Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

Кафедра экономической математики, информатики и статистики (ЭМИС)

РАЗРАБОТКА ПРОГРАММЫ ШИФРОВАНИЯ НА ОСНОВЕ МЕТОДА RSA

Отчет по практической работе по дисциплине «Защита информации»

Студент гр. 590-1

\_\_\_\_\_\_\_\_\_\_\_\_/Г.К. Петров

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 2023 г.

Доктор технических наук

\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_/ В.Г. Спицын

оценка подпись

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 2023 г.

Томск 2023

**Цель работы:** изучение метода шифрования с помощью метода RSA, а также его применение для шифрования и расшифровки фраз.

**Задание:**

1. Создать программную реализацию RSA;

2. Зашифровать любую фразу, введенную с клавиатуры, используя открытый ключ;

3. Расшифровать полученную в пункте 2 зашифрованную строку, используя закрытый ключ.

**Результат выполнения задания.**

Пример выполнения заданий 2-3 представлен на рисунках 1-3. Полный код на языке Python представлен в приложении А.

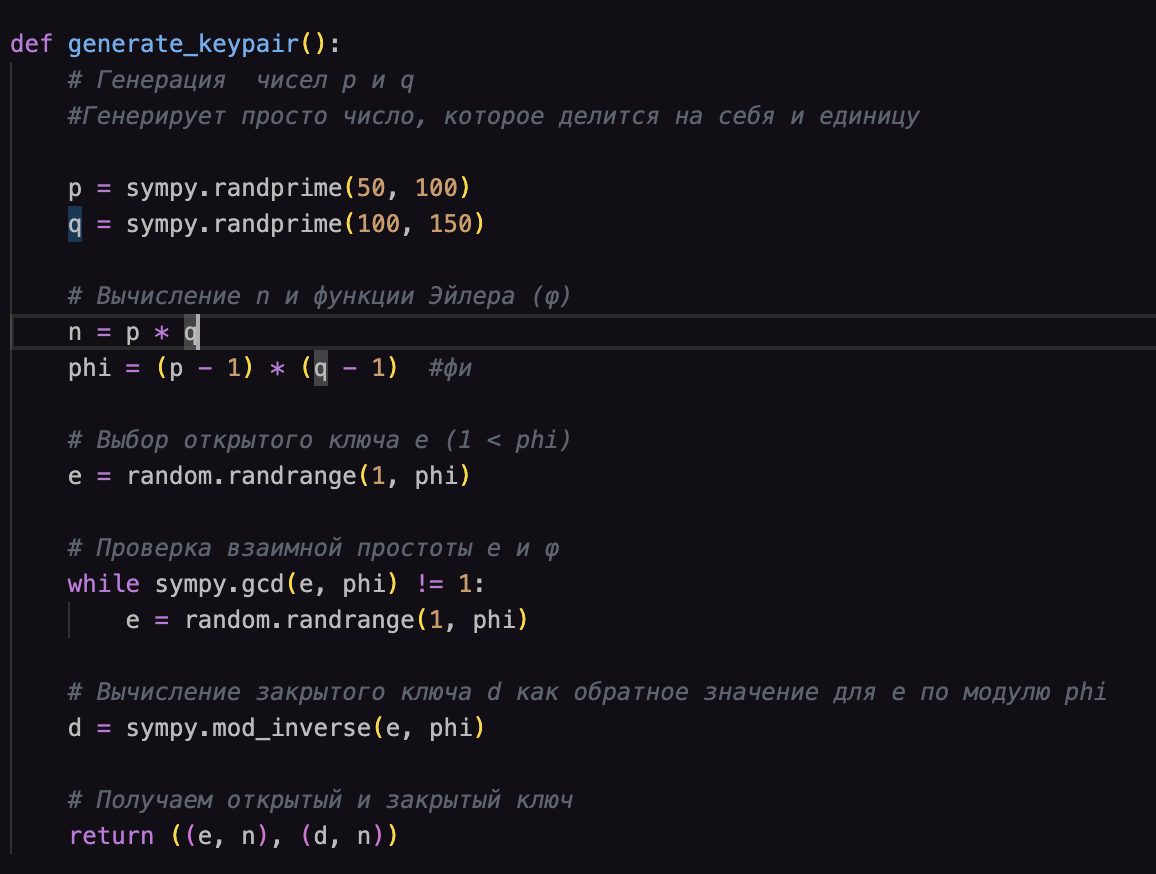


Рисунок 1 –Вычисление ключей

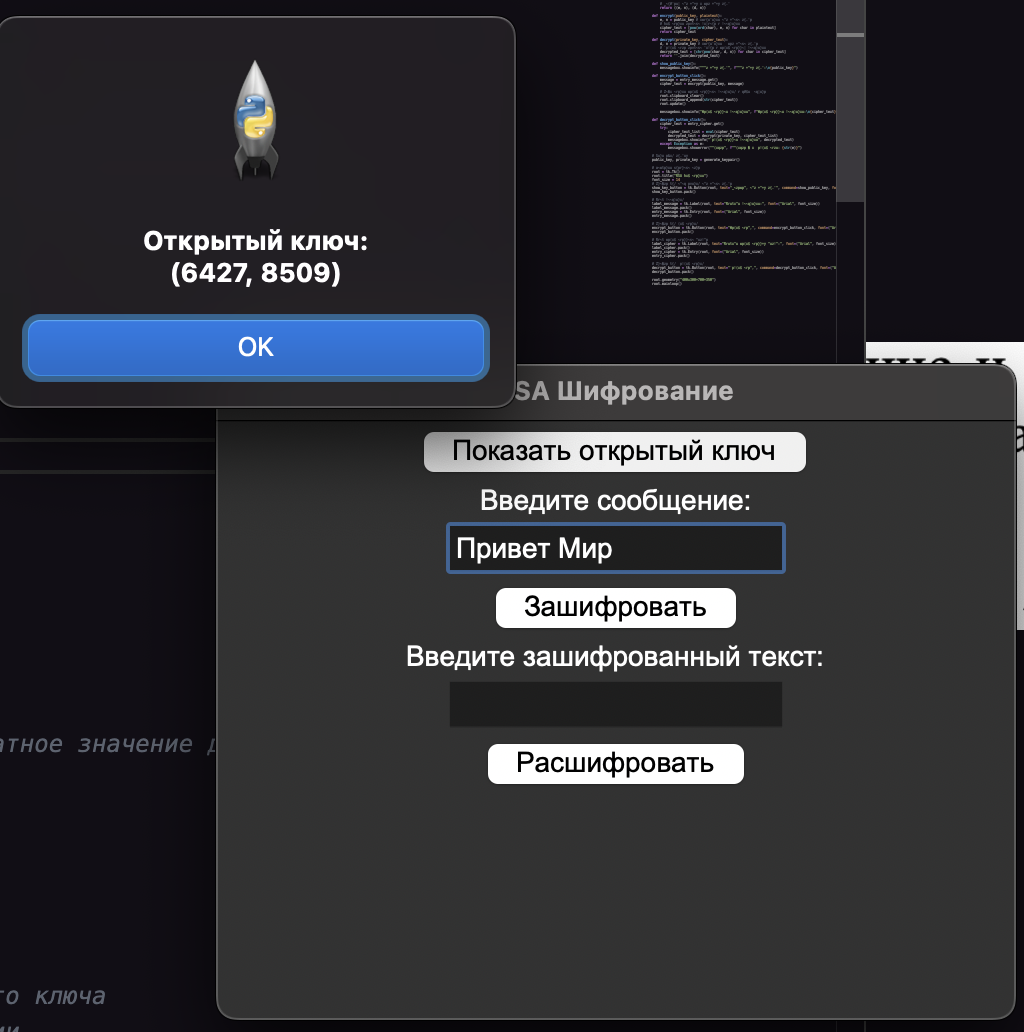


Рисунок 2 –Получившийся ключ

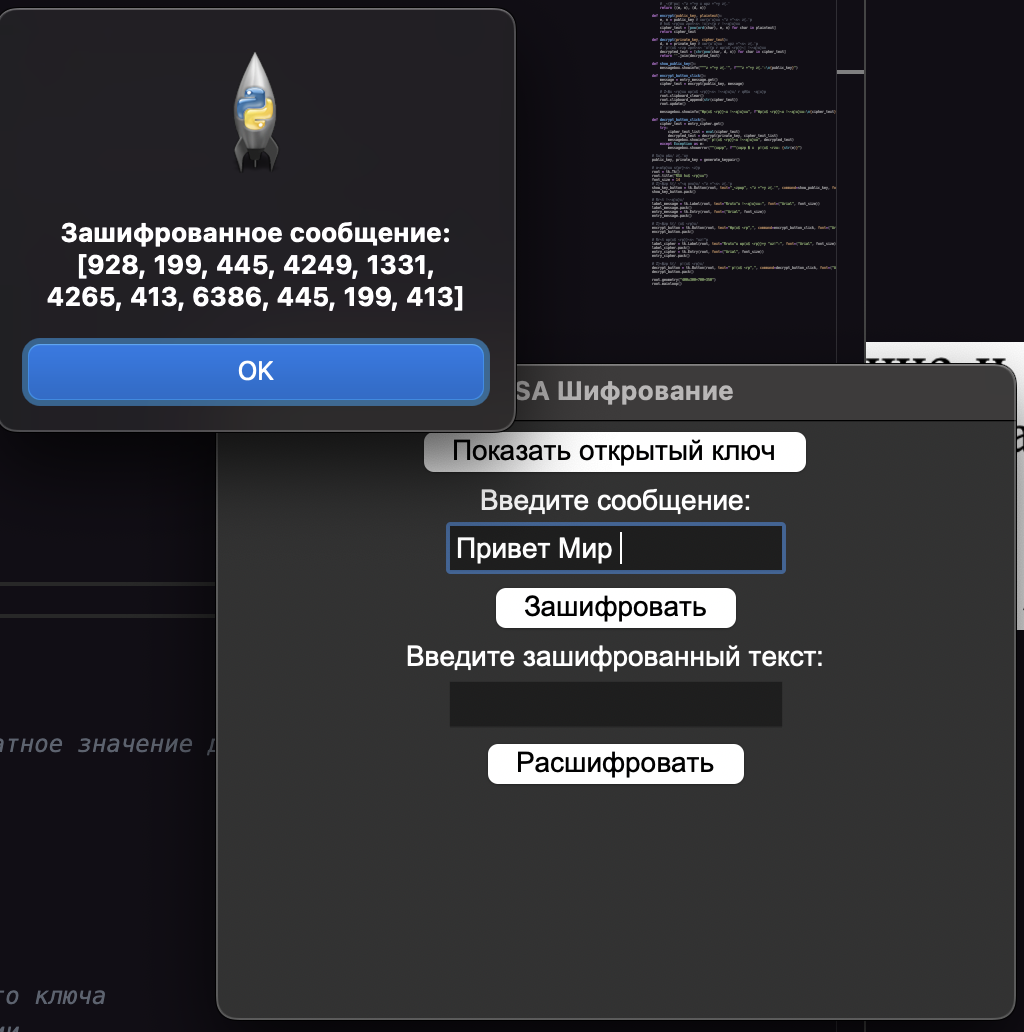


Рисунок 3 – Зашифрованное сообщение

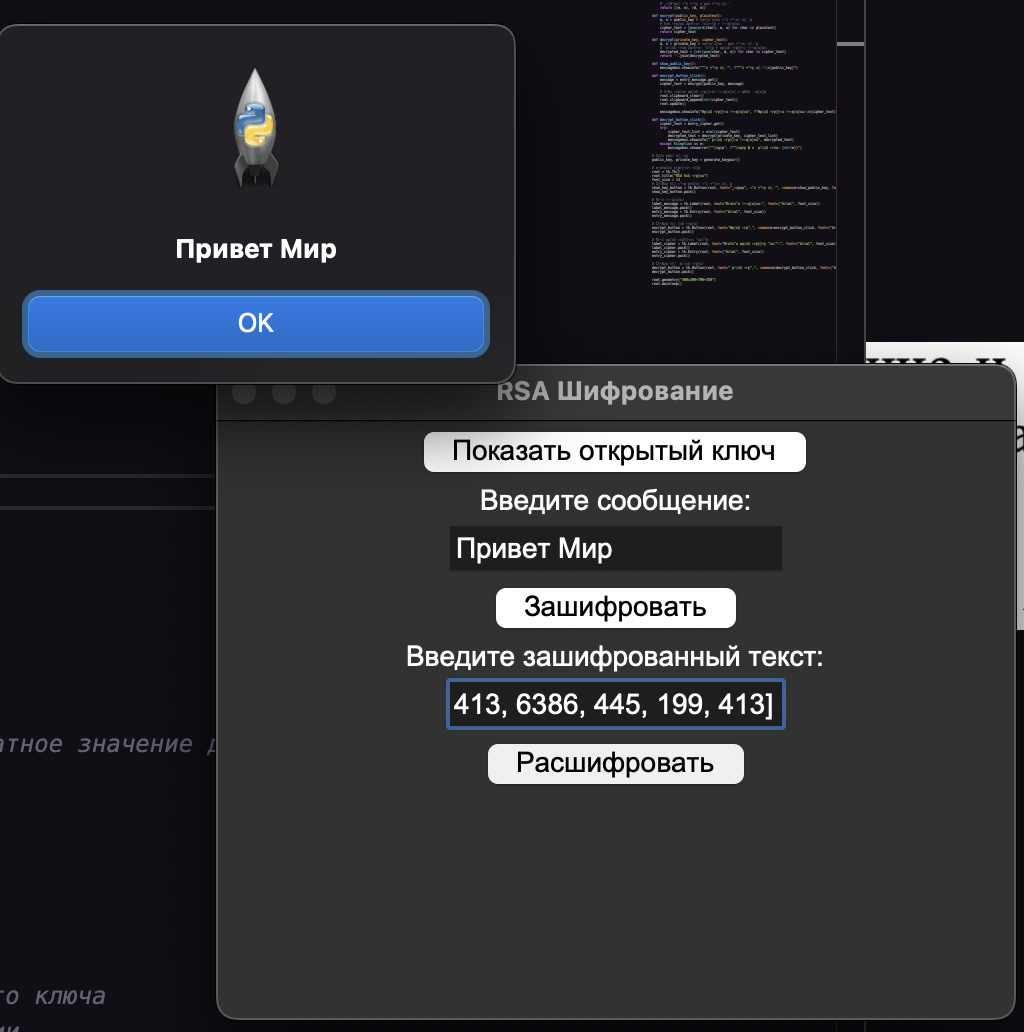


Рисунок 4 – Расшифрованное сообщение

Пример выполнения задания 1 представлен в приложении А.

**Вывод:** в процессе работы был изучен и применён метод шифрования RSA.