Министерство образования

Республики Беларусь

Учреждение образования

Белорусский государственный университет

информатики и радиоэлектроники

Кафедра: интеллектуальных информационных технологий

Отчёт

По дисциплине

«Средства и методы защиты информации в интеллектуальных системах»

Тема: «Ассиметричное шифрование и электронная цифровая подпись»

Написал: Проверил

Германенко В.В., гр. 321701 Сальников Д. А.

Минск 2025

Задача:

Разработать программное обеспечение, реализующее функции генерации секретного и открытого ключей, шифрования и цифровой подписи для алгоритма RSA. Обмен входными и выходными данными должен осуществляться через файлы:

– открытого ключа;

– секретного ключа;

– исходного сообщения;

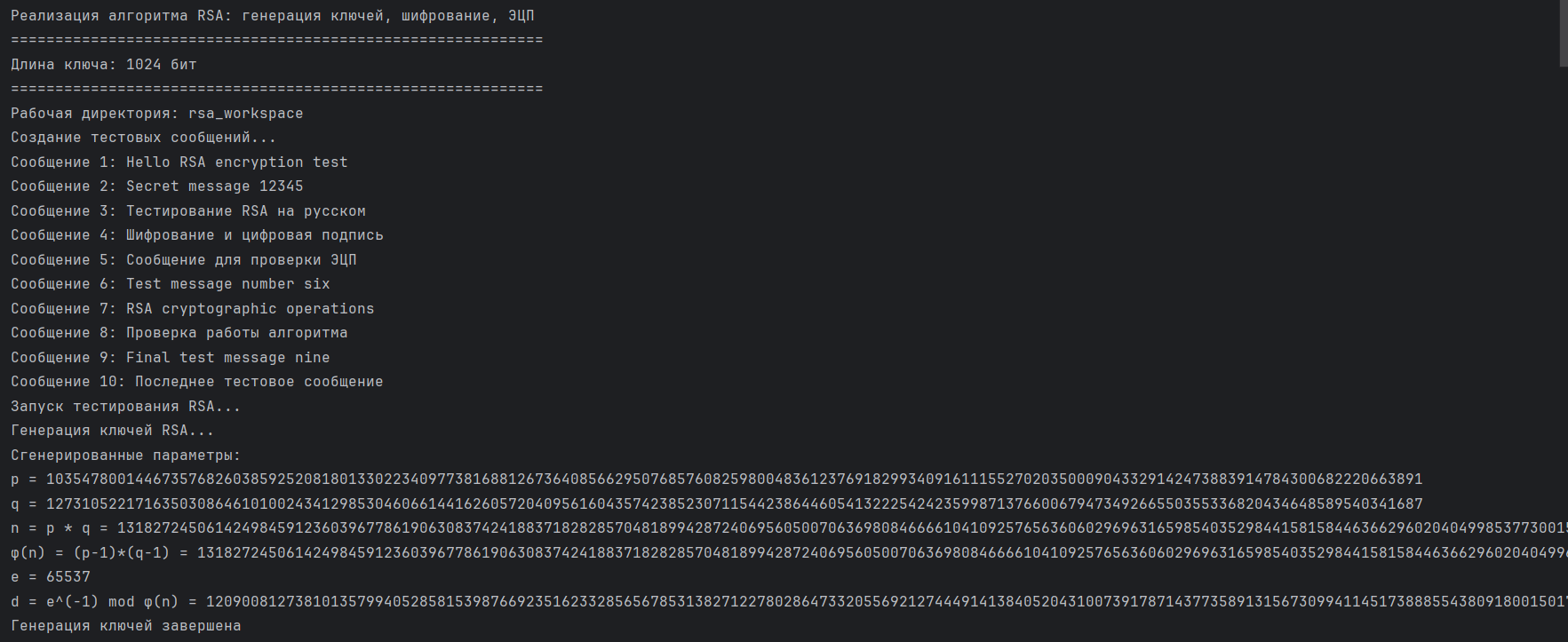
– зашифрованного сообщения.

