МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский Авиационный Институт»
(Национальный Исследовательский Университет)

Институт: №8 «Информационные технологии и прикладная математика»
Кафедра: 806 «Вычислительная математика и программирование»

Лабораторная работа № 1
по курсу «Криптография»

Группа: М8О-307Б-21

Студент(ка): Ф. А. Меркулов

Преподаватель: А. В. Борисов

Оценка:

Дата: 05.03.2024

Москва, 2024

ОГЛАВЛЕНИЕ

1 Тема

Темой данной лабораторной работы является знакомство с открытым стандартом для криптографических операций OpenPGP, а также создание и использование ключей OpenPGP для шифрования и цифровой подписи электронной корреспонденции

2 Задание

1. Создать пару OpenPGP-ключей, указав в сертификате свою почту. Создать её возможно, например, с помощью почтового клиента thunderbird, или из командной строки терминала ОС семейства linux, или иным способом.

2. Установить связь с преподавателем, используя созданный ключ, следующим образом:

2.1. Прислать собеседнику от своего имени по электронной почте сообщение, во вложении которого поместить свой сертификат открытого ключа.

2.2. Дождаться письма, в котором собеседник Вам пришлет сертификат своего открытого ключа.

2.3. Выслать сообщение, зашифрованное на открытом ключе собеседника.

2.4. Дождаться ответного письма.

2.5. Расшифровать ответное письмо своим закрытым ключом.

3. Собрать подписи под своим сертификатом открытого ключа.

3.0. Получить сертификат открытого ключа одногруппника.

3.1. Убедиться в том, что подписываемый Вами сертификат ключа принадлежит его владельцу - путём сравнения отпечатка ключа или ключа целиком, по доверенным каналам связи.

3.2. Подписать сертификат открытого ключа одногруппника.

3.3. Передать подписанный Вами сертификат полученный в п.3.2 его владельцу, т.е. одногруппнику.

3.4. Повторив п.3.0.-3.3., собрать 10 подписей одногруппников под своим сертификатом.

3.5. Прислать преподавателю свой сертификат открытого ключа, с 10-ю или более подписями одногруппников.

3. Подписать сертификат открытого ключа преподавателя и выслать ему

3 Теория

Стандарт OpenPGP

OpenPGP представляет собой не просто технологию, но и стандарт, который определяет форматы для зашифрованных сообщений, подписей и ключей для обмена сообщениями в электронной почте и других видах связи. Разработанный как открытый стандарт, он описывает системы шифрования, которые используют различные методы криптографии, в том числе и асимметричное шифрование.

Принцип работы асимметричного шифрования

Асимметричное шифрование, также известное как шифрование с открытым ключом, использует пару ключей для шифрования и расшифровки данных. Эти ключи математически связаны между собой и включают в себя:

- **Открытый ключ:** Предназначен для шифрования данных и может быть свободно распространен.
- **Закрытый ключ:** Используется для расшифровки данных и должен оставаться в секрете.

Шифрование и подпись данных

Шифрование позволяет пользователям передавать сообщения таким образом, что только предполагаемый получатель сможет их прочитать. Цифровая подпись удостоверяет подлинность отправителя и гарантирует целостность данных. Это осуществляется путем создания хеш-суммы

сообщения и ее шифрования с использованием приватного ключа отправителя, что может быть проверено любым, кто имеет открытый ключ.

Аутентификация и сеть доверия

Аутентификация через открытые ключи позволяет установить подлинность пользователя, который отправляет данные. Это может быть достигнуто через процесс проверки подписей на сертификатах открытых ключей, создавая тем самым сеть доверия. Пользователи могут подписывать сертификаты других лиц, тем самым удостоверяя их подлинность в рамках их собственной сети контактов.

Обмен ключами и коммуникации

Процесс обмена ключами начинается с распространения открытого ключа пользователя. После обмена открытыми ключами, отправитель может зашифровать сообщение с использованием открытого ключа получателя. Только получатель, владеющий соответствующим приватным ключом, сможет расшифровать это сообщение.

Важность сертификатов и их подписи

Сертификаты открытых ключей играют ключевую роль в процессе обеспечения безопасности. Подписание сертификатов - это метод удостоверения, что открытый ключ действительно принадлежит указанному владельцу. Это усиливает доверие в сети и помогает предотвратить атаки посредника.

Реализации OpenPGP

На практике стандарт OpenPGP реализуют такие утилиты как gpg (для unix систем) и gpg4win для ОС Windows. Для отправки и получения электронных писем существует отдельный почтоый клиент Thunderbird, который поддерживает стандарт OpenPGP, позволяя расшифровывать, зашифровать и просматривать расшифрованные письма прямо в программе.

