1251").hex().upper())

    b = []
    for i in range(len(text)):
        b.append("{:02x}".format(int(key[i], 16)^int(text[i],16)))
```

Мы написали функцию *findk( )*, определяющую ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста (рис.3)

```
def findk(a, fintext):
    newtext = []
    for i in a:
        newtext.append(i.encode("cp1251").hex())

    ftext = []
    for i in fintext:
        ftext.append(i.encode("cp1251").hex())
    key = [hex(int(i, 16) ^ int(j, 16))[2:] for
           (i, j) in zip(newtext, ftext)]
    return newtext, ftext, key
```

Вывод программы (рис.4-5)

```
Open text:
 С Новым Годом, друзья!

Open text in 16:
 ['d1', '20', 'cd', 'ee', 'e2', 'fb', 'ec', '20', 'c3', 'ee', 'e4',
 'ee', 'ec', '2c', '20', 'e4', 'f0', 'f3', 'e7', 'fc', 'ff', '21']

Key in 16:
 6e 7b 4 a 69 84 1e c ec 63 e0 7c 98 ad 4a c4 57 89 12 17 27 68

Cipher text in 16:
 bf 5b c9 e4 8b 7f f2 2c 2f 8d 04 92 74 81 6a 20 a7 7a f5 eb d8 49

Cipher text:
 ї[Йд‹0т,/Ќ0’tЃj §zхлШI
```

Вывод программы (рис.4-5)

```
Open text:
 С Новым Годом, друзья!

Cypher text:
 ï[Йд‹Ø т,/Ќ Ø’tЃj §zхлШI

Open text in 16:
 d1 20 cd ee e2 fb ec 20 c3 ee e4 ee ec 2c 20 e4 f0 f3 e7 fc ff 21

Cypher text in 16:
 bf 5b c9 e4 8b 7f f2 2c 2f 8d 04 92 74 81 6a 20 a7 7a f5 eb d8 49

Found key in 16:
 6e 7b 4 a 69 84 1e c ec 63 e0 7c 98 ad 4a c4 57 89 12 17 27 68
```

Рис. 5: Рис. 5

Выводы

Выводы

Мы освоили на практике применение режима однократного гаммирования