

# **Лабораторная работа № 8**

**Элементы криптографии. Шифрование (кодирование) различных  
исходных текстов одним ключом**

Байрамгельдыев Довлетмурат

# Содержание

Цель работы	4
Задание	5
Теоретическое введение	6
Выполнение лабораторной работы	7
Выводы	9
Список литературы	10

## Список иллюстраций

1	Функция шифрования . . . . .	7
2	Данные из условия . . . . .	7
3	Шифрование текста . . . . .	7
4	Расшифровка текста . . . . .	8
5	Результат . . . . .	8

## Цель работы

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

## Задание

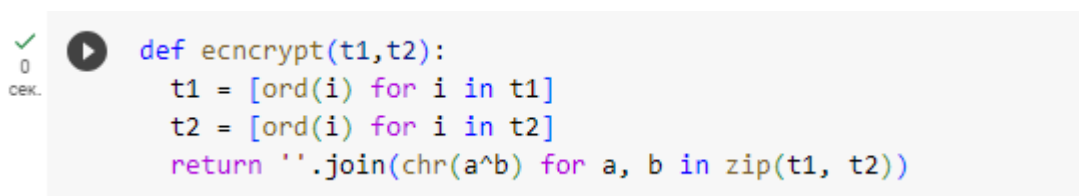
Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочесть оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты  $P_1$  и  $P_2$  в режиме однократного гаммирования. Приложение должно определить вид шифротекстов  $C_1$  и  $C_2$  обоих текстов  $P_1$  и  $P_2$  при известном ключе ; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочесть оба текста, не зная ключа и не стремясь его определить.

# Теоретическое введение

- Шифрование – это технология кодирования и декодирования данных. Зашифрованные данные – это результат применения алгоритма для кодирования данных с целью сделать их недоступными для чтения. Данные могут быть декодированы в исходную форму только путем применения специального ключа. [1].
- Гаммирование — это наложение (или снятие при расшифровке сообщений) на открытое (или зашифрованное) сообщение так называемой криптографической гаммы. Криптографическая гамма — это последовательность элементов данных, которая вырабатывается с помощью определенного алгоритма. [2].

# Выполнение лабораторной работы

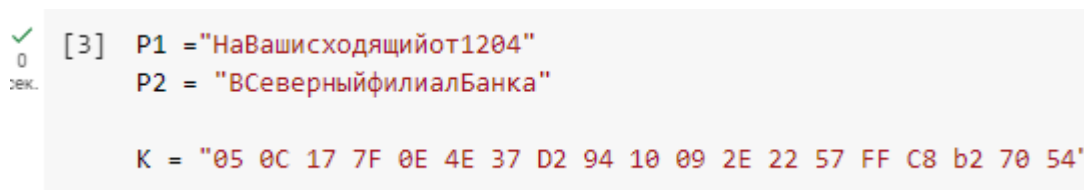
1. Создаем функцию шифрования (fig. 1).



```
def ecncrypt(t1,t2):  
    t1 = [ord(i) for i in t1]  
    t2 = [ord(i) for i in t2]  
    return ''.join(chr(a^b) for a, b in zip(t1, t2))
```

Рис. 1: Функция шифрования

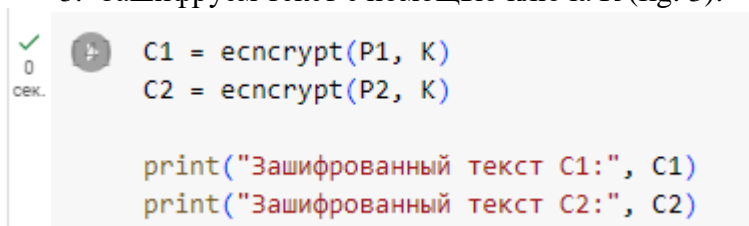
2. Введем данные из условия (fig. 2).



```
[3] P1 = "НаВашисходящийот1204"  
    P2 = "ВСеверныйфилиалБанка"  
  
    K = "05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 b2 70 54"
```

Рис. 2: Данные из условия

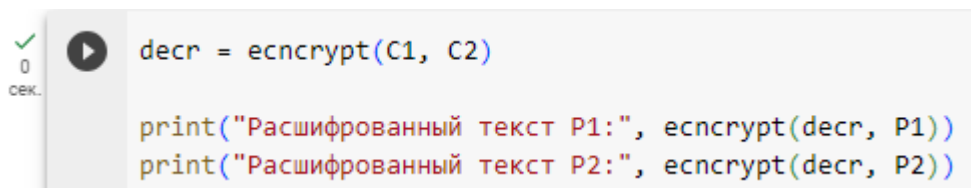
3. Зашифруем текст с помощью ключа K (fig. 3).



```
C1 = ecncrypt(P1, K)  
C2 = ecncrypt(P2, K)  
  
print("Зашифрованный текст C1:", C1)  
print("Зашифрованный текст C2:", C2)
```

Рис. 3: Шифрование текста

4. Создадим последовательность, с помощью которой будем расшифровывать текст.  
Передадим ее в функцию шифрования вместе с зашифрованным текстом (fig. 4).

A screenshot of a code editor with a light gray background. On the left, there is a green checkmark icon and a play button icon. Below the play button, the text "0 сек." is visible. The code is written in a monospaced font with syntax highlighting: 

```
decr = ecncrypt(C1, C2)

print("Расшифрованный текст P1:", ecncrypt(decr, P1))
print("Расшифрованный текст P2:", ecncrypt(decr, P2))
```

Рис. 4: Расшифровка текста

5. Запустим программу и получим результат (fig. 5).

Зашифрованный текст C1: ЭSвЁтИЩ00ГьJ00Vt000  
Зашифрованный текст C2: ТДЕЪŸQKŸЙёQJvLXvNЬI  
Расшифрованный текст P1: ВСеверныйфилиалБанка  
Расшифрованный текст P2: НаВашисходящийот1204

Рис. 5: Результат



## **Выводы**

В рамках данной лабораторной работы было освоено на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

## Список литературы

[1] <https://www.kaspersky.ru/resource-center/definitions/encryption>