

# Лабораторная работа №8

Элементы криптографии. Шифрование различных исходных текстов одним ключом

---

Кувшинова Ксения Олеговна<sup>1</sup>

21.10.2022, Moscow

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

Целью данной лабораторной работы является освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

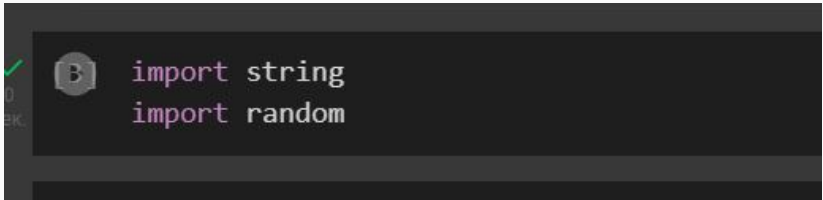
Режим шифрования однократного гаммирования одним ключом двух видов открытого текста реализуется в соответствии со схемой: (fig. 1)

$$\begin{aligned}C_1 &= P_1 \oplus K, \\C_2 &= P_2 \oplus K.\end{aligned}$$

**Figure 1:** Схема однократного гаммирования одним ключом двух видов открытого текста

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе ; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

Импортируем необходимые для работы библиотеки (fig. 2)

A screenshot of a code editor with a dark background. On the left side, there is a vertical toolbar with a green checkmark icon and a 'Век.' label. The main area of the editor displays two lines of Python code: 'import string' and 'import random'. The code is written in a light purple/pink color. A small icon with the letter 'B' is visible to the left of the first line of code.

```
import string
import random
```

Figure 2: Импорт библиотек

# Выполнение лабораторной работы

Напишем функции формирования ключа, перевода данных в 16 систему и шифрования текста. (fig. 3)

```
[4] #формирование ключа
def key(size):
    #генерируем ключ
    key1 = ''.join(random.choice(string.ascii_letters+string.digits) for _ in range(size))
    print("Key: ", key1)
    #переводим в 16 СИ
    key2 = coding(key1)
    print("Key in 16: ", key2)
    return key2

#функция перевода в 16 СИ
def coding(smth):
    smth1 = ' '.join(hex(ord(i))[2:] for i in smth)
    return smth1

#шифрование
def crypt(text, key):
    t = [ord(i) for i in text]
    k = [ord(j) for j in key]
    sixt_t = ''.join(chr(i^j) for i,j in zip(t,k))
    return sixt_t
```

## Выполнение лабораторной работы

Зашифруем и дешифруем тексты P1 и P2 в режиме однократного гаммирования. (fig. 4)

```
P1 = "I'm so lonely"
P2 = "Broken angels"

key = key(len(P1))
|
cp1 = crypt(P1, key)
cp2 = crypt(P2, key)
print("Зашифрованный текст1: ", cp1)
print("Зашифрованный текст2: ", cp2)

decrypt = crypt(cp1, cp2)
finp1 = crypt(decrypt, P2)
finp2 = crypt(decrypt, P1)

print("Расшифрованный текст1: ", finp1)
print("Расшифрованный текст1: ", finp2)
```

Key: WFR1TNs3Q0ffff

Key in 16: 57 46 52 31 54 4e 73 33 51 30 66 66 66

Зашифрованный текст1: |@M?E0B^0ITLL

В ходе выполнения лабораторной работы мы освоили на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.



1. Кулябов Д. С., Королькова А. В., Геворкян М. Н. Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом [Текст] / Кулябов Д. С., Королькова А. В., Геворкян М. Н. - Москва: - 3 с. [^1]: Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом.