# Лабораторная работа № 8

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

Нгуен Фыок Дат

[**Цель работы**](#_bookmark0) **4**

[**Задание**](#_bookmark1) **5**

[**Теоретическое введение**](#_bookmark2) **6**

[**Выполнение лабораторной работы**](#_bookmark3) **7**

[**Выводы**](#_bookmark9) **9**

[**Список литературы**](#_bookmark10) **10**

[1 Функция шифрования](#_bookmark4) . . . . . . . . . . . . . . . . . . . . . . . . . . . . 7

[2 Данные из условия](#_bookmark5) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 7

[3 Шифрование текста](#_bookmark6) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 7

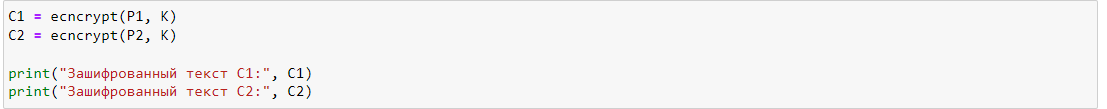
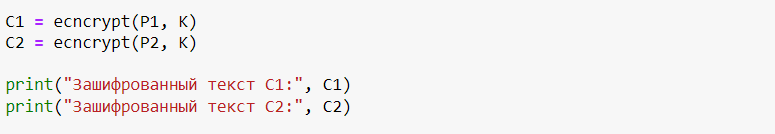
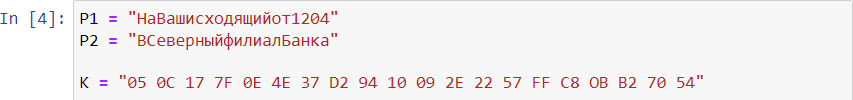
[4 Расшифровка текста](#_bookmark7) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8

[5 Результат](#_bookmark8) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8

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

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать при- ложение, 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.

* Шифрование – это технология кодирования и раскодирования данных.Зашифро- ванные данные -это результат применения алгоритма для кодирования данных с целью сделать их недоступными для чтения. Данные могут быть раскодированы в исходную форму только путем применения специальный 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].



1. Создаем функцию шифрования (fig. [1).](#_bookmark4)

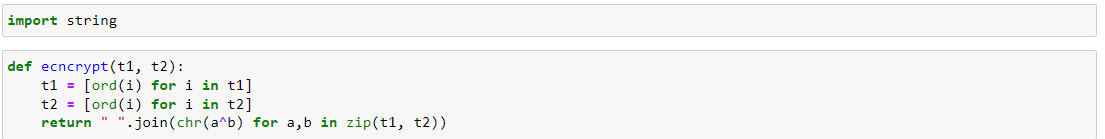
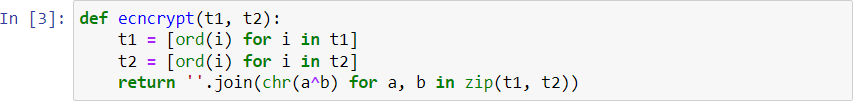


Рис. 1: Функция шифрования

1. Введем данные из условия (fig. [2).](#_bookmark5)

Рис. 2: Данные из условия

1. Зашифруем текст с помощью ключа К (fig. [3).](#_bookmark6)

Рис. 3: Шифрование текста

1. Создадим последовательность, с помощью которой будем расшифровывать текст. Передадим ее в функцию шифрования вместе с зашифрованным текстом (fig. [4).](#_bookmark7)

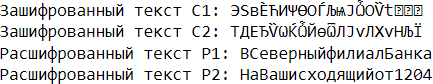
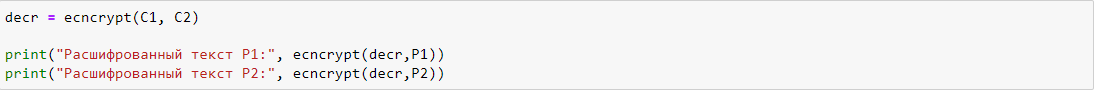
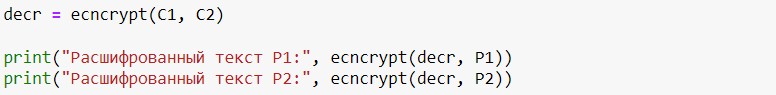


Рис. 4: Расшифровка текста

1. Запустим программу и получим результат (fig. [5).](#_bookmark8)

Рис. 5: Результат

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

1. [https://www.kaspersky.ru/resource-center/definitions/encryption](http://www.kaspersky.ru/resource-center/definitions/encryption)
2. https://xakep.ru/2019/07/18/crypto-xor/