**Учреждение образования**

**«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»**

**Кафедра интеллектуальных информационных технологий**

**Лабораторная работа №7 по курсу «СиМЗИИС» на тему:**

**«Установка, использование и анализ специализированных средств криптографического пакета OpenSSL»**

Выполнил студент: Исамиддинов Ботир

Группы: ***121731***

Проверил: Сальников Д.А

**МИНСК**

2023

**Задания**

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:

а) шифрование (зашифрование и расшифрование) посредством различных симметричных алгоритмов;

б) шифрование (зашифрование и расшифрование) посредством различных асимметричных алгоритмов;

в) 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:

а) результаты тестирования производительности;

б) времена шифрования (выполнить сравнительную оценку скорости шифрования DES и AES, AES и RSA, объяснить полученные результаты);

в) полученные хэш значения;

г) сертификат с описанием его компонентов.

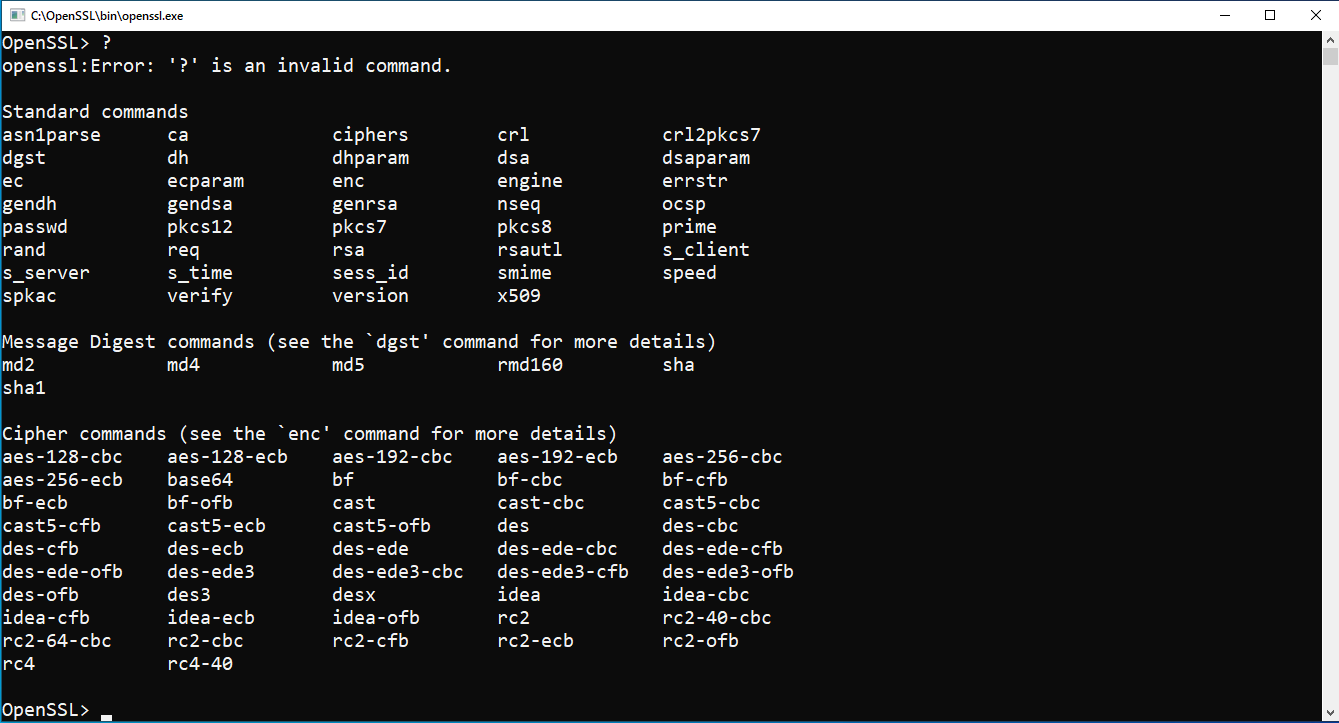
Для выполнения задания использовать:

1) ПК с установленной с ОС Windows 7 или более поздних версий, либо VMWare Player/Workstation с образом виртуальной машины с ОС Windows 7/8/10 по выбору обучаемого. Можно также использовать ПК под управлением Linux/Unix

2) Пакет Open SSL 0.9.8 или новее.

