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-20

Студент: И. П. Попов

Преподаватель: А. В. Борисов

Оценка:

Дата:

Москва, 2022

# **Создание и использование OpenPGP-ключей**

Задача:

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 - путем 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.

# **Что такое GPG**

**gpg** — это инструмент шифрования и электронного подписания. В его работе используется асимметричное шифрование, основанное на двух ключах: приватный и публичный. Приватный ключ иногда называют секретным. А публичный ключ называют открытым.

Суть работы в общих чертах следующая: любой желающий может сгенерировать себе пару ключей. Публичный ключ (как это можно понять из названия), не является секретным — этот ключ может находиться в открытом доступе. С помощью этого ключа можно шифровать сообщения и файлы. Причём сообщения и файлы шифруются только «в одну сторону» - расшифровать их, даже используя этот самый публичный ключ, уже невозможно. Их расшифровка возможна только при использовании соответствующего приватного ключа.

Таким образом, если вы хотите отправить секретное сообщение или зашифрованный файл определенному лицу, то вы берёте публичный ключ этого лица (который может быть в свободном доступе), зашифровываете информацию и отправляете ему эту зашифрованную информацию — кроме владельца соответствующего приватного ключа её уже никто не сможет узнать.

Если обмениваться публичными ключами, то вы с этим лицом можете вести зашифрованную беседу:

* вы шифруете свои сообщения публичным ключом вашего собеседника и отправляете ему
* он с помощью своего приватного ключа читает эти сообщения
* ваш собеседник шифрует свои сообщения вашим публичным ключом и отправляет вам
* вы с помощью своего приватного ключа читаете свои сообщения
* и так далее

Приватный ключ умеет делать ещё один интересный фокус: он умеет подписывать файлы. Причем, как можно уже догадаться, проверять подпись можно соответствующим публичным ключом.

# **Ход работы**

**Создание пары ключей**

gpg --gen-key

**Процесс шифрования сообщения на публичном ключе собеседника**

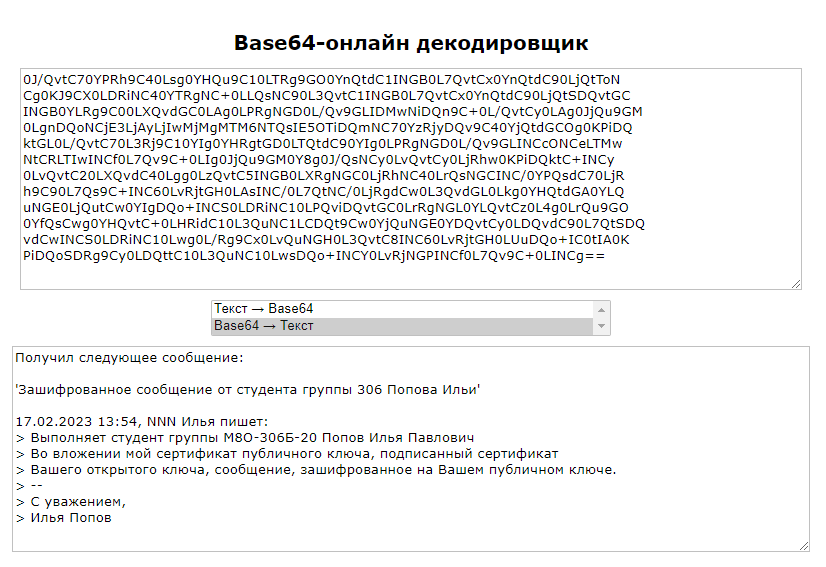
*echo 'текст' | gpg -e -a -r 'получатель' > 'файл\_с\_шифром'*

-a — для того, чтобы зашифрованное сообщение можно было скопировать и вставить в мессенджер или в email. Без этой опции будут выведены бинарные данные.

