

# Лабораторная работа № 8

---

Дугаева Светлана Анатольевна, НФИбд-01-18

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

# Выполнение лабораторной работы

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

```
1 hi1 = "С Новым Годом, друзья!"
```

```
1 hi2 = "До НГ осталось 15 дней"
```

```
1 def crypto (mes1, mes2):
2     tmp1 = []
3     for i in mes1:
4         tmp1.append(i.encode("cp1251").hex())
5     print("Открытое сообщение 1 в 16ричной системе:", tmp1)
6     tmp2 = []
7     for i in mes2:
8         tmp2.append(i.encode("cp1251").hex())
9     print("Открытое сообщение 2 в 16ричной системе:", tmp2)
10    d = np.random.randint(0, 255, len(mes1))
11    key = [hex(i)[2:] for i in d]
12    print("Ключ в 16ричной системе:", key)
13    xor1 = []
14    for i in range(len(tmp1)):
15        xor1.append("{:02x}".format(int(key[i],16) ^ int(tmp1[i], 16)))
16    print("Шифротекст 1 в 16ричной системе:", xor1)
17    code1 = bytearray.fromhex("".join(xor1)).decode("cp1251")
18    print("Текст шифра 1:", code1)
19    xor2 = []
20    for i in range(len(tmp2)):
21        xor2.append("{:02x}".format(int(key[i],16) ^ int(tmp2[i], 16)))
22    print("Шифротекст 2 в 16ричной системе:", xor2)
23    code2 = bytearray.fromhex("".join(xor2)).decode("cp1251")
24    print("Текст шифра 2:", code2)
25
26    return code1, code2
```

Рис. 1: Функция кодирования

```
1 code1, code2 = crypto(hi1, hi2)
```

Открытое сообщение 1 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']

Открытое сообщение 2 в 16ричной системе: ['c4', 'ee', '20', 'cd', 'c3', '20', 'ee', 'f1', 'f2', 'e0', 'eb', 'ee', 'f1', 'fc', '20', '31', '35', '20', 'e4', 'ed', 'e5', 'e9']

Ключ в 16ричной системе: ['bf', 'c5', '92', 'bb', 'd6', '46', 'fc', '9a', '5c', 'ee', 'ec', 'bf', '47', '54', 'b2', 'aa', 'ba', '95', '0', '7a', 'c', 'ae']

Шифротекст 1 в 16ричной системе: ['6e', 'e5', '5f', '55', '34', 'bd', '10', 'ba', '9f', '00', '08', '51', 'ab', '78', '92', '4e', '4a', '66', 'e7', '86', 'f3', '8f']

Текст шифра 1: ne\_U4SЮeuQ«x'NJfatyU

Шифротекст 2 в 16ричной системе: ['7b', '2b', 'b2', '76', '15', '66', '12', '6b', 'ae', '0e', '07', '51', 'b6', 'a8', '92', '9b', '8f', 'b5', 'e4', '97', 'e9', '47']

Текст шифра 2: {+Iv0f0k@00Q0É'>Uд-йG

Рис. 2: Вызов функции crypto

# Выполнение лабораторной работы

```
1 def decoder (code1, code2, mes1):
2     tmp1 = []
3     for i in code1:
4         tmp1.append(i.encode("cp1251").hex())
5     print("Шифротекст 1 в 16ричной системе:", tmp1)
6     tmp2 = []
7     for i in code2:
8         tmp2.append(i.encode("cp1251").hex())
9     print("Шифротекст 2 в 16ричной системе:", tmp2)
10    tmp3 = []
11    for i in mes1:
12        tmp3.append(i.encode("cp1251").hex())
13    print("Открытое сообщение 1 в 16ричной системе:", tmp3)
14    xor = []
15    result = []
16    for i in range(len(tmp2)):
17        xor.append("{:02x}".format(int(tmp1[i],16) ^ int(tmp2[i], 16)))
18        result.append("{:02x}".format(int(xor[i],16) ^ int(tmp3[i], 16)))
19    print("Открытое сообщение 2 в 16ричной системе:", result)
20    mes2 = bytearray.fromhex("".join(result)).decode("cp1251")
21    print("Открытое сообщение 2:", mes2)
```

Рис. 3: Функция для получения второго открытого сообщения

```
1 decoder(code1, code2, hi1)
```

Шифротекст 1 в 16ричной системе: ['6e', 'e5', '5f', '55', '34', 'bd', '10', 'ba', '9f', '00', '08', '51', 'ab', '78', '92', '4e', '4a', '66', 'e7', '86', 'f3', '8f']

Шифротекст 2 в 16ричной системе: ['7b', '2b', 'b2', '76', '15', '66', '12', '6b', 'ae', '0e', '07', '51', 'b6', 'a8', '92', '9b', '8f', 'b5', 'e4', '97', 'e9', '47']

Открытое сообщение 1 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']

Открытое сообщение 2 в 16ричной системе: ['c4', 'ee', '20', 'cd', 'c3', '20', 'ee', 'f1', 'f2', 'e0', 'eb', 'ee', 'f1', 'fc', '20', '31', '35', '20', 'e4', 'ed', 'e5', 'e9']

Открытое сообщение 2: До НГ осталось 15 дней

Рис. 4: Вызов функции decoder

Освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных тестов одним ключом. Закодировала два сообщения с помощью создания случайного ключа и нашла второе открытое сообщение исходя из открытого текста одного сообщения и двух зашифрованных.