**Задание 1**

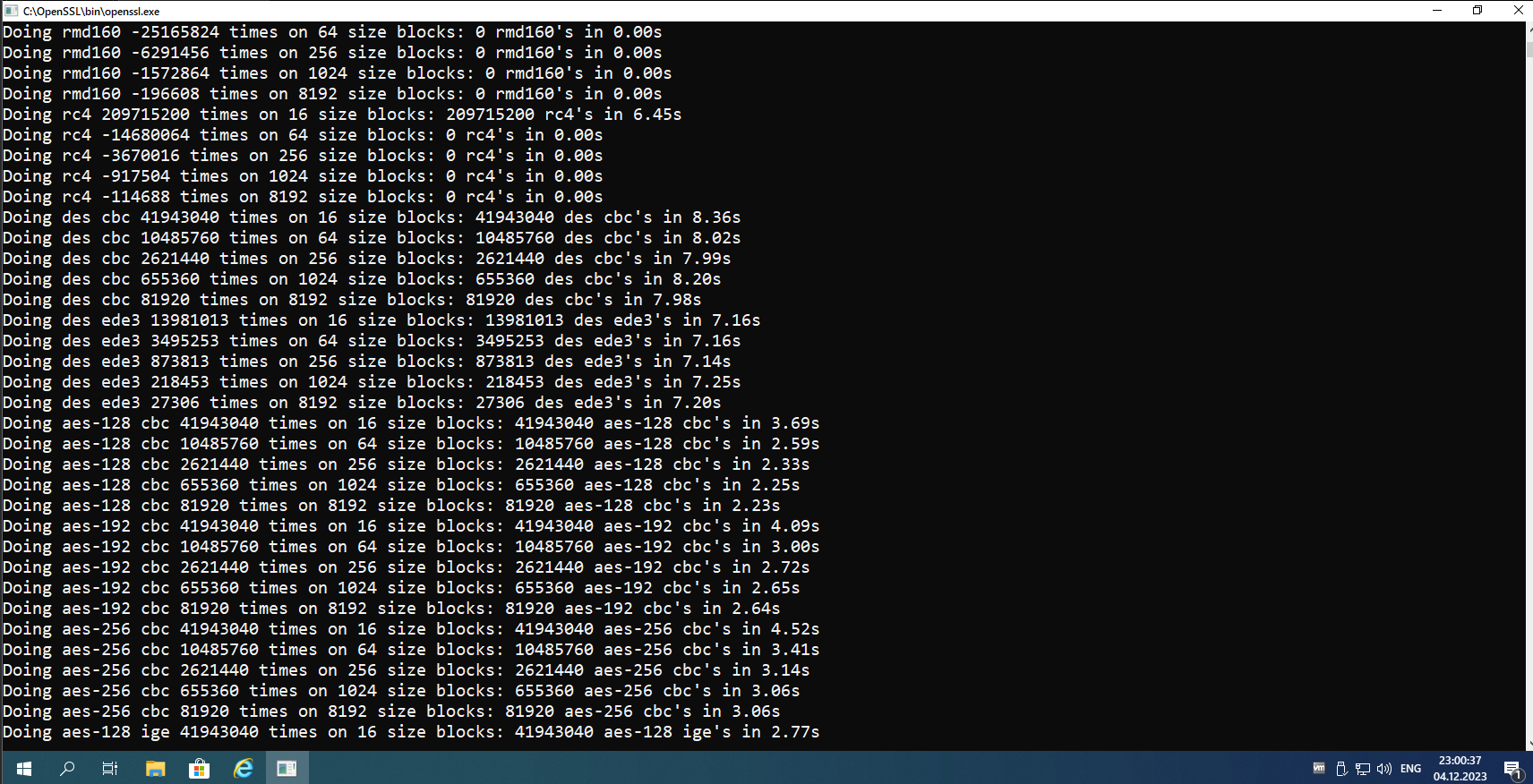
1) Установить OpenSSL на виртуальную машину (или рабочую версию ОС Windows 7/8/10 пользователя) и ознакомиться с возможностями библиотеки (команда «?»).