**Процесс расшифровки сообщения своим приватным ключом**

*gpg -d 'зашифрованный\_файл' > 'расшифрованный\_файл'*

*После дешифрации полученного от преподавателя сообщения утилитой gpg я получил сообщение, зашифрованное на стандарте кодирования base64. Для декодирования я использовал онлайн-декодер:*

**

**Процесс подписи сертификата публичного ключа одногруппника**

Импорт сертификата

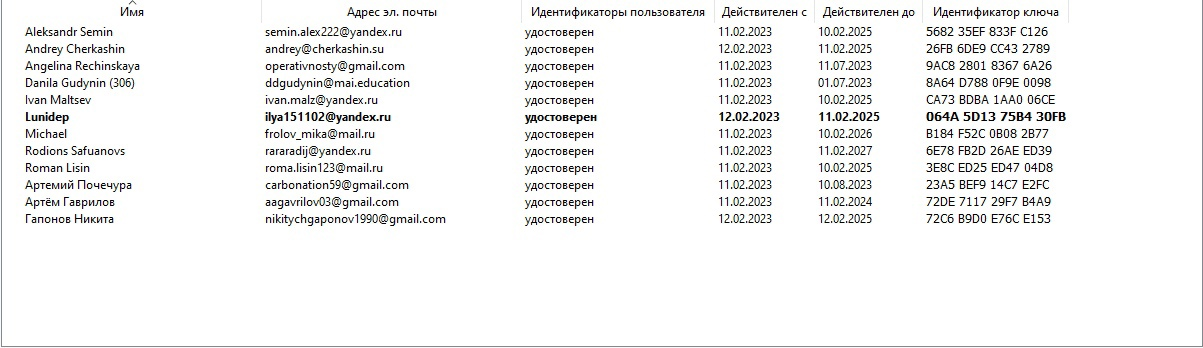
*gpg --import public.key*

при импорте также выводится ключ сертификата. Следующим шагом, этот ключ подписывается (--sign-key) ключом 064A5D1375B430FB. После подтверждения кодовой фразы моего сертификата, сертификат одногруппника, считается подписанным. В конце, сертификат экспортируется в файл

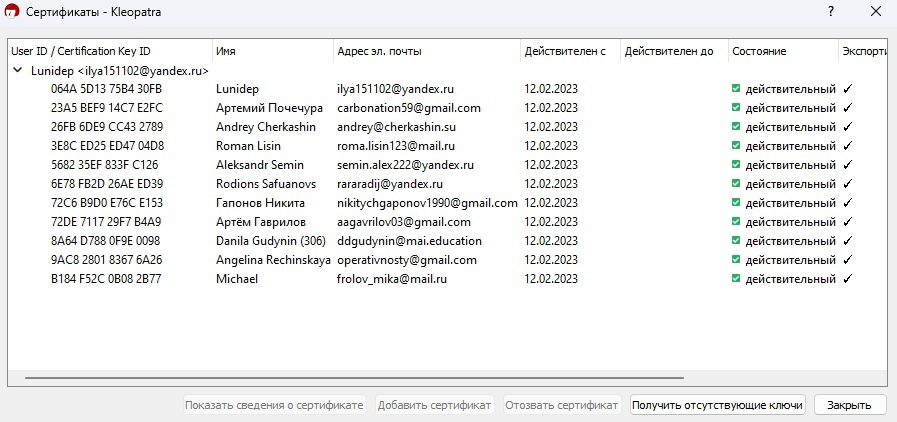
gpg --export *'*подписанный\_сертификат\_публичного\_ключа*'*

для возврата отправителю.

13 одногруппников подписали мой сертификат:



Мои данные сертификаций:



# **Выводы**

В ходе выполнения лабораторной работы я научился использовать шифрование и подписи на примере pgp-ключей. Самым сложным в работе было собрать нужное количество подписей сертификата, остальные этапы оказались проще.

В процессе работы использовалась программа семейства [GPG](https://www.gnupg.org/) (GNU Privacy Guard) “Kleopatra”.

GPG оказалась простой в освоении и очень удобной утилитой с помощью которой можно легко решать задачи асимметричного шифрования.