Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет информационный технологий и управления

Кафедра интеллектуальных информационных технологий

Дисциплина: «Средства и методы защиты информации в  
интеллектуальных системах»

Лабораторная работа №2 по теме:  
«АСИММЕТРИЧНОЕ ШИФРОВАНИЕ И ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ»

Студент гр. 121702

Колтович Д.С.

Проверил:

Сальников Д.А.

Минск 2023

**Тема**

Ассиметричное шифрование и электронная цифровая подпись

**Задание**

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

– открытого ключа;

– секретного ключа;

– исходного сообщения;

– зашифрованного сообщения.

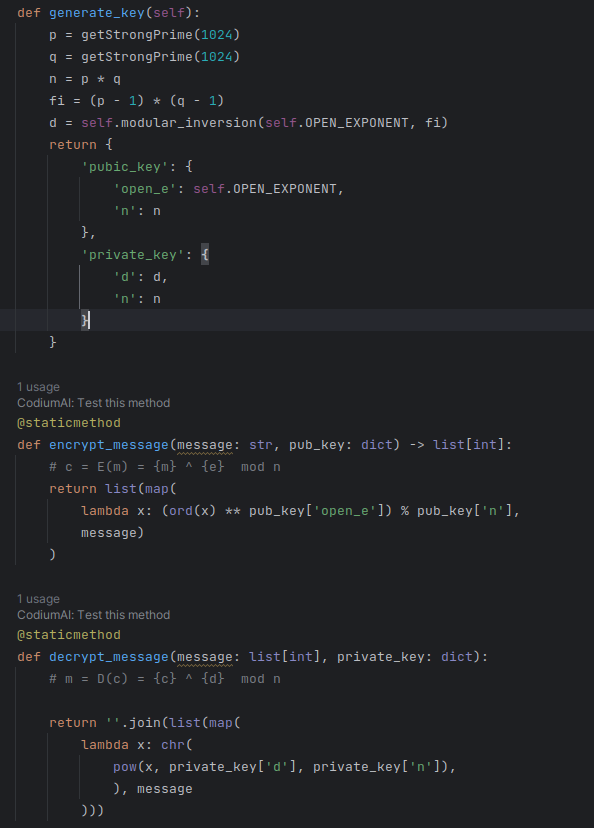
Для повышения скорости шифрования использовать метод последовательного возведения в квадрат и умножения.

Выполнить тестирование разработанного программного обеспечения на 10 наборах тестовых данных.

