

Лабораторная работа № 7

Дугаева Светлана Анатольевна, НФИбд-01-18

Освоить на практике применение режима однократного гаммирования.

Выполнение лабораторной работы

```
1 import numpy as np
2 import sys
3 import operator as op
```

```
1 hi = "С Новым Годом, друзья!"
```

```
1 def crypto (message):
2     tmp1 = []
3     for i in message:
4         tmp1.append(i.encode("cp1251").hex())
5     print("Открытое сообщение в 16ричной системе:", tmp1)
6     d = np.random.randint(0, 255, len(message))
7     key = [hex(i)[2:] for i in d]
8     print("Ключ в 16ричной системе:", key)
9     key_d = bytearray.fromhex("".join(key)).decode("cp1251")
10    print("Текст ключа:", key_d)
11    xor = []
12    for i in range(len(tmp1)):
13        xor.append("{}:02x".format(int(key[i],16) ^ int(tmp1[i], 16)))
14    print("Шифротекст в 16ричной системе:", xor)
15    code = bytearray.fromhex("".join(xor)).decode("cp1251")
16    print("Текст шифра:", code)
17    return code
```

Рис. 1: Функция кодирования

Выполнение лабораторной работы

```
1 code = crypto(hi)
```

Открытое сообщение в 16ричной системе: ['d1', '20', 'cd', 'ee', 'e2', 'fb', 'ec', '20', 'c3', 'ee', 'e4', 'ee', 'ec', '2c', '20', 'e4', 'f0', 'f3', 'e7', 'fc', 'ff', '21']

Ключ в 16ричной системе: ['c2', 'c', '1', '7c', '7', '8d', '9', 'e1', '47', '3d', 'c4', 'a', '1', '1d', 'f7', '3e', '7e', '7f', '2d', 'b5', '84', 'd0']

Текст ключа: ВБ|хЩБГ=ДУ@ч>~@-м,,Р

Шифротекст в 16ричной системе: ['13', '2c', 'cc', '92', 'e5', '76', 'e5', 'c1', '84', 'd3', '20', 'e4', 'ed', '31', 'd7', 'da', '8e', '8c', 'ca', '49', '7b', 'f1']

Текст шифра: @,M'eveB,,У дн1ЧЪЬЬКІ{с

Рис. 2: Вызов функции crypto

```
1 def decoder (message, code):
2     tmp1 = []
3     for i in message:
4         tmp1.append(i.encode("cp1251").hex())
5     tmp2 = []
6     for i in code:
7         tmp2.append(i.encode("cp1251").hex())
8     xor = [hex(int(k,16)^int(j,16))[2:] for (k,j) in zip(tmp1, tmp2)]
9     print("Нашли ключ в 16ричной системе:", xor)
10    xor_dec = bytearray.fromhex("".join(xor)).decode("cp1251")
11    print("Текст ключа:", xor_dec)
```

Рис. 3: Функция для получения ключа

Выполнение лабораторной работы

```
1 decoder(hi, code)
```

Нашли ключ в 16ричной системе: ['c2', 'c', '1', '7c', '7', '8d', '9', 'e1', '47', '3d', 'c4', 'a', '1', '1d', 'f7', '3e', '7e', '7f', '2d', 'b5', '84', 'd0']
Текст ключа: ВБ|хЩбG=ДУѠч>~Ѡ-м„Р

Рис. 4: Вызов функции decoder

Освоила на практике применение режима однократного гаммирования. Закодировала сообщение с помощью создания случайного ключа и нашла ключ исходя из открытого текста и шифротекста.