Лабораторная работа № 7. Элементы криптографии. Однократное гаммирование

Ильин Никита Евгеньевич, НФИбд-01-19

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования.

# 2 Задание

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно:

1. Определить вид шифротекста при известном ключе и известном открытом тексте.
2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

# 3 Выполнение работы

1. Была написана программа, которая соответствует требоваиям задачи, и проверяет полученный ключ с изначально сгенерированным.

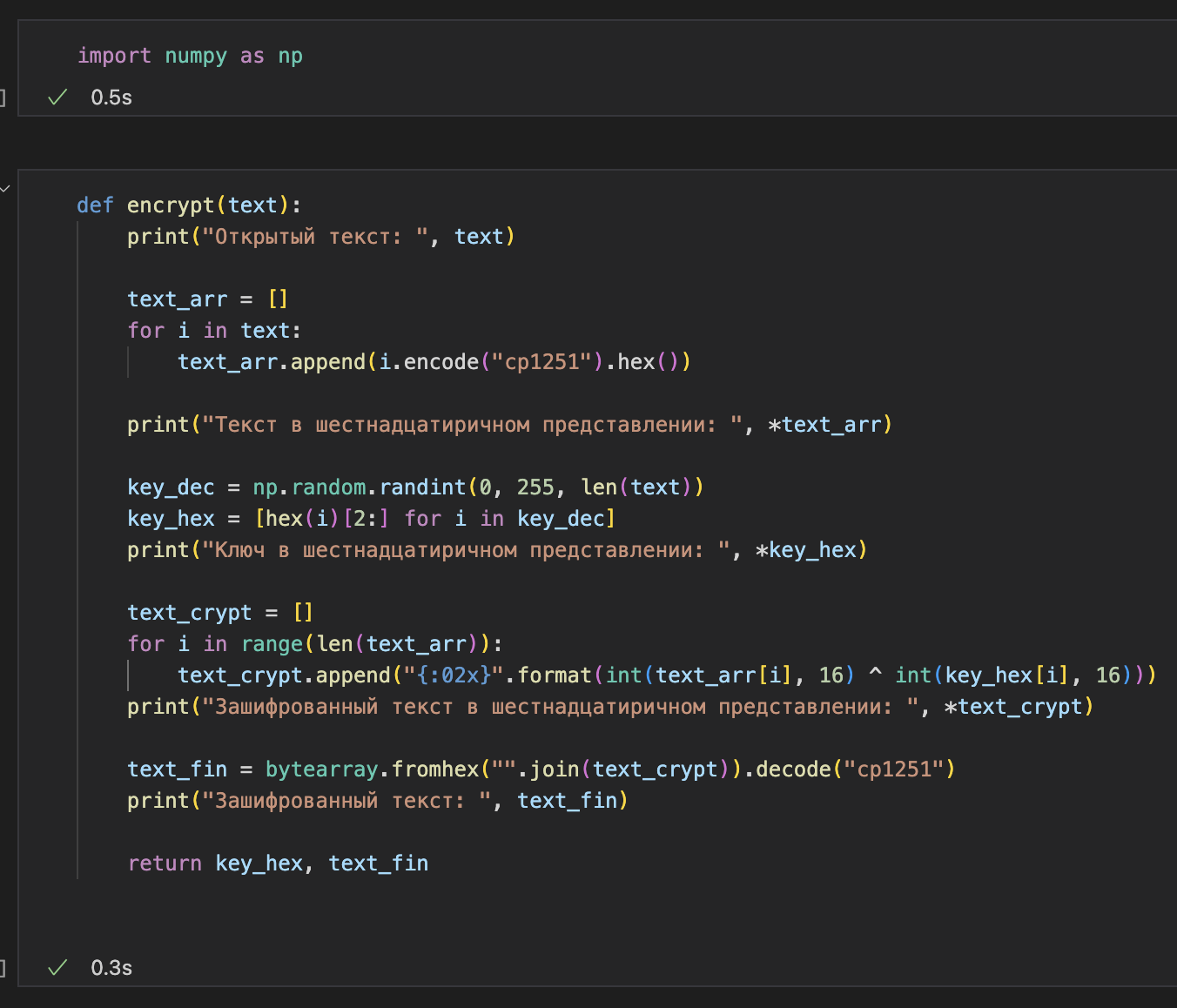


