ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

ОТЧЕТ  
ПО ЛАБОРАТОРНОЙ РАБОТЕ

ПО ДИСЦИПЛИНЕ

«Защита информации»

Руководители \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Е.А. Харченко

Москва 2023

СПИСОК ИСПОЛНИТЕЛЕЙ

Студ. группы 201-361 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.Е. Сильченко

**Ход работы:**

1. Генерируем открытый и приватный ключ рисунок 1.

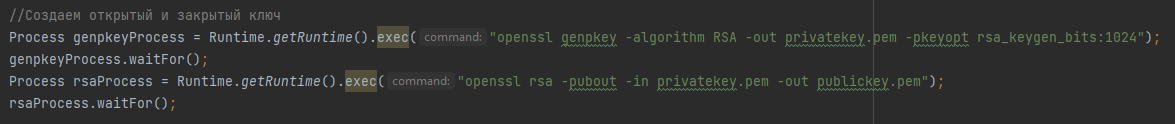


Рисунок 1 – Генерация ключей.

1. Получаем модуль используя команду OpenSSL “openssl rsa -in privatekey.pem -noout -modulus” рисунок 2. Получаем публичную экспоненту рисунок 3.

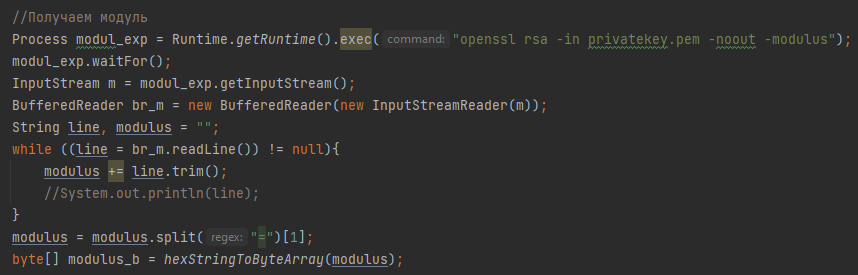


Рисунок 2 – Получаем модуль.

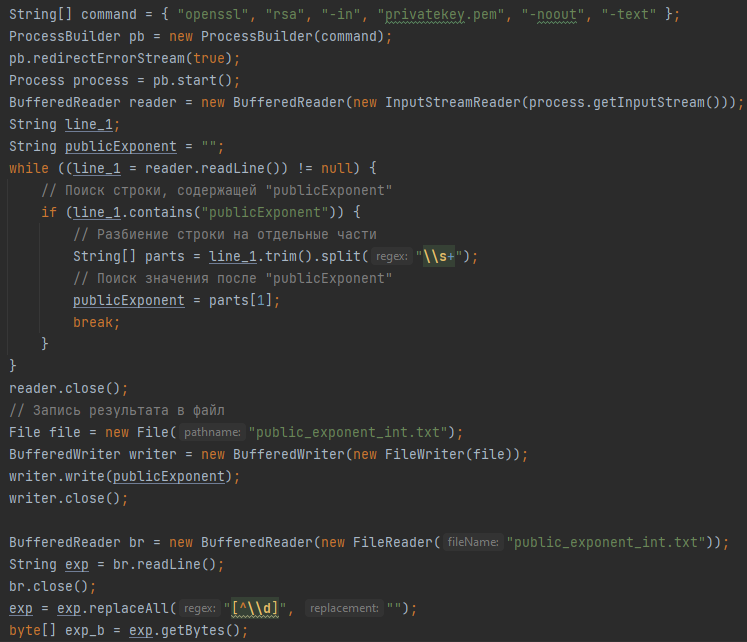


Рисунок 3 – Получение публичной экспоненты.

1. На клиенте генерируем текстовый файл исходя из голоса пользователя рисунок 4.

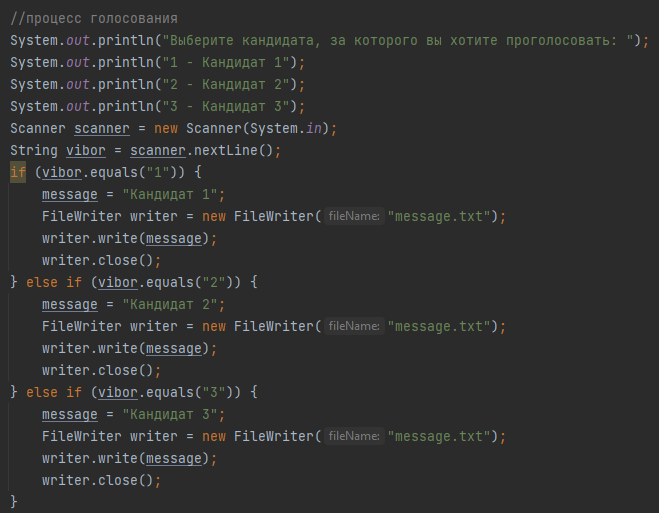


Рисунок 4 – Генерация текстового файла.