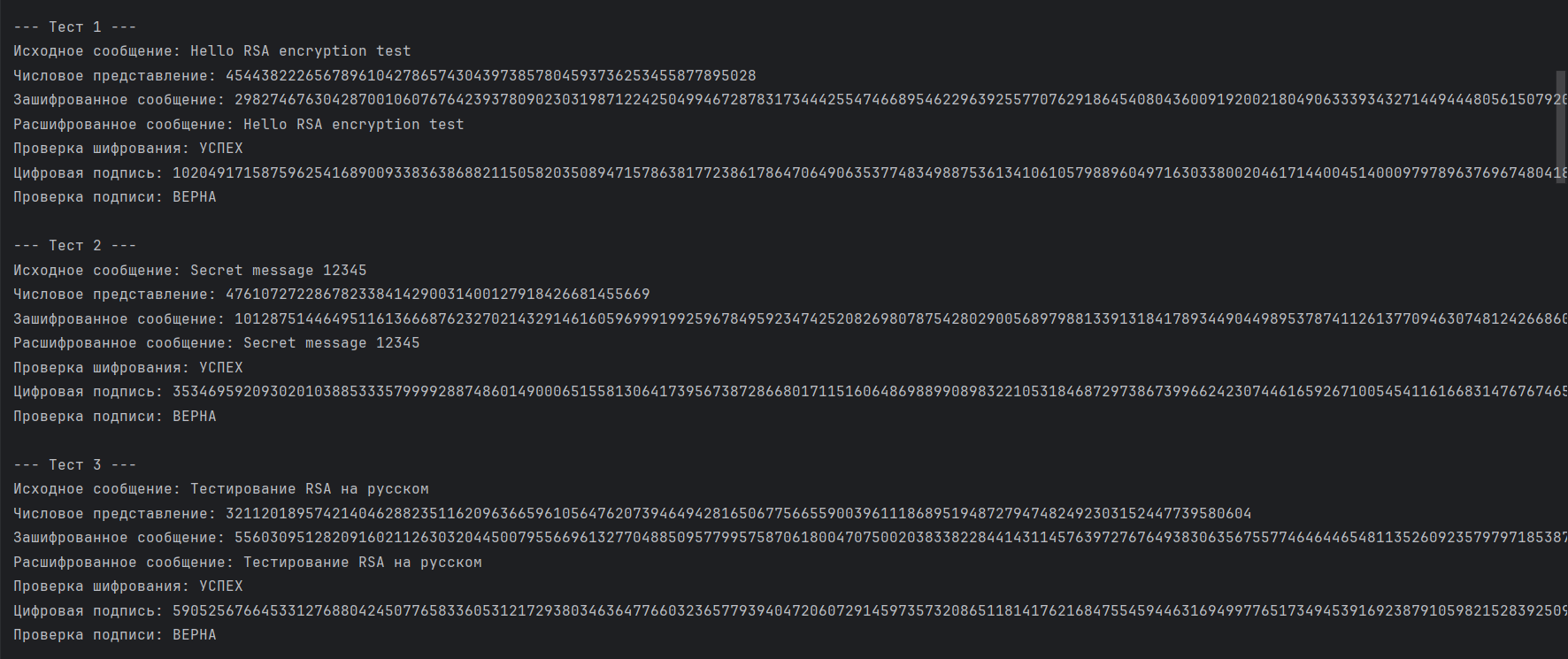
Для повышения скорости шифрования использовать метод последовательного возведения в квадрат и умножения.

