Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

Кафедра информационных технологий автоматизированных систем

Отчет по лабораторной работе №6

по курсу «ИТОКБ»

на тему: «Знакомство с OpenSSL»

Вариант 4

|  |  |
| --- | --- |
| Выполнил магистрант группы 025941: | Колесников В.Г. |
| Проверил: | Боброва Т.С. |

МИНСК

2021

**Задание 1:** Установить OpenSSL, ознакомиться с возможностями библиотеки.

Результат выполнения команды «help» приведен на рисунке 1.1.

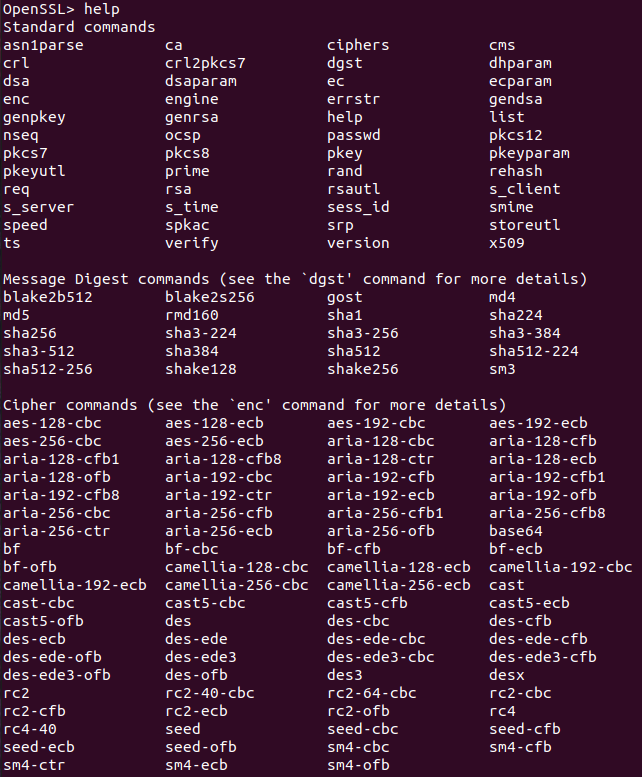


Рисунок 1.1 — Результат команды «help»

**Задание 2:** Выполнить тестирование скорости выполнения различных алгоритмов шифрования.

Скорость выполнения алгоритмов шифрования можно проверить с помощью команды «speed». Результаты выполнения алгоритмов приведены на рисунках 2.1-2.4.

