Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет информационный технологий и управления

Кафедра интеллектуальных информационных технологий

Дисциплина: «Средства и методы защиты информации в  
интеллектуальных системах»

Лабораторная работа №7 по теме:  
«УСТАНОВКА, ИСПОЛЬЗОВАНИЕ И АНАЛИЗ СПЕЦИАЛИЗИРОВАННЫХ СРЕДСТВ КРИПТОГРАФИЧЕСКОГО ПАКЕТА OPENSSL»

Студент гр. 121702

Колтович Д.С.

Проверил:

Сальников Д.А.

Минск 2023

**Тема**

Установка, использование и анализ специализированных средств криптографического пакета OpenSSL.

**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:

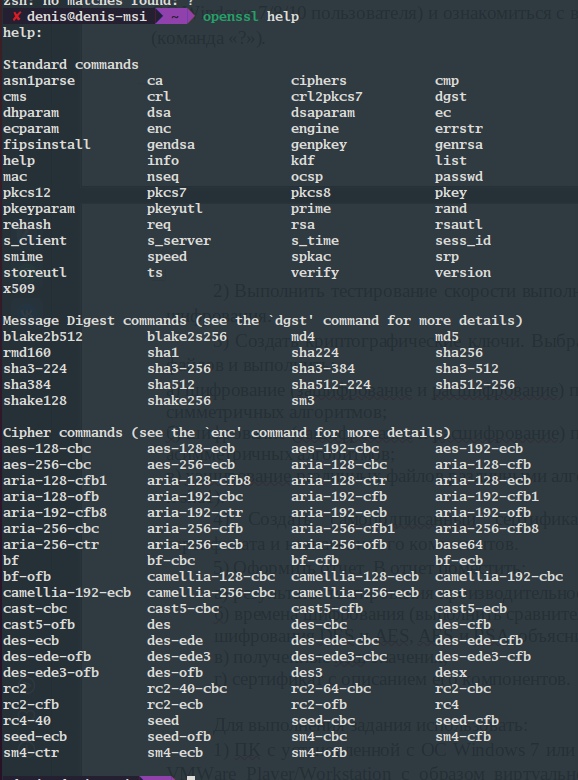
а) шифрование (зашифрование и расшифрование) посредством различных симметричных алгоритмов;

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

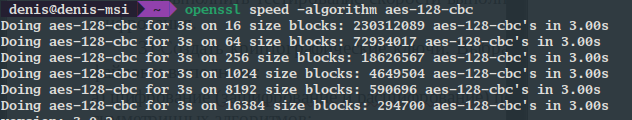
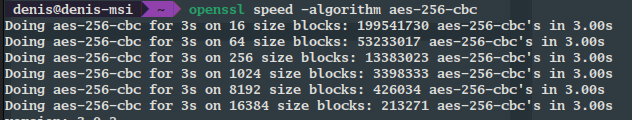
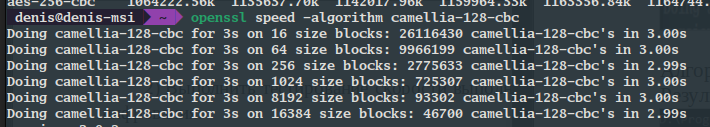
в) хэширование различных файлов различными алгоритмами (обязательно md5 и sha1).

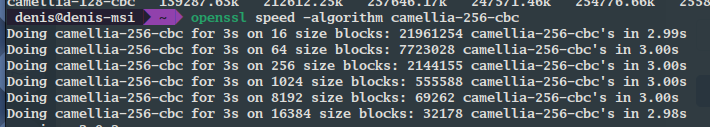
4) Создать самоподписанный сертификат X509. Изучить состав сертификата и назначение его компонентов.

**Выполнение задания**

Задание 1 на Ubuntu  


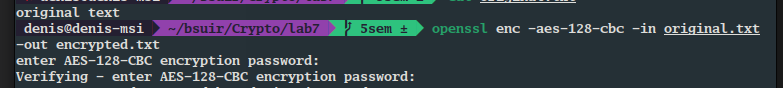
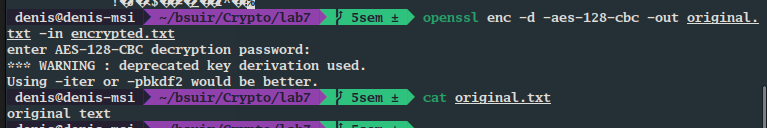
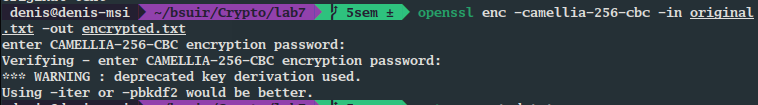
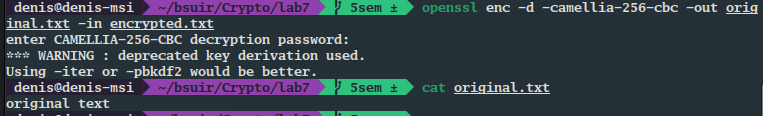
Задание 2

Алгоритм: aes-128-cbc  
Результаты  
  
  
Алгоритм: aes-256-cbc  
Результаты  
  
  
Алгоритм: camellia-128-cbc  
Результаты  


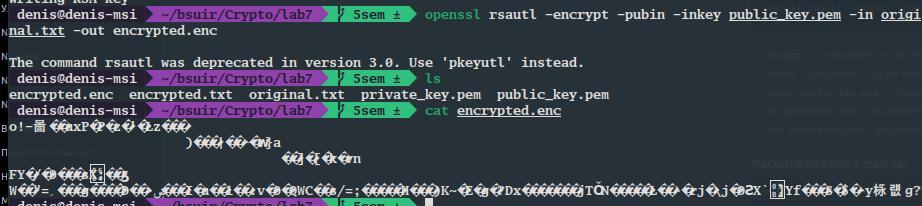
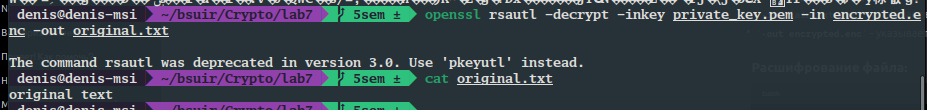
Алгоритм: camellia-256-cbc  
Результаты  