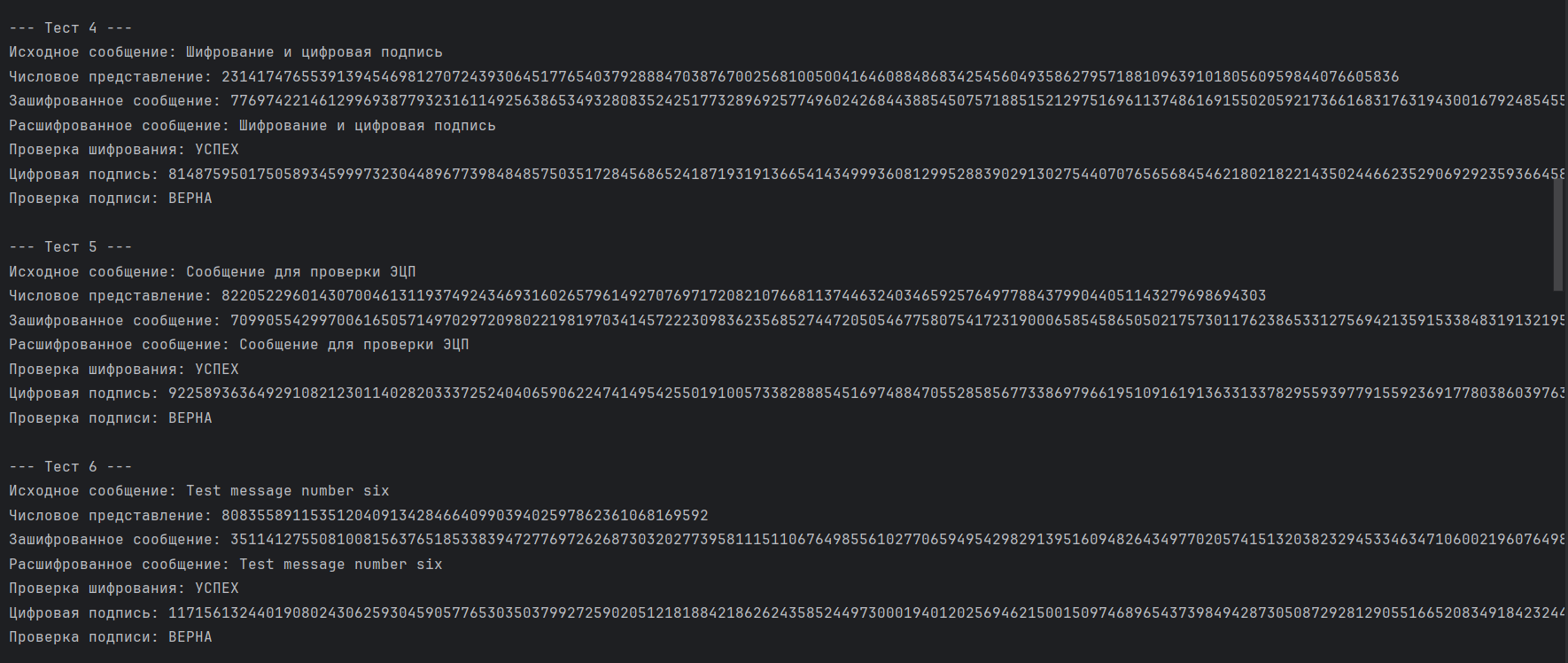
Выполнить тестирование разработанного программного обеспечения на 10 наборах тестовых данных.