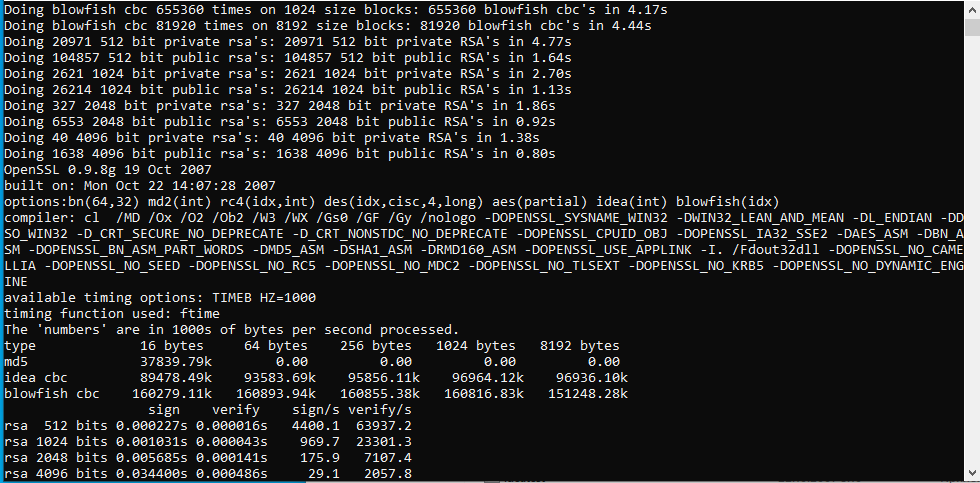
Результат выполнения команды «help»

**Задание 2**

2) Выполнить тестирование скорости выполнения различных алгоритмов шифрования.



Результат тестирования различных алгоритмов и режимов шифрования



При проверки скорости на режимах speed md5 rsa idea blowfish des 3des sha1.выводится общая скорость работы различных алгоритмов(в 1000-х байт в секунду), для обработки различной длины блоков.

**Задание 3**

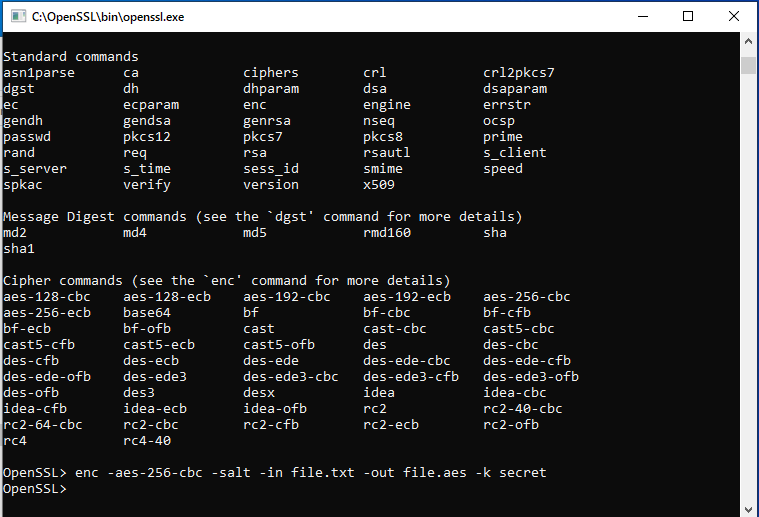
3) Создать криптографические ключи. Выбрать несколько произвольных файлов и выполнить:

а) шифрование (зашифрование и расшифрование) посредством различных симметричных алгоритмов;