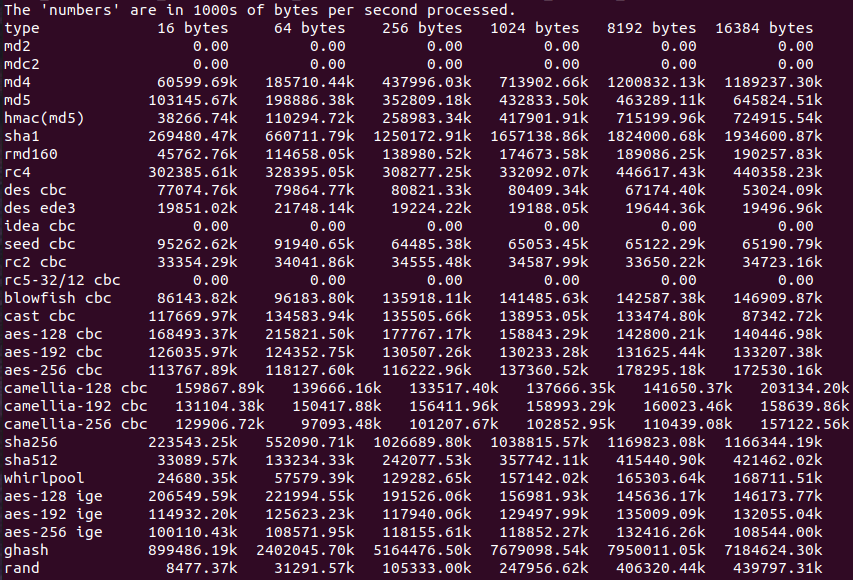


Рисунок 2.1 — Скорость выполнения алгоритмов

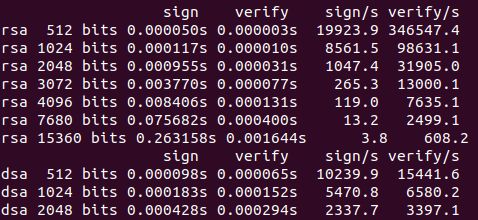


Рисунок 2.2 — Скорость выполнения RSA и DSA

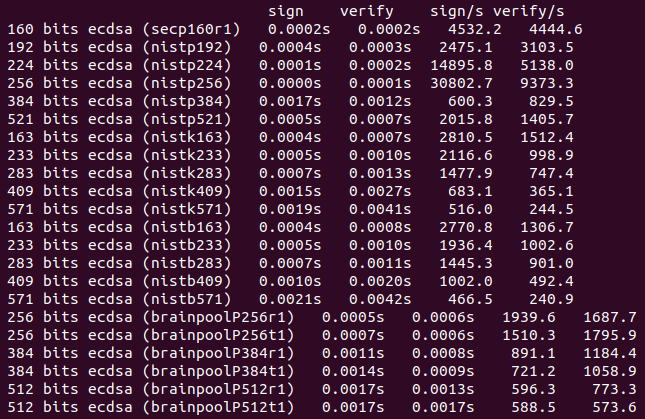


Рисунок 2.3 — Скорость выполнения ECDSA

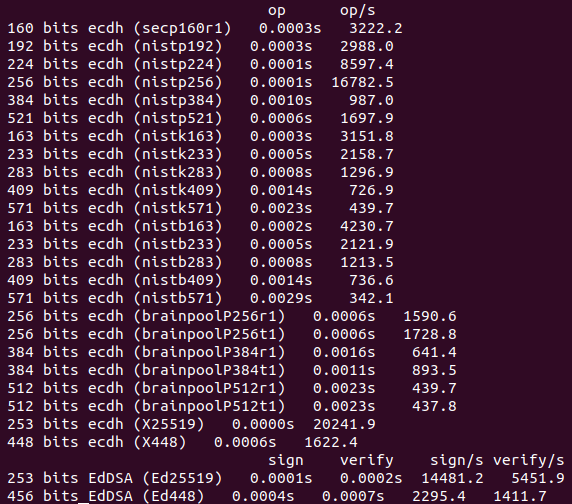


Рисунок 2.4 — Скорость выполнения ECDH и EdDSA

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

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

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

- хэширование различных файлов различными алгоритмами (обязательно md5 и sha1)

Процесс и результат выполнения команд создания криптографических ключей через «genrsa» приведен на рисунке 3.1.

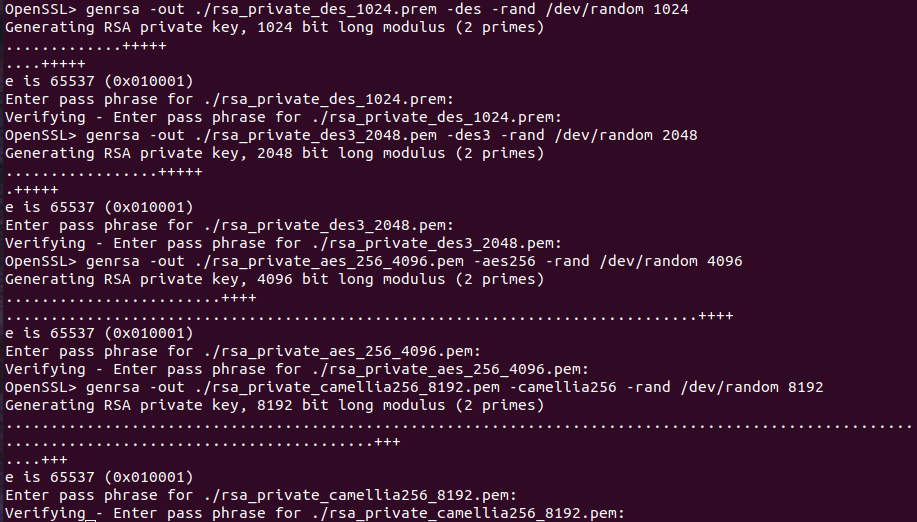


Рисунок 3.1 — Процесс и результат создания криптографических ключей через «genrsa»

