Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет Информационных технологий и управления

Кафедра Интеллектуальных информационных технологий

**ОТЧЁТ**

по дисциплине «Средства и методы защиты информации в интеллектуальных системах»

Лабораторная работа №7

Тема: Установка, использование и анализ специализированных средств криптографического пакета OpenSSL

Выполнил: Самута Д. В.

гр. 221703

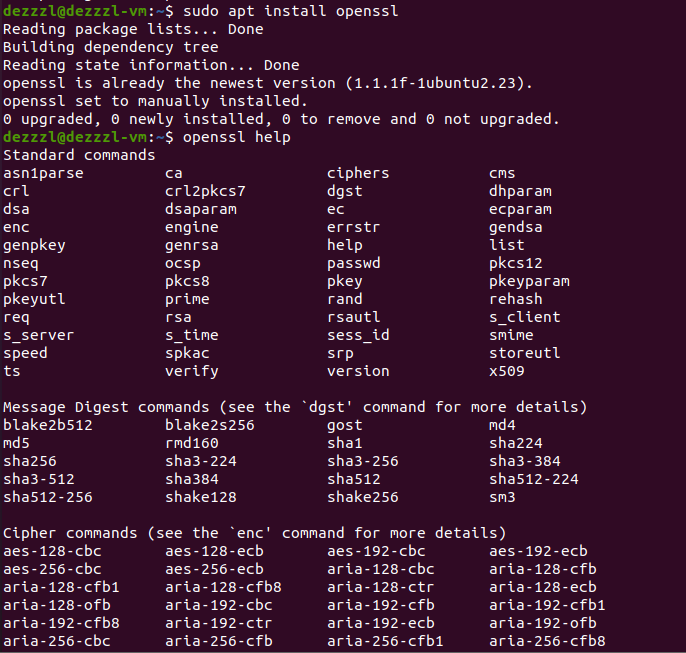
Проверил: Крищенович В. А.

Минск 2024

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.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Type | 16 bytes | 64 bytes | 256 bytes | 1024 bytes | 8192 bytes | 16384 bytes |
| aes-128 cbc | 95281.07k | 96343.98k | 100368.70k | 98719.76k | 100676.95k | 101663.27k |
| aes-192 cbc | 81165.42k | 85097.29k | 85756.07k | 84856.83k | 84273.49k | 84089.92k |
| aes-256 cbc | 72349.32k | 74082.99k | 75488.06k | 75807.06k | 72308.78k | 73586.01k |
| des cbc | 25305.06k | 25844.18k | 28686.30k | 28546.39k | 29051.56k | 29054.29k |

Данные в таблице означают скорость шифрования в секунду.

По таблице можно увидеть, что AES имеют большую скорость шифрования. При увеличении блока скорость шифрования растет, а при увеличении размера ключа – падает, т.к. большой размер ключа приводит к более сложным вычислениям.

DES же по сравнению с AES имеет малую скорость, из-за того что алгоритм старый и его использование сегодня ограничено по причине слабой криптостойкости, но по-прежнему медленнее, чем современные стандарты, такие как AES.

RSA:



**Статистика RSA 2048 бит:**

* **Sign:** Время, необходимое для создания цифровой подписи с использованием RSA 2048-битного ключа. Операция занимает примерно 0.00168 секунд.
* **Verify:** Время для проверки цифровой подписи с RSA 2048-битным ключом, занимает 0.000049 секунд — эта операция значительно быстрее, чем создание подписи.
* **sign/s:** Количество операций подписи в секунду, которое может выполнить алгоритм с 2048-битным ключом — около 595 операций в секунду.
* **verify/s:** Количество операций проверки подписи в секунду для 2048-битного ключа — около 20,488 операций в секунду. Это показывает, что проверка подписи намного быстрее, чем её создание.

AES по сравнению с RSA имееют большую скорость шифрования. Это связано с тем, что симметричные алгоритмы, такие как AES, требуют меньше вычислительных ресурсов и выполняются гораздо быстрее.

