БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Кафедра интеллектуальных информационных технологий

ОТЧЁТ  
по лабораторной работе №7  
по дисциплине

«СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРАМЦИИ В ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ»

Выполнил студент гр. 121701  
Липский Р. В.  
Проверил  
Сальников Д. А.

Минск 2023

**Тема:** установка, использование и анализ специализированных средств

криптографического пакета OpenSSL

**Цель:** установить пакет OpenSSL, сравнить скорость выполнения

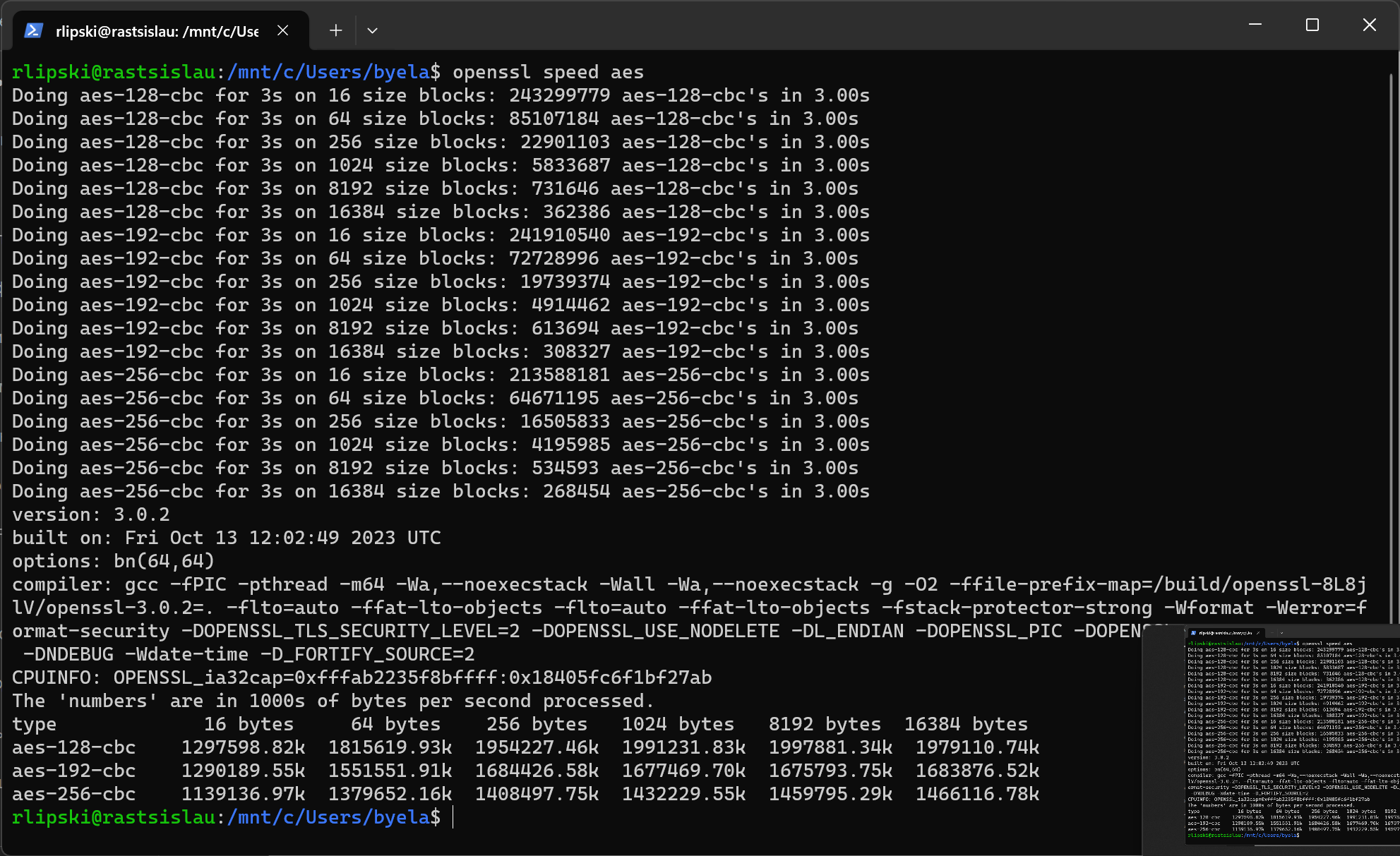
шифрования различных алгоритмов и детально разобраться в компонентах