Для установки параметров шифрования DSA создаются файлы параметров на 1024, 2048, 4086 и 8192 бит. Процесс и результат создания файла параметров через «dsaparm» приведен на рисунке 3.2.

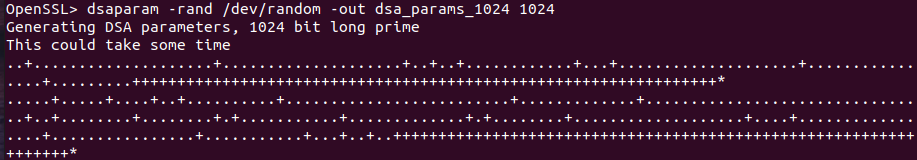
****

Рисунок 3.2 — Процесс и результат создания файла параметров через «dsaparm»

Процесс и результат выполнения команд создания криптографических ключей через «gendsa» приведен на рисунке 3.3.

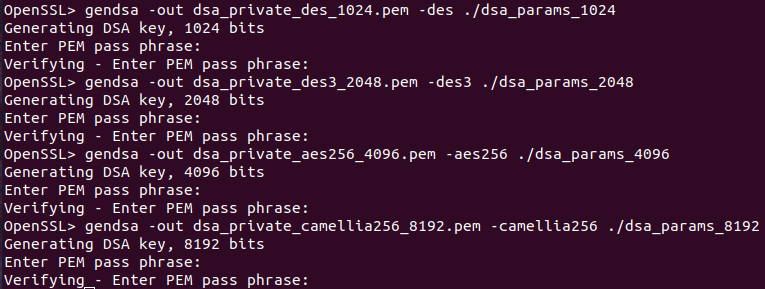


Рисунок 3.3 — Процесс и результат создания криптографических ключей через «gendsa»

Процесс шифрования посредством различных симметричных алгоритмов представлен на рисунке 3.4. На рисунке 3.5 показаны файлы, используемые при шифровании. На рисунках 3.6 и 3.7 представлено сравнение исходных и расшифрованных файлов.

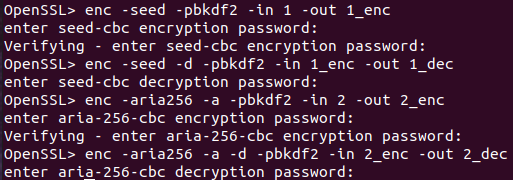


Рисунок 3.4 — Шифрование с использованием симметричных алгоритмов



Рисунок 3.5 — Файлы, используемые при шифровании симметричными алгоритмами

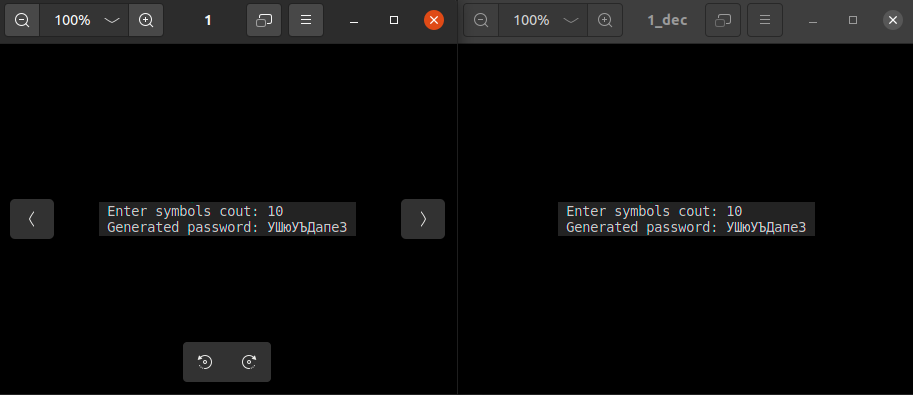


Рисунок 3.6 — Сравнение исходного и расшифрованного файла «1»