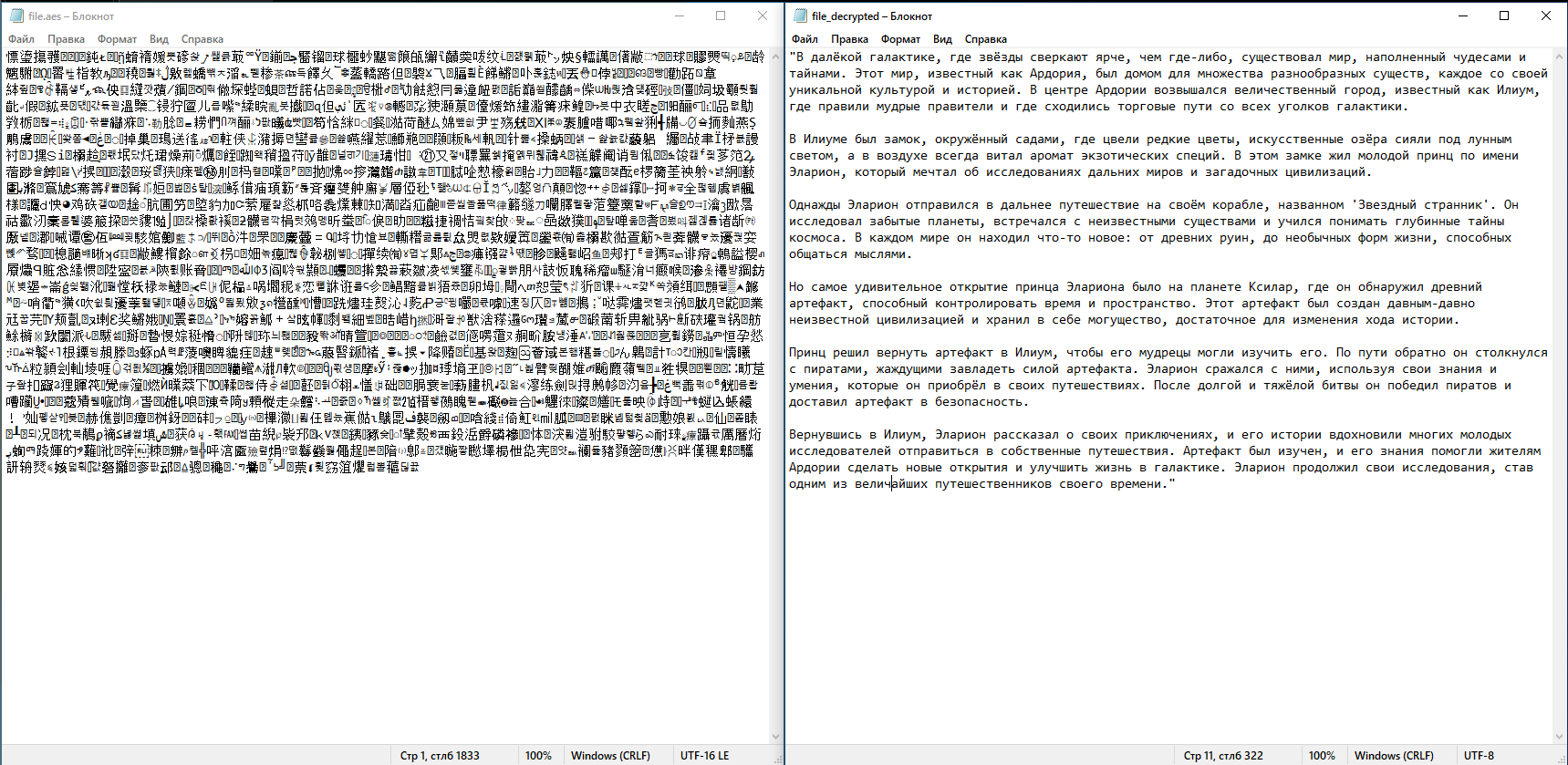
б) шифрование (зашифрование и расшифрование) посредством различных асимметричных алгоритмов;

в) хэширование различных файлов различными алгоритмами (обязательно md5 и sha1).

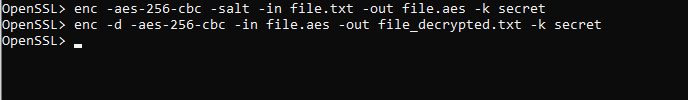
а) шифрование (зашифрование и расшифрование) посредством различных симметричных алгоритмов;