сертификата X.509

**Задание:**

1. Установить OpenSSL на виртуальную машину (или рабочую версию ОС Windows 7/8/10 пользователя) и ознакомиться с возможностями библиотеки (команда «?»).
2. Выполнить тестирование скорости выполнения различных алгоритмов шифрования.
3. Создать криптографические ключи. Выбрать несколько произвольных файлов и выполнить:
   1. шифрование (зашифрование и расшифрование) посредством различных симметричных алгоритмов;
   2. шифрование (зашифрование и расшифрование) посредством различных асимметричных алгоритмов;
   3. хэширование различных файлов различными алгоритмами (обязательно md5 и sha1).
4. Создать самоподписанный сертификат X509. Изучить состав сертификата и назначение его компонентов.
5. Оформить отчет. В отчет поместить:
   1. результаты тестирования производительности;
   2. времена шифрования (выполнить сравнительную оценку скорости шифрования DES и AES, AES и RSA, объяснить полученные результаты);
   3. полученные хэш значения;
   4. сертификат с описанием его компонентов.

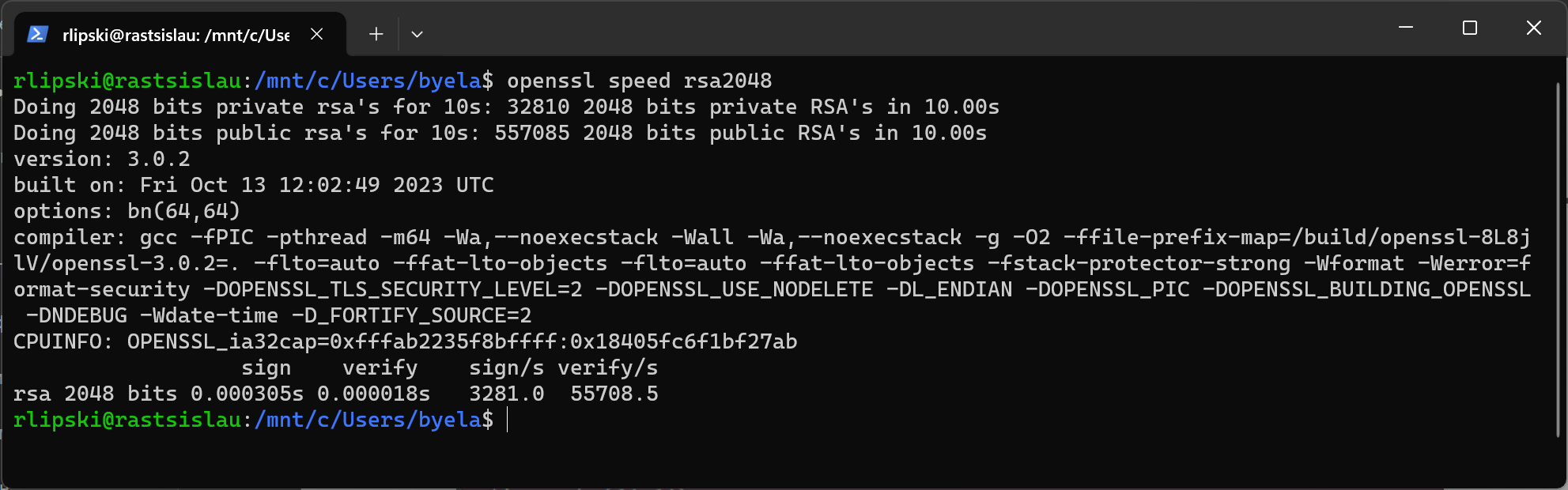
Протестируем несколько алгоритмов: AES, RSA2048, SHA256.



Вывод разделен на разделы для разных алгоритмов шифрования (**aes-128-cbc**, **aes-192-cbc** и **aes-256-cbc**) и различных размеров блоков (16 байт, 64 байта, 256 байт, 1024 байта, 8192 байта и 16384 байта). Числа под каждым разделом указывают, сколько килобайт данных может быть обработано в секунду для

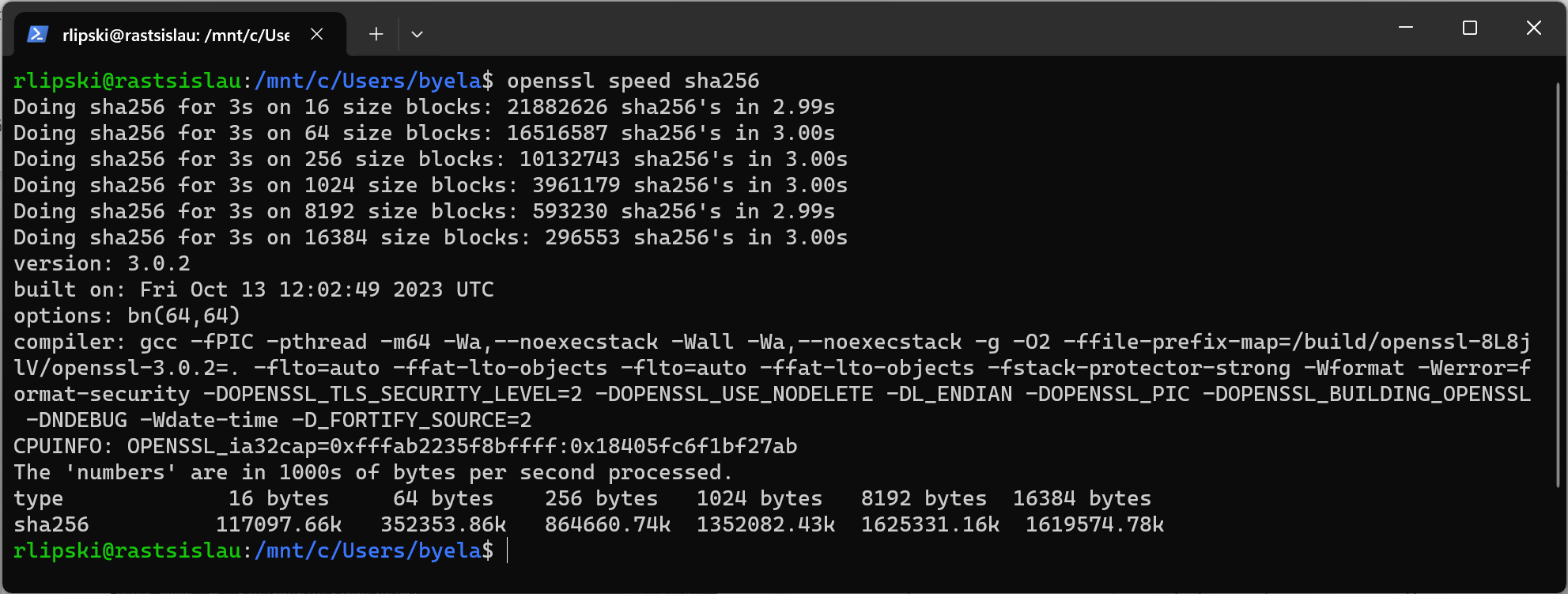
данного алгоритма и размера блока.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Тип | 16 байт | 64 байта | 256 байт | 1024 байта | 8192 байта | 16384 байта |
| Aes-128-cbc | 1297598 | 1815619 | 1954227 | 1991231 | 1997881 | 1979110 |
| Aes-192-cbc | 1290189 | 1551551 | 1684426 | 1677469 | 1675793 | 1683876 |
| Aes-256-cbc | 1139136 | 1379652 | 1408497 | 1432229 | 1459795 | 1466116 |



