**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-310Б-21

Студент: А. С. Личковаха

Преподаватель: А. В. Борисов

Оценка:

Дата: 15.03.24

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**

Коммуникация с использованием PGP-ключей.

# **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 (Pretty Good Privacy) - это открытый стандарт шифрования, подписи и аутентификации данных, который используется для обеспечения конфиденциальности и целостности информации. Он базируется на алгоритмах с открытым исходным кодом, таких как RSA (Rivest-Shamir-Adleman) для шифрования и подписи, SHA (Secure Hash Algorithm) для генерации хэшей и т.д.

Для создания OpenPGP-ключей необходимо сгенерировать открытый и закрытый ключи, которые будут использоваться для шифрования и подписи сообщений.

Установление защищенной связи:

1. Отправка открытого ключа: Для установления защищенной связи с кем-либо, необходимо отправить свой открытый ключ собеседнику по электронной почте в зашифрованном виде. Это позволит собеседнику шифровать сообщения для вас.

2. Обмен открытыми ключами: Получив открытый ключ вашего собеседника, необходимо сохранить его в своем клиенте OpenPGP. Также, для обеспечения конфиденциальности, можно зашифровать и послать сообщение, используя его открытый ключ.

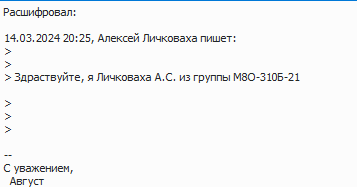
3. Подписи и доверие: Для убедительности, можно собирать подписи под своим открытым ключом. Это поможет другим убедиться в подлинности ключа.

По завершении процесса сбора подписей и установления доверия между участниками, необходимо передать свой сертификат открытого ключа собеседникам и преподавателю для обеспечения безопасной и защищенной коммуникации в дальнейшем.

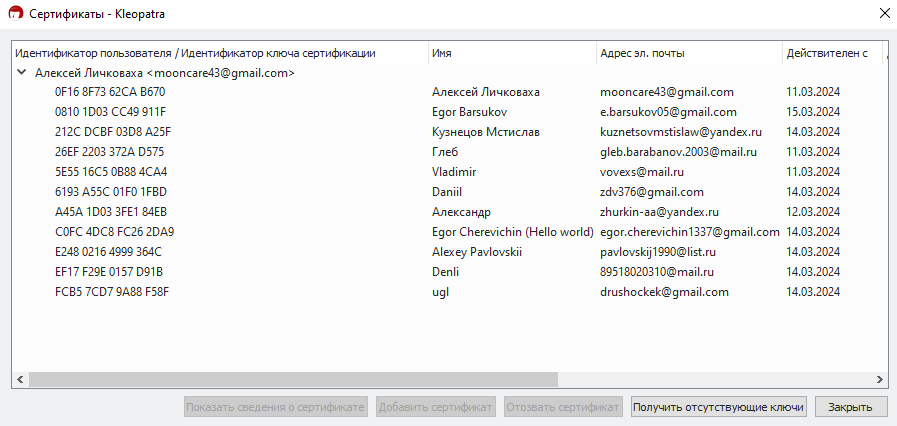
Таким образом, процесс использования OpenPGP для обеспечения безопасной связи включает в себя создание ключей, обмен открытыми ключами, установление доверия через подписи, а также передачу сертификатов для обеспечения конфиденциальности и целостности данных при общении в интернете.

# **Ход лабораторной работы**

1. Была создана пара OpenPGP-ключей с использованием Kleopatra, указана в сертификате своя почту.
2. Зашифровано сообщение открытым ключом преподавателя.
3. Отправлено ему на почту, вместе с моим открытым ключом.
4. Полученное ответное письмо было расшифровано моим закрытым ключом:



1. Собраны 10 подписей однокурсников под своим ключом, мой ключ с подписями прикреплён к отчёту:



# **Выводы**

Проделав лабораторную работу, я познакомился с программным обеспечением Kleopatra и разобрал концепцию шифрования сообщений с помощью PGP-ключей.