Отчёт по лабораторной работе №8

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

Акопян Изабелла Арменовна

Содержание

[1 Цель работы 1](#_Toc149426245)

[2 Задание 1](#_Toc149426246)

[3 Теоретическое введение 1](#_Toc149426247)

[4 Выполнение лаборатной работы 2](#_Toc149426248)

[5 Выводы 2](#_Toc149426249)

[Список литературы 3](#_Toc149426250)

# 1 Цель работы

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

# 2 Задание

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.

# 3 Теоретическое введение

Основной принцип действия любого типа кодировки заключается в шифраторе и дешифраторе. С одного устройства информация в конвертированном виде отправляется,

на другое она поступает и преобразуется в нужный текст. Для кодирования и раскодирования информации потребуется обменяться ключом. Он помогает провести раскодировку письма.

Имеются две большие группы шифров: шифры перестановки и шифры замены.

Шифр перестановки изменяет только порядок следования символов исходного сообщения. Это такие шифры, преобразования которых приводят к изменению только следования символов открытого, исходного сообщения.

Шифр замены заменяет каждый символ кодируемого сообщения на другой(ие) символ(ы), не изменяя порядок их следования.

Это такие шифры, преобразования которых приводят к замене каждого символа открытого сообщения на другие символы,

причем порядок следования символов закрытого сообщения совпадает с порядком следования соответствующих символов открытого сообщения.

# 4 Выполнение лаборатной работы

1. Написала приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования (рис. fig.001 – fig.002).

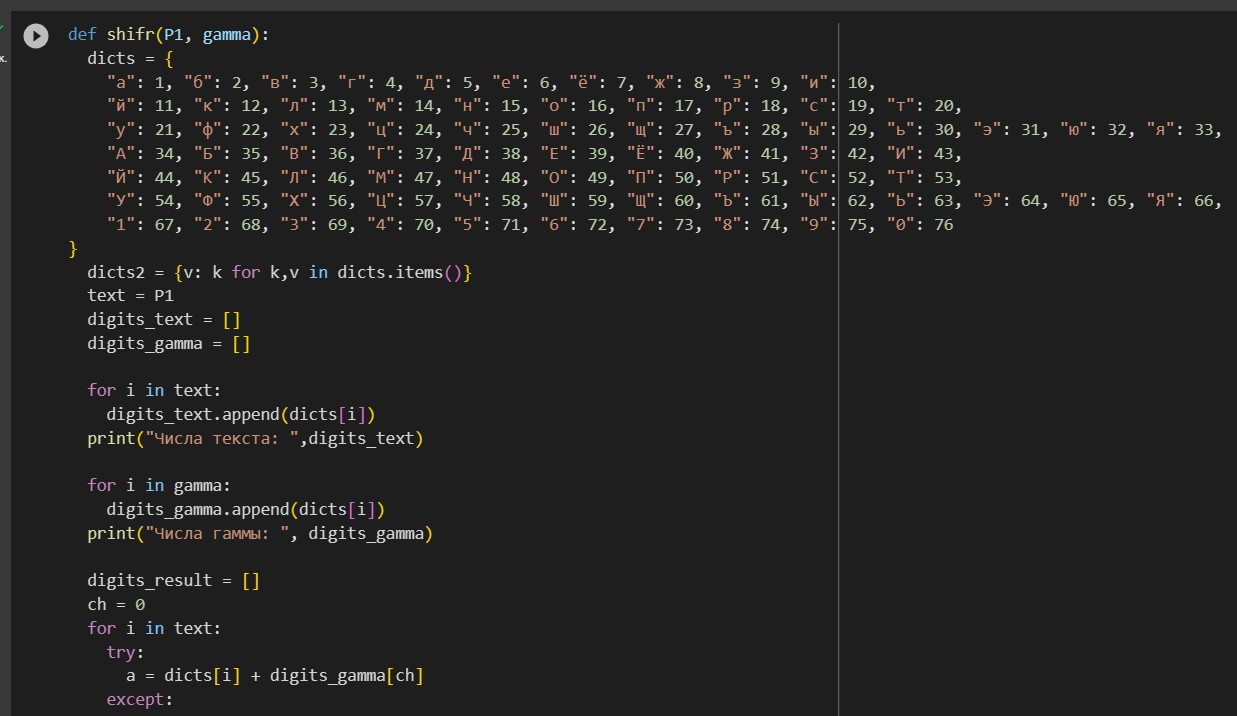
Она определяет вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе

Figure 1: Первая часть программы

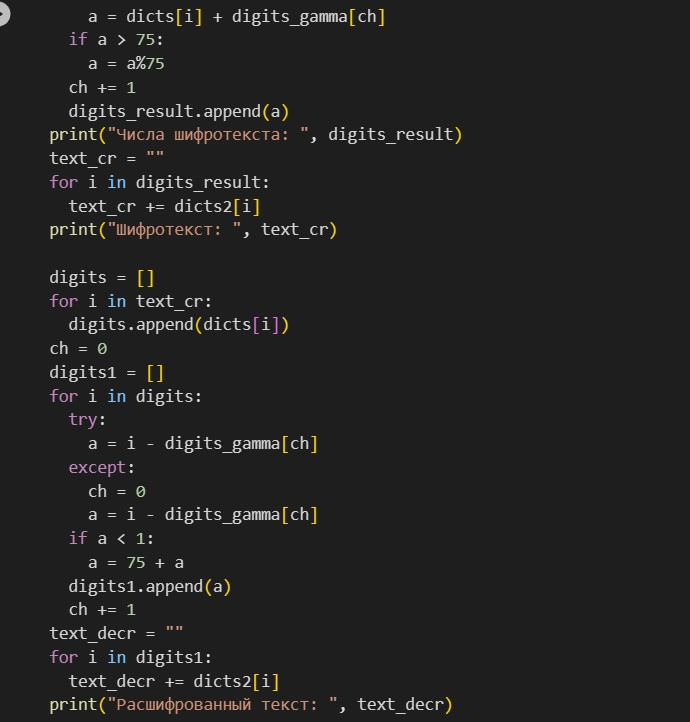


Figure 2: Вторая часть программы

Ниже показан результат работы приложения ( рис. fig.003)

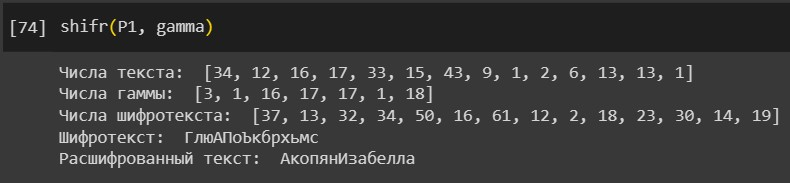


Figure 3: Результат

2. Взяла тексты из задания лабораторной работы и запустила программу ( рис. fig.004)

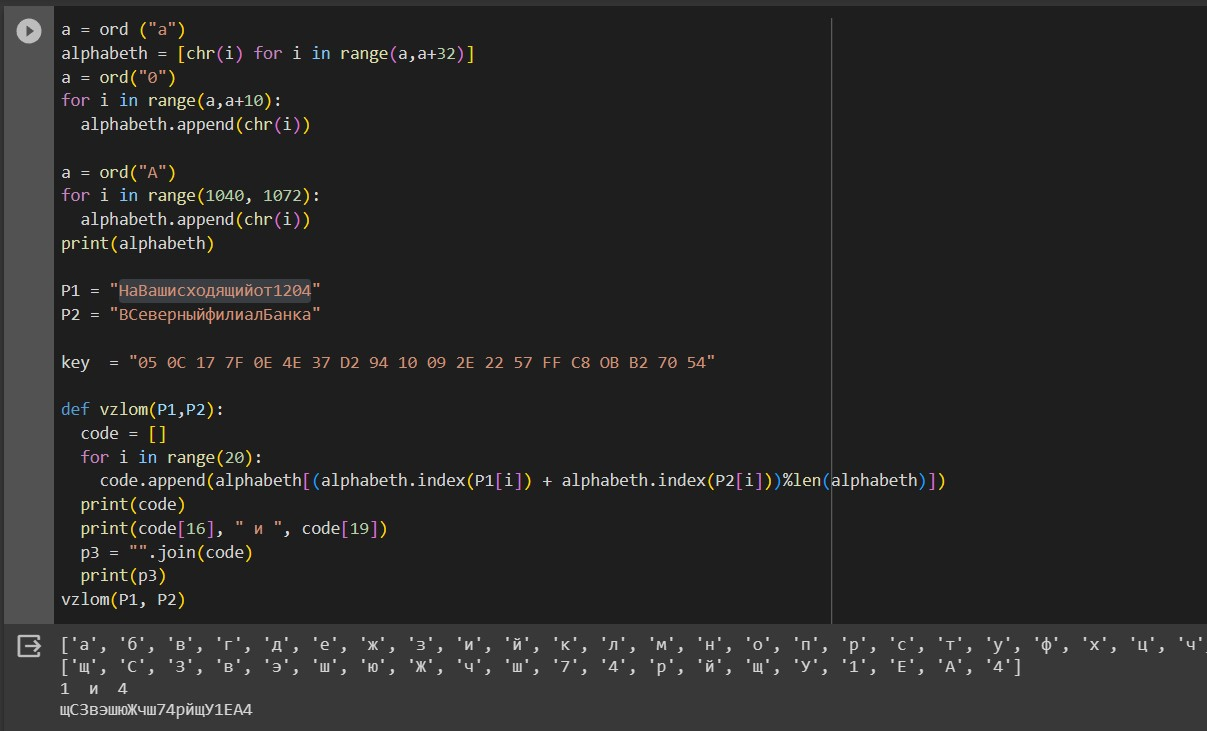


Figure 4: Результат выполнения для Р2

# 5 Выводы

Я овладела навыками использования режима однократного гаммирования на практике, применяя его для кодирования разнообразных исходных текстов с использованием одного и того же ключа.

Мною было разработано приложение, которое способно зашифровывать и расшифровывать тексты в режиме однократного гаммирования, а также определять тип шифротекста при наличии известного ключа.

# Список литературы

[Лабораторная работа № 8. Элементы](https://esystem.rudn.ru/pluginfile.php/2090423/mod_resource/content/2/008-lab_crypto-key.pdf) криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

[Однократное гаммирование](https://studfile.net/preview/272674/page:7/)