Московский авиационный институт
(национальный исследовательский университет)

Факультет информационных технологий и прикладной математики

Кафедра вычислительной математики и программирования

Лабораторная работа №2 по курсу «Криптография»

Студент: М. А. Бронников
Преподаватель: А. В. Борисов
Группа: М8О-307Б
Дата:
Оценка:
Подпись:

Москва, 2020

Задание

Задача:

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:

   (a) 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).

   (b) Дождаться письма, в котором собеседник Вам пришлет сертификат своего открытого ключа.

   (c) Выслать сообщение, зашифрованное на ключе собеседника.

   (d) Дождаться ответного письма.

   (e) Расшифровать ответное письмо своим закрытым ключом.

3. Собрать подписи под своим сертификатом открытого ключа.

   (a) Получить сертификат открытого ключа одногруппника.

   (b) Убедиться в том, что подписываемый Вами сертификат ключа принадлежит его владельцу - путём сравнения отпечатка ключа или ключа целиком, по доверенным каналам связи.

   (c) Подписать сертификат открытого ключа одногруппника.

   (d) Передать подписанный Вами сертификат полученный в п.3.2 его владельцу, т.е. одногруппнику.

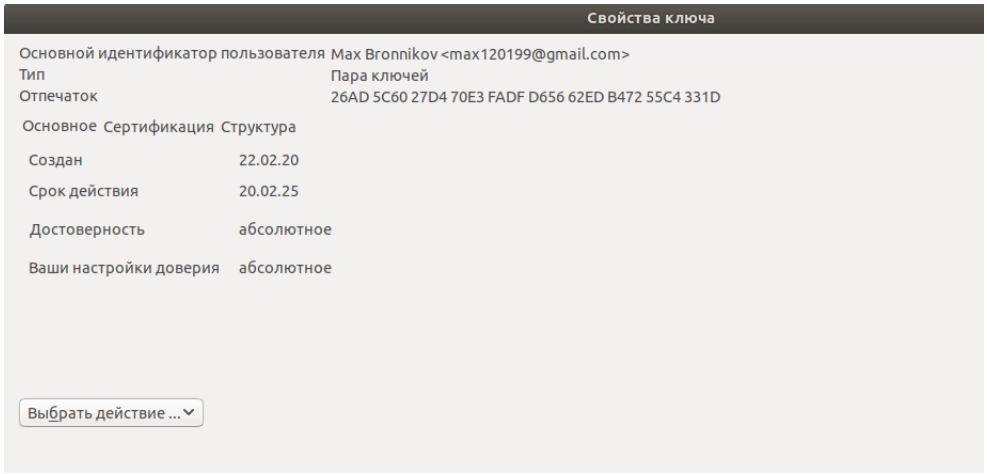
   (e) Повторив п.3.0.-3.3., собрать 10 подписей одногруппников под своим сертификатом.

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

4. Подписать сертификат открытого ключа преподавателя и выслать ему.

