**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-309Б-22

Студент: О. С. Концебалов

Преподаватель: А. В. Борисов

Оценка:

Дата: 14.03.2025

Москва, 2025

**ОГЛАВЛЕНИЕ**

[1 Тема 3](#_Toc158983147)

[2 Задание 3](#_Toc158983148)

[3 Теория 4](#_Toc158983149)

[4 Ход лабораторной работы 5](#_Toc158983150)

[5 Выводы 6](#_Toc158983151)

# **Тема**

«Использование OpenPGP для шифрования, подписи и создания сети доверия»

# **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**

Криптография с открытым ключом (асимметричная криптография) — это метод шифрования, при котором используются два ключа: открытый (public key) и закрытый (private key). Открытый ключ доступен всем и используется для шифрования данных, а закрытый ключ хранится в секрете и используется для расшифровки данных. Этот подход решает проблему безопасного обмена ключами, которая существует в симметричной криптографии.

OpenPGP — это стандарт шифрования, основанный на асимметричной криптографии. Он используется для шифрования, подписи и проверки подлинности данных, таких как электронные письма, файлы и сообщения. OpenPGP позволяет создавать пары ключей (открытый и закрытый), подписывать данные, шифровать сообщения и обмениваться ключами с другими пользователями.

GnuPG (GNU Privacy Guard) — это опенсорсная реализация открытого стандарта OpenPGP. GnuPG состоит из набора программ и библиотек, однако нас будет интересовать только консольная программа gpg. Она существует под все операционные системы, однако наиболее комфортно используется в linux и macos.

Концептуально OpenPGP представляет собой крайне сложную для понимания систему понятий и действий. Поскольку OpenPGP не навязывает какой-либо конкретный сценарий использования, его конкретные реализации очень легко можно использовать небезопасно. И даже если вы понимаете все концепты, то даже в такой ситуации не застрахованы от ошибки из-за большой гибкости инструментов.

При использовании gnupg буквально заваливает вас тоннами различных предупреждений и сообщений, степень важности которых неочевидна. И наоборот, в критичных ситуациях нет сообщений, предупреждающих о небезопасности действия. Пример последнего — расшифровка файла без дополнительной подписи.

Продвигаемая в OpenPGP система доверия Web of trust является более гибкой, чем традиционная PKI (public key infrastructure) с делегированием проверки на удостоверяющие центры в TLS, например. Однако эта гибкость даётся ценой очень высокой концептуальной сложности и требованием тщательного изучения концептов. В результате идеи и реализации OpenPGP широкого распространения не получили даже в корпоративной среде, где, в теории, такой подход был бы очень полезен.

Главный компонент OpenPGP — ключ. В рабочей конфигурации обычно хранится несколько ключей: ваш собственный и чужие ключи. Каждый ключ состоит из двух частей: обязательной открытой и опциональной закрытой. Закрытая хранится только у владельца ключа в зашифрованном виде. Открытая распространяется свободно в интернете.

Закрытая часть используется для:

* подписывания/удостоверения данных;
* дешифрования зашифрованных файлов.

Закрытый ключ зашифрован симметричным алгоритмом и при его использовании нужно вводить пароль (парольную фразу), которым ключ зашифрован в хранилище.

Открытая часть используется для:

* проверки подписи данных;
* шифрования данных.

В закрытой части хранятся закрытые криптоключи, в открытой соответственно открытые криптоключи.

Таким образом, если вы хотите кому-то отправить зашифрованный текст, который получатель сможет расшифровать, вы берёте открытый криптоключ этого пользователя, шифруете этим ключом данные. Получатель берёт у себя закрытую компоненту криптоключа и расшифровывает.

Если вы хотите подтвердить/удостоверить подлинность текста, берёте свой закрытый криптоключ, вычисляете при помощи него и первоначального текста специальный набор байтов, называемый *электронной подписью*, и отправляете *подпись* вместе с документом. Получатель берёт ваш открытый криптоключ, текст и *подпись*, скармливает это всё специальному алгоритму, который говорит: «да, эта подпись соответствует этому открытому криптоключу для этого текста». Таким образом получатель может быть уверен, что он получил точно тот же документ, который вы ему отправили.

Центральной частью OpenPGP-ключа является *мастер-криптоключ*, который служит для подтверждения и удостоверения принадлежности данных внутри ключа. Например, все дополнительные крипто-ключи внутри OpenPGP-ключа (их называют *подчинёнными ключами*/*subkeys*) подписаны мастер-ключом, чтобы удостоверить их принадлежность. Мастер-криптоключ обычно используется только для подписывания, а для шифрования создаются отдельные подчинённые криптоключи.