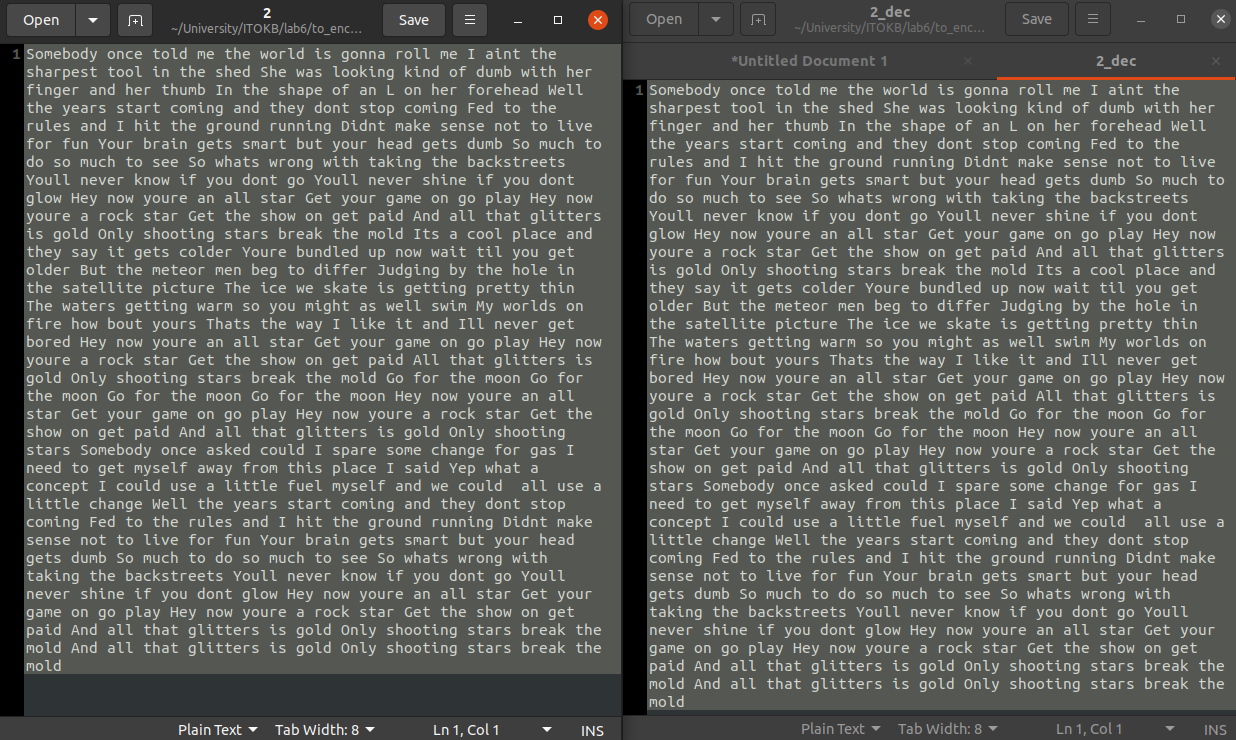


Рисунок 3.7 — Сравнение исходного и расшифрованного файла «2»

Для шифрования асимметричными алгоритмами необходим публичный ключ. Он создается с помощью флага «-pubout» и указания файлов секретного («-in») и выходного публичного («-out») ключей. Процесс создания публичных ключей показан на рисунке 3.8.