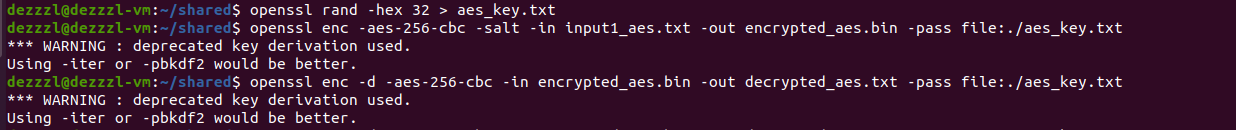
3) Создать криптографические ключи. Выбрать несколько произвольных

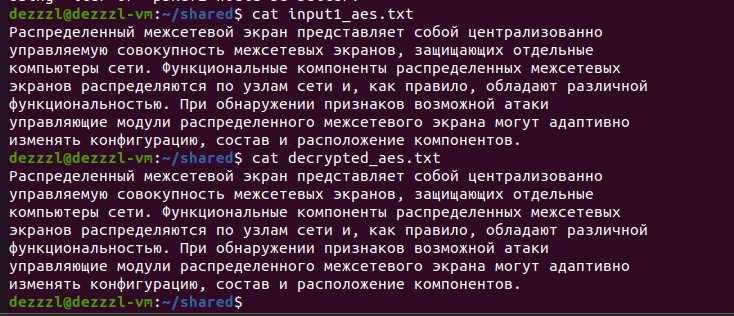
файлов и выполнить:

а) шифрование (зашифрование и расшифрование) посредством различных

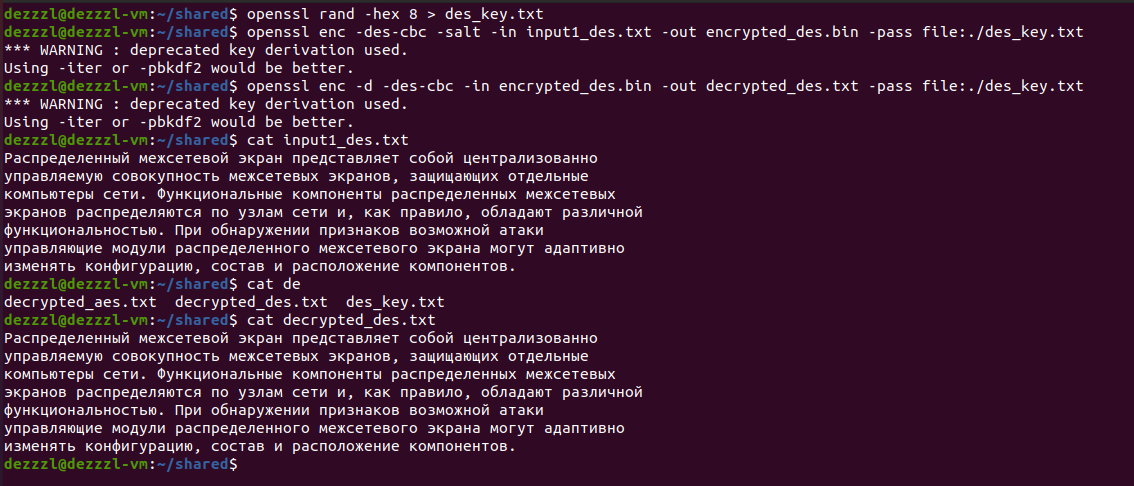
симметричных алгоритмов;

AES:





DES:

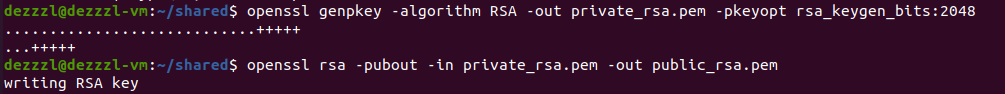


б) шифрование (зашифрование и расшифрование) посредством различных

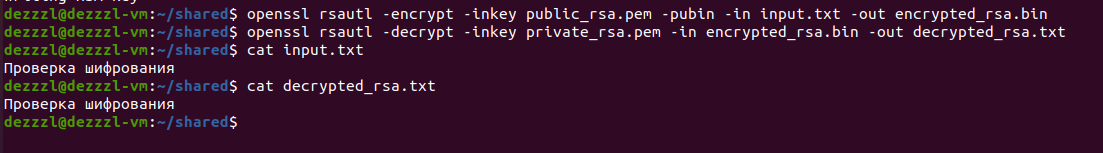
асимметричных алгоритмов;

