

# Лабораторная работа №7

Василий О. Худицкий

РУДН, 22 октября 2022, Москва, Россия

# Цель лабораторной работы

- Освоить на практике применение режима однократного гаммирования.

# 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.

# Выполнение лабораторной работы

# Определение вида шифротекста при известном ключе и известном открытом тексте

```
def encrypt(text):
    print("Открытый текст: ", text)

    new_text = []
    for i in text:
        new_text.append(i.encode("cp1251").hex())
    print("\nОткрытый текст в 16-ой системе: ", new_text)

    r = np.random.randint(0, 255, len(text))
    key = [hex(i)[2:] for i in r]
    print("\nКлюч в 16-ой системе: ", key)

    xor_text = []
    for i in range(len(new_text)):
        xor_text.append("{:02x}".format(int(key[i], 16) ^ int(new_text[i], 16)))
    print("\nШифротекст в 16-ой системе: ", xor_text)

    en_text = bytearray.fromhex("".join(xor_text)).decode("cp1251")
    print("\nШифротекст: ", en_text)

    return key, en_text
```

# Результат вызова первой функции

Открытый текст: С Новым Годом, друзья!

Открытый текст в 16-ой 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 16-ой системе: ['15', '74', '5c', 'b3', '91', 'aa', '82', '10', '79', '64', 'ba', 'c6', '7', 'ce', '96', 'de', '2c', '5e', 'f', '6b', '9b', 'eb']

Шифротекст в 16-ой системе: ['c4', '54', '91', '5d', '73', '51', '6e', '30', 'ba', '8a', '5e', '28', 'eb', 'e2', 'b6', '3a', 'dc', 'ad', 'e8', '97', '64', 'ca']

Шифротекст: ДТ' ]sQn0€Л^(лвЉ:би—dK

**Рис.1 Определение вида шифротекста при известном ключе и известном открытом тексте**

# Определение вида ключа при известном тексте и шифротексте

```
def find_key(text, en_text):  
    print("Открытый текст: ", text)  
    print("\nШифротекст: ", en_text)  
  
    new_text = []  
    for i in text:  
        new_text.append(i.encode("cp1251").hex())  
    print("\nОткрытый текст в 16-ой системе: ", new_text)  
  
    tmp_text = []  
    for i in en_text:  
        tmp_text.append(i.encode("cp1251").hex())  
    print("\nШифротекст текст в 16-ой системе: ", tmp_text)  
  
    key = [hex(int(k,16)^int(t,16))[2:] for (k,t) in zip(new_text, tmp_text)]  
    print("\nНайденный ключ в 16-ой системе: ", key)  
    return key
```

# Результат вызова второй функции

Открытый текст: С Новым Годом, друзья!

Шифротекст: ДТ' ]sQn0€Л^(лвЉ:Ыи-dK

Открытый текст в 16-ой системе: ['d1', '20', 'cd', 'ee', 'e2', 'fb', 'ec', '20', 'c3', 'ee', 'e4', 'ee', 'ec', '2c', '20', 'e4', 'f0', 'f3', 'e7', 'fc', 'ff', '21']

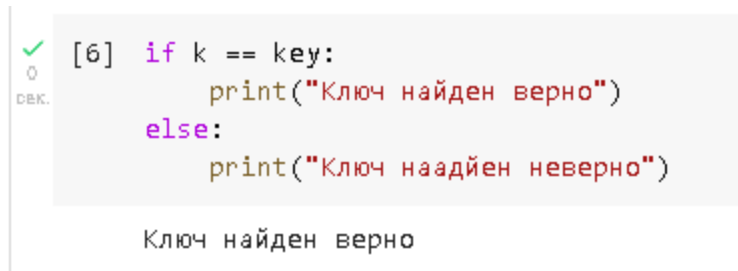
Шифротекст текст в 16-ой системе: ['c4', '54', '91', '5d', '73', '51', '6e', '30', 'ba', '8a', '5e', '28', 'eb', 'e2', 'b6', '3a', 'dc', 'ad', 'e8', '97', '64', 'ca']

Найденный ключ в 16-ой системе: ['15', '74', '5c', 'b3', '91', 'aa', '82', '10', '79', '64', 'ba', 'c6', '7', 'ce', '96', 'de', '2c', '5e', 'f', '6b', '9b', 'eb']

Рис.2 Определение вида ключа



# Проверка правильности нахождения ключа



```
[6] if k == key:
    print("Ключ найден верно")
else:
    print("Ключ наадйен неверно")
```

Ключ найден верно

Рис.3 Проверка правильности нахождения ключа

# Выводы

В ходе выполнения данной лабораторной работы я освоил на практике применение режима однократного гаммирования.