**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-308Б-21

Студент(ка): К.А.Белоносов

Преподаватель: А. В. Борисов

Оценка:

Дата: 05.03.2024

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**

Генерация и работа с OpenPGP ключами

# **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.

2.4. 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.

3. Подписать сертификат открытого ключа преподавателя и выслать ему

# **Теория**

OpenPGP (Open Pretty Good Privacy) — это протокол для шифрования электронной почты с использованием криптографии с открытым ключом. В 1991 году Фил Циммерманн разработал программное обеспечение Pretty Good Privacy (PGP), которое предоставляло возможность шифрования и подписи электронных сообщений с помощью открытых и закрытых ключей. OpenPGP является открытой версией протокола шифрования PGP, разрабатываемой OpenPGP Working Group в рамках Internet Engineering Task Force (IETF). OpenPGP подразумевает следующие варианты использования:

1. Генерация ключей: Сначала нужно сгенерировать пару ключей: открытый и закрытый. Открытый ключ можно распространять, а закрытый ключ следует хранить в секрете.
2. Шифрование сообщений: Чтобы зашифровать сообщение, используйте открытый ключ получателя. Он сможет расшифровать сообщение с помощью своего закрытого ключа.
3. Цифровая подпись: Чтобы подписать сообщение, используйте свой закрытый ключ. Получатель может проверить подпись с помощью вашего открытого ключа.
4. Интеграция с почтовыми клиентами: Множество почтовых клиентов поддерживает OpenPGP. Установите соответствующее расширение или плагин, чтобы начать использовать шифрование и подпись.

OpenPGP использует ассиметричное шифрование с открытым ключом. Оно базируется на следующих принципах:

1. Можно сгенерировать пару очень больших чисел (открытый ключ и закрытый ключ) так, чтобы, зная открытый ключ, нельзя было вычислить закрытый ключ за разумный срок.
2. Имеются надёжные методы шифрования, позволяющие зашифровать сообщение открытым ключом так, чтобы расшифровать его можно было только закрытым ключом.
3. Владелец двух ключей никому не сообщает закрытый ключ, но передает открытый ключ контрагентам или делает его общеизвестным.

# **Ход лабораторной работы**

1. Создал пару открытый и закрытый ключ с помощью thunderbird
2. С помощью ключа преподавателя, подписал письмо. В результате которого было установлено общение
3. Получил от преподавателя письмо, расшифровал его
4. Произвел сбор подписей среди одногруппников
   1. Подписывал открытые ключи, которые присылали мне одногруппники
   2. Отправил свой ключ на подпись 10 одногруппникам
   3. Подписал сертификат открытого ключа преподавателя

# **Выводы**

В результате данной лабораторной работы я познакомился со стандартом шифрования OpenPGP, научился генерировать пару ключей и подписывать другие ключи. Также были изучены основные принципы ассиметричного шифрования с открытым ключом. Полученные знания имеют большую практическую ценность, т.к. шифрование OpenPGP часто используется в почтовых системах.

# **Список используемой литературы**

<https://www.openpgp.org/>

<https://wiki.archlinux.org/title/OpenPGP_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29>

<https://habr.com/ru/articles/358182/>