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. 321701  
Романов К.В.  
Проверил  
Сальников Д. А.

**Минск 2025**

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

криптографического пакета OpenSSL

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

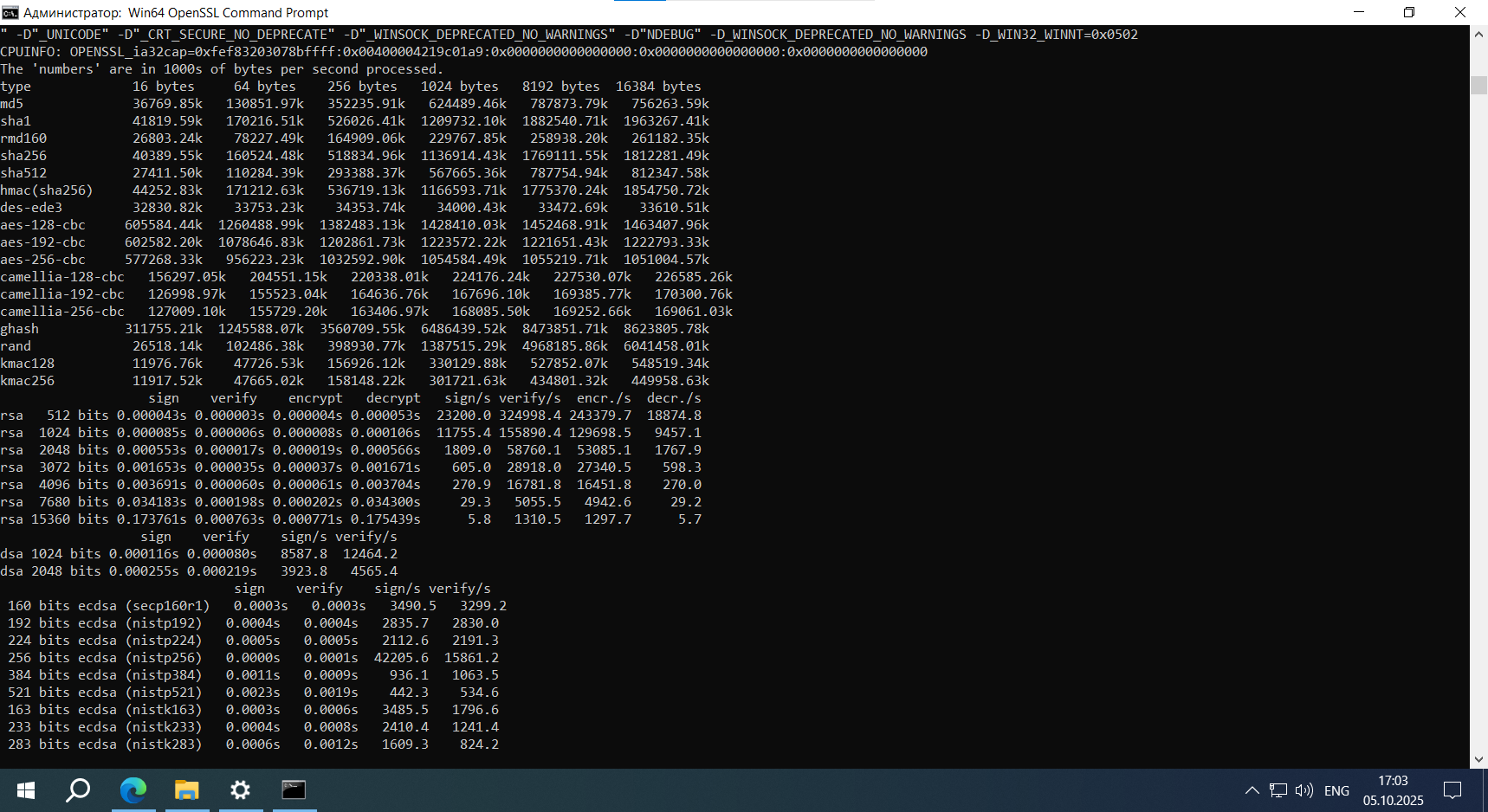
шифрования различных алгоритмов и детально разобраться в компонентах