Результат выдаётся в виде количества килобайтов, обработанных за ~3с. Большее значение означает лучший результат

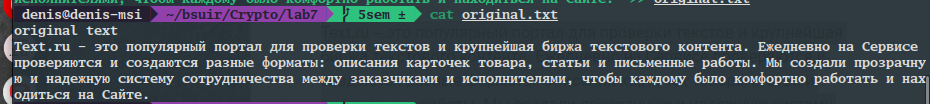
Задание 3

А)Алгоритм aes-128-cbc  
Ключ: password  
  
  
  
  
  
Алгоритм camellia-256-cbc  
Ключ: password  
  
  


Б) Алгоритм RSA  
Генерация ключей:  
  
  
Зашифрованный текст:

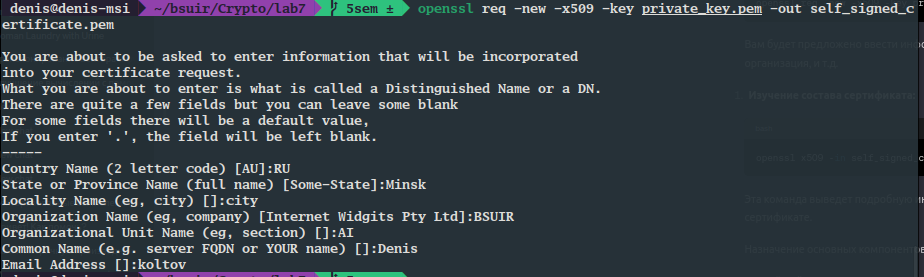
  
  
Расшифрованный текст:  


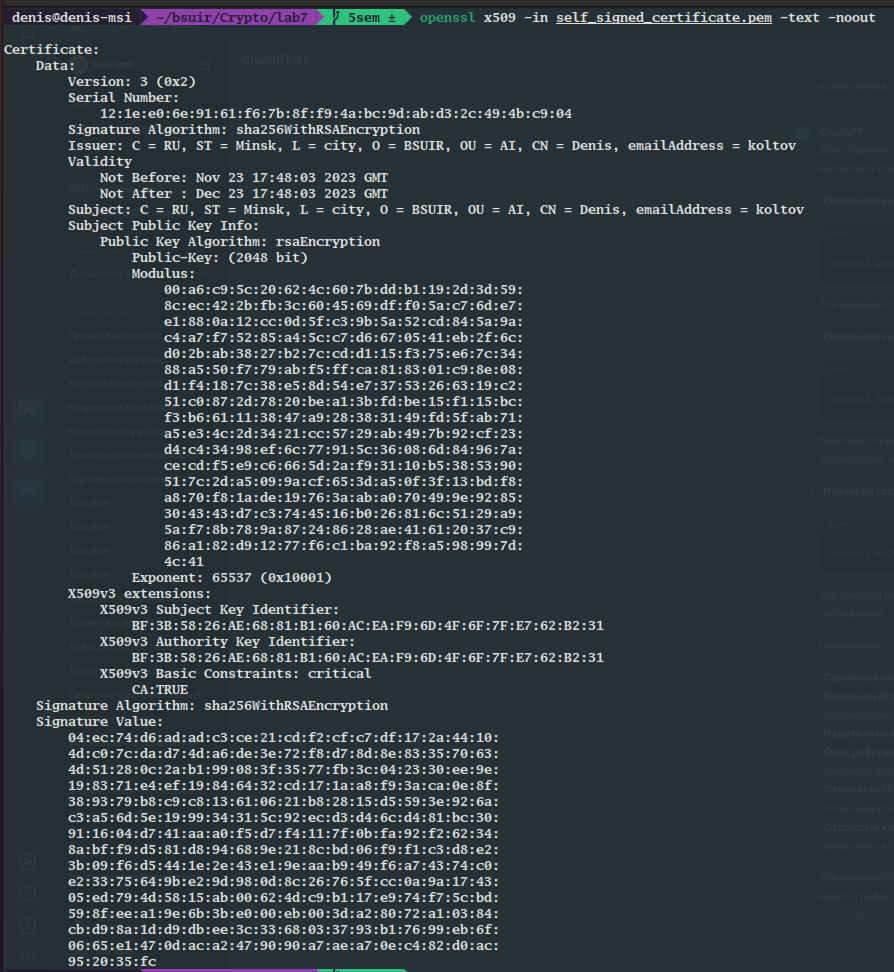
В)Алгоритм хеширования MD5  
Оригинальный текст:





Задание 4

Создание сертификата:  


Состав сертификата:  


Сертификат X509 содержит в себе следующую информацию

1. Имя владельца сертификата  
2. Издатель сертификата  
3. Информация об открытом ключе  
4. Серийный номер сертификата  
5. Период действия сертификата  
6. Дополнительные детали  
7. Идентификатор издателя  
8. Идентификатор субъекта

**Вывод**

В ходе лабораторной работы были получены основы работы с библиотекой OpenSSL. Данная библиотека обладает обширными возможностями в области криптографии: хеширование, шифрование. Были рассмотрены различные алгоритмы шифрования и хеширование. Также был создан сертификат стандарта X.509.