Московский авиационный институт
(Национальный исследовательский университет)

Институт: «Информационные технологии и прикладная математика»
Кафедра: 806 «Вычислительная математика и программирование»

Лабораторная работа № 2
по курсу «Криптография»

Студент:	Обыденкова Ю. Ю.
Группа:	М8О-308Б-18
Вариант:	16
Преподаватель:	Борисов А. В.
Оценка:	
Дата:	

Москва, 2021

Постановка задачи

1. Создать пару OpenPGP-ключей, указав в сертификате свою почту. Создать её возможно, например, с помощью дополнения Enigmail к почтовому клиенту thunderbird, или из командной строки терминала ОС семейства linux.

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 и сам открытый ключ (как правило, они умещаются в одном файле).

2.2. Дождаться письма, в котором собеседник Вам пришлет сертификат своего открытого ключа.

2.4. Выслать сообщение, зашифрованное на 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.

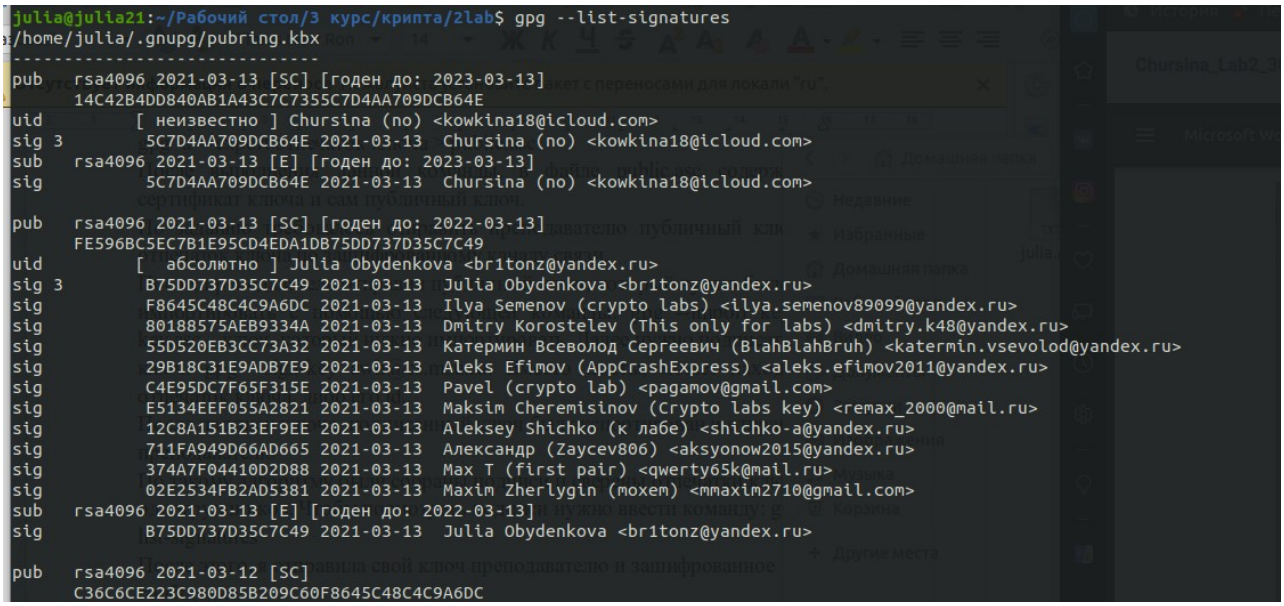
3.5. Прислать преподавателю свой сертификат открытого ключа, с 10-ю или более подписями одногруппников.

3. Подписать сертификат открытого ключа преподавателя и выслать ему.

Общие сведения о программе

Для выполнения данной работы я использовала утилиту gpg. Данная утилита предоставляет возможность работать с сертификатами.

Команда на создание ключа: gpg –full-generate-key
После чего будет выведено диалоговое окно, в котором надо выбрать размер ключа, ввести почту и придумать кодовую фразу, которую нужно обязательно запомнить, так как с помощью этой фразы будет выполняться большинство взаимодействий с ключом.
Как итог вызова команды, был сгенерирован новый PGP ключ размером 4096 байт.
Чтобы экспортировать ключ нужно написать команду:
gpg -a -–export отпечаток ключа > public.asc
После выполнения данной команды, в файле public.asc содержится сертификат ключа и сам публичный ключ.
По заданию требовалось отправить преподавателю публичный ключ и отпечаток ключа по зашифрованному каналу связи.
После, преподаватель отправил публичный ключ, который нужно было импортировать с помощью следующей команды: gpg --import key.asc key.asc – ключ, который нужно импортировать. Далее нужно подписать ключ: gpg --sign-key awh@cs.msu.ru. Вместо почты, может находится отпечаток ключа, либо его id.
После подписи ключа, подписанный ключ был экспортирован и отправлен преподавателю
По такому алгоритму были собраны подписи и сверены отпечатки ключей одногруппников. Чтобы посмотреть подписи нужно ввести команду: gpg --list-signatures
После этого, я отправила свой ключ преподавателю и зашифрованное сообщение.
Скриншот моих подписей:



Вывод

Выполняя данную лабораторную работу, я изучила утилиту gpg. Мною была сгенерирована пара ключей. Кроме того, я научилась подписывать публичным ключом сертификаты и зашифровывать сообщения.