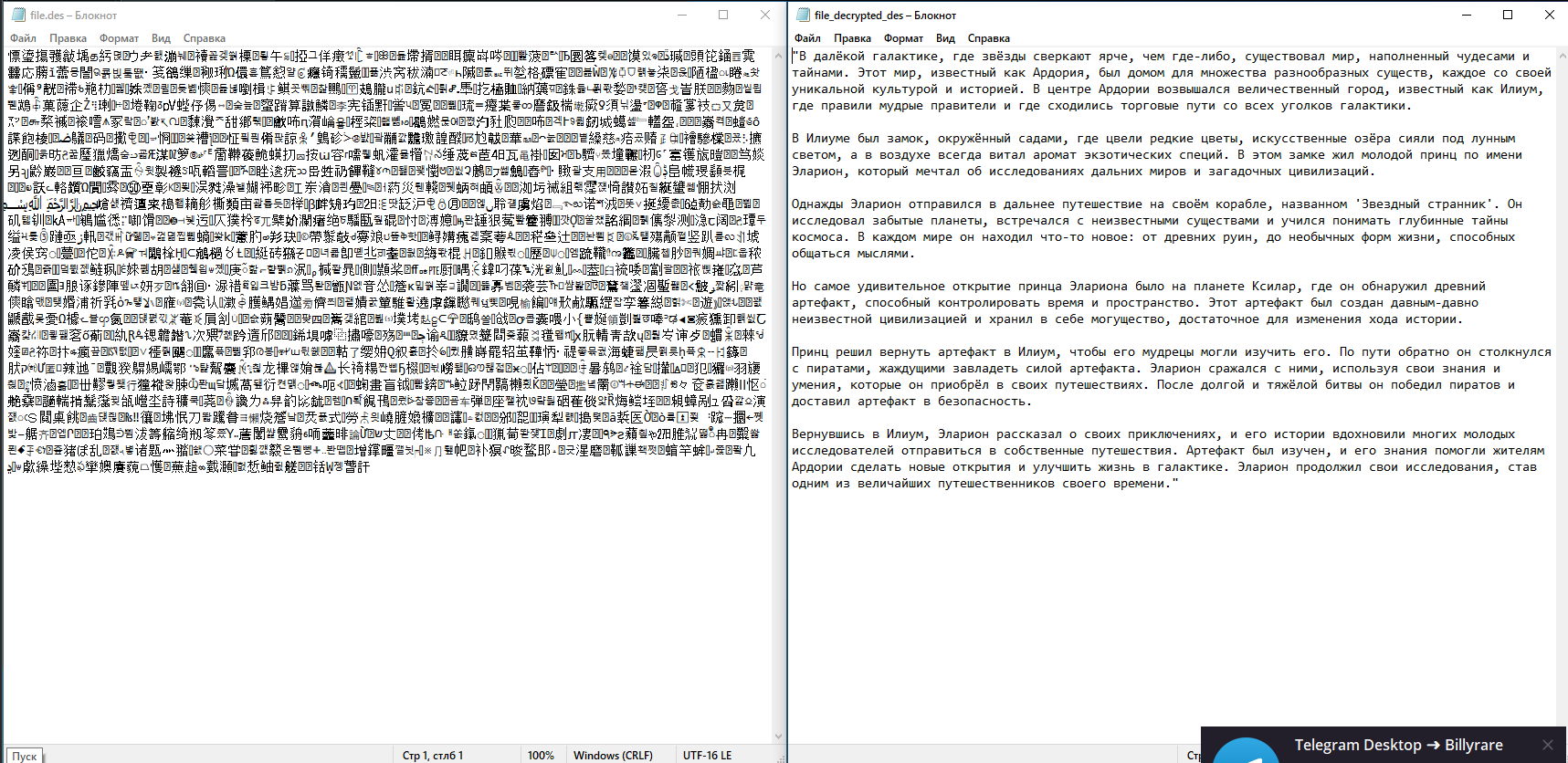


Зашифровка стандартом aes режим cbc и размером 256bit текстового файла и выходящий зашифрованный file.aes

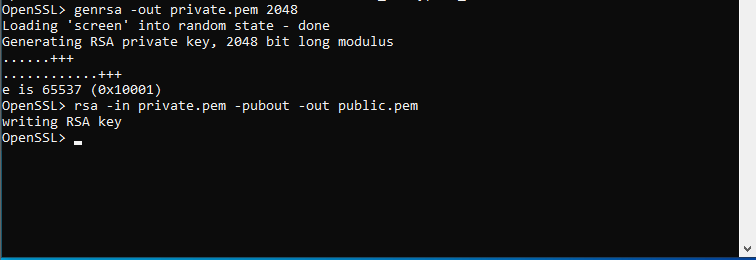


Расшифровка зашифрованного file.txt – file.aes to file\_decrypted.txt

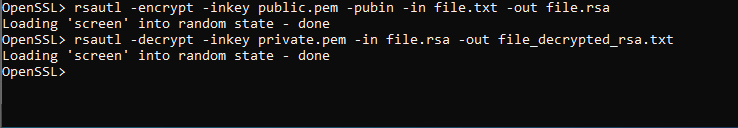




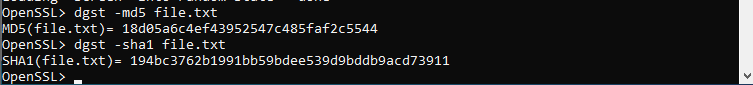
Расшифровка зашифровка file.txt – стандартом des



