### Лабораторная работа №7

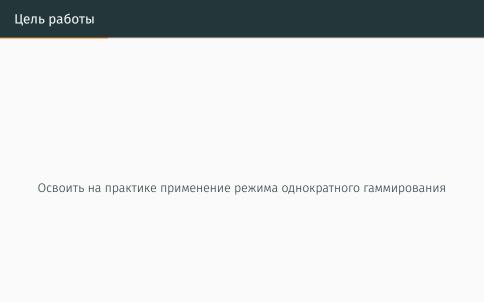
Кондрашина Мария Сергеевна<sup>1</sup>

18.10.2022, Moscow

<sup>1</sup>RUDN University, Moscow, Russian Federation

Элементы криптографии.

Однократное гаммирование



## Теоретические сведения

### Теоретические сведения

Гаммирование представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Иными словами, наложение гаммы — это сложение её элементов с элементами открытого (закрытого) текста по некоторому фиксированному модулю, значение которого представляет собой известную часть алгоритма шифрования.

Выполнение лабораторной работы

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно:

- Определить вид шифротекста при известном ключе и известном открытом тексте.
- Оределить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста,представляющий собой один из возможных вариантов прочтения открытого текста.

# Работа с открытым текстом. Перевод в шестнадцатеричное представление

```
1) Определить вид шифротекста при известном ключе и известном открытом тексте.

Ввод [102]: 
my_str = "C Новым Годом, друзья!"
print("Открытый текст: ", my_str)

Открытый текст: С Новым Годом, друзья!

Ввод [103]: 
def to_16(strM):
    stn_16 = []
    for i in strM:
    stn_16 = []
    for i in
```

### Создание ключа и шифрование текста

### Определение ключа по отрытому и зашифрованному тексту

```
2) Оределить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из
            возможных вариантов прочтения открытого текста
Ввод [109]: print("Открытый текст: ", my str)
            print("Зашифрованный текст: ", new_text)
            Открытый текст: С Новым Годом, друзья!
            Зашифрованный текст: ['E', '"', '>', 'A', 'N", 'P', '9', ',,', 'P', '\x02', 'X', 'p', 'Й', ':', 'ē', '{', 'ſ', '-', 'ħ', 'A',
            '3', 'y']
Ввод [110]: def find_key(str_16, c_text_16):
                kev new = []
                for i, j in zip(str 16, c text 16):
                    key new.append(('{:02x}'.format(int(i,16) ^ int(j, 16))).upper())
                return key new
Ввод [111]: print("Найденный ключ: ", find key(to 16(my str), to 16(new text)))
            Найденный ключ: ['94', '83', 'F3', '2E', '5B', '2B', 'D5', 'A4', '93', 'EC', '31', '1E', '25', '16', '98', '9F', '55', '44',
            '79', '3C', '38', 'D2']
Ввод [115]: if (find key(to 16(my str), to 16(new text)) -- key):
                print("Ключ совпал с ранее созданным")
            else:
                print("Ключи различны")
            Ключ совпал с ранее созданным
```

### Результат

- · Выполнила лабораторную работу №7.
- Освоила на практике применение режима однократного гаммирования

### Список литературы

1. Методические материалы курса. "Информационная безопасность компьютерных сетей" Кулябов Д. С., Королькова А. В., Геворкян М. Н.