Figure 1: функция шифрования

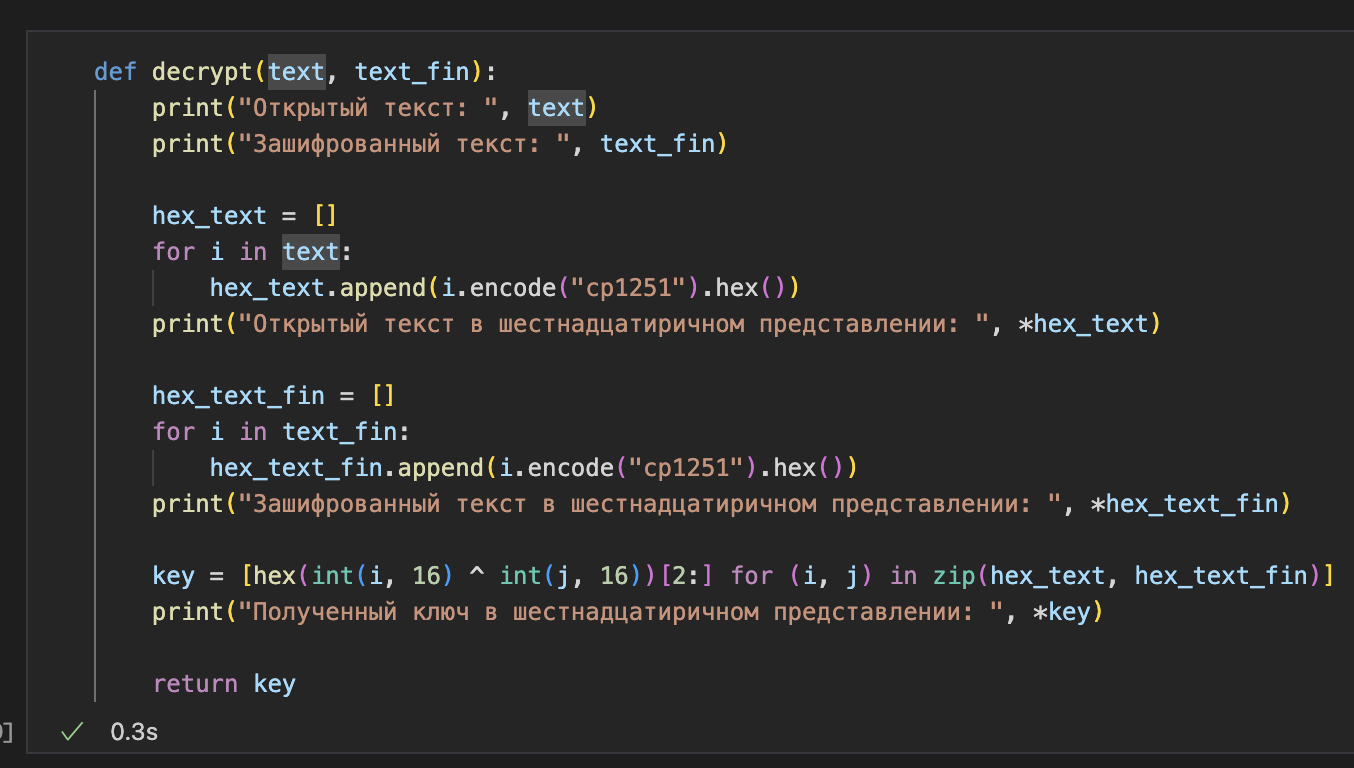


Figure 2: функция расшифровки

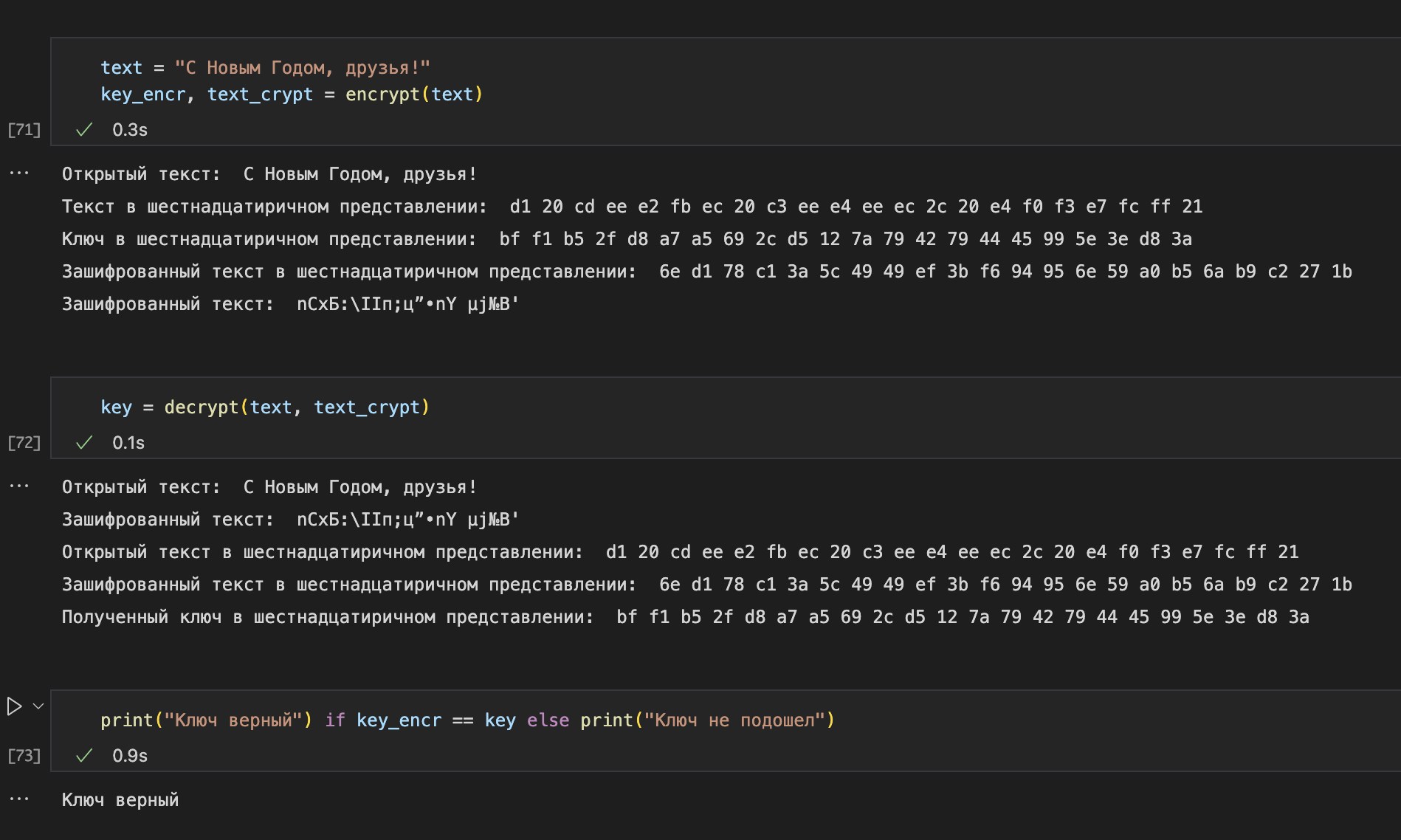


Figure 3: Работа программы

# 4 Выводы

Освоено на практике применение режима однократного гаммирования.

# 5 Библиография

1. Методические материалы курса