Генерация ключей RSA



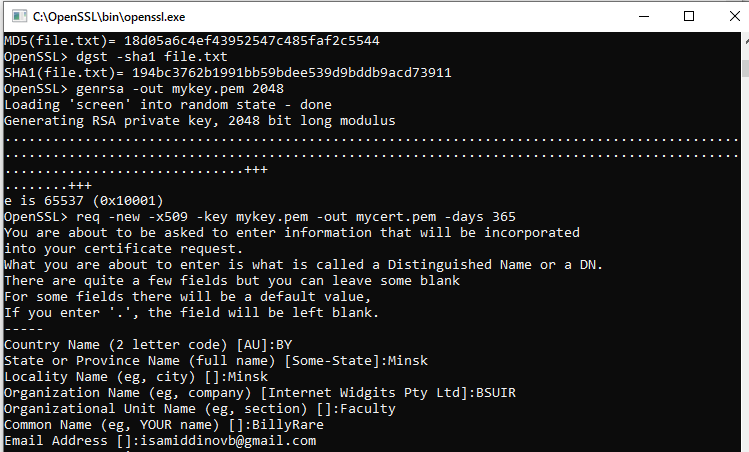
RSA шифрование – расшифрование текстового файла с размером ключа 2048



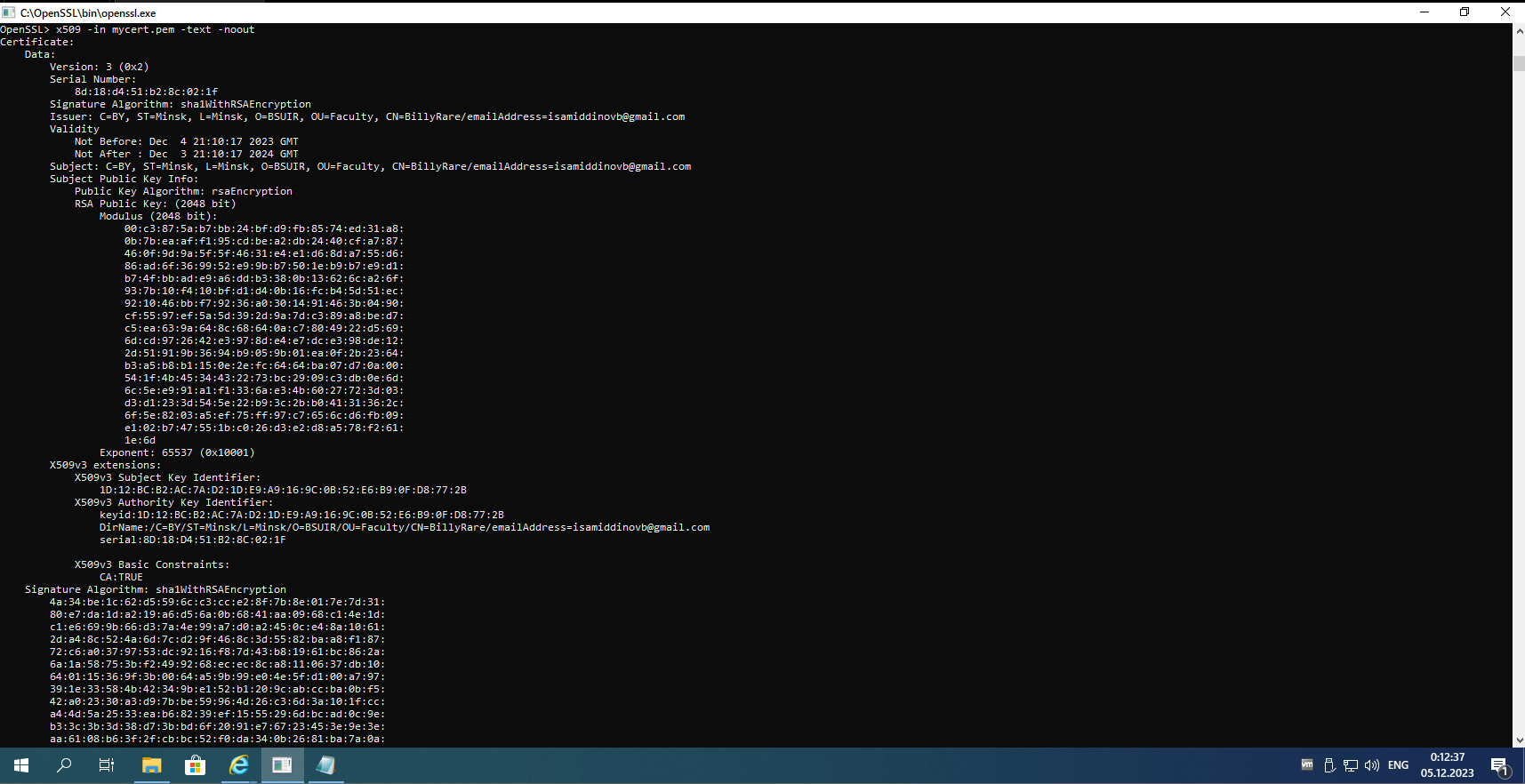
Хэширование md5 и sha1

**Задание 4**

Создать самоподписанный сертификат X509. Изучить состав сертификата и назначение его компонентов.



Создание самоподписанного сертификата x509



Изучение содержимого openssl x509 -in mycert.pem -text -noout

Это покажет детальную информацию о сертификате, включая следующие ключевые компоненты:

* **Subject**: Идентифицирует, кто владеет сертификатом. Включает в себя детали, такие как имя организации, страна, и т.д.
* **Issuer**: Поскольку это самоподписанный сертификат, здесь будет та же информация, что и в "Subject".
* **Validity**: Даты начала и окончания действия сертификата.
* **Serial Number**: Уникальный идентификатор сертификата.
