Министерство образования

Республики Беларусь

Учреждение образования

Белорусский государственный университет

информатики и радиоэлектроники

Кафедра: интеллектуальных информационных технологий

Отчёт

По дисциплине

«Средства и методы защиты информации в интеллектуальных системах»

Тема: «Установка, использование и анализ специализированных средств криптографического пакета openssl»

Написал: Проверил

Германенко В.В., гр. 321701 Сальников Д. А.

Минск 2025

Задача:

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.

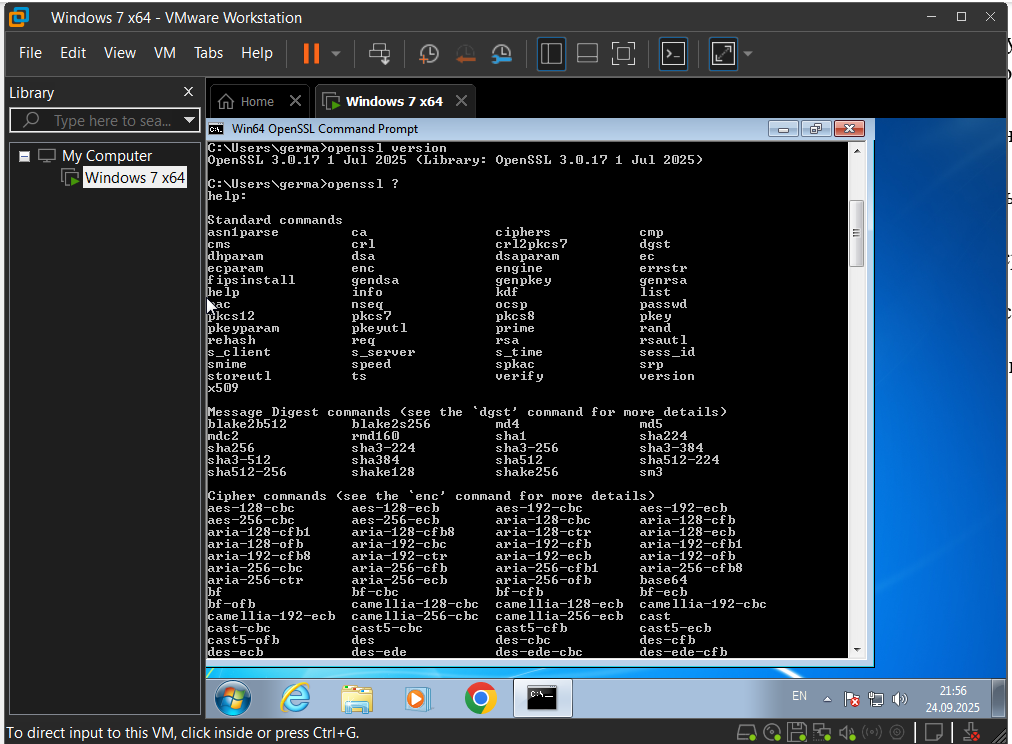
3) Создать криптографические ключи. Выбрать несколько произвольных файлов и выполнить:

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

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

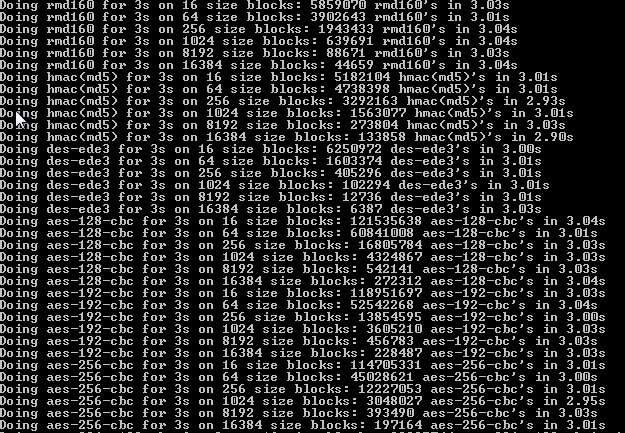
в) хэширование различных файлов различными алгоритмами (обязательно md5 и sha1).

