Государственное учреждение образования

“БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ”

Кафедра: Интеллектуальных информационных технологий

Дисциплина: Средства и методы защиты информации в интеллектуальных системах

**Отчет по лабораторной работе №7**

**“Установка, использование и анализ специализированных средств криптографического пакета OpenSSL”**

Выполнил:

студент гр.121702

Витковская С. И.

Проверил:

Сальников Д.А.

Минск 2023

**Содержание**

[**Задача: 3**](#_gl8o1xw3chrw)

[**Ход работы: 3**](#)

[**Вывод: 6**](#_nbycu7w9oxkv)

#### **Задача:**

1) Установить OpenSSL и ознакомиться с возможностями библиотеки.

2) Выполнить тестирование скорости выполнения различных алгоритмов шифрования.

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

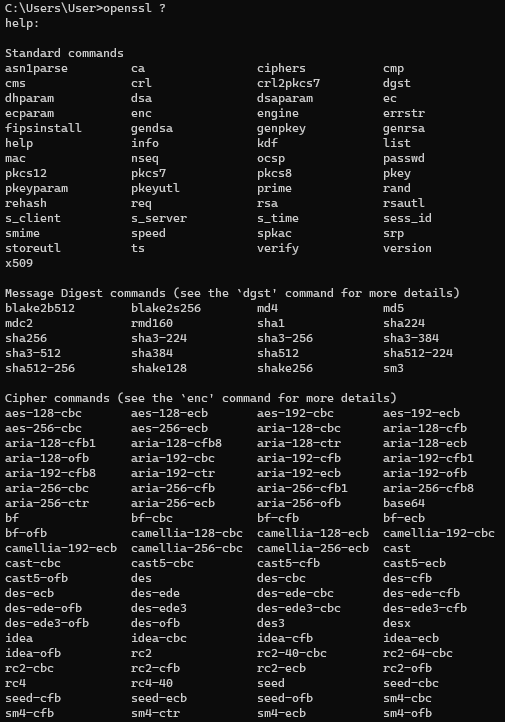
а) шифрование (зашифрование и расшифрование) посредством различных симметричных алгоритмов;

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

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

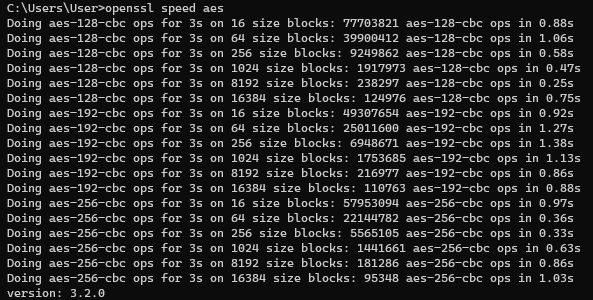
4) Создать самоподписанный сертификат X509. Изучить состав сертификата и назначение его компонентов.

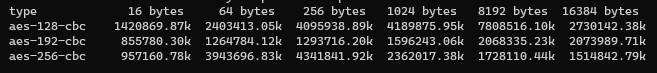
## **Ход работы:**



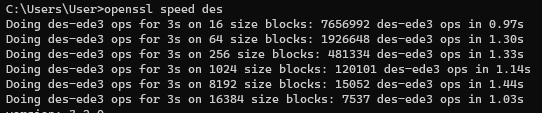
1)

2)

Алгоритм AES



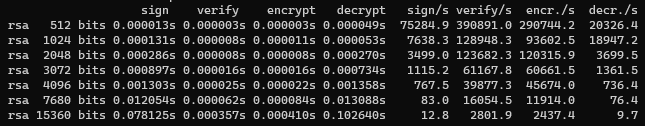
Алгоритм DES



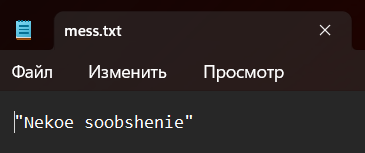


Алгоритм RSA



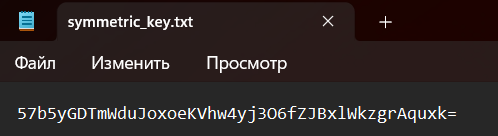


3a) Запишем в файл mess.txt сообщение "Nekoe soobshenie"



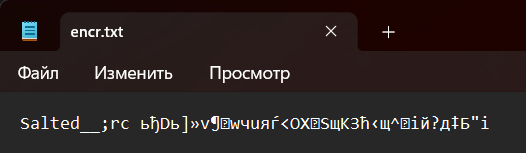
Сгенерируем ключ:





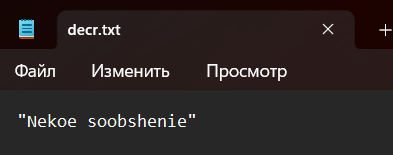
Зашифруем сообщение с помощью алгоритма AES с использованием режима шифрования cbc:





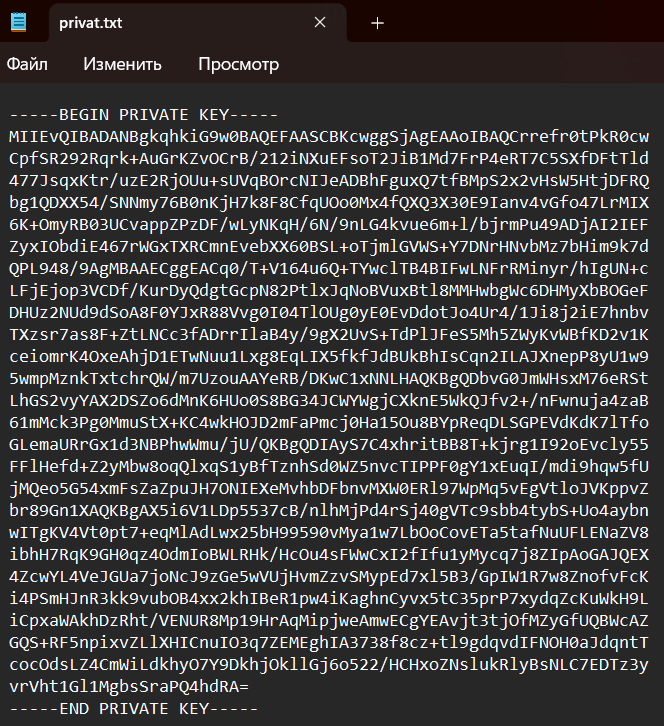
Расшифруем сообщение:





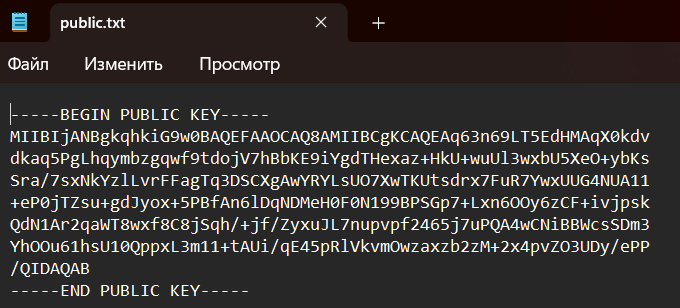
3б) Сгенерируем секретный ключ алгоритма RSA:





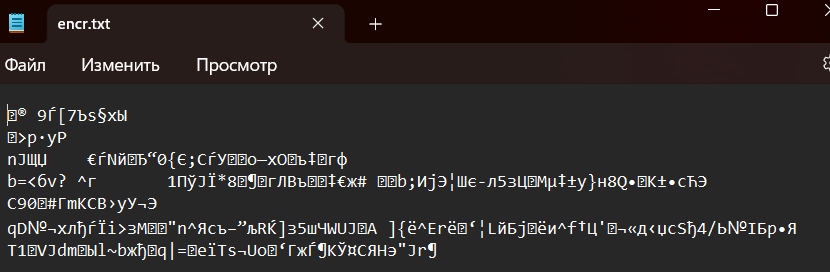
Сгенерируем открытый ключ:





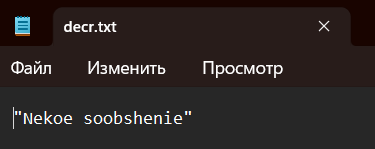
Зашифруем сообщение:





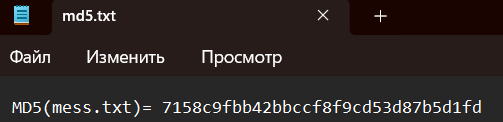
Расшифруем сообщение:

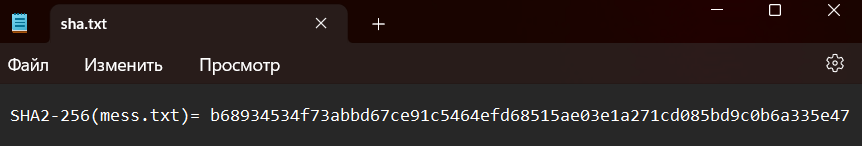




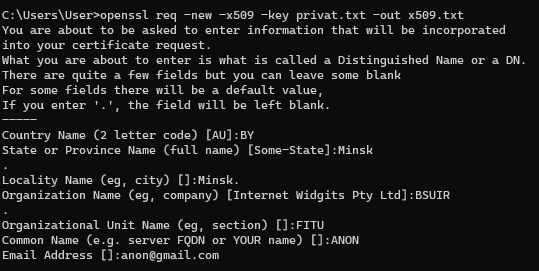
3в) Захэшируем файл:

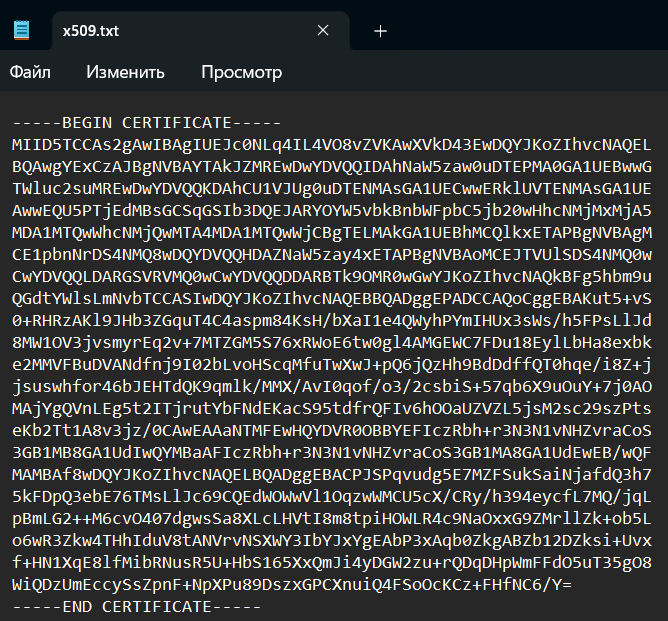






4) Создадим сертификат:





**Вывод**:

В ходе выполнения данной лабораторной работы изучили криптографическую библиотеку OPENSSL, реализующую возможности генерации ключей, шифрования файлов, их хэширования, проверки скорости работы алгоритмов шифрования.