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

**Выполнение задания**

**Функции генерации, шифрования и расшифровки сообщения**

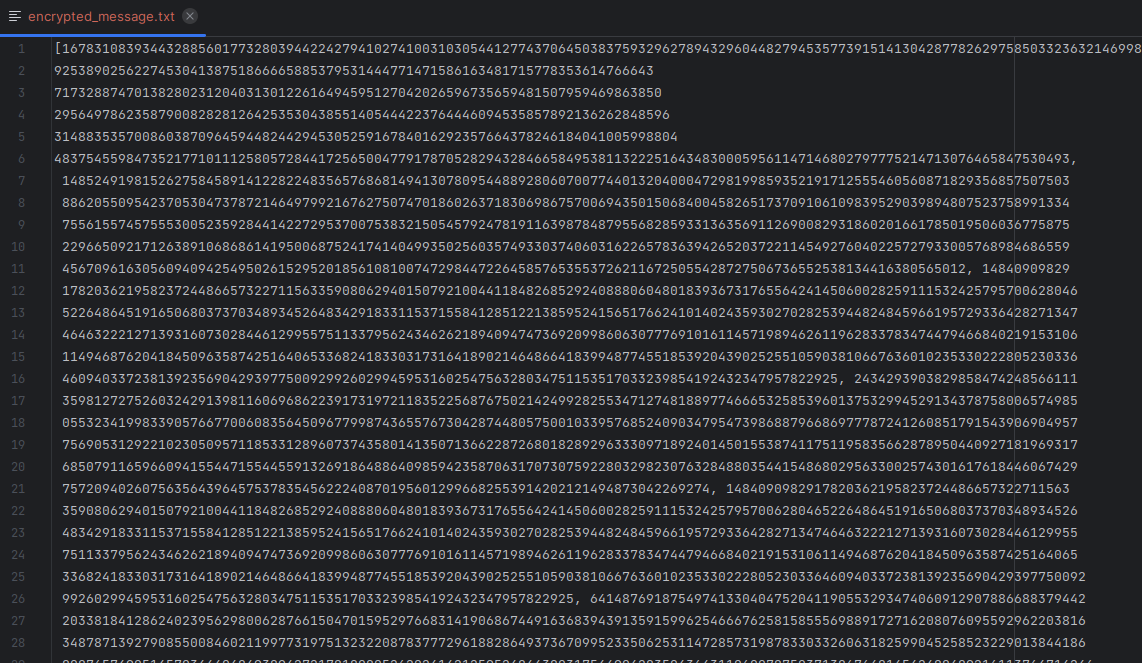


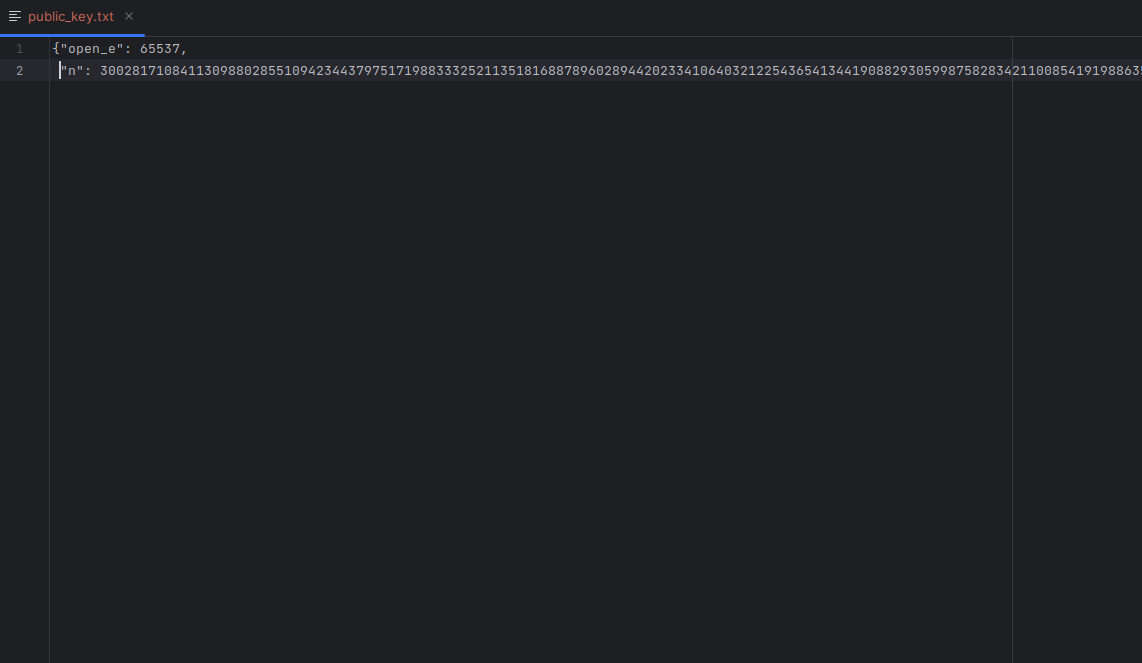
Для нахождения закрытой экспоненты использовался расширенный алгоритм Евклида.

**Пример работы программы**

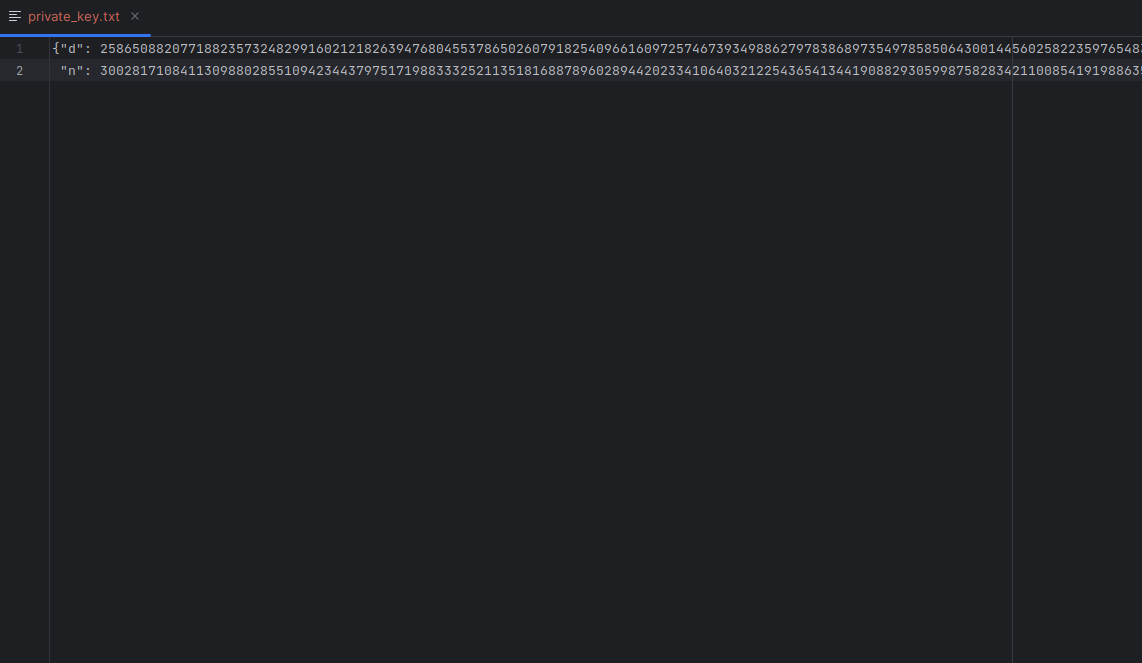


**Часть зашифрованного сообщения**

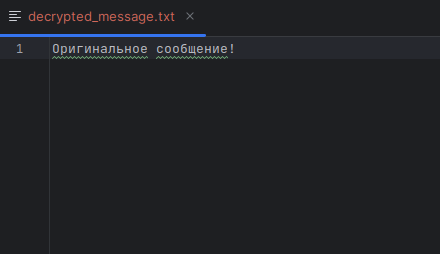
**Открытый ключ**

****

**Закрытый ключ**



**Расшифрованное сообщение**



**Вывод**

В ходе лабораторной работы были реализованы программные средства шифрования и дешифрования текстов при помощи шифрования методом RSA. При длине простых чисел p и q равных 1024 бита каждое соответственно данный метод даёт стойкое шифрование, не поддающееся взлому за разумное время.