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 №2

по курсу «Криптография»

Студент:	Хренникова А. С.
Группа:	М8О-308Б-19
Преподаватель:	Борисов. А. В.
Подпись:	
Оценка:	
Дата:	

Москва, 2022

Лабораторная работа №2

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.

2.3. 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.

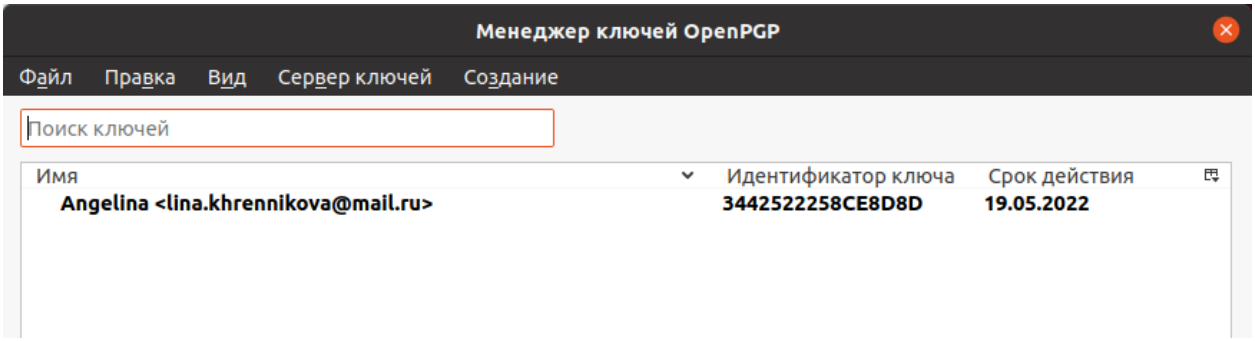
3.5. Прислать преподавателю свой сертификат открытого ключа, с 10-ю или более подписями одногруппников.

4. Подписать сертификат открытого ключа преподавателя и выслать ему.

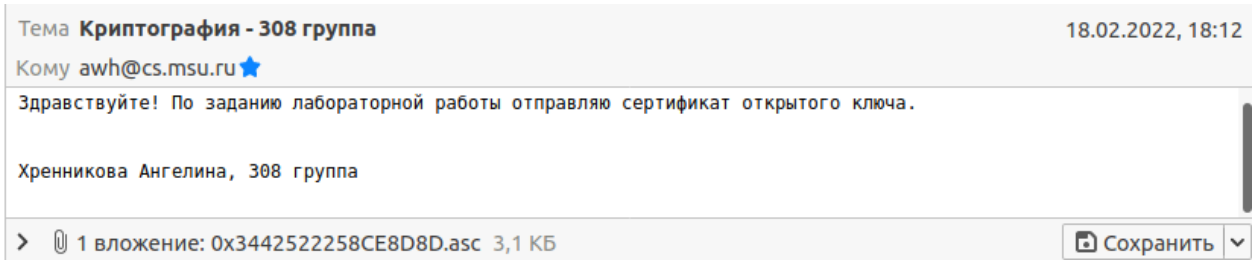
1 Описание

Для выполнения данной лабораторной работы я пользовалась как утилитой gpg, так и почтовым клиентом thunderbird.

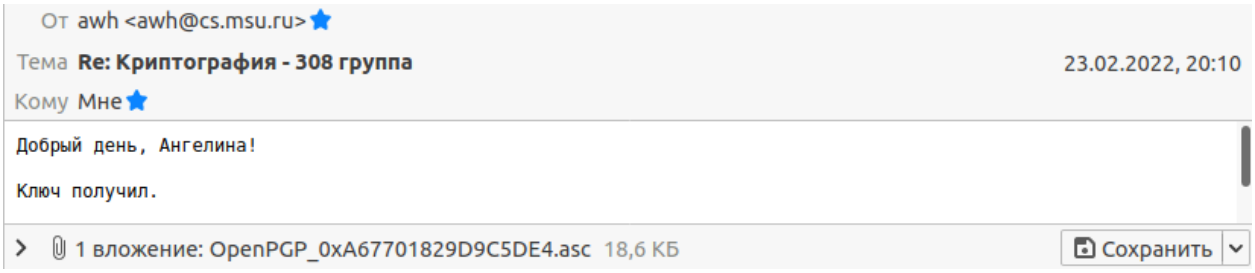
Создала пару ключей, указав в сертификате свою почту:



Отправила преподавателю сертификат открытого ключа:

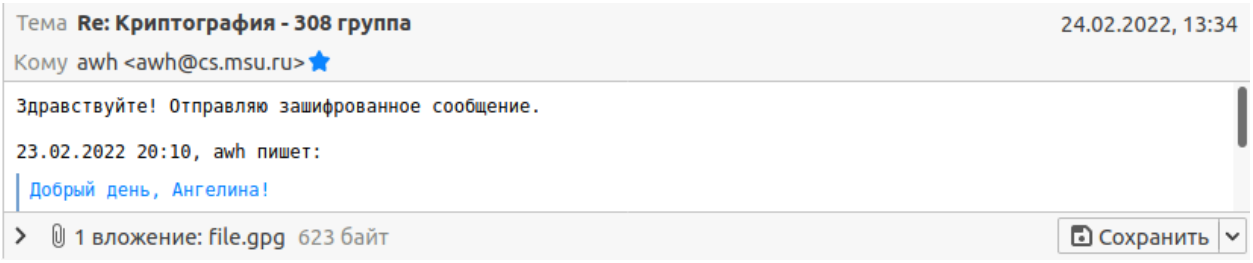


Дождалась письма с сертификатом открытого ключа преподавателя:



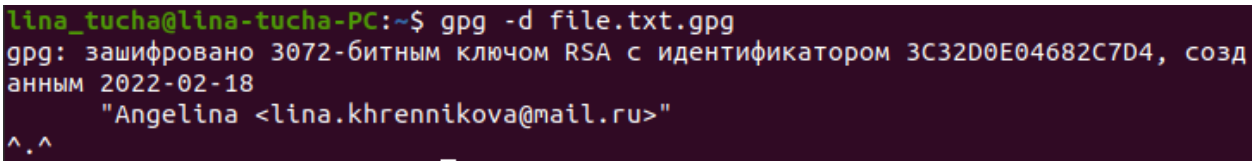
Выслала сообщение, зашифрованное на открытом ключе преподавателя:

Москва, 2022

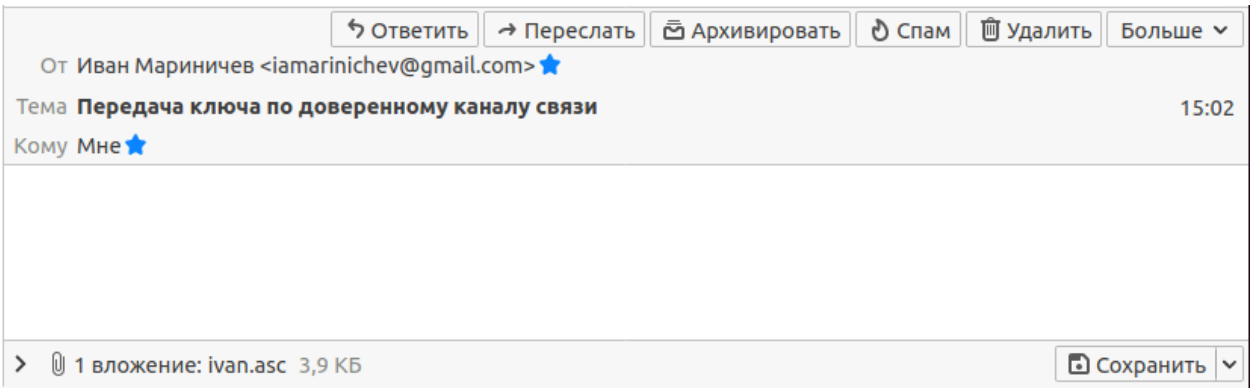


Дождалась ответного письма:

Расшифровала письмо:

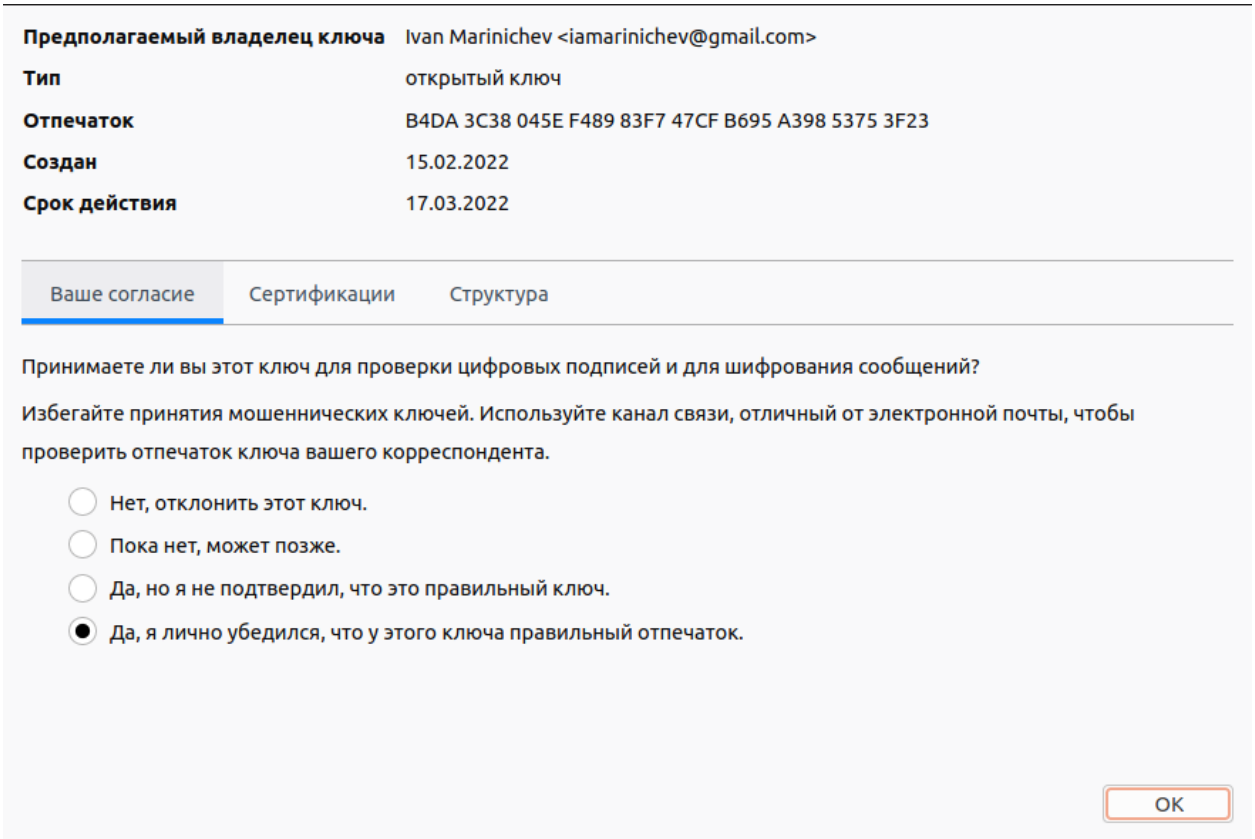


Получила код открытого ключа от одногруппника:



Убедилась, что данный сертификат ключа принадлежит его владельцу:

Москва, 2022

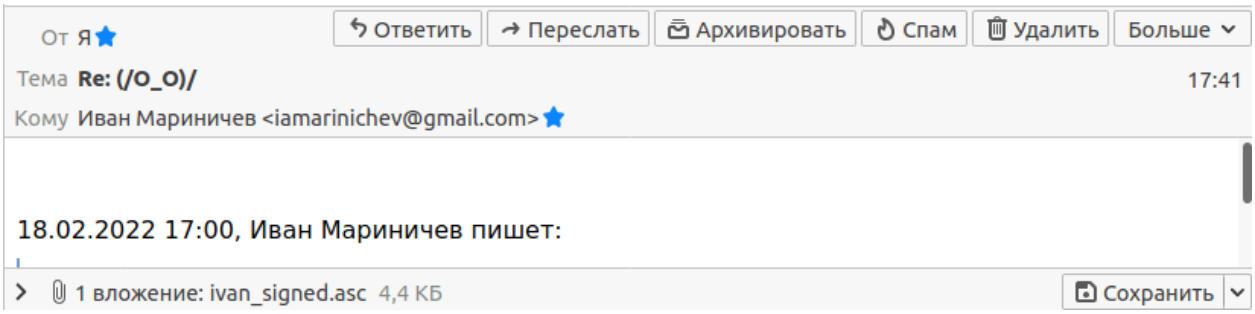


Подписала:

```
lina_tucha@lina-tucha-PC:~$ gpg --sign-key B695A39853753F23

pub  rsa4096/B695A39853753F23
     создан: 2022-02-15  годен до: 2022-03-17  назначение: SC
     доверие: неизвестно достоверность: неизвестно
sub  rsa4096/0609E69B27CE8D56
     создан: 2022-02-15  годен до: 2022-03-17  назначение: E
[ неизвестно ] (1). Ivan Marinichev <iamarinichev@gmail.com>


pub  rsa4096/B695A39853753F23
     создан: 2022-02-15  годен до: 2022-03-17  назначение: SC
     доверие: неизвестно достоверность: неизвестно
 Отпечаток первичного ключа: B4DA 3C38 045E F489 83F7  47CF B695 A398 5375 3F23

     Ivan Marinichev <iamarinichev@gmail.com>

Срок действия данного ключа истекает 2022-03-17.
Вы уверены, что хотите подписать этот ключ
своим ключом "Angelina <lina.khrennikova@mail.ru>" (3442522258CE8D8D)?

Действительно подписать? (y/N) y
```

Отправила подписанный сертификат одногруппнику:

Москва, 2022



Собрала 10 подписей:

Идентификатор пользователя / Сертифицировано	Идентификатор ключа	Создан
Angelina <lina.khrennikova@mail.ru>	3442522258CE8D8D	18.02.2022
Angelina <lina.khrennikova@mail.ru>	3442522258CE8D8D	18.02.2022
Ivan Marinichev <iamarinichev@gmail.com>	B695A39853753F23	18.02.2022
Игорь Королев <ikorolew02@gmail.com>	CF722A6EA0FFCCB9	19.02.2022
Simon Krassotkin <semen.krassotkin@gmail.com>	922AB26384CDF3D4	20.02.2022
Oleg Artamonov <eartqk@gmail.com>	B57C92DDB797671D	21.02.2022
Lyubov Ivenkova <lyubov.iven@mail.ru>	D87624AA4FF6F826	21.02.2022
Andrew Polyakov (MAI 2022) <mr.dijoy@gmail.com>	37B7F362EBEAB83C	21.02.2022
Andrey Chernobaev (hi) <rugivit@gmail.com>	855AA626C33F9BEF	21.02.2022
?	C725AD6BF2357DAD	21.02.2022
Natalia Timofeeva <volcha2001@yandex.ru>	9A077388B07AEA17	21.02.2022
Ivanov Fedor (Key for cripta labs) <kenola82007@gmail.com>	9FE64CEE5AE4BAF0	21.02.2022
Grigoriy Shubin (x) <garigoriy.gear@gmail.com>	8E5ABC302DFE7C5E	21.02.2022
dukend-Egor (kek) <workdukend@gmail.com>	5EC776B79907F6A0	22.02.2022

(? – просто брак)

2 Исходный код:

gpg --import andrewbun.asc – импорт открытого ключа

gpg --sign-key 37B7F362EBEAB83C - подпись

gpg -a -o ansrewbun_signed.asc --export 37B7F362EBEAB83C – экспорт подписанного ключа

gpg --import Angelina_signed.asc – импорт моего подписанного ключа

gpg --list-signatures – все ключи и подписи

3 Выводы:

Я познакомилась с утилитой gpg и возможностями почтового клиента thunderbird. Также научилась шифровать сообщения и использовать подпись.

Москва, 2022