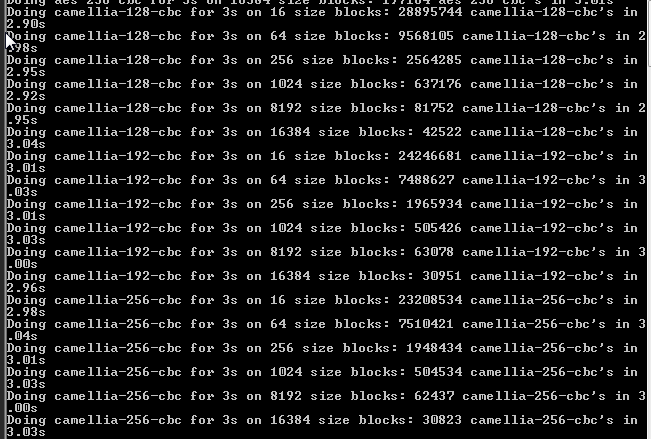
4) Создать самоподписанный сертификат X509. Изучить состав сертификата и назначение его компонентов.

1) 

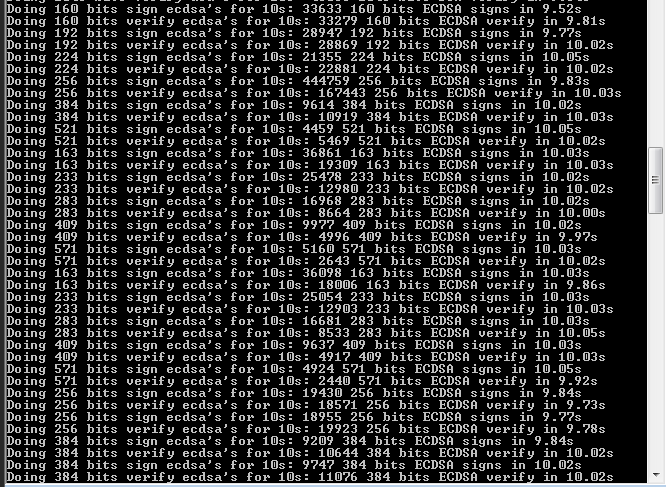
2)