RSA-2048

Для начала сгенерируем приватный и общий ключи

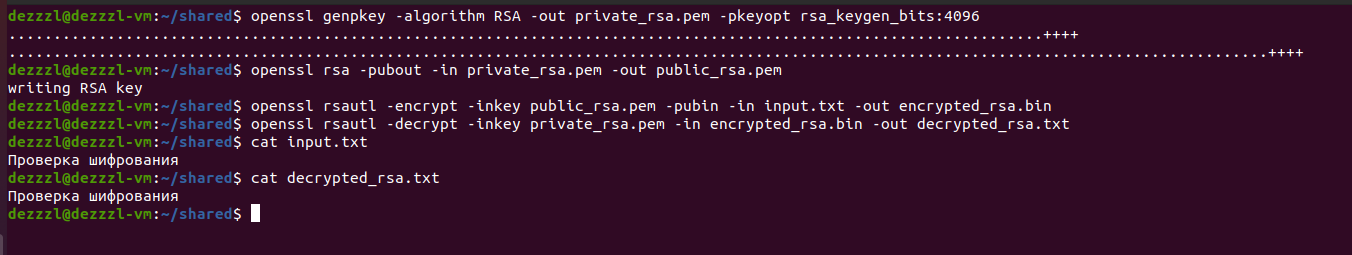


Зашифруем текст



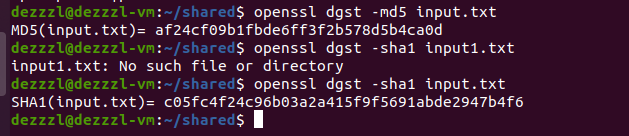
Важно, чтобы текст был не слишком длинным, т.к. полностью его зашифровать не получится.

RSA-4096



в) хэширование различных файлов различными алгоритмами (обязательно md5

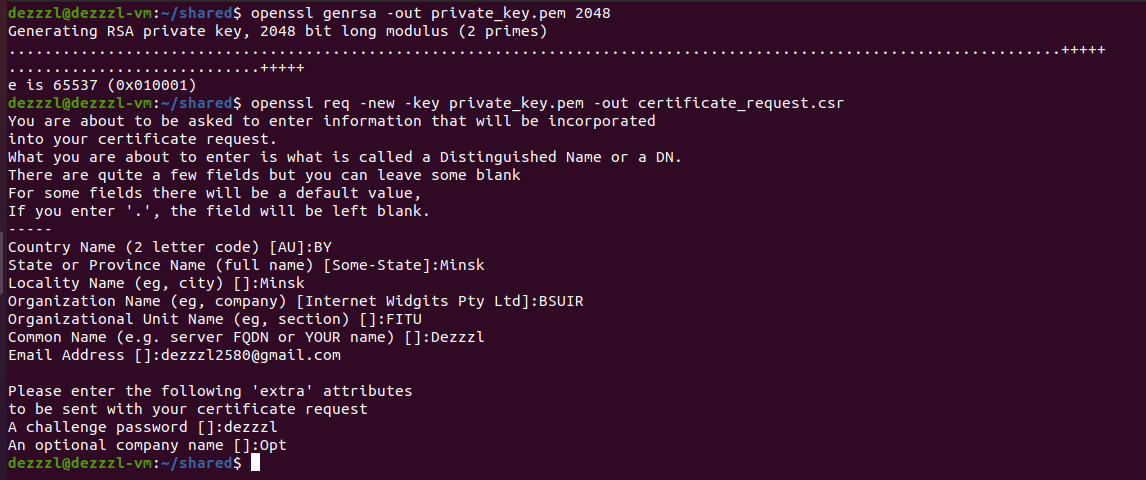
и sha1).



4) Создать самоподписанный сертификат X509. Изучить состав

сертификата и назначение его компонентов.

Для генерации сертификата нужно ввести сгенерировать ключ, а также ввести информацию о сертификате.