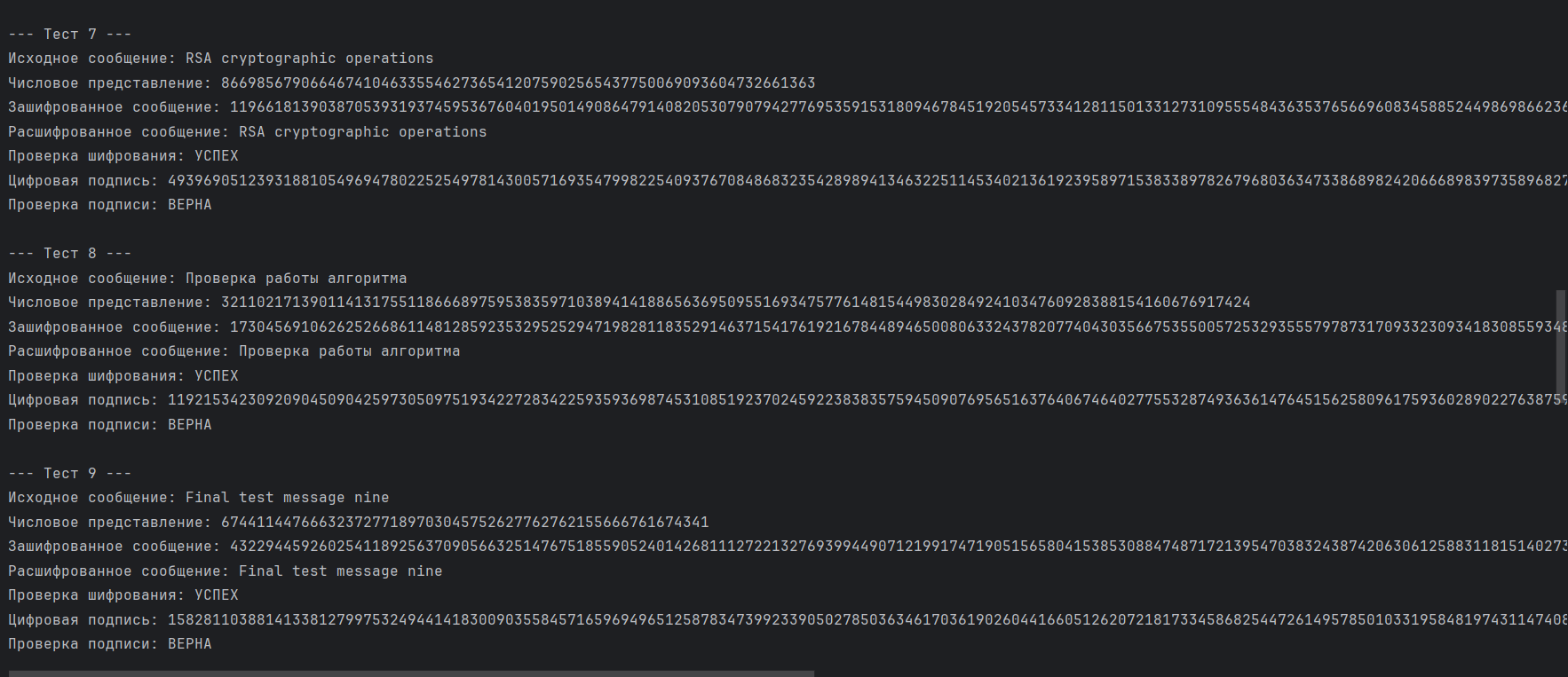
Длина чисел p и q должна быть не менее 1024 бит.

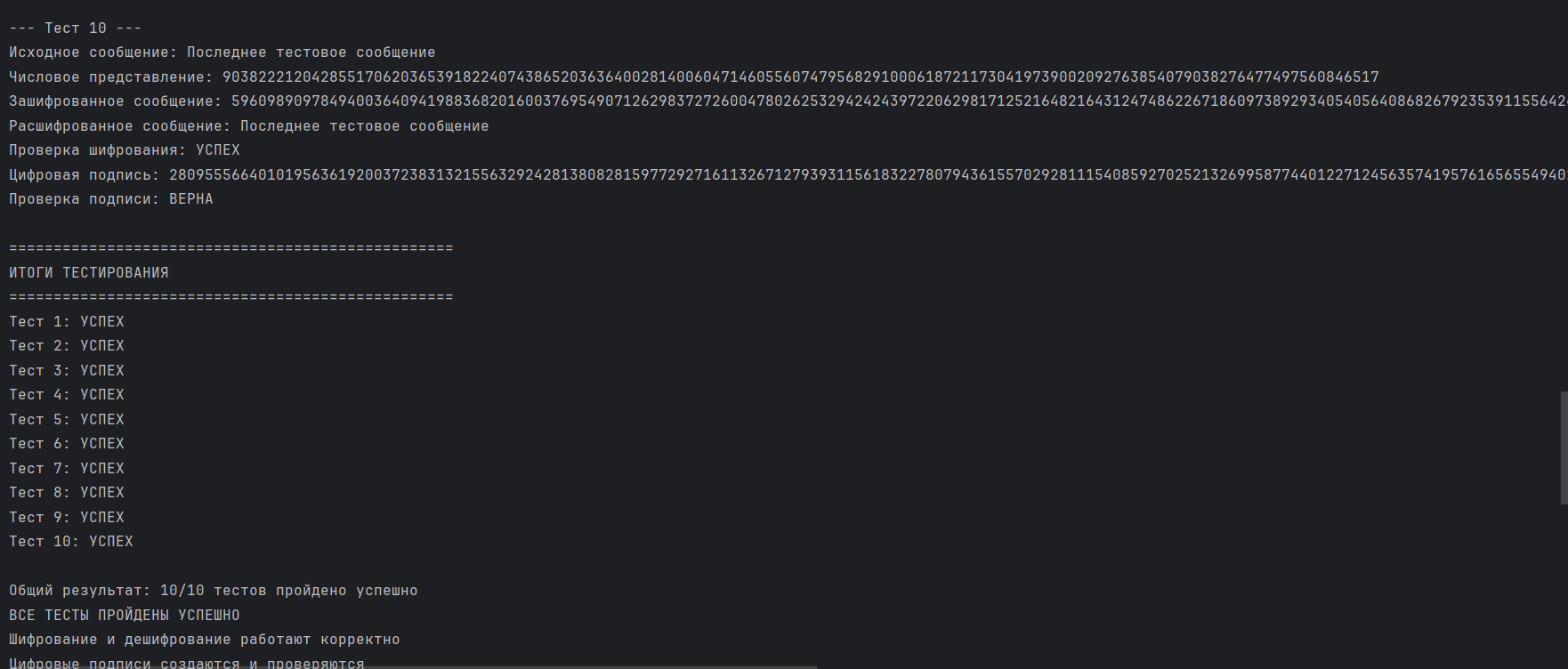
Реализация:

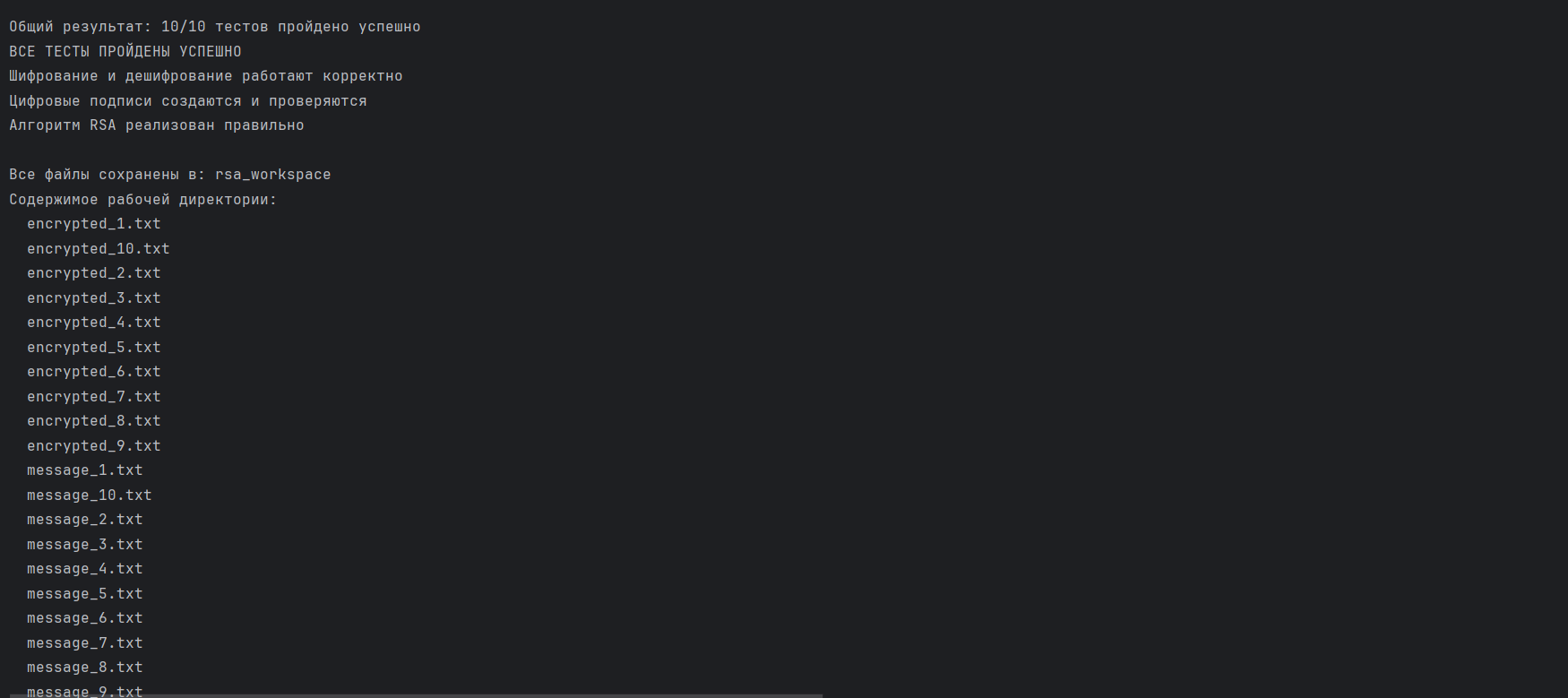


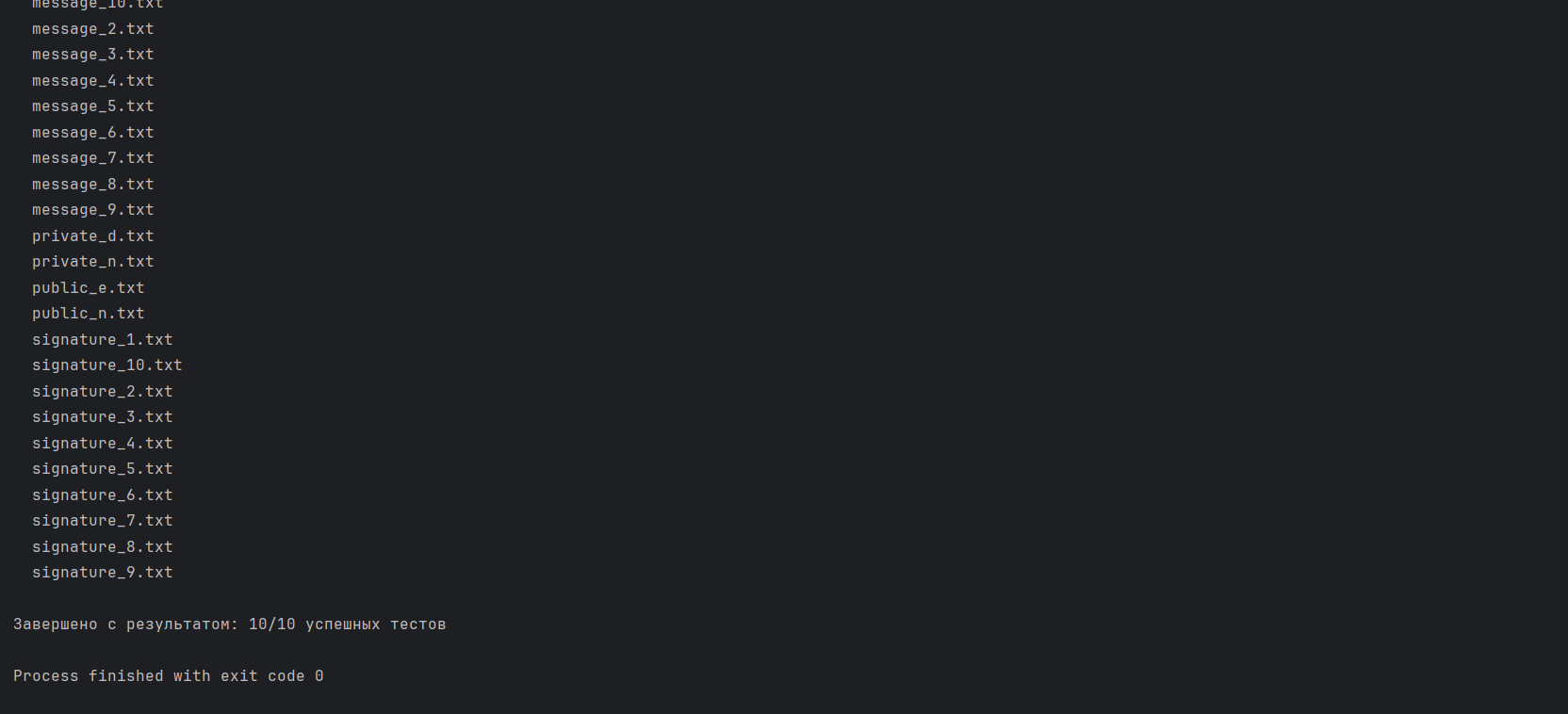












Вывод: Освоил принципы работы с ассиметричным шифрованием и цифровыми подписями, изучены алгоритмы ассиметричного шифрования.