**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: Дубровин Дмитрий

Преподаватель: А. В. Борисов

Оценка:

Дата: 14.03.2024

Москва, 2024

**ОГЛАВЛЕНИЕ**

[1 Тема 3](#_Toc158983147)

[2 Задание 3](#_Toc158983148)

[3 Теория 4](#_Toc158983149)

[4 Ход лабораторной работы 5](#_Toc158983150)

[5 Выводы 6](#_Toc158983151)

# **Тема**

Шифрование и подпись на примере OpenGPG ключей и почтового сервиса Thunderbird.

# **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.

2.5. Дождаться ответного письма.

2.6. 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.

4. Подписать сертификат открытого ключа преподавателя и выслать ему.

# **Теория**

**OpenPGP ключи** — это ключи, используемые в криптографической системе OpenPGP для шифрования и подписи данных. OpenPGP является стандартом, который определяет форматы и алгоритмы для шифрования и подписи данных, а также для управления ключами.

В OpenPGP используются два вида ключей: приватные (секретные) и публичные. Публичный ключ можно свободно распространять, и он используется для шифрования данных или для проверки подписи. Приватный ключ держится в секрете и используется для расшифровки данных или создания подписи.

Когда данные шифруются с использованием публичного ключа, они могут быть расшифрованы только соответствующим приватным ключом. Это обеспечивает конфиденциальность передачи данных. Когда данные подписываются с использованием приватного ключа, любой может проверить подпись с помощью соответствующего публичного ключа, что обеспечивает аутентификацию и целостность данных.

**Thunderbird** — это бесплатный почтовый клиент, разработанный Mozilla Foundation. Он позволяет пользователям управлять своими электронными письмами, контактами и календарями в одном приложении. Thunderbird поддерживает различные протоколы электронной почты, включая POP3, IMAP и SMTP, что делает его совместимым с большинством почтовых сервисов.

Thunderbird поддерживает использование OpenPGP ключей для шифрования и подписи электронных писем. Пользователи могут генерировать пару ключей (публичный и приватный) непосредственно в Thunderbird или импортировать существующие ключи. При отправке зашифрованного письма, Thunderbird использует публичный ключ получателя для шифрования содержимого, так что только приватный ключ получателя может расшифровать сообщение. Это обеспечивает конфиденциальность сообщения. Кроме того, пользователи могут подписывать свои письма с использованием своего приватного ключа. Получатель может проверить подпись, используя публичный ключ отправителя, что подтверждает аутентичность отправителя и целостность сообщения. Thunderbird также позволяет управлять ключами OpenPGP, включая их импорт, экспорт и отзыв, что облегчает обмен публичными ключами с другими пользователями для установления зашифрованной коммуникации.

# **Ход лабораторной работы**

Мною была создана пара ключей с помощью Windows Terminal командой ***`gpg --gen-key`***. Были заданы такие параметры: RSA 4096.

Дальше я применил свои социальные навыки и начал коммуницировать с людьми ради получения от них их сертификатов.

Кстати получить свой сертификат можно командой ***`gpg --export --armor [идентификатор\_ключа] > signed\_key.asc`***.

Так вот, получив от собеседника сертификат, я возвращался в терминал, дабы подписать их сертификат своим ***secret key***. Я импортировал их ключ к себе командой ***`gpg --import public\_key.asc`*** и подписывал его командой ***`gpg --sign-key [идентификатор\_ключа]`***. Ну и экспортировал, и отдавал собеседнику. С их стороны процесс проистекал также.

И так 10 раз.

Получив все сертификаты, я установил такой сервиса как Thunderbird, подключил свою почту и отправил сообщение на почту преподавателя, прислав свой сертификат с 10-ю подписями, подписанный моим ключом сертификат преподавателя и конечно же данный отчет. При это я зашифровал содержимое письма открытым ключом преподавателя, который я получил ранее.

# **Выводы**

Я узнал о существовании OpenGPG ключей и шифровании писем. Мне это тема показалась интересной, потому что я не ожидал, что это будет так просто. Я думал процесс труднее. Трудностей при выполнении не возникло. Резюмируя: лабораторная работа была необычной и интересной.

# **Список используемой литературы**

1. <https://www.openpgp.org/>
2. <https://ssd.eff.org/ru/module/%D1%80%D1%83%D0%BA%D0%BE%D0%B2%D0%BE%D0%B4%D1%81%D1%82%D0%B2%D0%BE-%D0%BF%D0%BE-pgp-%D0%B4%D0%BB%D1%8F-windows>