## Front matter

lang: ru-RU title: Lab08 author: | Anna D. Zaytseva\inst{1,3} institute: | \inst{1}RUDN University, Moscow, Russian Federation date: NEC--2024, 26 October, Moscow

## **Formatting**

toc: false slide\_level: 2 theme: metropolis header-includes:

- \metroset{progressbar=frametitle,sectionpage=progressbar,numbering=fraction}
- '\makeatletter'
- '\beamer@ignorenonframefalse'
- 'makeatother' aspectratio: 43 section-titles: true

# Цель работы

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

# Выполнение этапа индивидуального проекта

## Step 1

Я выполнила лабораторную работа на языке программирования Python, используя функции, написанные в своей предыдущей работе.

Сперва я использовала функцию для генерации случайного ключа, а потом зашифровала с его помощью два разных текста (Рис. [-@fig:001]):

```
√ import random

   import string

√ def hex_key_generator(text):
       key = ''
       for i in range(len(text)):
       key += random.choice(string.ascii_letters + string.digits) # generation of a number for each character in the te
       return key

√def encrypt_decrypt(text, key):
       new_text = ''
       for i in range(len(text)):
           new text += chr(ord(text[i]) ^ ord(key[i % len(key)]))
       return new text
   t1 = 'C Новым Годом, друзья!'
   key = hex_key_generator(t1)
   encrypt_t1 = encrypt_decrypt(t1, key)
   decrypt_t1 = encrypt_decrypt(encrypt_t1, key)
   t2 = 'Сойти с ума давно пора'
   encrypt_t2 = encrypt_decrypt(t2, key)
   decrypt_t2 = encrypt_decrypt(encrypt_t2, key)
{ #fig:001 width=70% }
```

#### Step 2

Расшифровала оба текста сначала с помощью одного ключа, затем предположила, что мне неизвестен ключ, но извествен один из текстов, и уже расшифровала второй, зная шифротексты и первый текст (Рис. [-@fig:002]):

```
print('Открытый текст: ', t1, "\nKлюч: ", key, '\nШифратекст: ', encrypt_t1, '\nИсходный текст: ', decrypt_t1)
      print('Открытый текст: ', t2, "\nKлюч: ", key, '\nШифратекст: ', encrypt_t2, '\nИсходный текст: ', decrypt_t2)
      print()
      p = encrypt decrypt(encrypt t2, encrypt t1) #C1^C2
      print('Расшифровать второй текст, зная первый: ', encrypt_decrypt(t1, p)) print('Расшифровать первый текст, зная второй: ', encrypt_decrypt(t2, p))
  Открытый текст: С Новым Годом, друзья!
  Ключ: vstdU1qZExQ6gF1HpCLoGq
  Шифротекст: ӵЅѩњѧѺэziцѥJħj@ѼаÈфУJР
  Исходный текст: С Новым Годом, друзья!
  Открытый текст: Сойти с ума давно пора
  Ключ: vstdU1qZExQ6gF1HpCLoGq
  Шифротекст: їээЦж@аzІфw@ŕѶЃvюсөёЇс
  Исходный текст: Сойти с ума давно пора
  Расшифровать второй текст, зная первый: Сойти с ума давно пора
  Расшифровать первый текст, зная второй: С Новым Годом, друзья!
#fig:002 width=70% }
```

## Вывод

Приобрела навыки применения режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# Библиография

- https://www.youtube.com/watch?v=tAjBULW\_OjQ
   https://bugtraq.ru/library/books/crypto/chapter7/
   https://xakep.ru/2019/07/18/crypto-xor/

#### {.standout}

Спасибо за внимание!