Сначала мы выполняем операции с закрытыми ключами длиной 2048 бит в течение 10 секунд. За это время было выполнено 32,810 операций с закрытыми ключами длиной 2048 бит, и это заняло 10 секунд. Далее мы выполняем операции с открытыми ключами длиной 2048 бит в течение 10 секунд. За это время было выполнено 557,085 операции с открытыми ключами длиной 2048 бит, и это заняло 10 секунд. В последней строке указаны результаты теста для операций RSA с ключами длиной 2048 бит:

1. sign - Время, затраченное на операцию подписи (закрытый ключ), которое составляет приблизительно 0.000305 секунд.
2. verify - Время, затраченное на операцию проверки (открытый ключ), которое составляет приблизительно 0.000018 секунд.
3. sign/s - Скорость операций подписи, которая составляет приблизительно 3,281 операций в секунду.
4. verify/s - Скорость операций проверки, которая составляет приблизительно 55708.5 операций в секунду



В начале производятся операции SHA-256 с блоками размером 16, 64, 256 и т.

д. байт. Например, 3 секунды было обработано 24,315,579 хэшей SHA-256 с

блоком 16 байт. Затем следуют сведения о версии OpenSSL, настройках

компиляции и информация о вашем процессоре. В конце вывода приведены

результаты производительности операции SHA-256 для разных размеров

блоков, измеряемые в тысячах байт в секунду (KB/s):

1. Для блоков размером 16 байт скорость составляет примерно 129,683.09 KB/s.
2. Для блоков размером 64 байта скорость составляет примерно 398,339.14 KB/s.
3. Для блоков размером 256 байт скорость составляет примерно 941,508.27 KB/s.
4. Для блоков размером 1024 байта скорость составляет примерно 1,436,645.97 KB/s.
5. Для блоков размером 8192 байта скорость составляет примерно 1,688,734.38 KB/s.
6. Для блоков размером 16384 байта скорость составляет примерно 1,699,397.63 KB/s.

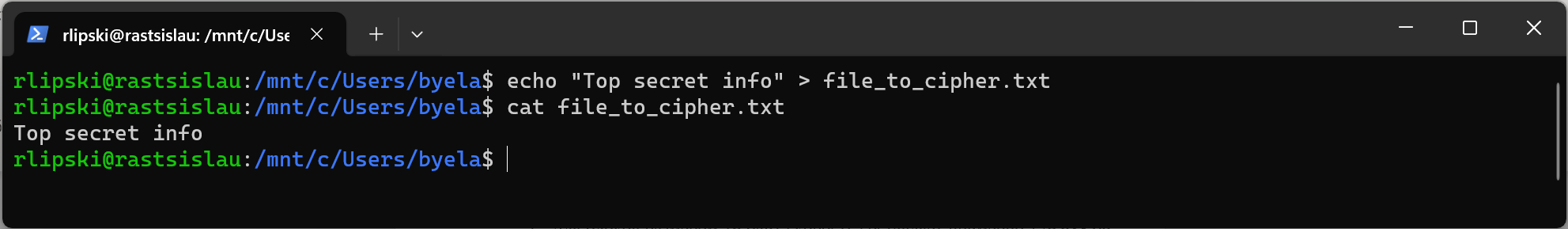
Из этих данных можно сделать общий вывод: если вам нужно шифрование данных, AES может быть более быстрым вариантом, особенно при использовании AES-256-CBC. Если требуется хэширование данных, SHA-256 предоставляет приемлемую скорость и является стандартным выбором для хэширования. RSA-2048, как асимметричный алгоритм, будет медленнее, чем симметричное шифрование (AES) и хэширование (SHA-256). RSA обычно используется для подписи и проверки цифровых подписей, а не для шифрования больших объемов данных.

