Отчет по лабораторной работе №7

Лабораторная работа №7: Элементы криптографии. Однократное гаммирование.

Ширяев Кирилл Владимирович, НФИбд-03-18

Содержание

List of Figures

1 Цель работы

Освоить на практике применение режима однократного гаммирования.

2 Выполнение работы

2.1 Алфавит

Задал алфавит из русских букв и алфавит из соответствующих им шестнадцетиричных чисел.

Figure 2.1: Алфавиты

2.2 Сообщение

Ввел сообщение.

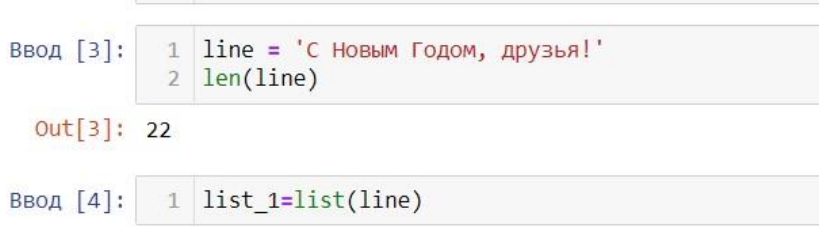

Figure 2.2: Сообщение

2.3 Ключ

Создал рандомный ключ.

Ввод [6]:

```
from random import randint

key=[]
for i in range(len(line)):
    x=randint (0,255)
    x=hex(x)
    key.append(x)
    print(x.replace("0x",""))
```

```
e7
34
46
83
1
f
a9
22
b9
16
e8
5b
48
a0
48
f1
5a
25
8e
26
5c
de
```

Figure 2.3: Создание ключа

2.4 Перевод сообщения

Перевел заданное сообщение в шестнадцетиричные числа.

```python
list_16=[]
def into_list_16(list_1, alphabet, alphabet_16, list_16):
    for i in range(len(list_1)):
        for j in range(len(alphabet)):
            if list_1[i]==alphabet[j]:
                for k in range (len(alphabet_16)):
                    if j==k:
                        list_16.append(alphabet_16[k])
                        print(alphabet_16[k].replace("0x",""))
into_list_16(list_1, alph, alph_16, list_16)
```

```
d1
20
cd
ee
e2
fb
ec
20
c3
ee
e4
ee
ec
22
20
e4
f0
f3
e7
fc
ff
21
```

Figure 2.4: Шестнадцетиричная система

2.5 Шифрование

Определил вид шифротекста при известном ключе и известном открытом тексте.

Ввод [8]:

```
cipher=[]
def into_cipher(list_16, key, cipher):
    for i in range(len(list_16)):
        for j in range(len(key)):
            if i==j:
                x=hex(int(list_16[i],16) ^ int(key[j],16))
                cipher.append(x)
                print(x.replace("0x",""))
into_cipher(list_16, key, cipher)
```

```
36
14
8b
6d
e3
f4
45
2
7a
f8
c
b5
a4
82
68
15
aa
d6
69
da
a3
ff
```

Figure 2.5: Шифрование

2.6 Расшифровка

Один из вариантов расшифровки полученного шифра.

```
line_1 = 'С Новым Мячом, друзья!'
len(line_1)
```

```
22
```

```
list_2=list(line_1)
list_2
```

Figure 2.6: Расшифровка

2.7 Перевод сообщения

Перевел один из возможных вариантов расшифровки сообщения в шестнадцетиричные числа.

```
list_16_2=[]
into_list_16(list_2, alph, alph_16, list_16_2)
```

```
d1
20
cd
ee
e2
fb
ec
20
cc
ff
f7
ee
ec
22
20
e4
f0
f3
e7
fc
ff
21
```

Figure 2.7: Шестнадцетиричная система

2.8 Ключ

Определил ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

Ввод [12]:

```
key_2=[]
def into_key(cipher, list_16, key):
    for i in range(len(cipher)):
        for j in range(len(list_16)):
            if i==j:
                x=hex(int(cipher[i],16) ^ int(list_16[j],16))
                key_2.append(x)
                print(x.replace("0x",""))
into_key(cipher, list_16_2, key_2)
```

```
e7
34
46
83
1
f
a9
22
b6
7
fb
5b
48
a0
48
f1
5a
25
8e
26
5c
de
```

Figure 2.8: Возможный ключ

3 Выводы

Я освоил на практике применение режима однократного гаммирования.