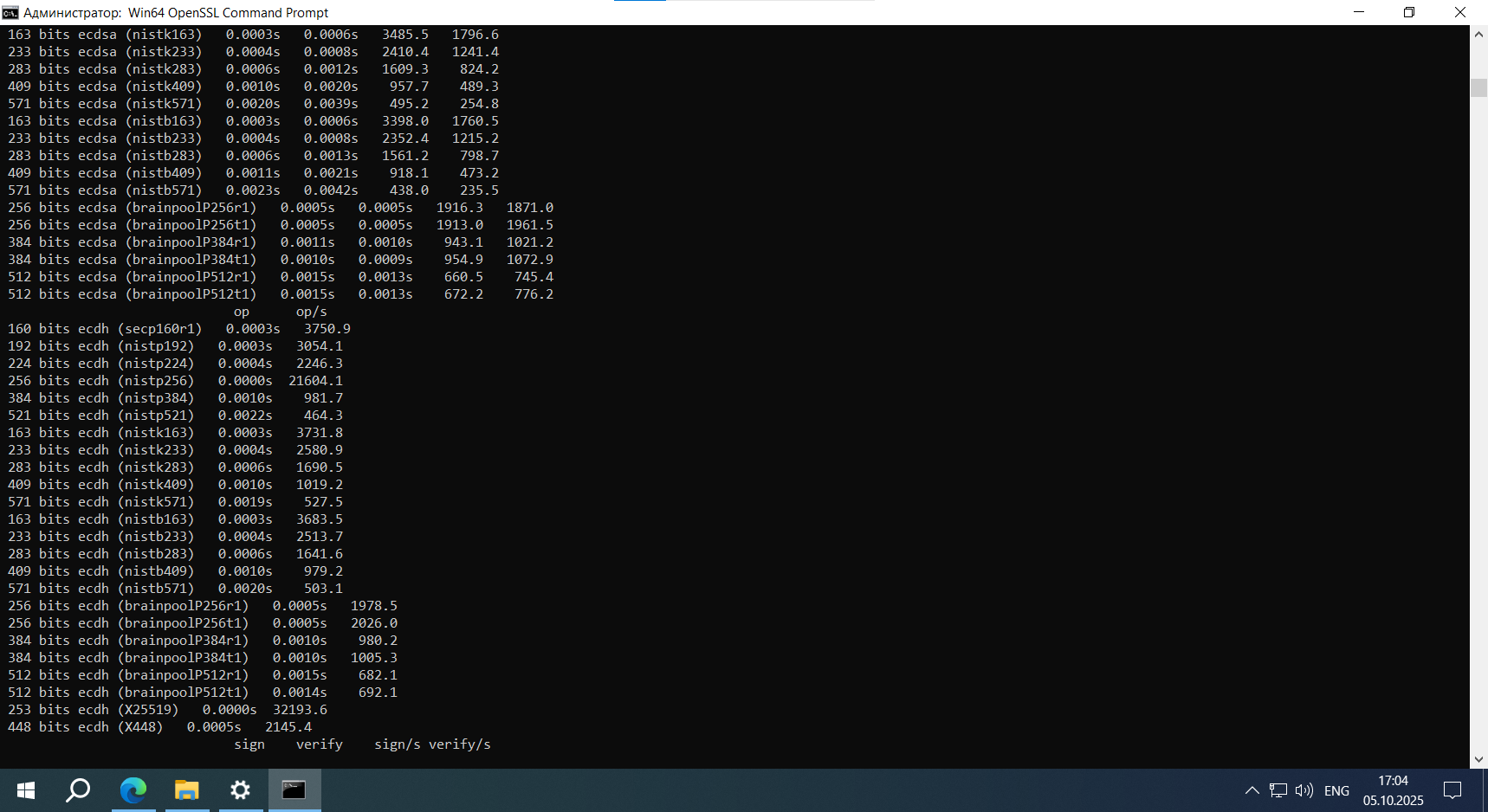
сертификата X.509

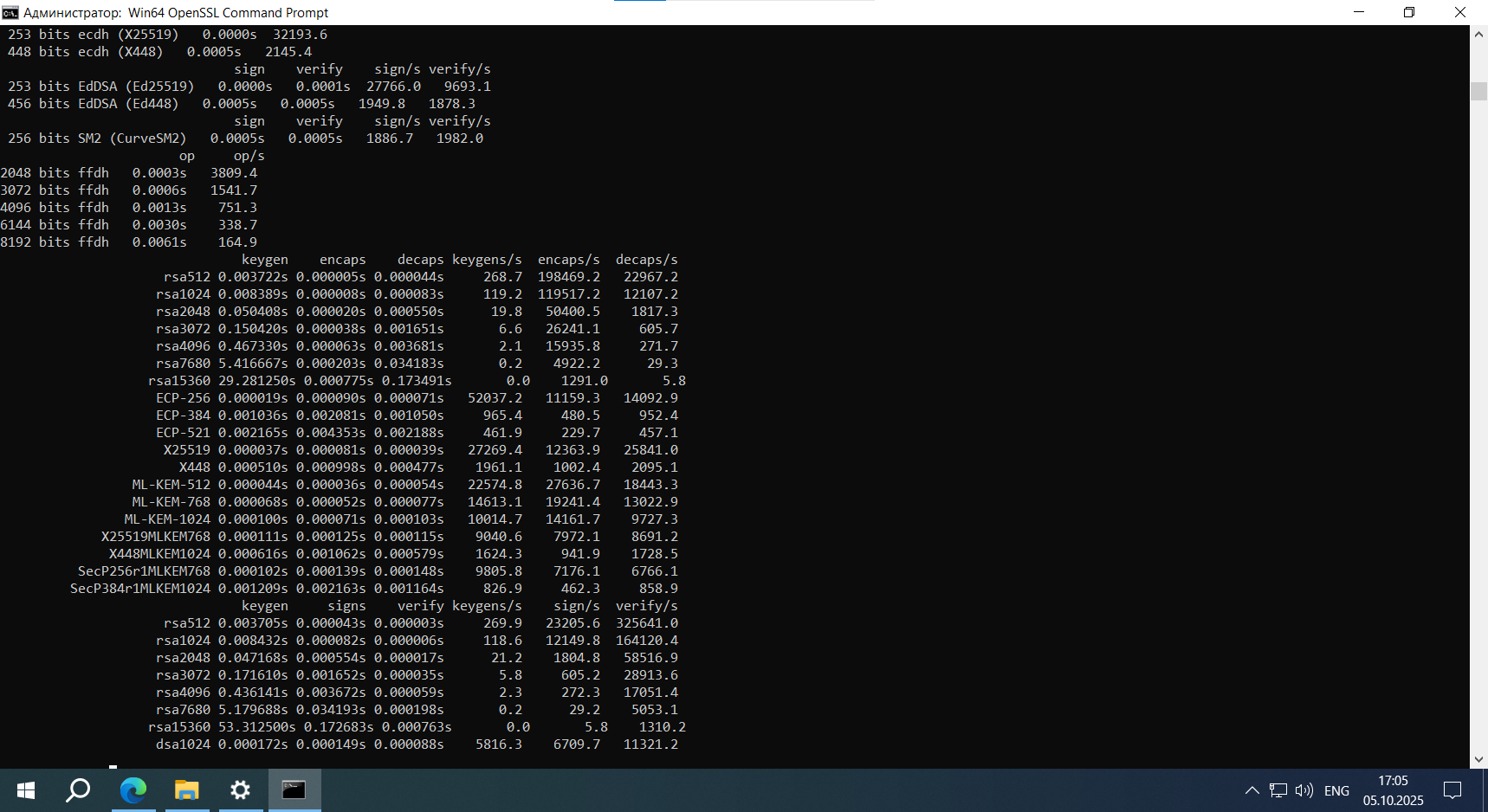
**Задание:**

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 все алгоритмы.

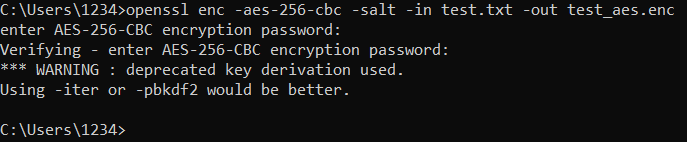


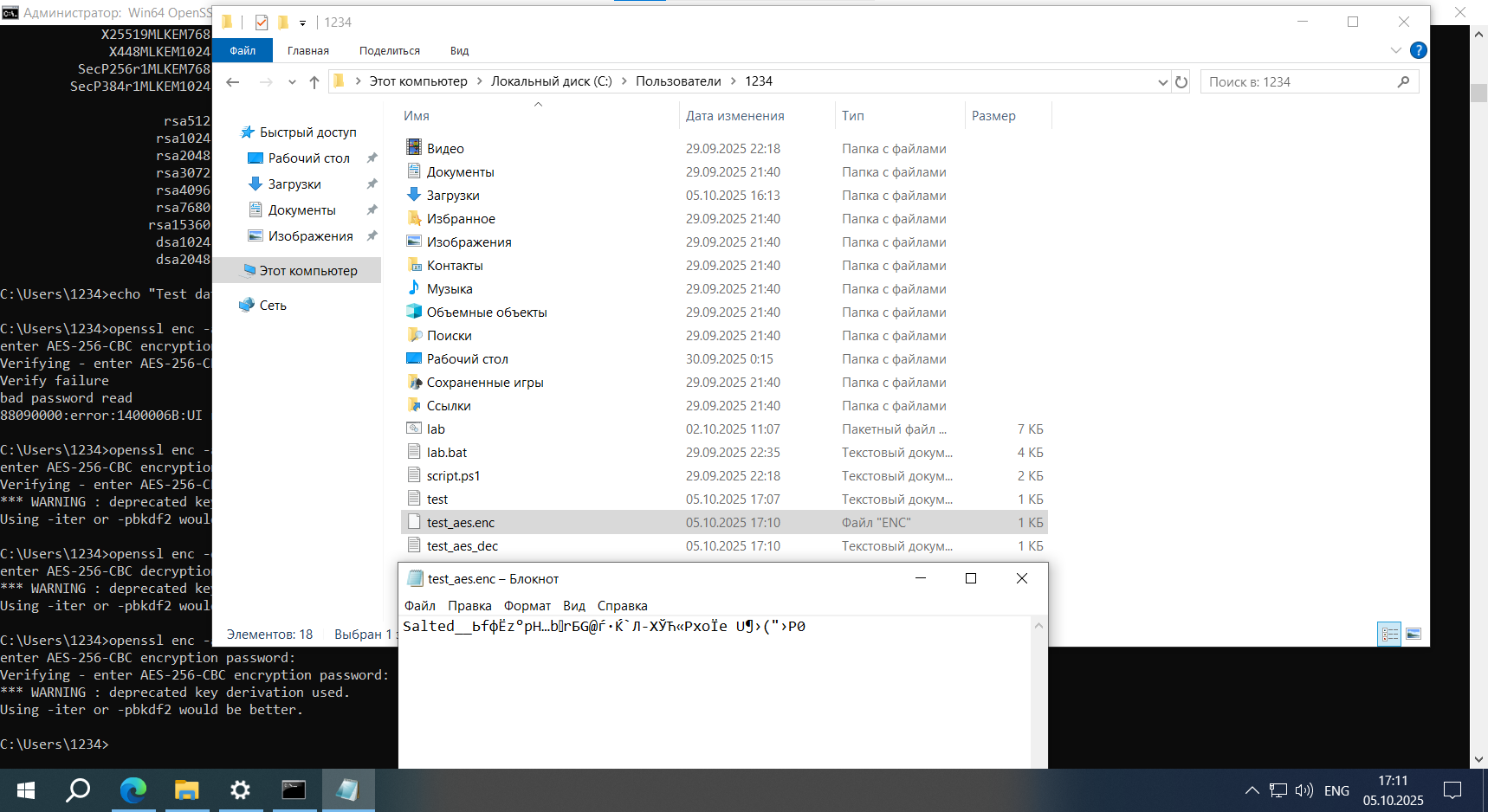




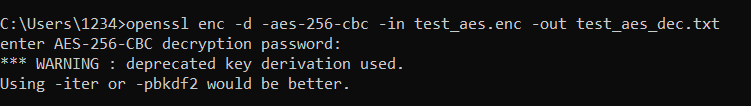
**Шифрование:**

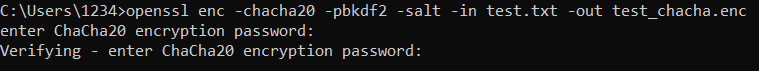
Зашифруем файл с помощью AES:

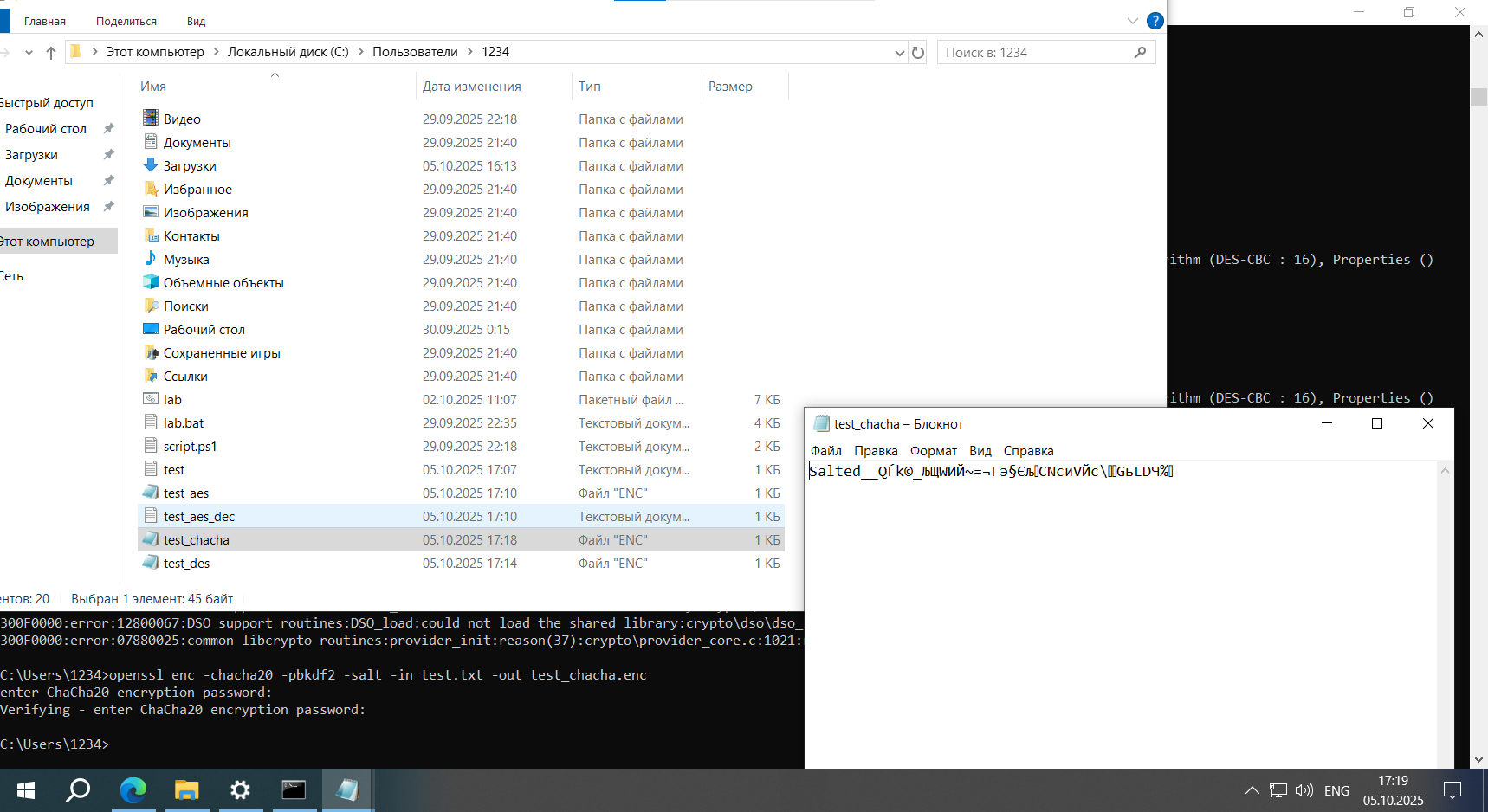


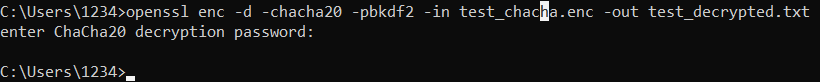


Расшифрем:

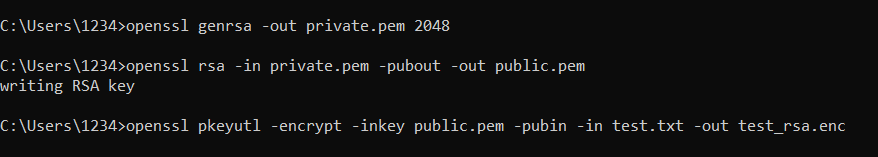
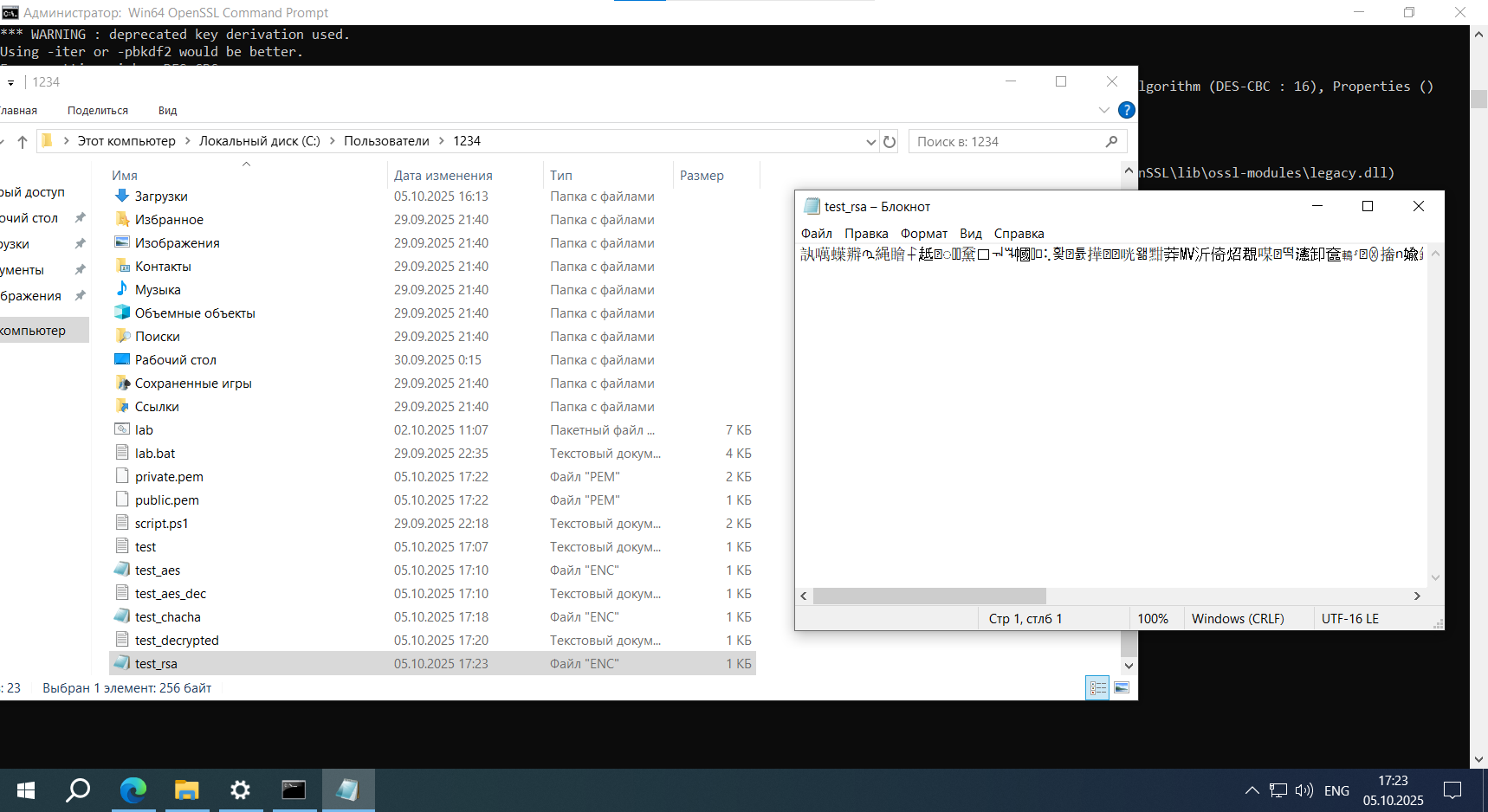


Для ChaCha20:  




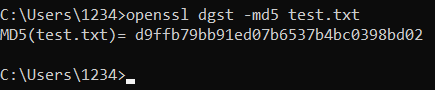


Ассиметричное шифрование(RSA):

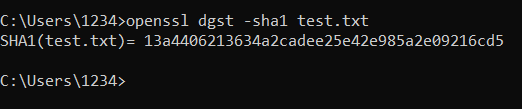
  
  
  
  
  


**Хэширование**

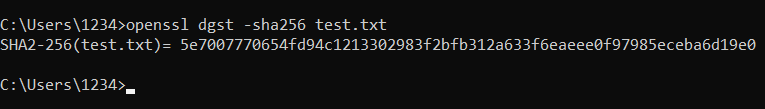
Для MD5:



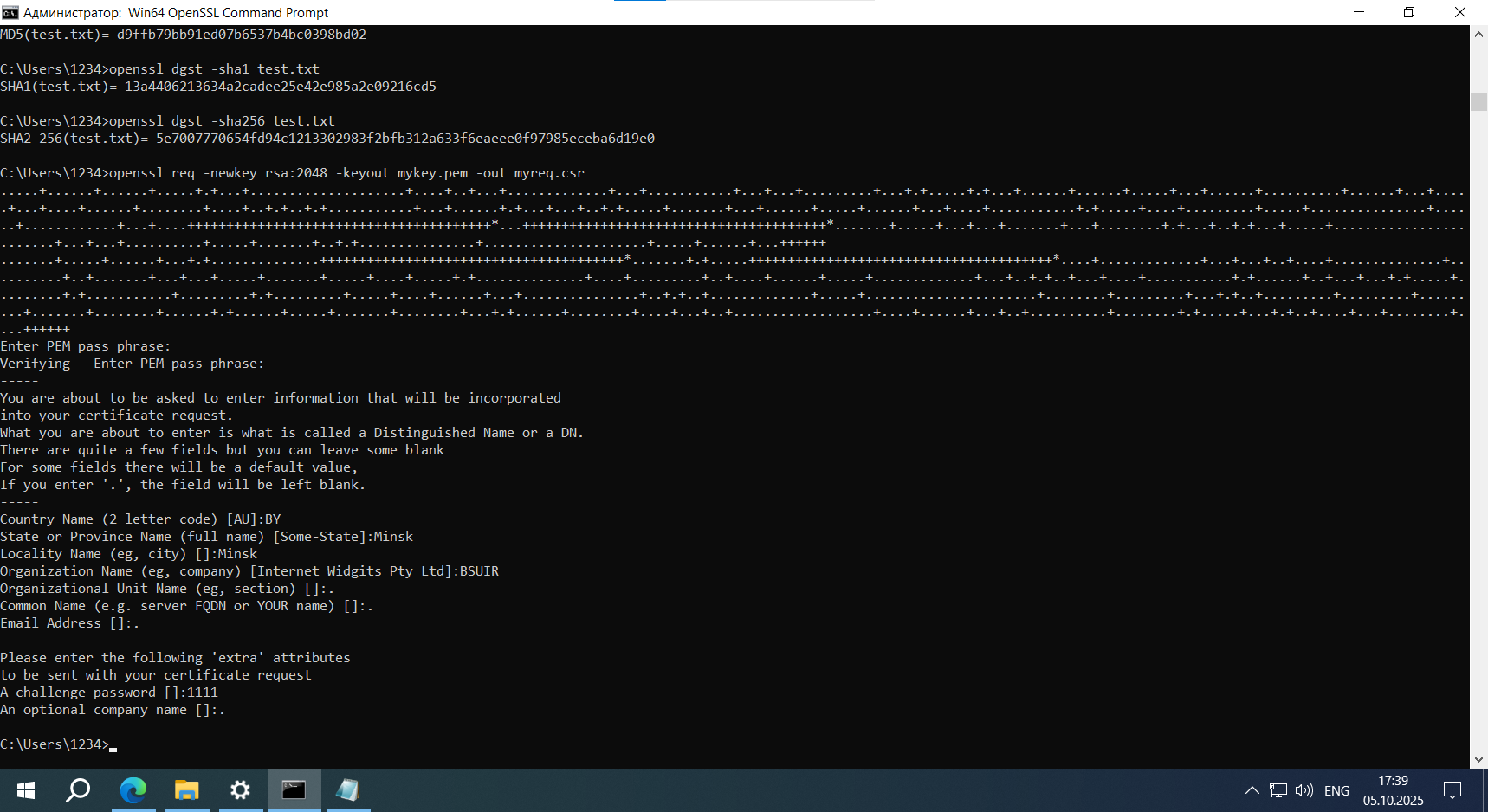
Для SHA1:

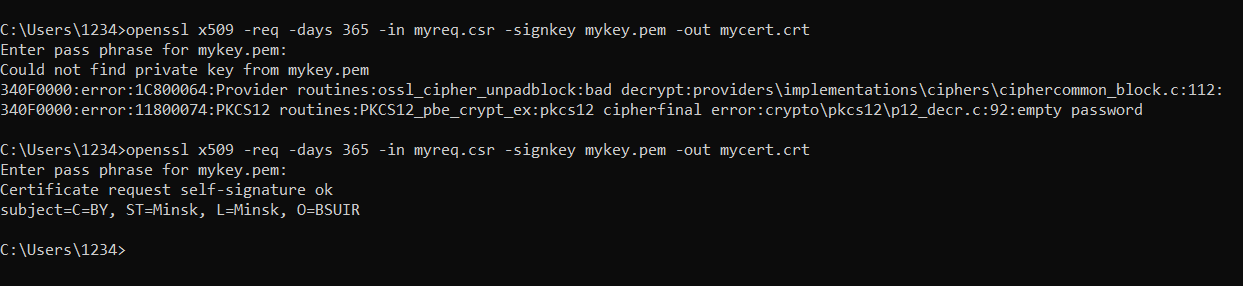


Для других алгоритмов (например, SHA256):