**Сравнительная оценка скорости шифрования DES, AES, RSA:**

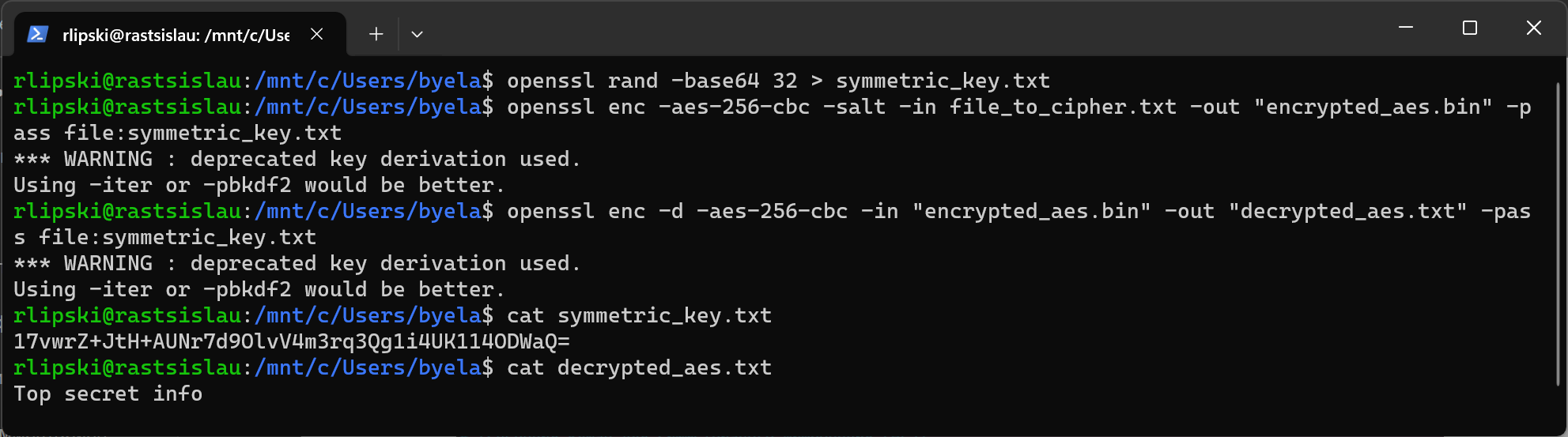
AES обеспечивает хороший баланс между безопасностью и производительностью. Скорость зависит от длины ключа, и более длинные ключи требуют больше времени для обработки. DES уступает по скорости и безопасности по сравнению с AES, поэтому не рекомендуется для использования. RSA медленнее симметричных алгоритмов, и его скорость зависит от длины ключа.

**Создание криптографических ключей:**

Создадим файл, который мы хотим зашифровать:

****

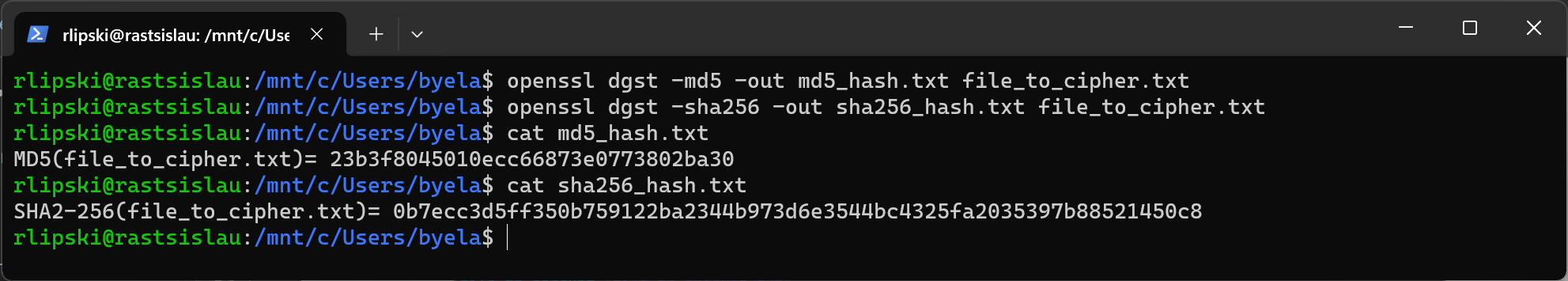
Для AES создадим симметричный ключ, зашифруем и расшифруем файл:



