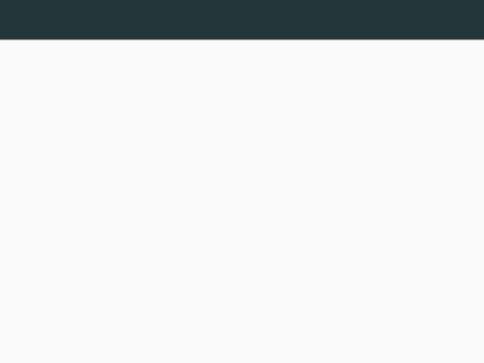
Лабораторная работа №7: Элементы криптографии. Однократное гаммирование.

дисциплина: Информационная безопасность

Цель работы



Освоить на практике применение режима однократного гаммирования.

Выполнение работы

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

Figure 1: Алфавиты

Ввел сообщение.

```
Ввод [3]: 1 line = 'C Новым Годом, друзья!'
2 len(line)

Out[3]: 22

Ввод [4]: 1 list_1=list(line)
```

Figure 2: Сообщение

Создал рандомный ключ.

```
Ввод [6]: 1 from random import randint
             3 key=[]
             4 for i in range(len(line)):

x=randint (0,255)
             6
                     x=hex(x)
                     key.append(x)
print(x.replace("0x",""))
            e7
            34
            46
            83
            a9
            22
            b9
            16
            e8
            5b
            48
            a0
            48
            f1
            5a
            25
            8e
            26
            5c
            de
```

Figure 3: Создание ключа

Перевел заданное сообщение в шестнадцетиричные числа.

```
1 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
fh
ec
20
c3
ee
64
ee
ec
22
20
e4
fa
f3
e7
fc
ff
21
```

Figure 4: Шестнадцетиричная система

Зашифровал сообщение с помощью ключа.

```
Ввод [8]:
           1 cipher=[]
           2 def into_cipher(list_16, key, cipher):
                  for i in range(len(list_16)):
                      for j in range(len(key)):
           4
                          if i==j:
                              x=hex(int(list_16[i],16) ^ int(key[j],16))
                              cipher.append(x)
                              print(x.replace("0x",""))
           9 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 5: Шифрование

Один из вариантов расшифровки полученного шифра.

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

list 2=list(line 1)
```

2 list 2

Figure 6: Расшифровка

Перевел один из возможных вариантов расшифровки сообщения в шестнадцетиричные числа.

```
1 list_16_2=[]
2 into_list_16(list_2, alph, alph_16, list_16_2)
d1
20
cd
e2
fb
ec
20
CC
ff
f7
ee
ec
22
20
e4
f0
f3
e7
fc
ff
21
```

Figure 7: Шестнадцетиричная система

Получил ключ, при использовании которого могло быть получено данное сообщение.

```
Ввод [12]: 1 key_2=[]
             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",""))
            9 into_key(cipher, list_16_2, key_2)
           e7
           34
           46
           83
           a9
           22
           b6
           7
           fb
           5b
           48
           ae
           48
           f1
           Sa
           25
           8e
           26
           5c
           de
```

Figure 8: Возможный ключ

Выводы

Выводы

Я освоил на практике применение режима однократного гаммирования.