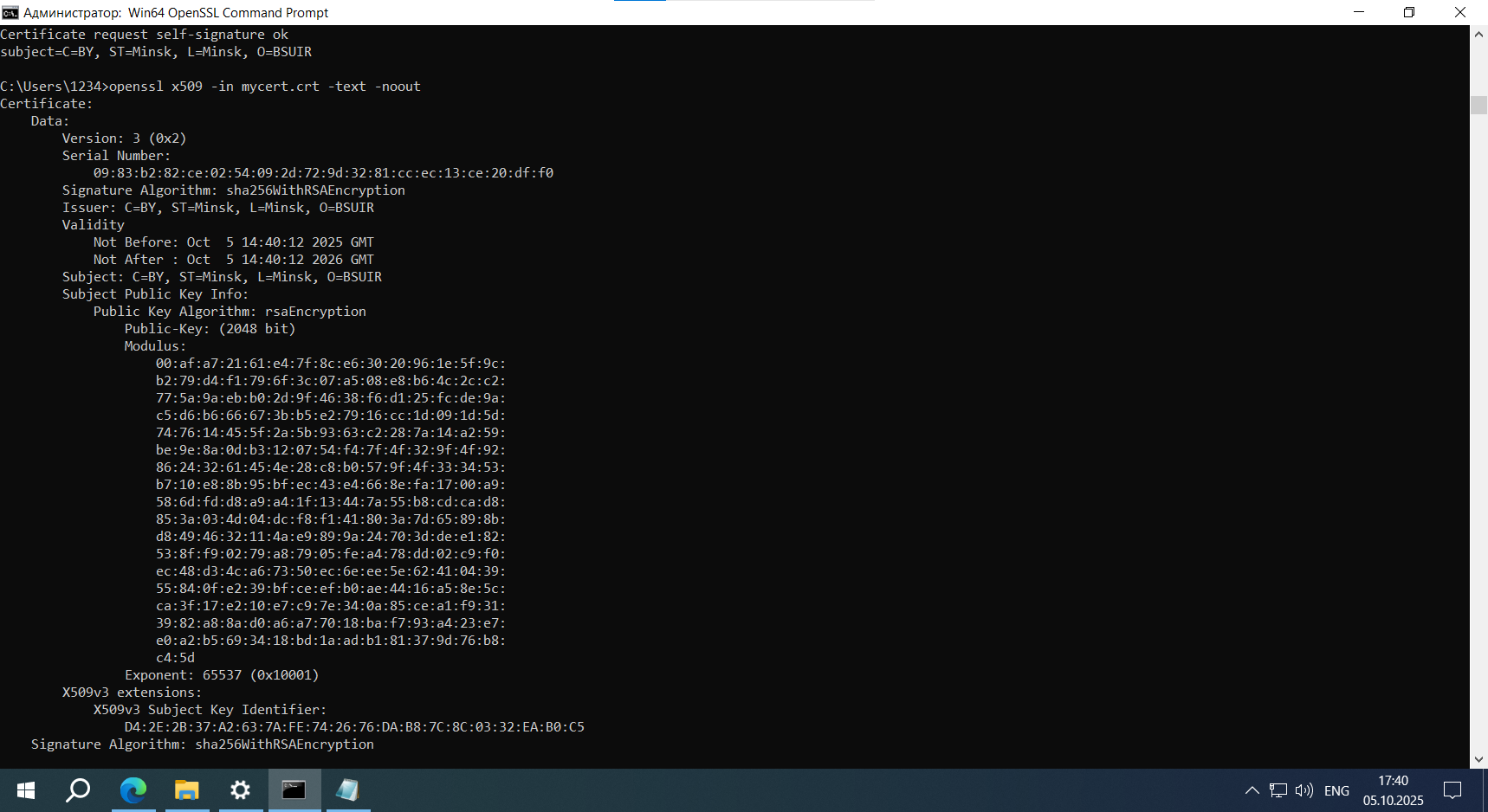


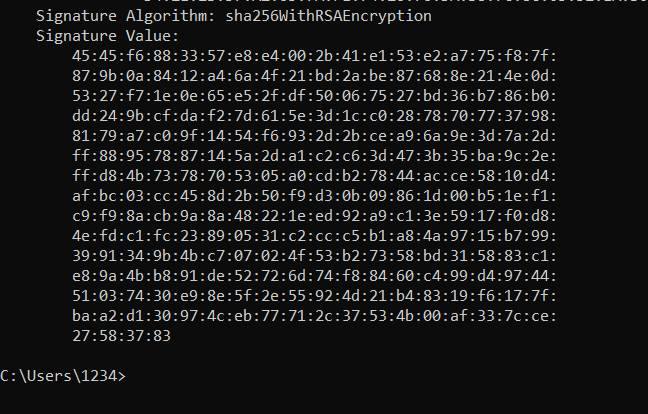
**Создание самоподписанного сертификата X.509:**





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.