**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-306Б-21

Студент(ка): О. А. Мезенин

Преподаватель: А. В. Борисов

Оценка:

Дата: 03.03.2024

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**

OpenPGP-ключи. Шифрование, дешифрование, подпись сертификатов.

# **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.

4. Подписать сертификат открытого ключа преподавателя и выслать ему.

# **Теория**

# Для выполнения лабораторной работы потребовалось изучить работу инструмента GPG и его основные команды.

# GPG — это инструмент для шифрования и электронной подписи, который использует асимметричное шифрование с двумя ключами: приватным и публичным. Процесс работы GPG заключается в следующем: пользователь создаёт себе пару ключей. С помощью публичного ключа он шифрует сообщение, а расшифровать его можно только с помощью соответствующего приватного ключа.

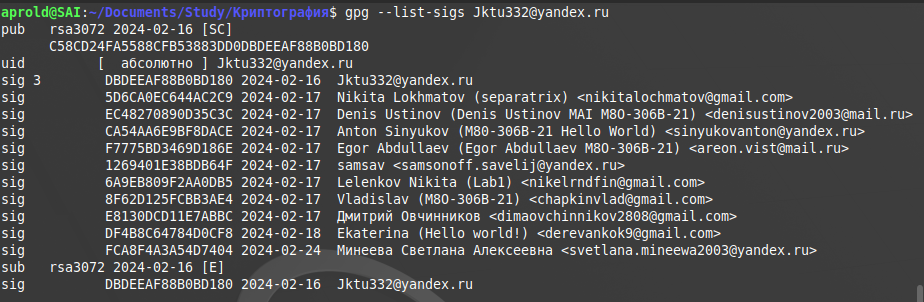
# Подпись сертификатов в GPG нужна для верификации сообщений. Они применяются для того, чтобы удостовериться, что сообщение пришло от доверенного лица.

# **Ход лабораторной работы**

Лабораторная работа выполнялась в соответствии с планом. В ходе работы были применены следующие команды:

* gpg --full-generate-key — создать пару ключей;
* gpg --list-keys — показать список ключей;
* gpg --import key.asc — импортировать ключ;
* gpg -a --export email — экспортировать ключ;
* gpg --encrypt -a --recipient email message.txt — зашифровать сообщение message.txt с помощью открытого ключа;
* gpg -d message.asc — расшифровать сообщение message.asc с помощью закрытого ключа;
* gpg --sign-key email — подписать сертификат;
* gpg --list-sigs email — показать подписи ключа;
* gpg --fingerprint email — показать отпечатки ключа.

Вывод подписей под моим сертификатом:



Расшифровка сообщения преподавателя:



# **Выводы**

В ходе лабораторной работы ознакомился с работой асимметричного шифрования с помощью инструмента GPG. Научился создавать открытые и закрытые ключи, зашифровывать и расшифровывать сообщения, подписывать сертификаты.

# **Список используемой литературы**

1. Сайт OpenPGP - https://www.openpgp.org/
2. Документация GnuPG - <https://www.gnupg.org/>
3. Асимметричная криптография для чайников - https://habr.com/ru/articles/748226/