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

Студент гр. 121702

Заломов Р.А.

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:

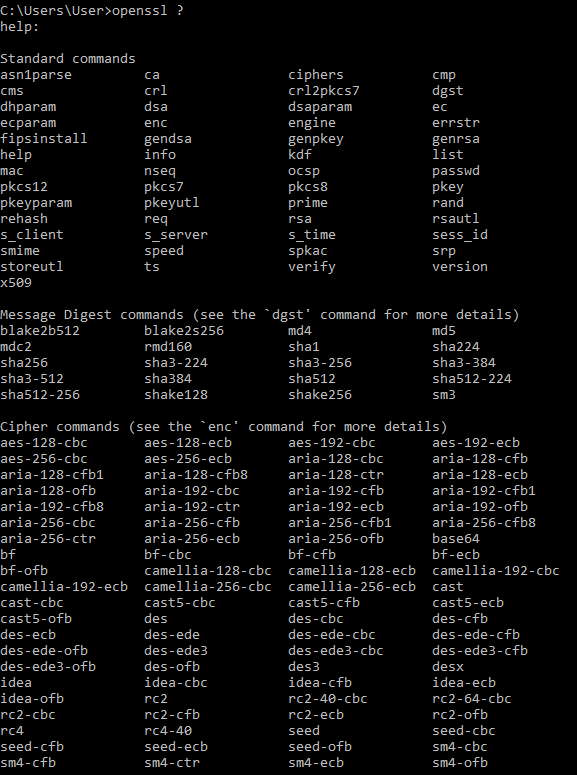
а) шифрование (зашифрование и расшифрование) посредством различных симметричных алгоритмов;

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

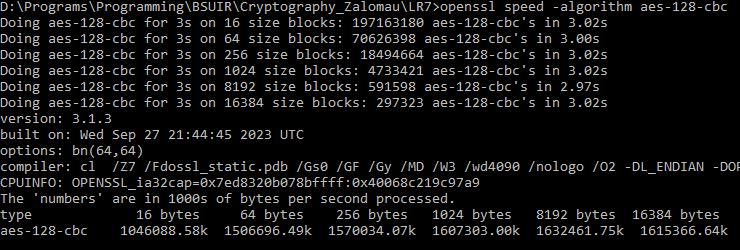
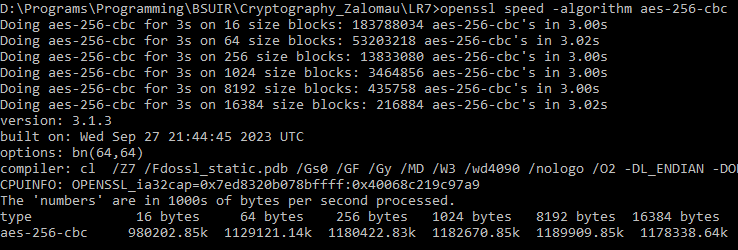
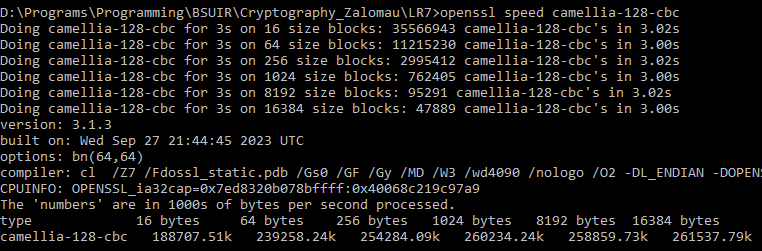
в) хэширование различных файлов различными алгоритмами (обязательно md5 и sha1).

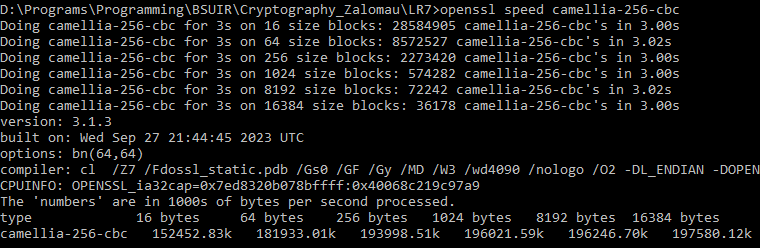
4) Создать самоподписанный сертификат X509. Изучить состав сертификата и назначение его компонентов.

**Выполнение задания**

Задание 1  


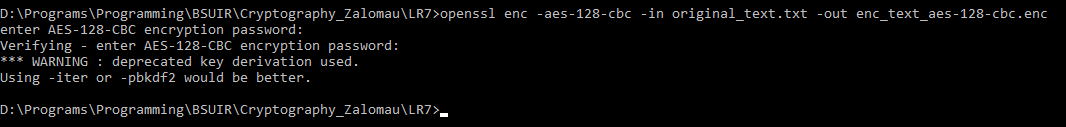
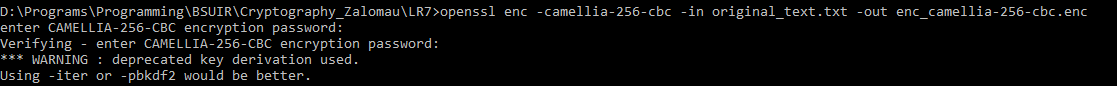
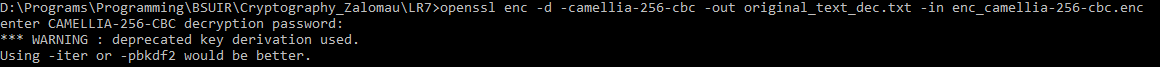
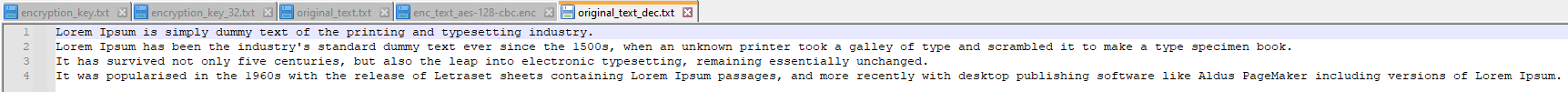
Задание 2