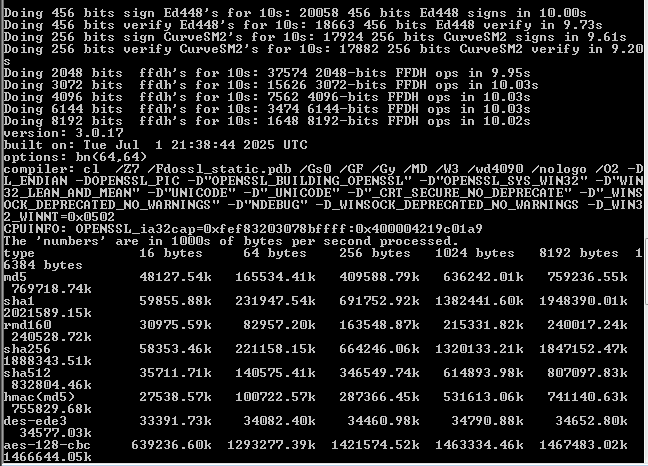


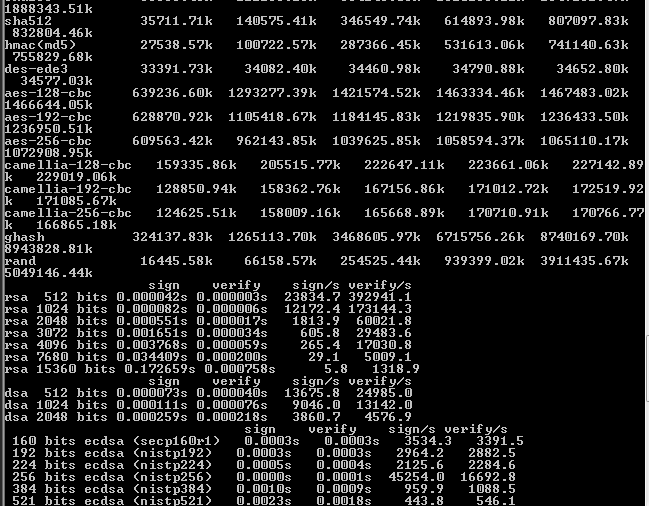


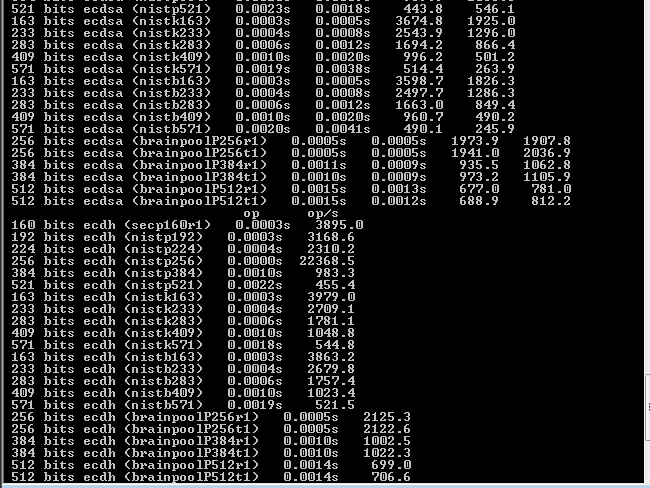


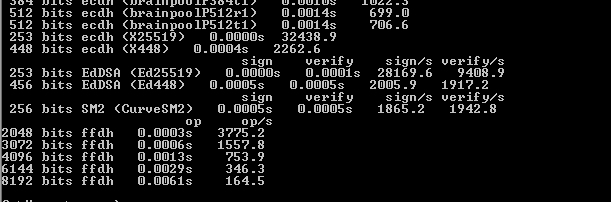








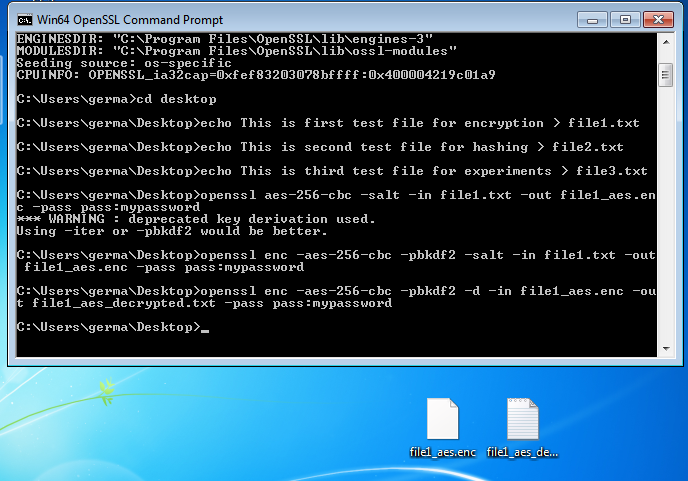




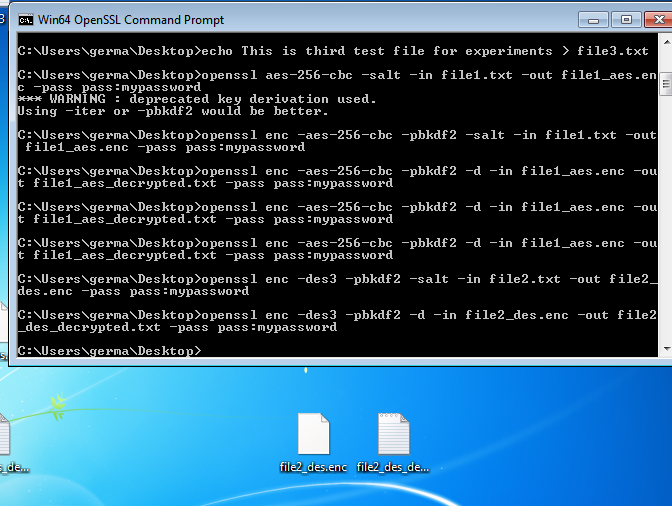
3)

А)

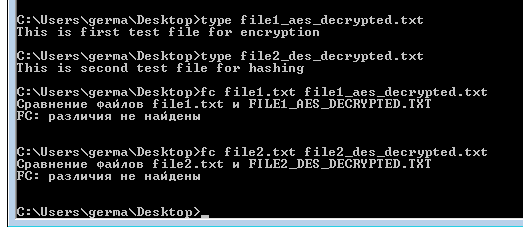
Шифрование симметричным алгоритмом AES



DES



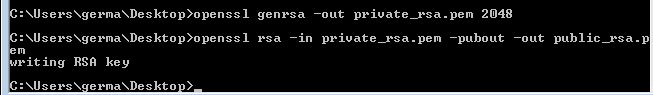
Сравнение:



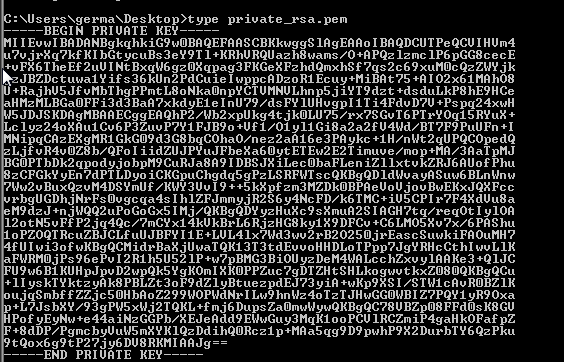
Б)