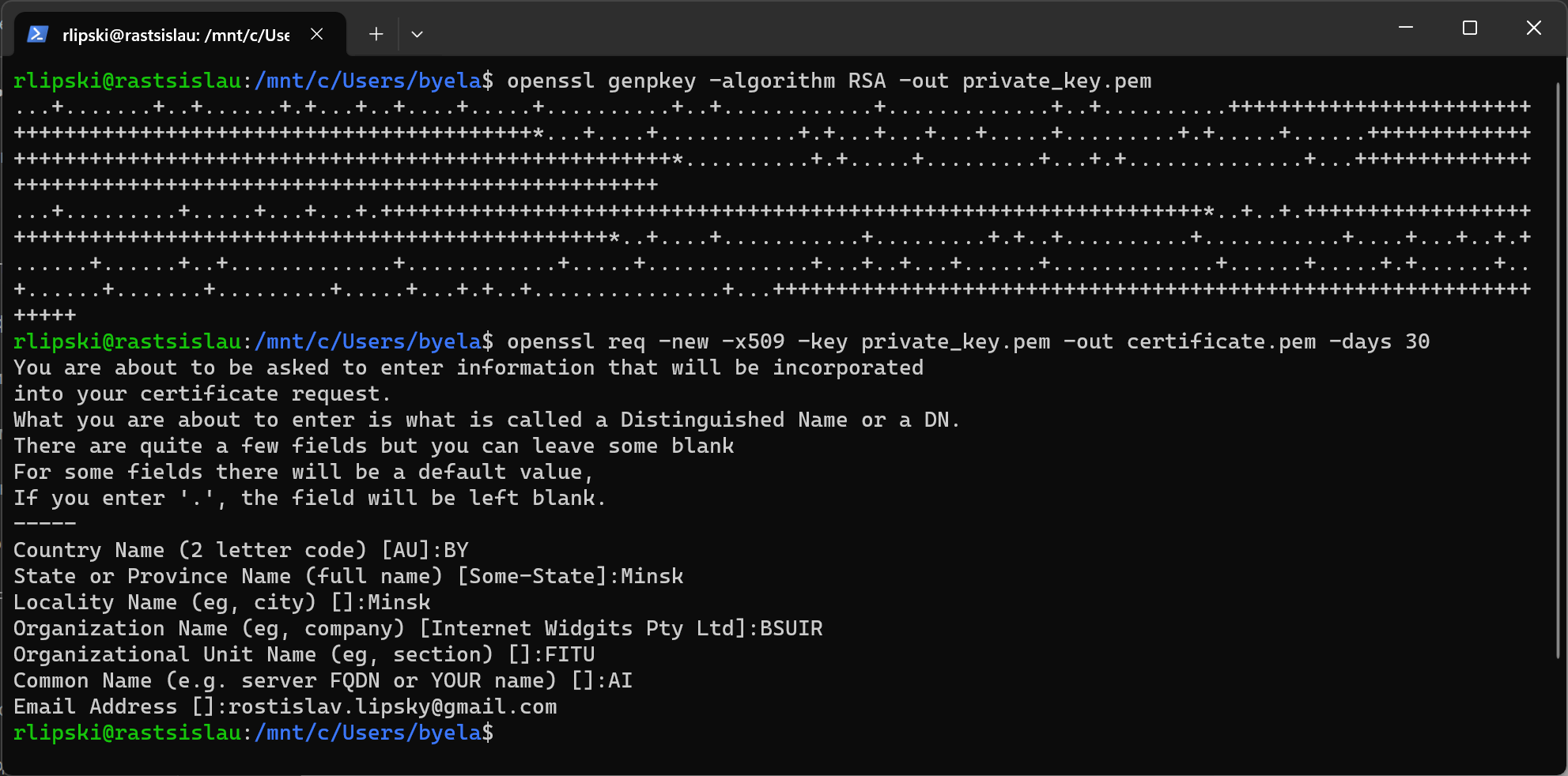
Для RSA создадим публичный и закрытый ключи, зашифруем и расшифруем файл:



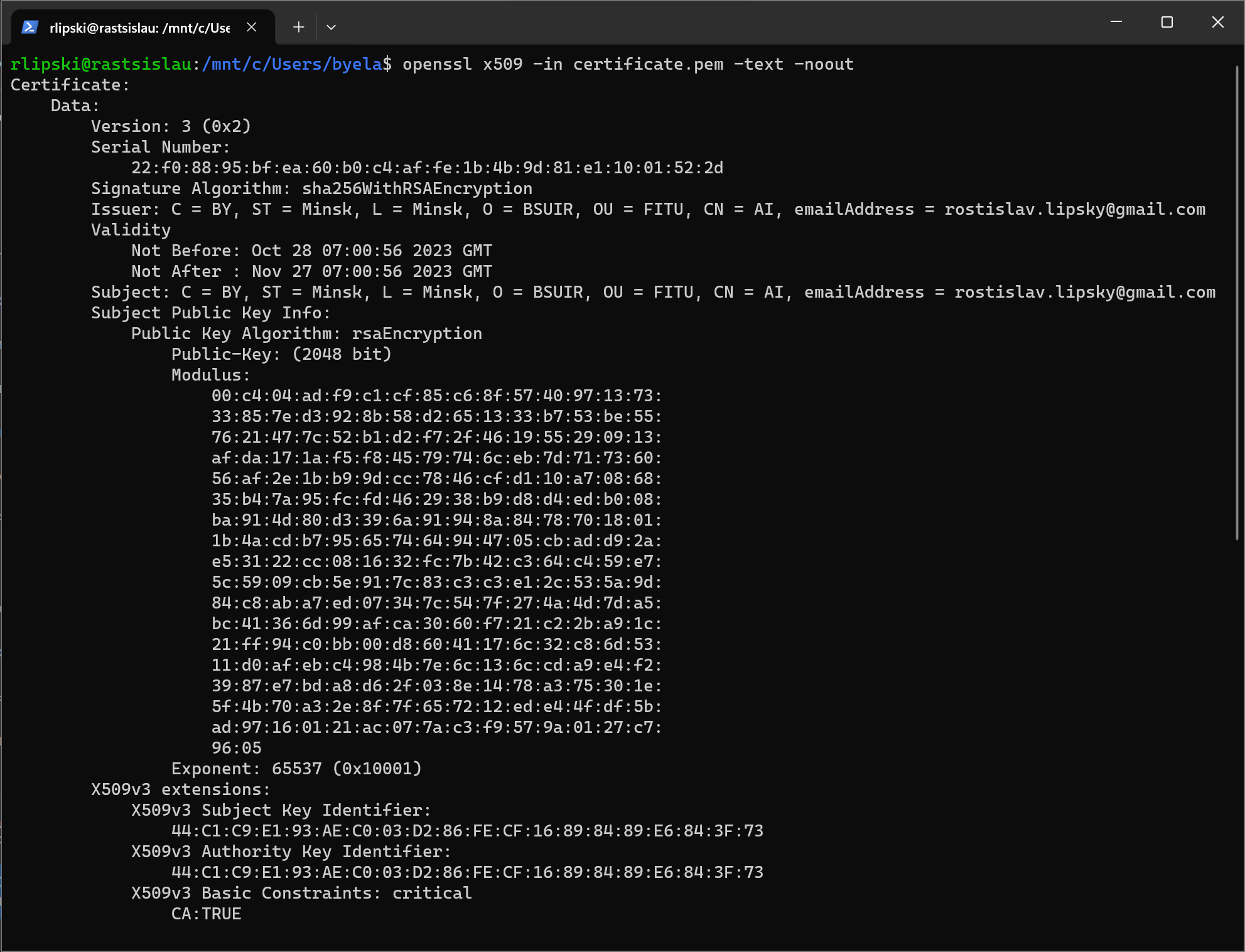
Захешируем файл при помощи MD5 и SHA256:



**Создание самоподписанного сертификата X.509:**



Просмотрим сертификат:



**Вывод:**

Мы изучили криптографическую библиотеку OpenSSL: узнали какие алгоритмы шифрования она поддерживает, оценили скорость выполнения нескольких алгоритмов и выполнили сравнительную оценку различных алгоритмов шифрования. Также мы самостоятельно зашифровали и дешифрование данных с помощью OpenSSL библиотеки, а также самостоятельно подписали сертификат X.509 и изучили его компоненты.