1. Генерируем маскирующий множитель r, который взаимно простой с модулем рисунок 5.

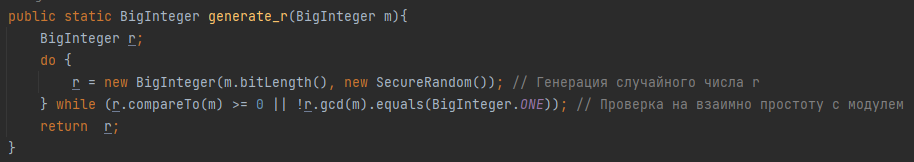


Рисунок 5 – Генерация маскировочного множителя r.

1. Маскируем сообщение, которое было сгенерировано на шаге 3 умножая его на маскирующий множитель в степени публичной экспоненты по модулю рисунок 6. Далее мы отправляем замаскированное сообщение на сервер Б.

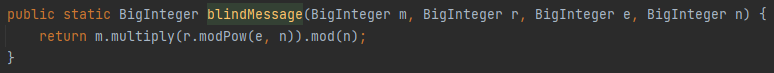


Рисунок 6 – Маскировка сообщения.

1. Получаем частную экспоненту для дальнейшей слепой подписи рисунок 7.

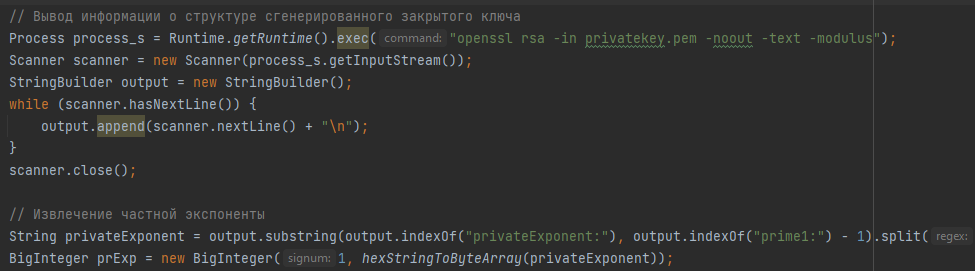


Рисунок 7 – Получение частной экспоненты.

1. Слепая подпись файла рисунок 8. Возводим замаскированное сообщение в степень частной экспоненты по модулю. Далее отправляем подписанное сообщение клиенту.



Рисунок 8 – Слепая подпись файла.

1. Клиент принимает подписанное замаскированное сообщение и снимает маскировку, умножая подписанное замаскированное сообщение на число обратное маскирующему множителю рисунок 9.

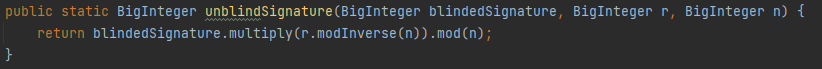


Рисунок 9 – Снятие маскировки.

1. Подписанное сообщение без маскировки, оригинальное сообщение, модуль и публичная экспонента отправляются на сервер С для проверки подписи. Метод для проверки подписи представлен на рисунке 10. Для проверки подписи мы возводим подписанное сообщение в степень публичной экспоненты по модулю и сравниваем результат с исходным сообщением.

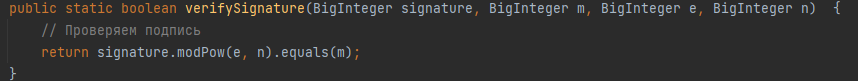


Рисунок 10 – Проверка подписи.

1. В случае удачной проверки происходит подсчет голосов и результат передается на клиент рисунок 11.



Рисунок 11 – Отправка подчитанных голосов клиенту.

**Итог:**

Результат проведенного голосования рисунок 12.

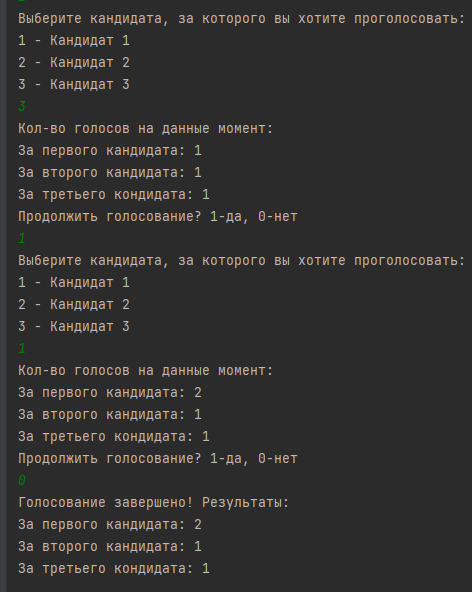


Рисунок 12 – Результат проведенного голосования.