Помимо криптоключей в OpenPGP-ключе могут находиться и другие блоки данных: информация об именах пользователей (identity), электронные подписи, даже фотографии.

В рабочей конфигурации gnupg обычно хранится один ваш ключ и несколько ключей других людей или организаций. У сторонних ключей тоже есть мастер-криптоключ, только без закрытой части.

# **Ход лабораторной работы**

1) Установил утилиту gpg

2) Создал открытый ключ с помощью команды *gpg --full-generate-key.* Ключ экспортировал в файл с помощью команды *gpg --export -a "baron-pipistron@yandex.ru" > Kontsebalov\_public\_key.asc*

3) Начал обмениваться ключами с товарищами с потока, чтобы взаимно подписать ключи. Для подписания ключа использовались следующие команды

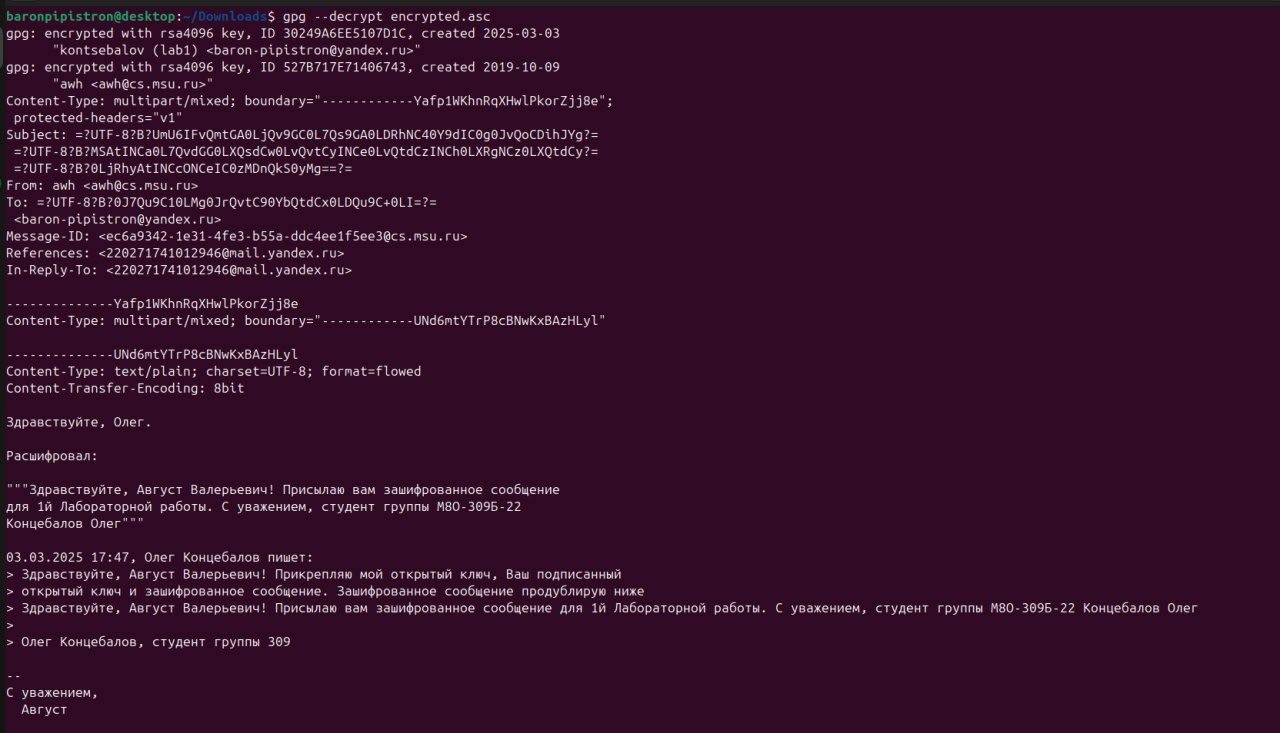
*gpg --import фамилия\_public\_key.asc*

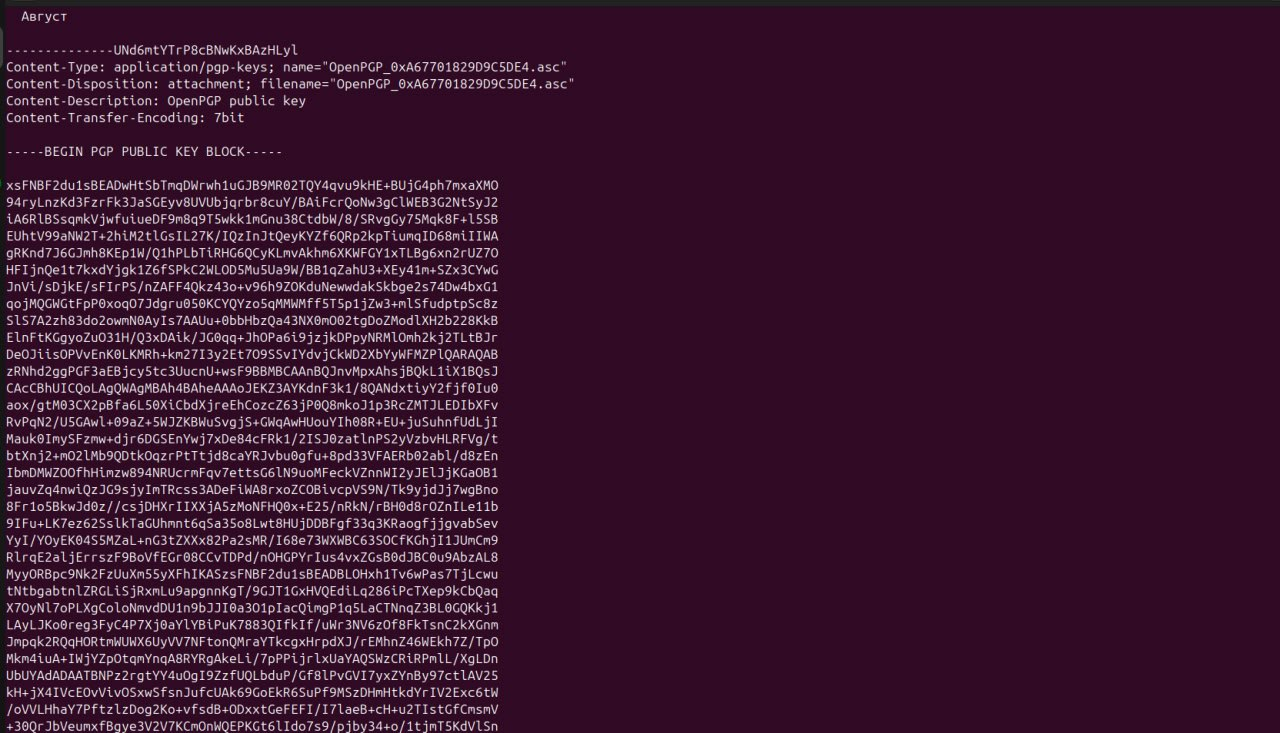
*gpg --sign-key "почта одногруппника"*

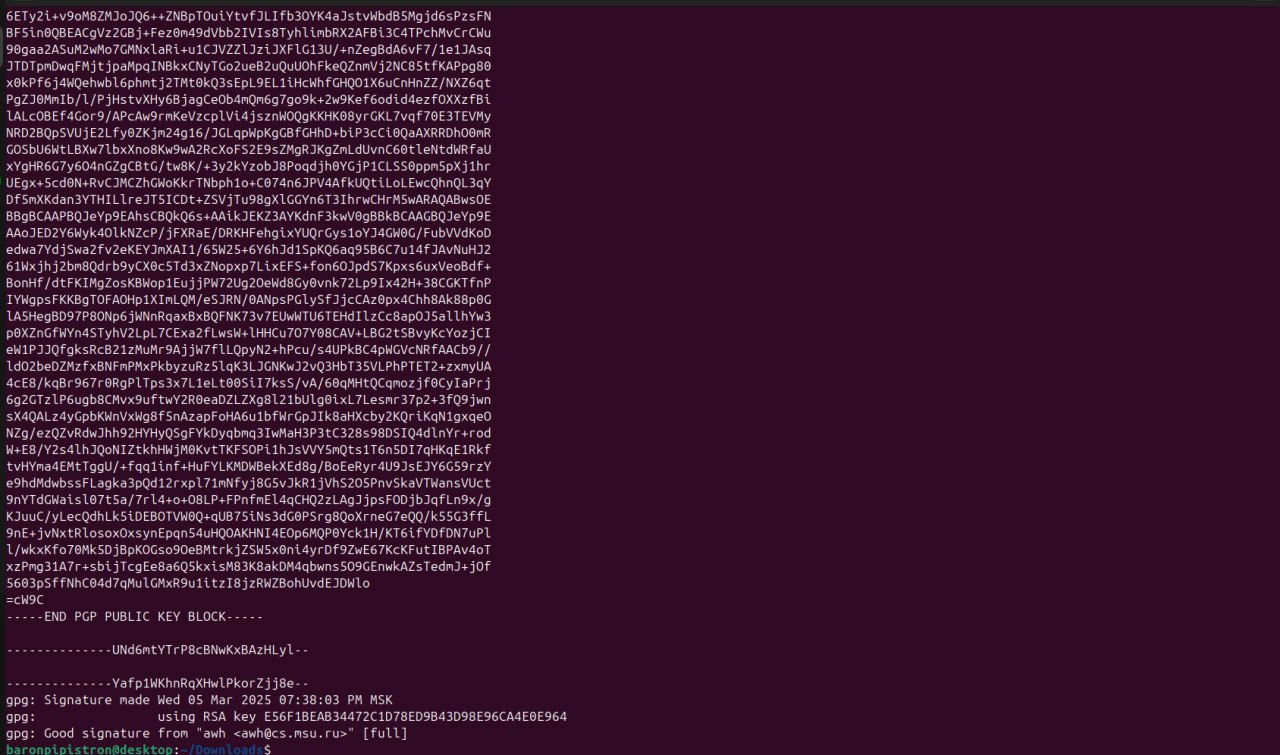
*gpg --export -a "почта одногруппника" > signed\_key.asc*