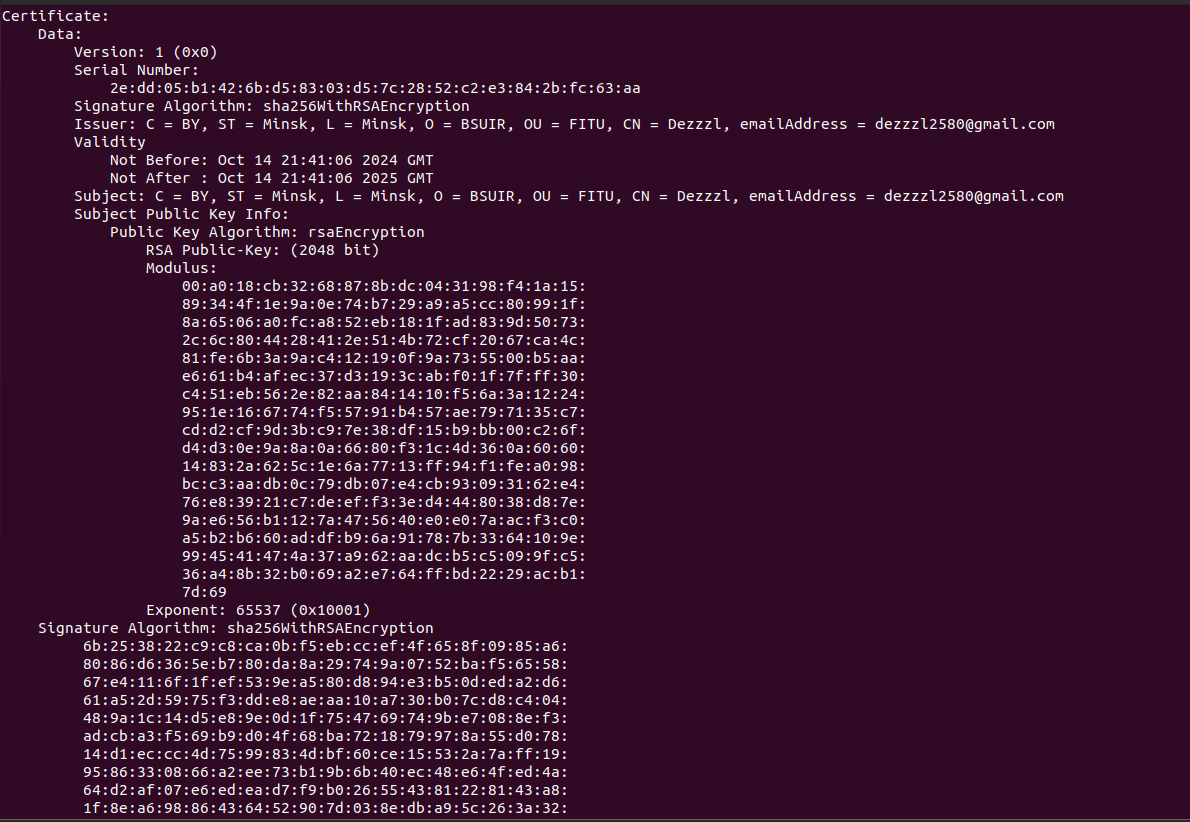


Информация будет включать в себя:

* Страна
* Штат или провинция
* Город
* Организация
* Подразделение
* Имя общего домена (Common Name, CN)
* Электронная почта

При просмотре сертификата можно увидеть несколько ключевых компонентов:

1. **Версия**. Указывает версию формата сертификата (обычно это v3).
2. **Субъект**. Содержит информацию о владельце.
3. **Публичный ключ**. Содержит публичный ключ, соответствующий приватному ключу, использованному для подписи сертификата.
4. **Издатель**. В случае самоподписанного сертификата это будет тот же субъект.
5. **Срок действия**. Указывает дату начала и окончания действия сертификата.
6. **Алгоритм подписи**. Указывает, какой алгоритм был использован для подписи сертификата (например, SHA256 с RSA).
7. **Серийный номер**. Уникальный номер сертификата, выданного удостоверяющим центром.
8. **Расширения**. Дополнительные параметры, такие как ограничение на использование ключа (например, для шифрования или подписи).



Вывод:

OpenSSL — это мощная библиотека для выполнения криптографических операций. В ходе работы с ней были выполнены несколько задач. Исследовались скорости различных симметричных (AES, DES) и асимметричных (RSA) алгоритмов шифрования. Были проведены шифрование и расшифрование файлов с использованием как симметричных, так и асимметричных алгоритмов. Также получены хэш-значения файлов с помощью алгоритмов MD5 и SHA1 для проверки их целостности. Сгенерирован самоподписанный сертификат X.509, изучены его компоненты и назначение. Эти операции продемонстрировали широкий спектр возможностей OpenSSL в области криптографии и управления безопасностью данных.