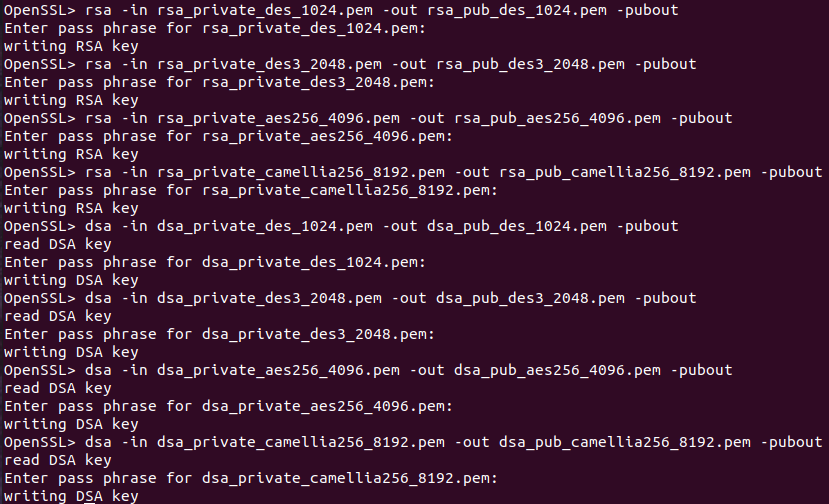


Рисунок 3.8 — Процесс создания публичных ключей RSA и DSA

Процесс шифрования посредством различных асимметричных алгоритмов представлен на рисунке 3.9. На рисунке 3.10 показаны файлы, используемые при шифровании. На рисунках 3.11 и 3.12 представлено сравнение исходных и расшифрованных файлов.

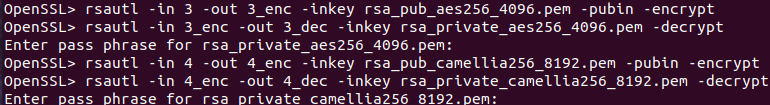


Рисунок 3.9 — Шифрование с использованием асимметричных алгоритмов

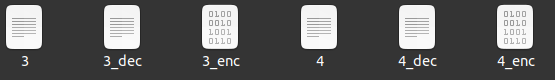


Рисунок 3.10 — Файлы, используемые при шифровании симметричными алгоритмами

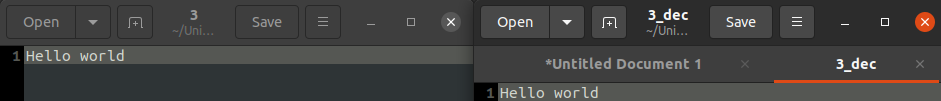


Рисунок 3.11 — Сравнение исходного и расшифрованного файла «3»

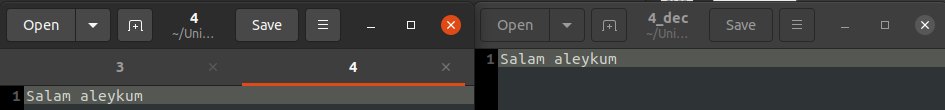


Рисунок 3.12 — Сравнение исходного и расшифрованного файла «4»

Для вычисления хэшей используется функция «dgst» с названием хэша в виде параметра «-\*», где \* - название хэша. Вычисленные хэш-суммы файлов представлены на рисунке 3.13.

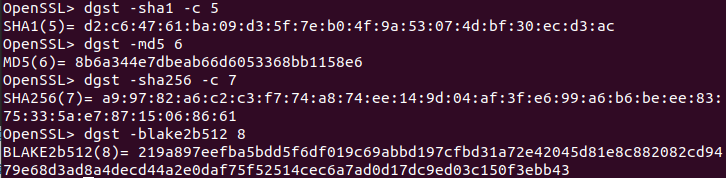


Рисунок 3.13 — Вычисление хэш-сумм различными алгоритмами

**Задание 4:** Создать самоподписанный сертификат X509. Изучить состав сертификата и назначение его компонентов.

Для создания самоподписанного сертификата X509 используется команда «req» с аргументом «-x509». Процесс создания сертификата приведен на рисунке 3.14.

