Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет Информационных технологий и управления

Кафедра Интеллектуальных информационных технологий

**ОТЧЁТ**

по дисциплине «Средства и методы защиты информации в интеллектуальных системах»

Лабораторная работа №5

Тема: Асимметричное шифрование и электронная цифровая подпись

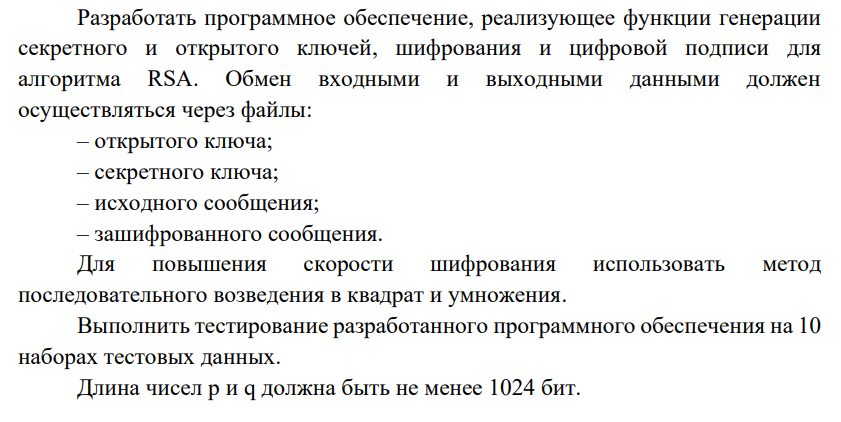
Выполнил: Самута Д. В.

гр. 221703

Проверил: Крищенович В. А.

Минск 2024

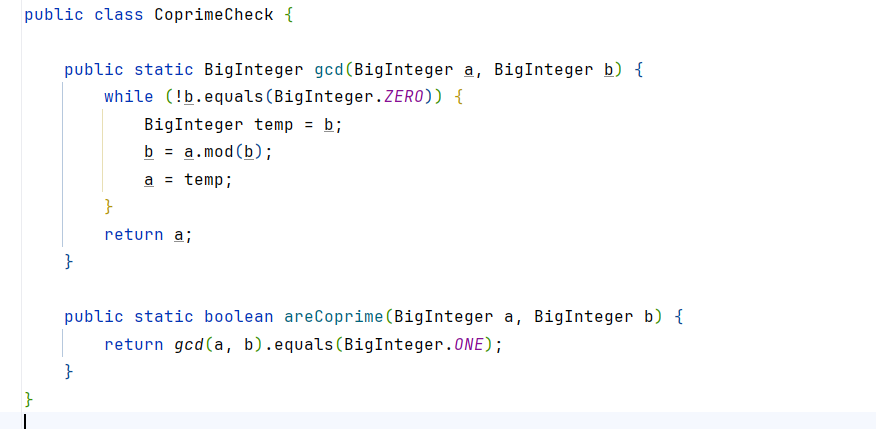
**Задание:**



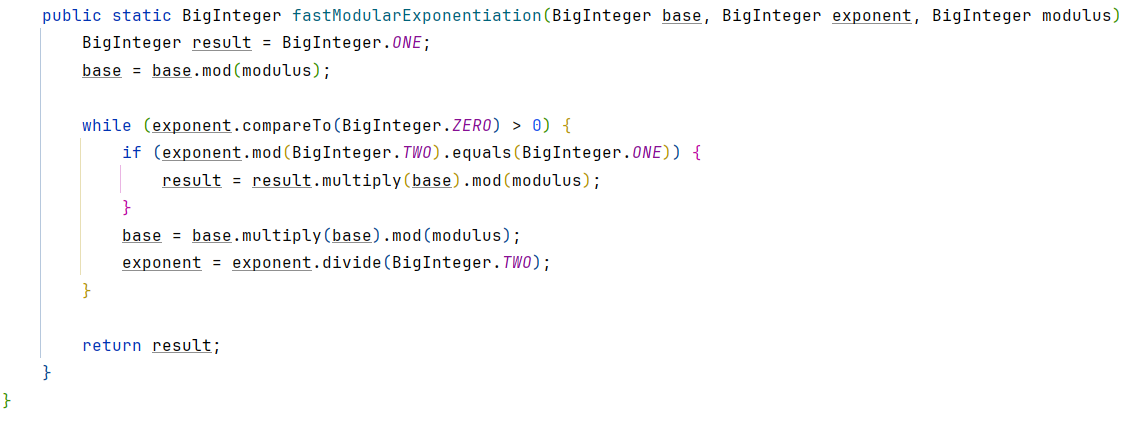
Метод генерации открытого и секретного ключа.



