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.

```python
def generate_keypair():
    # Генерация  чисел p и q
    #Генерирует просто число, которое делится на себя и единицу

    p = sympy.randprime(50, 100)
    q = sympy.randprime(100, 150)

    # Вычисление n и функции Эйлера (φ)
    n = p * q
    phi = (p - 1) * (q - 1)  #фи

    # Выбор открытого ключа e (1 < phi)
    e = random.randrange(1, phi)

    # Проверка взаимной простоты e и φ
    while sympy.gcd(e, phi) != 1:
        e = random.randrange(1, phi)

    # Вычисление закрытого ключа d как обратное значение для e по модулю phi
    d = sympy.mod_inverse(e, phi)

    # Получаем открытый и закрытый ключ
    return ((e, n), (d, n))
```

Рисунок 1 –Вычисление ключей

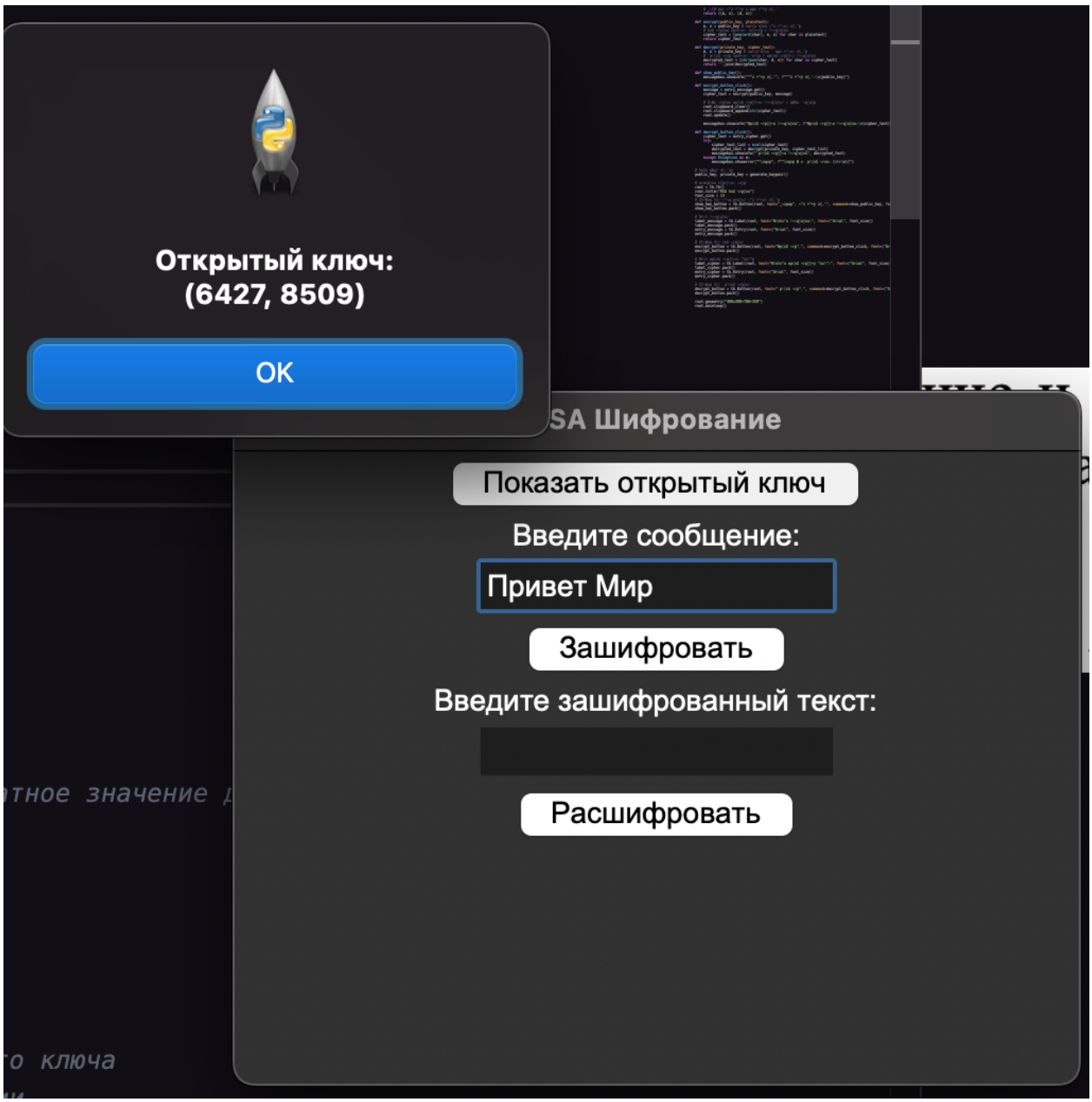

Рисунок 2 –Получившийся ключ

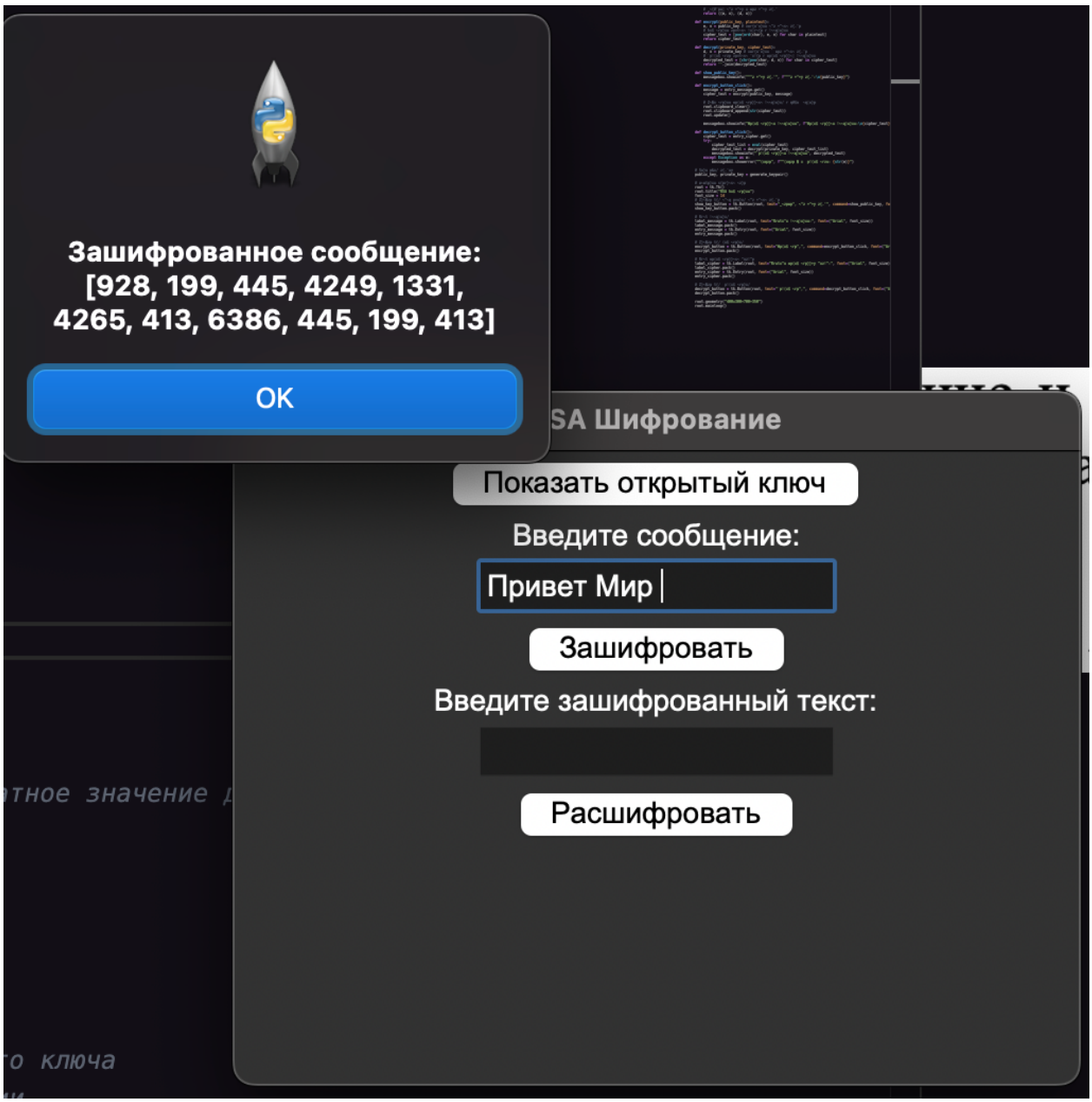

Рисунок 3 – Зашифрованное сообщение

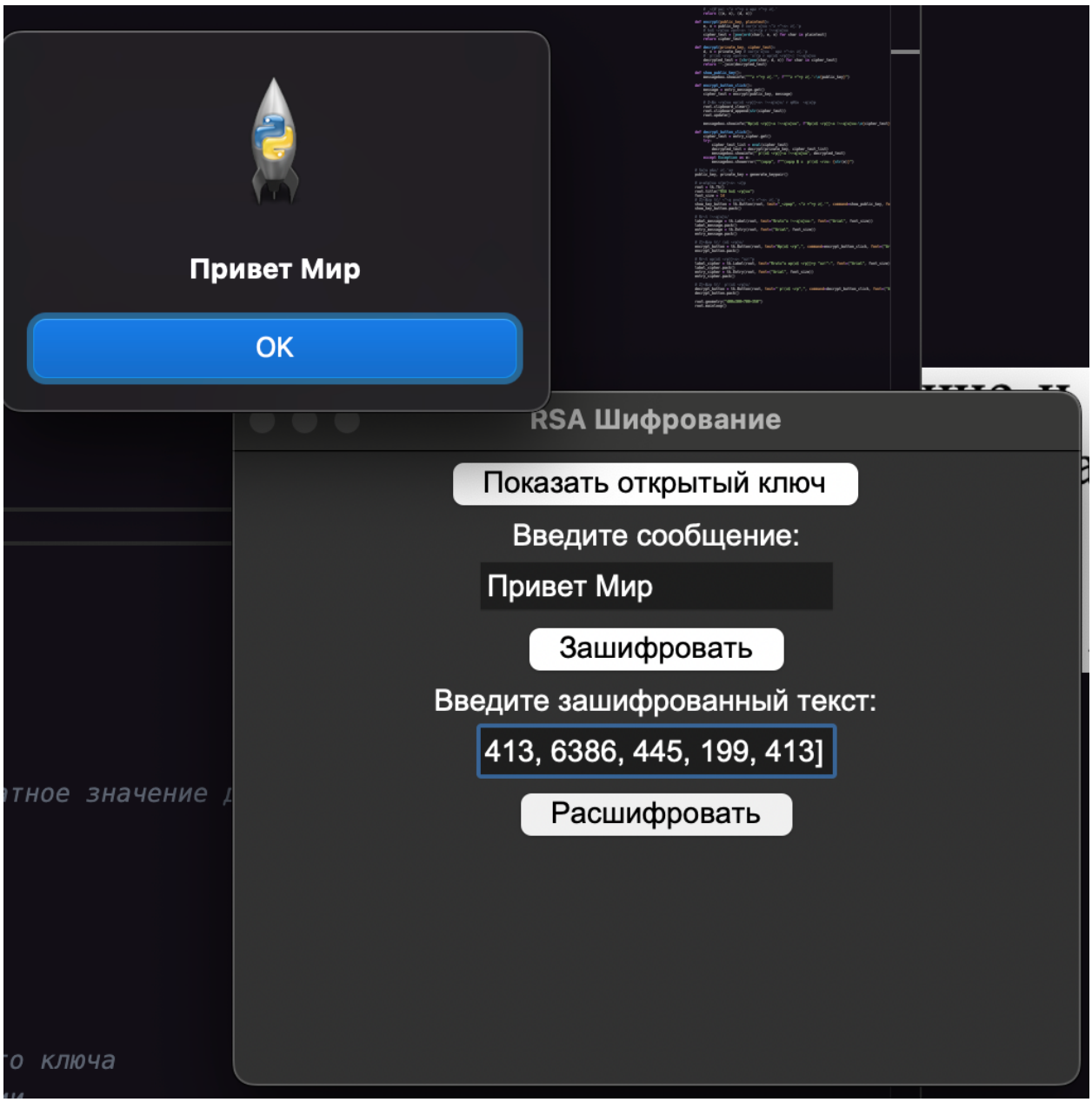

Рисунок 4 – Расшифрованное сообщение

Пример выполнения задания 1 представлен в приложении А.

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