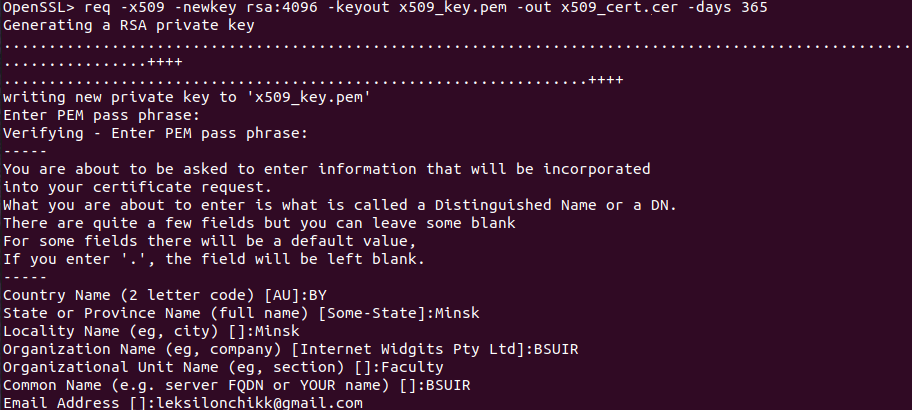


Рисунок 3.14 — Создание самоподписанного сертификата

В результате выполнения команды создается два файла:

1) x509\_key.pem — зашифрованный секретный ключ

2) x509\_cert.cer — файл сертификата

На рисунке 3.15 показаны созданные файлы сертификата и секретного ключа.

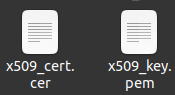


Рисунок 3.15 — Файлы секретного ключа и сертификата

Состав сертификата приведен на рисунках 3.16 и 3.17.

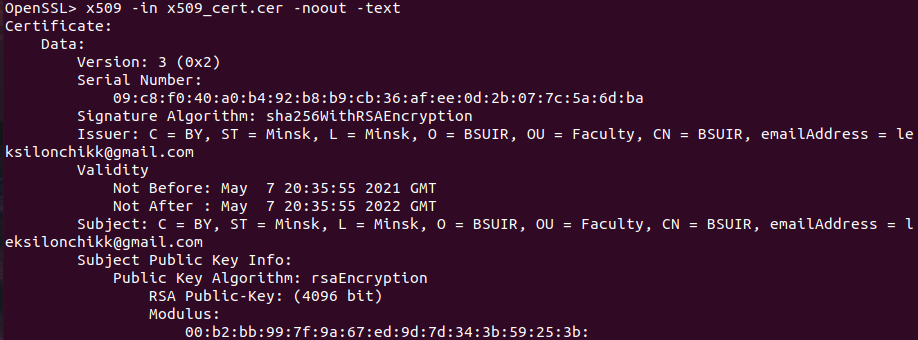


Рисунок 3.16 — Состав сертификата, часть 1

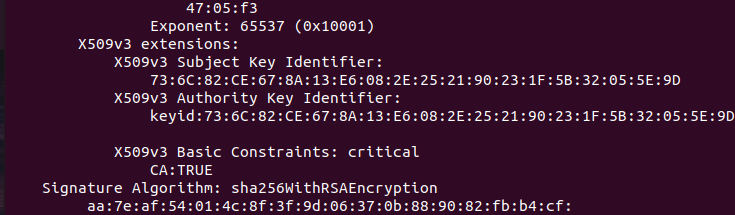


Рисунок 3.17 — Состав сертификата, часть 2

Структура сертификата:

- Данные:

- Версия

- Серийный номер

- Идентификатор алгоритма подписи

- Информация об издателе

- Период действия:

- Не ранее

- Не позднее

- Информация о субъекте

- Информация об открытом ключе субъекта:

- Алгоритм открытого ключа:

- Открытый ключ субъекта

- Дополнения

- Алгоритм подписи сертификата

- Подпись сертификата