4 Ход лабораторной работы

При выполнении лабораторной работы я использовал утилиту gpg для создания ключей и произведения операций над ними (например, подпись).

1. **Подготовка рабочего пространства**

   Перед началом выполнения лабораторной работы я скачал утилиту gpg с помощью команды sudo apt-get install —only-upgrade gpg

2. **Создание ключа**

   Перед началом работы я создал у себя пару из закрытого и открытого ключей через утилиту gpg, введя команду gpg —full-generate-key. Далее в интерактивном режиме я ввел свое имя, почту, фразу-пароль, промежуток времени, в течение которого ключ будет считаться действительным, и размер ключа.

3. **Отправка сертификата публичного ключа**

   Я сгенерировал сертификат моего публичного ключа через команду gpg --armor --export [Почта ключа] >> [Имя файла].asc и предоставил его своему собеседнику и получил от него сертификат его публичного ключа.

4. **Шифрование сообщения**

   Для того чтобы отправить сообщение собеседнику мне необходимо было зашифровать его с помощью открытого ключа, который собеседник мне отправил до этого.

   Для добавления открытого ключа собеседника в базу данных gpg я использовал команду gpg --import [Имя файла].asc

   Для шифрования сообщения я использовал команду: gpg –encrypt –armor --recipient [Почта ключа] [Имя Файла].asc.

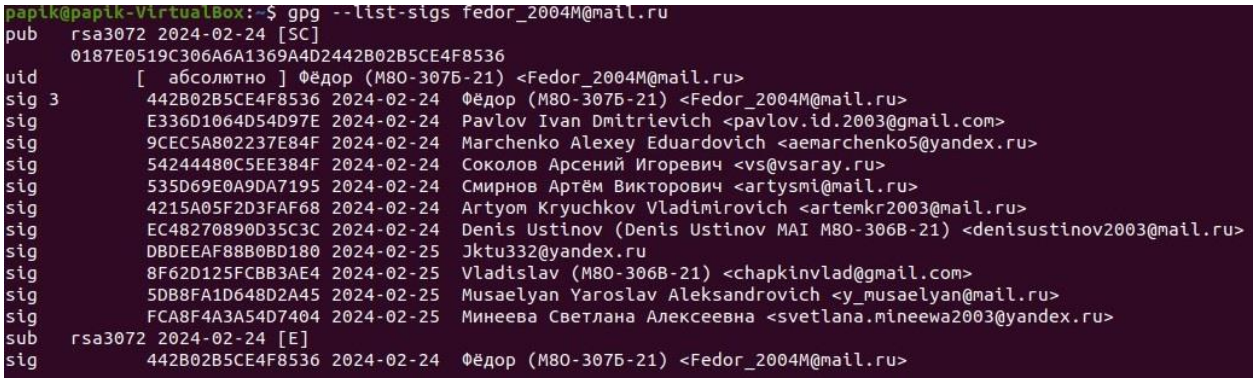
5. **Расшифровка сообщения**

   После того как я получил зашифрованное сообщение от собеседника мне необходимо было его расшифровать. Для этого я использовал команду: gpg --decrypt [Имя Файла].asc

6. Подпись сертификата однокурсников

Одним из заданий лабораторной работы была подписать сертификатов открытого ключа однокурсников. Для этого я использовал команду gpg --sign-key [Почта ключа]. После этого я экспортировал уже подписанный мною сертификат открытого ключа и отправил его обратно однокурсникам.

С другой стороны, я также собрал 10 подписей одногруппников. Для получения информации о подписях сертификата я использовал команду gpg –list-sigs [Почта ключа].



5 Выводы

В ходе выполнения данной лабораторной работы я научился пользоваться утилитой gpg, изучил основы зашифрованного обмена сообщениями на основе стандарта OpenPGP, ознакомился с базовыми процессами: создание ключей, передача публичных ключей, шифровка/расшифрока сообщения, подпись ключей и сообщений, которые возникают при защищённом обмене сообщениями.

Подпись в контексте стандарта OpenPGP заслуживает особого внимания благодаря своей универсальности и возможности адаптации к различным сферам применения. Этот элемент криптографической безопасности может сыграть ключевую роль в процессах идентификации пользователей, например, в системах контроля доступа сотрудников. Кроме того, функционал подписей может быть эффективно использован для верификации подлинности данных, что придает ему значимую роль в обеспечении информационной надежности.

6 Список используемой литературы

- GPG man page: https://linux.die.net/man/1/gpg
- Документация OpenPGP: https://www.openpgp.org/about/documentation/