* **Public Key**: Публичный ключ, ассоциированный с этим сертификатом.
* **Signature Algorithm**: Алгоритм, использованный для подписи сертификата.
* **Thumbprint (или Fingerprint)**: Хеш сертификата, используемый для его идентификации.

Эти компоненты играют важную роль в идентификации владельца сертификата, в подтверждении подлинности сертификата и в обеспечении безопасного обмена ключами. В самоподписанных сертификатах эмитент (issuer) и субъект (subject) обычно одинаковы, так как сертификат не выдается удостоверяющим центром (CA).

**Задание 5**

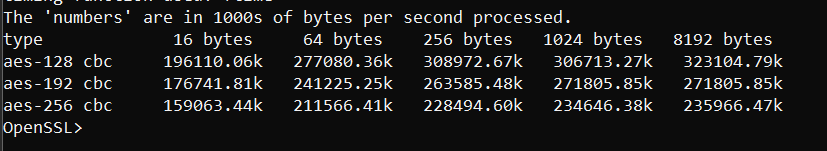
а) результаты тестирования производительности;

б) времена шифрования (выполнить сравнительную оценку скорости шифрования DES и AES, AES и RSA, объяснить полученные результаты);

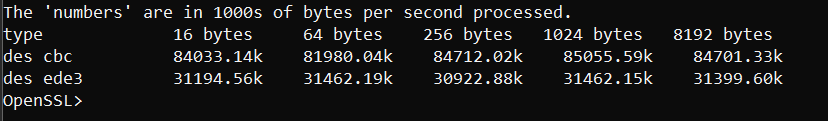
в) полученные хэш значения;

г) сертификат с описанием его компонентов.