Для выбора e используется метод проверки двух чисел на взаимообратность.



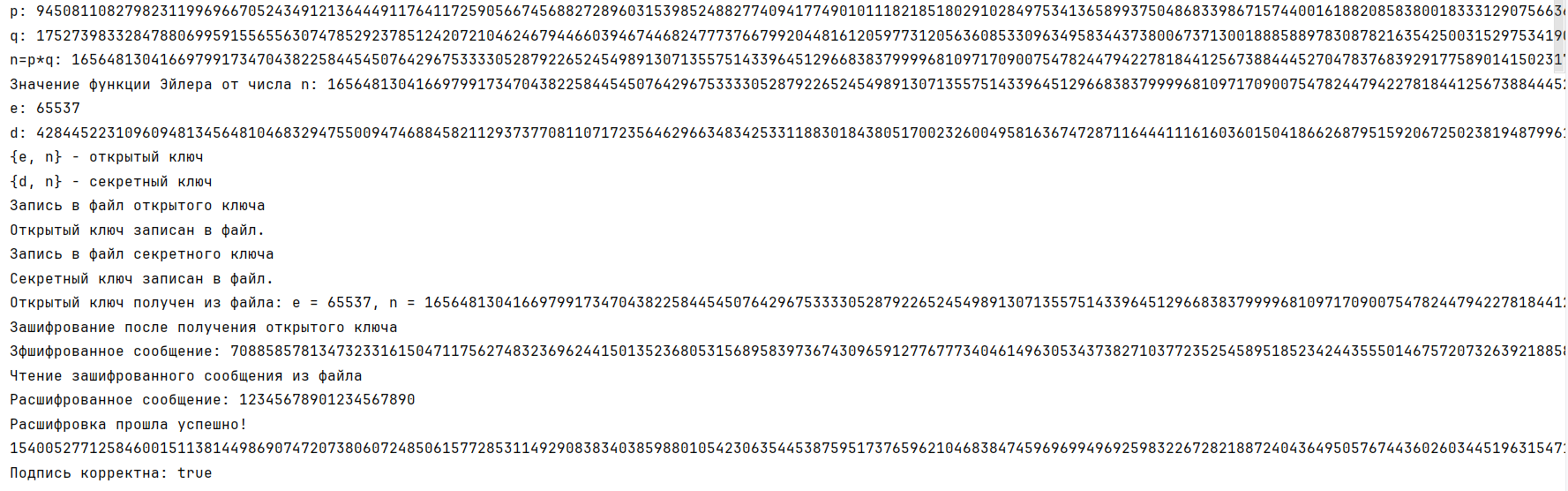
Для шифрование и дешифрования сообщения/подписи используется алгоритм быстрого возведения в степень

Программа работает для 10 тестовых данных, а также в процессе выполнения сохраняет/читает ключи/сообщения из файлов.



Пример работы:



Вывод: Алгоритм RSA представляет собой один из наиболее распространённых методов асимметричного шифрования, обеспечивающий безопасность данных. К его преимуществам относятся высокая степень безопасности благодаря использованию открытых и закрытых ключей, простота реализации и поддержка цифровой подписи для аутентификации и целостности данных. Однако у RSA есть и недостатки. К ним относятся медленная скорость шифрования по сравнению с симметричными алгоритмами, что делает его менее подходящим для работы с большими объёмами данных. Кроме того, алгоритм подвержен атакам на основе факторизации, что требует тщательного выбора параметров. Таким образом, хотя RSA нужно совмещать с другими методами для хорошего уровня защиты.