Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования

**«Московский Государственный Технический Университет**

**имени Н.Э. Баумана»**

Национальный исследовательский университет техники и технологий

(**МГТУ им. Н.Э.Баумана**)

*Факультет* ***«Робототехника и комплексная автоматизация» (РК)***

*Кафедра* ***«Системы автоматизированного проектирования»***

***(РК-6)***

**ОТЧЕТ**

По лабораторным работам

По курсу «Методы и средства защиты компьютерной информации»

Группа РК6-83

Преподаватель: Беломойцев Д.Е.

Москва, 2018

Задание №1

Сгенерировать пару ключей RSA, выполнить шифрование и расшифрование произвольного набора данных.

Создаем cекретный ключ длиной 4096 бит с помощью алгоритма шифрования des3:

***openssl genrsa -out secret\_key.pem -des3 4096***

Пароль для ключа (Pass phrase): love

Создаем открытый ключ на основе ранее созданного закрытого ключа:

***openssl rsa -in secret\_key.pem -out public\_key.pem -des3 –pubout***

Алгоритм шифрования тот же - des3.

Создаем файл с произвольным набором данных – data.txt

Текст файла:   
– Люди, – Геральт повернул голову, – любят выдумывать страшилищ и страхи. Тогда сами себе они кажутся не столь уродливыми и ужасными.

Шифруем файл data.txt используя утилиту rsautl и созданный ранее открытый ключ:

***openssl rsautl -in data.txt -out data.cr -inkey public\_key.pem -pubin –encrypt***

Получили файл с зашифрованными данными data.cr

Расшифруем только что зашифрованный файл, используя секретный ключ:

***openssl rsautl -in data.cr -out data\_decr.txt -inkey secret\_key.pem –decrypt***

Мы получили файл data\_decr.txt с содержимым аналогичным исходному файлу data.txt.

Задание №2

Осуществить генерацию запроса на сертификат и выпуск self-signed сертификата на данный запрос.

Cоздаем конфигурационный файл configuration со следующим содержимым:

[ req ]

default\_bits = 2048

default\_keyfile = secret\_key.pem

distinguished\_name = req\_distinguished\_name

prompt = no

[ req\_distinguished\_name ]

CN=RU

ST=MO

L=Moscow

O=BMSTU

OU=RK6

CN=PBS

[emailAddress=rk6@bmstu.ru](mailto:emailAddress=rk6@bmstu.ru)

Этот файл необходим нам, для создания запроса на сертификацию.

Создаем запроса на сертификацию (-new) на основе создаваемого секретного ключа rsa (-newkey rsa:2048),

который записывается в файл rsa\_key.pem (и шифруется с помощью des3).

***openssl req -new -newkey rsa:2048 -keyout rsa\_key.pem -config configuration -out certreq.pem***

Пароль для ключа (Pass phrase):hate

Создаем self-signed сертификат с помощью утилиты x509 и ранее созданного секретного ключа:

***openssl req -x509 -new -key rsa\_key.pem -config configuration -out selfcert.pem -days 365***

Созданный нами сертификат будет действителен в течение 365 дней.

Задание №3

Рассчитать хеш по алгоритму SHA для произвольного набора данных.

Помещаем произвольный набор данных в файл data.txt

Для расчета хеша по алгоритму SHA воспользуемся командой:

***openssl sha data.txt***

Получим результат:

SHA(data.txt)= 63dd5423c9cb154ee1f32e73b019abff056b3772

Задание №4

Выпустить ЭЦП для произвольного набора данных на базе ключей и сертификатов из п.2.

Помещаем произвольный набор данных в файл data.txt

Cоздаем ЭЦП для нашего файла с данными:

***openssl dgst -sign rsa\_key.pem -out signature -sha data.txt***

Стоит заметить, что созданная нами ЭЦП находится в отдельном файле с именем signature.