4) Параллельно с п.3 взял открытый ключ преподавателя из чата в Telegram, подписал его. Зашифровал сообщение с помощью команды *gpg --encrypt --recipient "почта преподавателя" --armor message.txt.* Отправил преподавателю его подписанный ключ и зашифрованное сообщение, а также мой открытый ключ

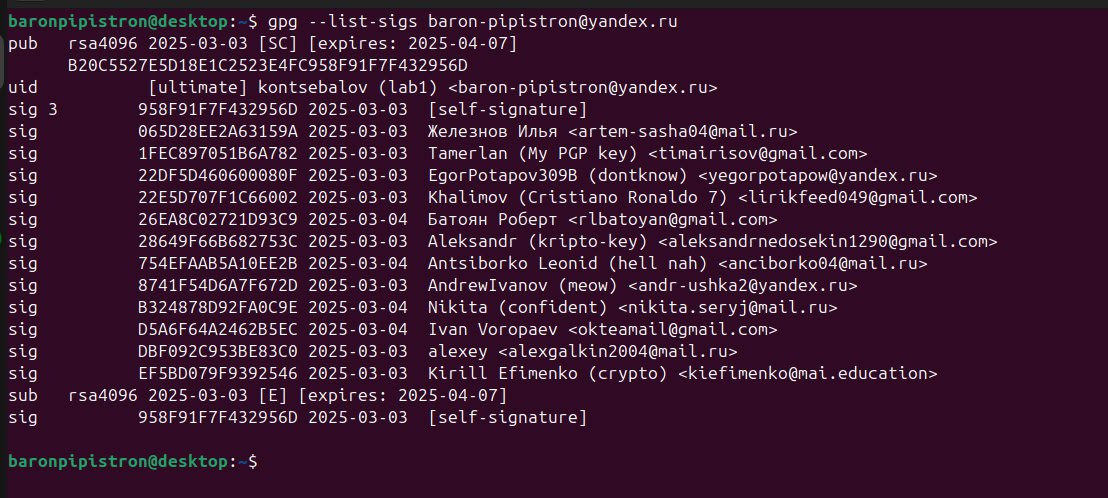
5) Получил от преподавателя зашифрованное сообщение. Расшифровал его с помощью команды *gpg --decrypt message.asc*







6) Собрал 12 подписей на своем экземпляре ключа. Проверил подписи с помощью команды *gpg --list-sigs baron-pipistron@yandex.ru*



7) Отправил преподавателю свой ключ с 12 подписями и отчет к лабораторной работе

# **Выводы**

В ходе лабораторной работы я познакомился со стандартом шифрования OpenPGP, а также освоил работу с утилитой GPG (создание и подписание ключей, шифрование и дешифрование сообщений). Была создана пара ключей (открытый и закрытый) с указанием личного email-адреса в сертификате. Это позволило обеспечить идентификацию отправителя и получателя в дальнейшем обмене сообщениями. Так же были подписаны ключи моих товарищей с потока. Благодаря этому мы создали сеть доверия, а также подтвердили подлинность ключей друг друга. Полученные навыки можно будет применить для защиты как своих повседневных данных, так и данных компании, в которой работаю.

# **Список используемой литературы**

* <https://blog.regolit.com/2013/03/06/understanding-gnupg>
* <https://habr.com/ru/articles/358182/>
* <https://www.gnupg.org/>