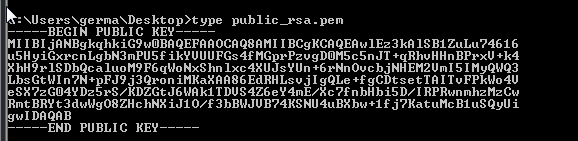
RSA

Создание ключей:

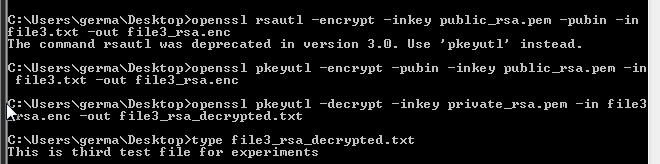


Просмотр ключей:



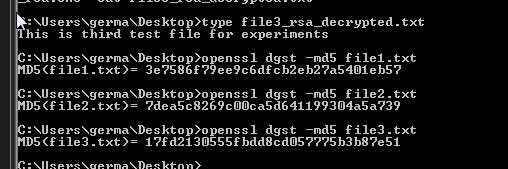


Шифрование публичным и расшифрование приватным ключом:

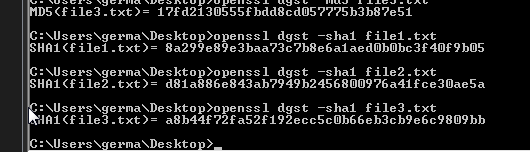


В)

Md5:

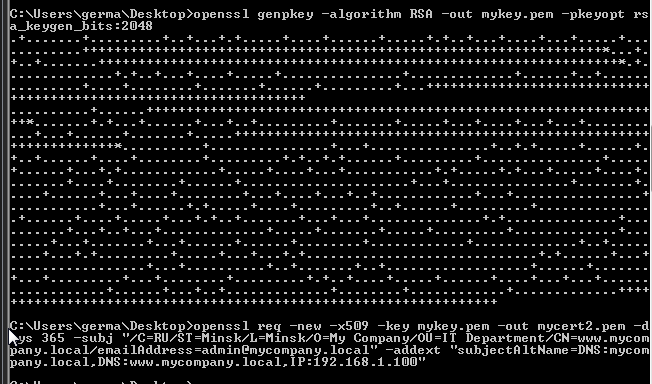


Sha1:

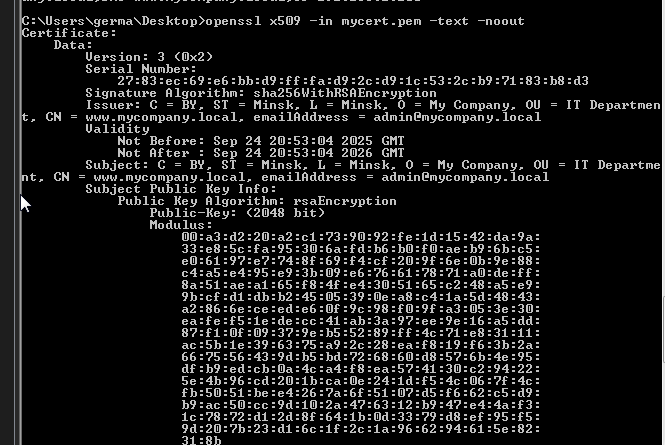


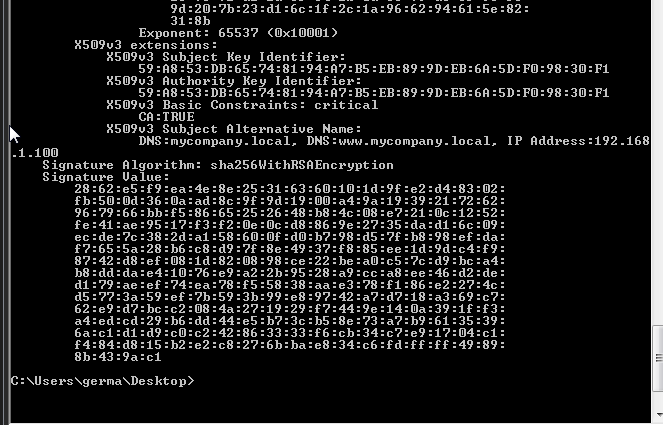
4)

Создание:



Просмотр:





Вывод: Получил навыки работы с криптографическим пакетом OpenSSL, изучил различные алгоритмы и сертификаты.