**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-312Б-22

Студент(ка): Л. Д, Андрюшин

Преподаватель: А. В. Борисов

Оценка:

Дата: 20.03.2025

Москва, 2025

**ОГЛАВЛЕНИЕ**

[1 Тема 3](#_Toc158983147)

[2 Задание 3](#_Toc158983148)

[3 Теория 5](#_Toc158983149)

[4 Ход лабораторной работы 6](#_Toc158983150)

[5 Выводы 8](#_Toc158983151)

# **Тема**

Лабораторная работа №1

# **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*** — это открытый криптографический стандарт, который определяет, как должны работать системы шифрования, цифровых подписей и управления ключами. Он основан на PGP (Pretty Good Privacy), который был создан Филом Циммерманом в 1991 году. OpenPGP представляет собой протокол, описанный в RFC 4880, и служит основой для различных программ, обеспечивающих безопасность передачи и хранения данных. Он позволяет шифровать сообщения и файлы, подписывать их для подтверждения подлинности и управлять ключами, обеспечивая систему доверия между пользователями.

***GnuPG (GNU Privacy Guard, или GPG)*** — это конкретная программа, реализующая стандарт OpenPGP. Она является свободным программным обеспечением, разработанным в рамках проекта GNU, и предоставляет пользователям инструменты для шифрования данных, цифровых подписей и управления криптографическими ключами. GnuPG позволяет генерировать пары ключей (открытый и закрытый), шифровать сообщения так, чтобы их мог прочитать только владелец соответствующего закрытого ключа, подписывать файлы для подтверждения их подлинности и проверять подписи других пользователей. Одной из ключевых особенностей GnuPG является поддержка "сети доверия" (Web of Trust), где пользователи могут подписывать ключи друг друга, тем самым создавая систему подтверждения личности без центрального органа сертификации.

# **Ход лабораторной работы**

В начале мы генерируем ключ с помощью команды gpg --full-generate-key. По ходу генерации мы выбираем различные параметры: тип ключа, размер ключа, срок действия ключа, имя и пароль.

После этого мы вводим команду gpg --list-keys, чтобы проверить, что мы создали ключ.

После этого я ввел команду gpg --export --armor Vingael.36@gmail.con > vingael\_key.asc для создания файла, который буду отправлять одногруппникам для получения подписи.

После этого я обменялся 10 подписями с одногруппниками. Вот алгоритм подписи чужого ключа:

gpg –import – импортируем ключ к себе

gpg --fingerprint– сравниваем отпечатки ключа

gpg --sign-key– подписываем ключ

gpg –export– экспортируем ключ

После этого нужно просто импортировать подписанный ключ

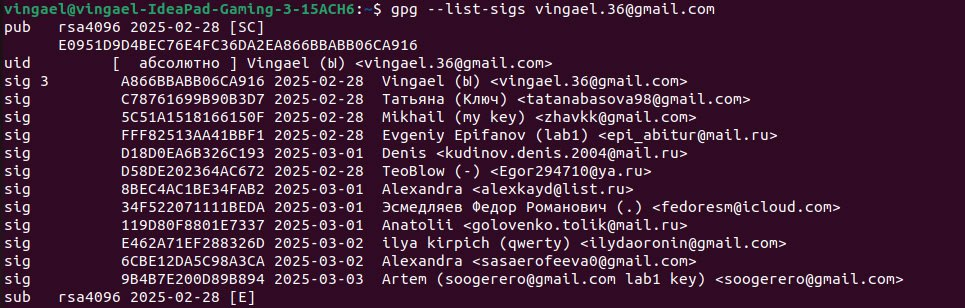
Для зашифровки сообщения мы изначально должны создать текстовый файл. Можно сделать это вручную, а можно, например, с помощью команды echo:

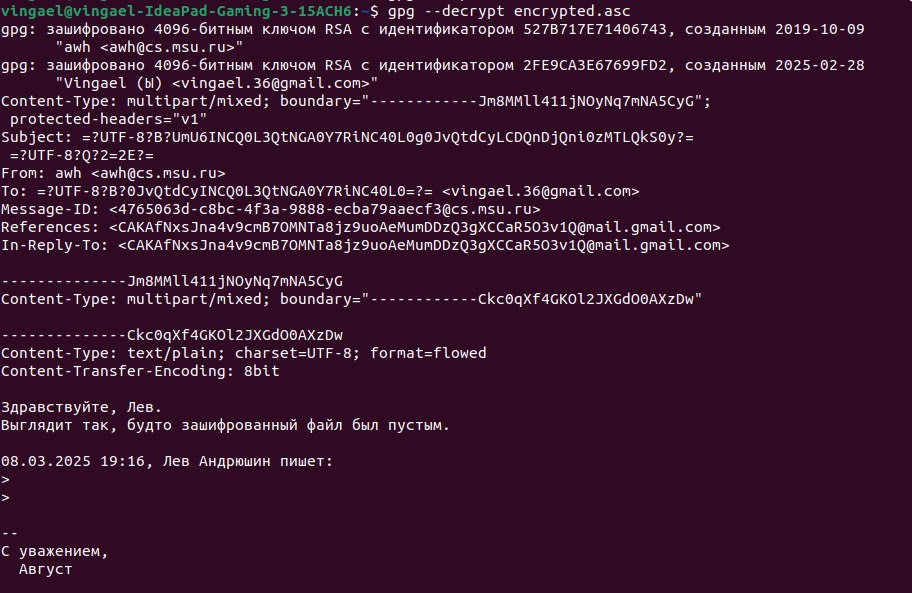
echo "Ляляля-траляля." > message.txt

Потом шифруем сообщение ключом собеседника:

gpg --encrypt --armor -r

Для расшифровки сообщения используем вот эту команду:  
gpg --decrypt

*рис. 1 Подписи под ключом*



*рис. 2 расшифровка подписей*

# **Выводы**

В ходе выполнения лабораторной работы были изучены и практически применены методы асимметричного шифрования с использованием OpenPGP и GnuPG. В процессе работы была освоена генерация ключевой пары, обмен открытыми ключами, цифровое подписание и проверка подписей, а также шифрование и расшифровка сообщений. Полученные знания могут быть использованы для обеспечения конфиденциальности и аутентичности электронной переписки, защиты данных при передаче, а также организации системы доверия в цифровых коммуникациях.

# **Список используемой литературы**

1. https://www.gnupg.org/