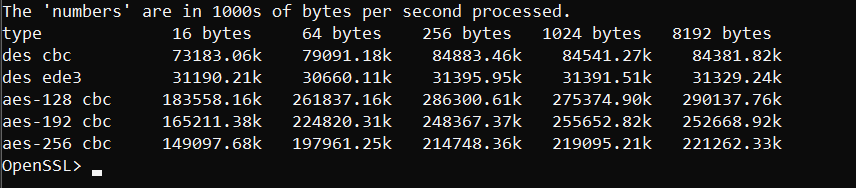
**Отчет**



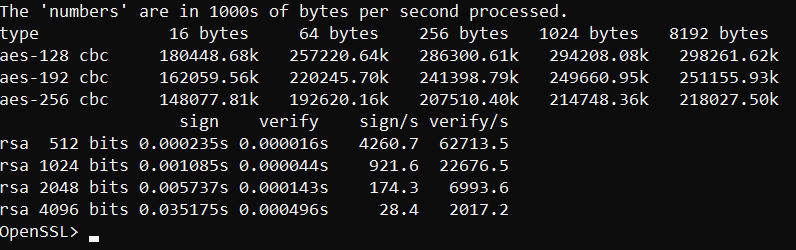
Скорость шифрования AES



Скорость шифрования DES

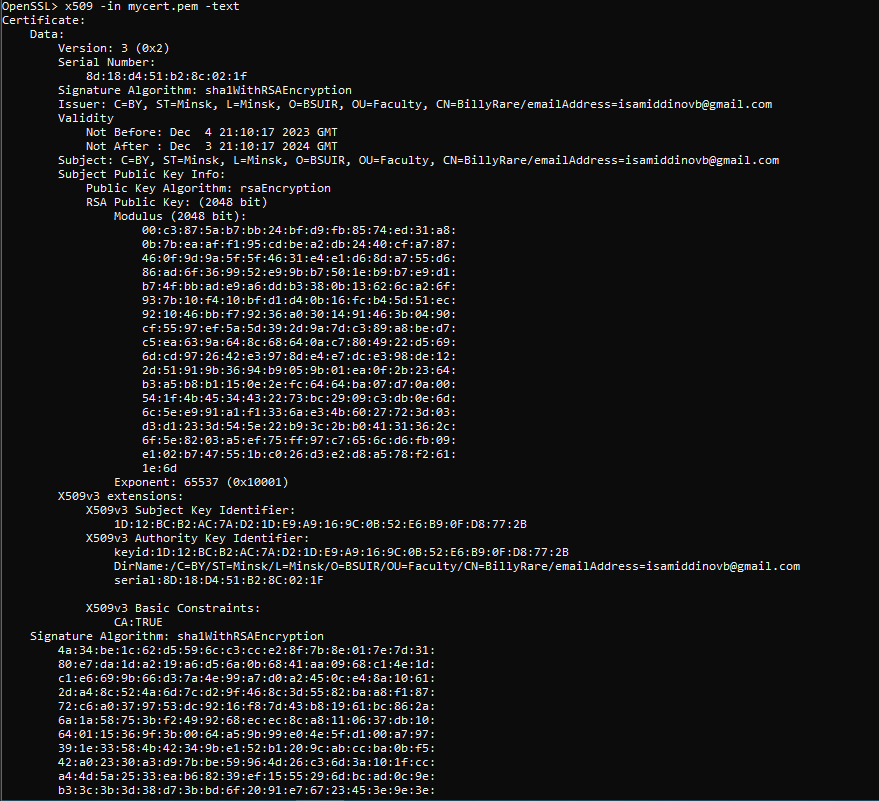


Скорость шифрования AES DES

  
Скорость шифрования aes rsa



вычисления хэш-значения с использованием OpenSSL



Просмотр содержимого mycert.pem

**Вывод**

В ходе данной лабораторной работы были успешно изучены и применены основные функции библиотеки OpenSSL, включая установку на ОС Windows и ознакомление с интерфейсом командной строки. Было выполнено тестирование скорости различных алгоритмов шифрования, что позволило оценить их эффективность в различных условиях использования.

Создание криптографических ключей и шифрование выбранных файлов с помощью различных симметричных и асимметричных алгоритмов продемонстрировало практическое применение криптографии для обеспечения конфиденциальности данных. Сравнительная оценка скорости шифрования DES и AES, а также AES и RSA показала, что алгоритмы имеют различную производительность и уровень безопасности, что должно быть учтено при выборе метода шифрования для конкретных задач.

Хэширование файлов различными алгоритмами, включая md5 и sha1, позволило оценить их пригодность для обеспечения целостности и аутентичности данных. Полученные хеш-значения подтвердили, что даже небольшие изменения в исходных данных приводят к значительным изменениям в результатах хеширования, что является ключевым аспектом в обеспечении безопасности информации.

Создание самоподписанного сертификата X509 и анализ его состава раскрыли назначение и важность каждого из компонентов сертификата для установления безопасного соединения и обмена данными в сети Интернет.

Таким образом, выполнение лабораторной работы позволило углубить понимание криптографических принципов и методов их применения с использованием инструментов OpenSSL. Полученные знания и навыки могут быть использованы для решения практических задач в области информационной безопасности.