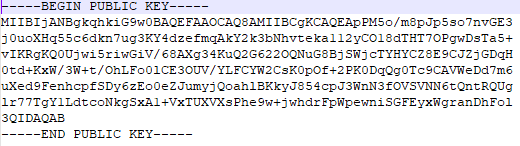
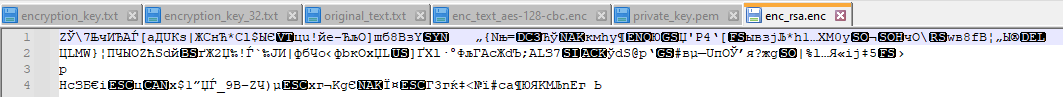
Алгоритм: aes-128-cbc  
Результаты  
  
  
Алгоритм: aes-256-cbc  
Результаты  
  
  
Алгоритм: camellia-128-cbc  
Результаты  


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: OeAW7Akq2Ta+mxELody/SA==  
  
  
  
  
  
Алгоритм camellia-256-cbc  
Ключ: zC/rEE6wJXaTO5ahAOtUWq8IHdu4p0uNq3nD1IgpBcQ=  
  
  


Б) Алгоритм RSA  
Открытый ключ:  
  
Закрытый ключ:  
  
Зашифрованный текст:  
  
Расшифрованный текст:  


В)Алгоритм хеширования MD5  
Оригинальный текст:  
Contrary to popular belief, Lorem Ipsum is not simply random text.

It has roots in a piece of classical Latin literature from 45 BC, making it over 2000 years old.

Richard McClintock, a Latin professor at Hampden-Sydney College in Virginia, looked up one of the more obscure Latin words, consectetur, from a Lorem Ipsum passage, and going through the cites of the word in classical literature, discovered the undoubtable source.

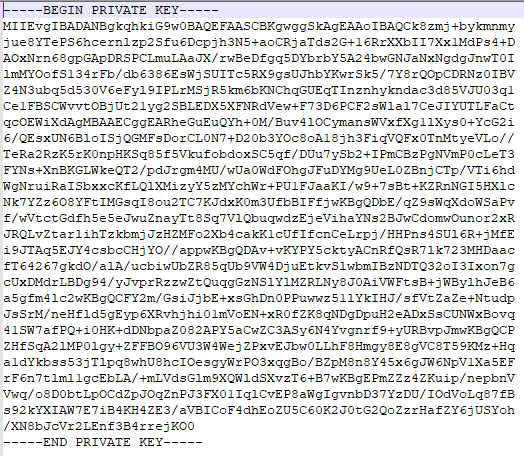
Lorem Ipsum comes from sections 1.10.32 and 1.10.33 of "de Finibus Bonorum et Malorum" (The Extremes of Good and Evil) by Cicero, written in 45 BC.

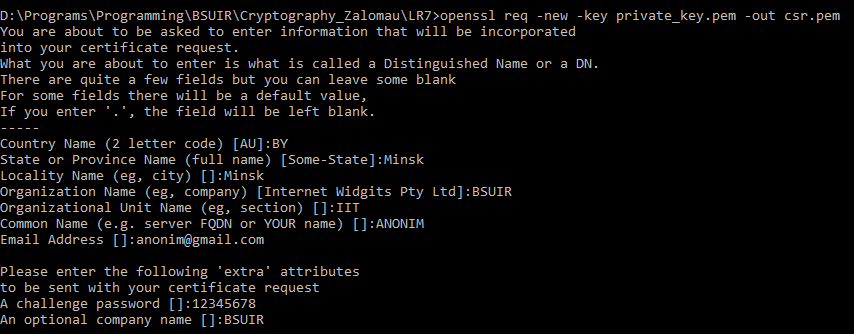
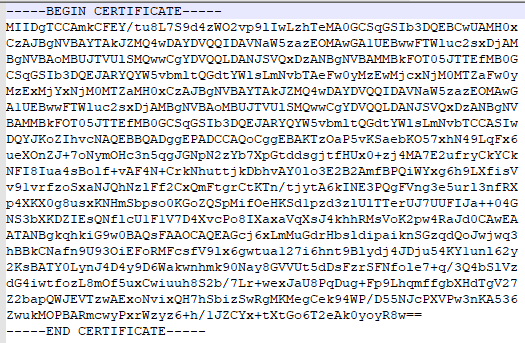
This book is a treatise on the theory of ethics, very popular during the Renaissance. The first line of Lorem Ipsum, "Lorem ipsum dolor sit amet..", comes from a line in section 1.10.32.  
Хеш: 40c396434f4bce8d250eacae66218a91

Алгоритм хеширования: sha256  
Оригинальный текст: тот же, что и для MD5  
Хеш: a2840d18b66dd9efd10d5e1c6be6b5674644ac876f5542fb5b53013054fcb8b6

Алгоритм хеширования: sha1  
Оригинальный текст: тот же, что и для MD5  
Хеш: ab391996f748f7c5e4552018aa6d2f8ca479a002

Задание 4

Закрытый ключ:  


Создание запроса на сертификат:  
  
  
  
Сгенерированный сертификат  


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.