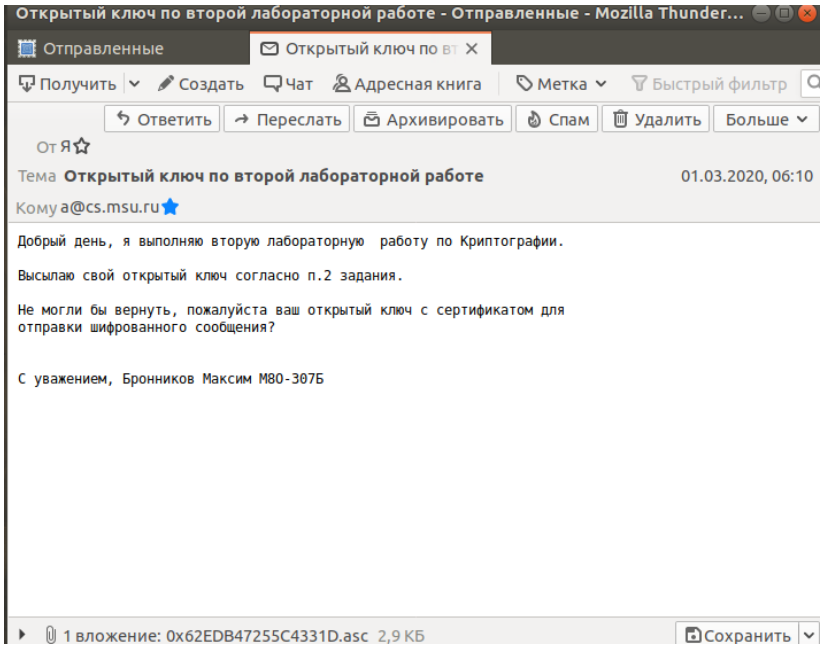
1 Описание

1. Для создание пары OpenPGP-ключей я установил расширение *Enigmail* для почтового клиента *Thunderbird* в *OS Linux* и создал с его помощью пару ключей для своего адреса электронной почты во встроенном менеджере:

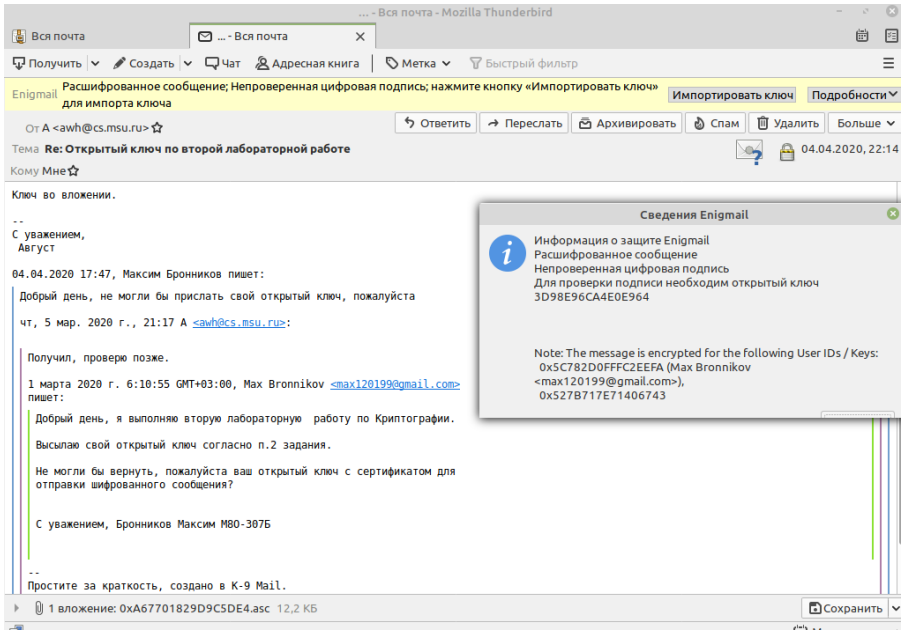


2. Я установил связь с преподавателем слудующим образом:

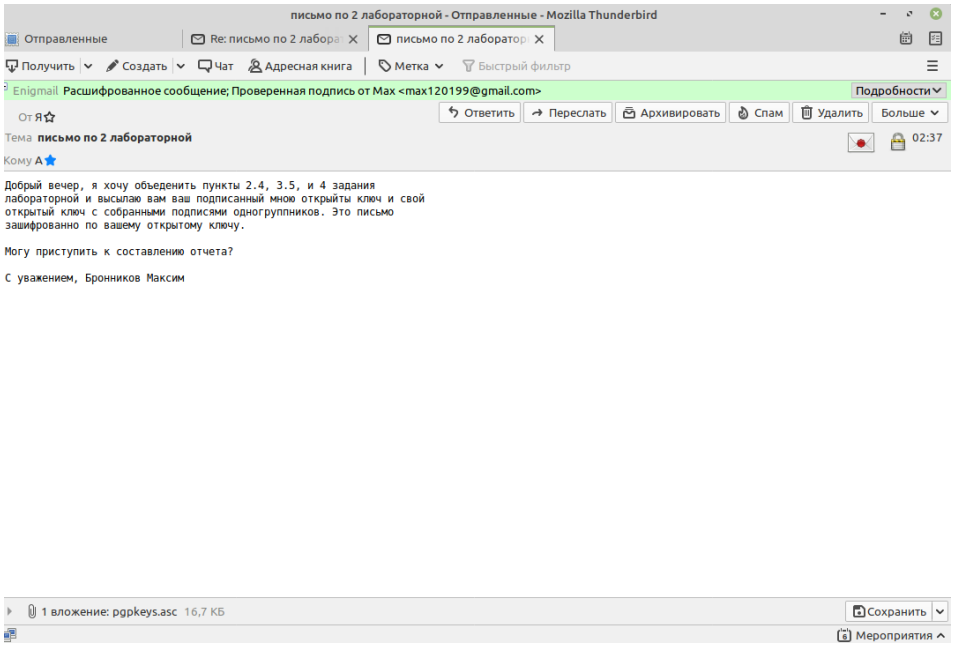
   (a) Отправил на его адрес электронной почты **a@cs.msu.ru** сообщение, во вложении которого лежит сертификат с моим открытым ключом:



(b) Дождался его зашифрованного по моему открытому ключу ответа на моё письмо. Письмо было расшифровано, в нем находился открытый ключ, который я импортировал в менеджер ключей *Enigmail*:

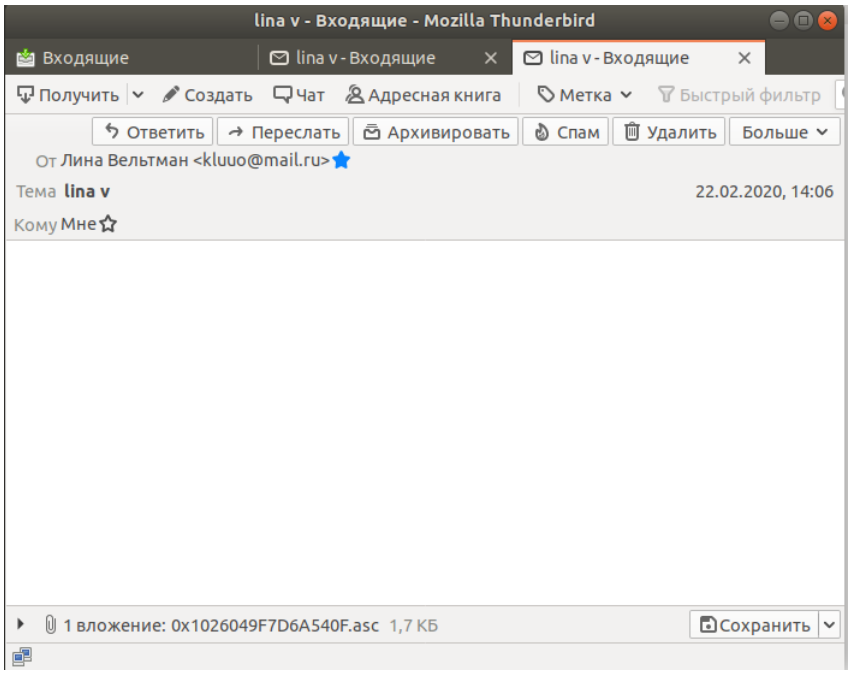


(c) При помощи клиента *Enigmail* и импортированного открытого ключа преподователя я отправил ему на почту зашифрованное письмо:

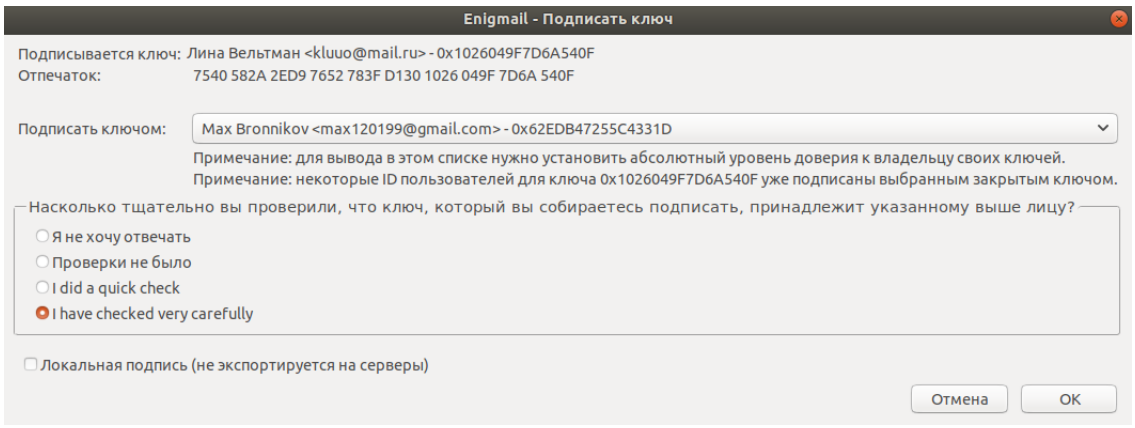


3. Я выполнял следующую последовательность действий для получения необходимого количества подписей одногруппников:

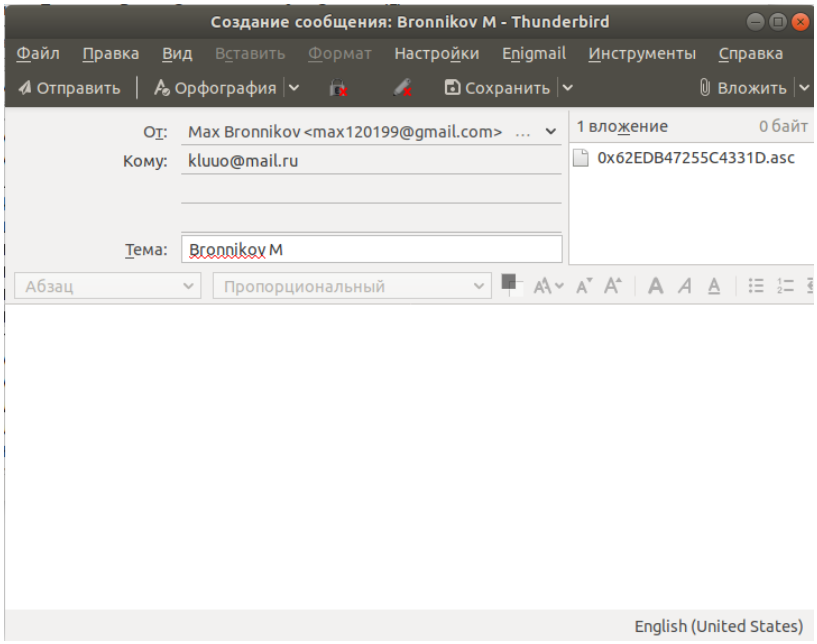
   (a) Получил письмо с открытым ключом одногруппницы и ипортировал этот ключ в менеджер ключей:



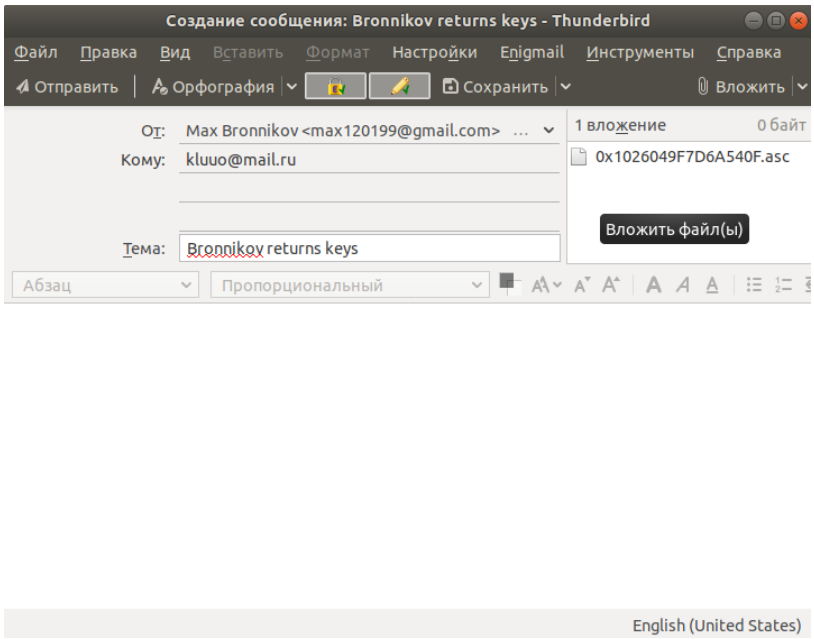
   (b) Я убедился в том, что полученный мною ключ действительно принадлежит одногруппнице, сравнив отпечаток полученного ключа с открытым ключом отправителя в ходе личной беседы, и подписал ключ своим ключом, используя *Enigmail*:



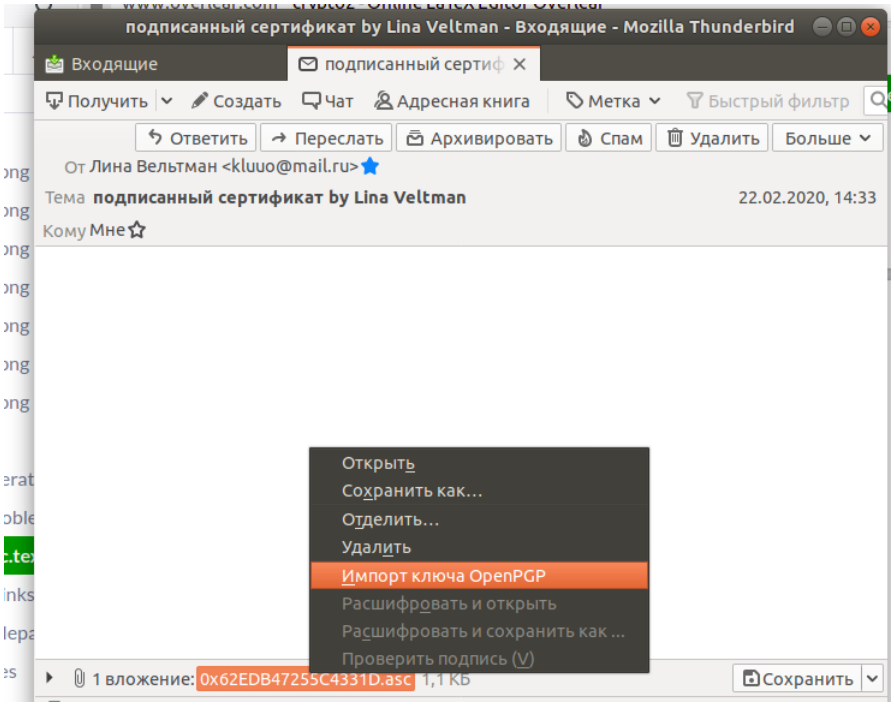
(c) Отправил письмо со своим сертификатом открытого ключа ей на почту для подписи:



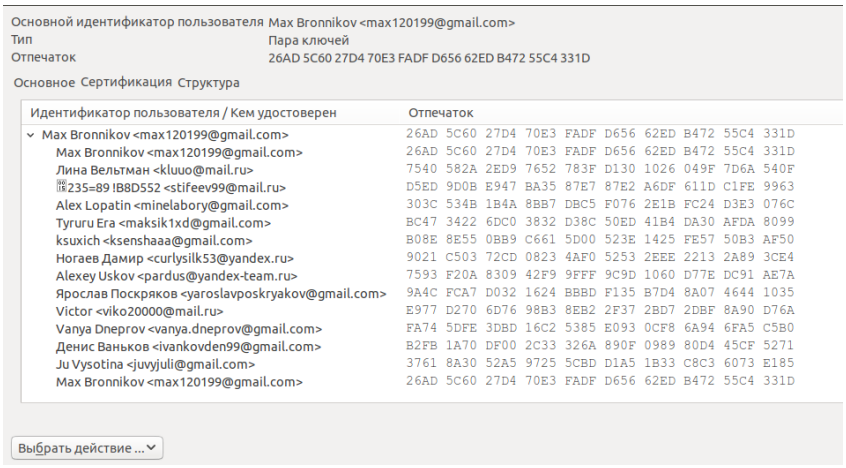
(d) Зашифрованным на её ключе письмом я отправил подписанный ключ одногруппницы ей обратно:



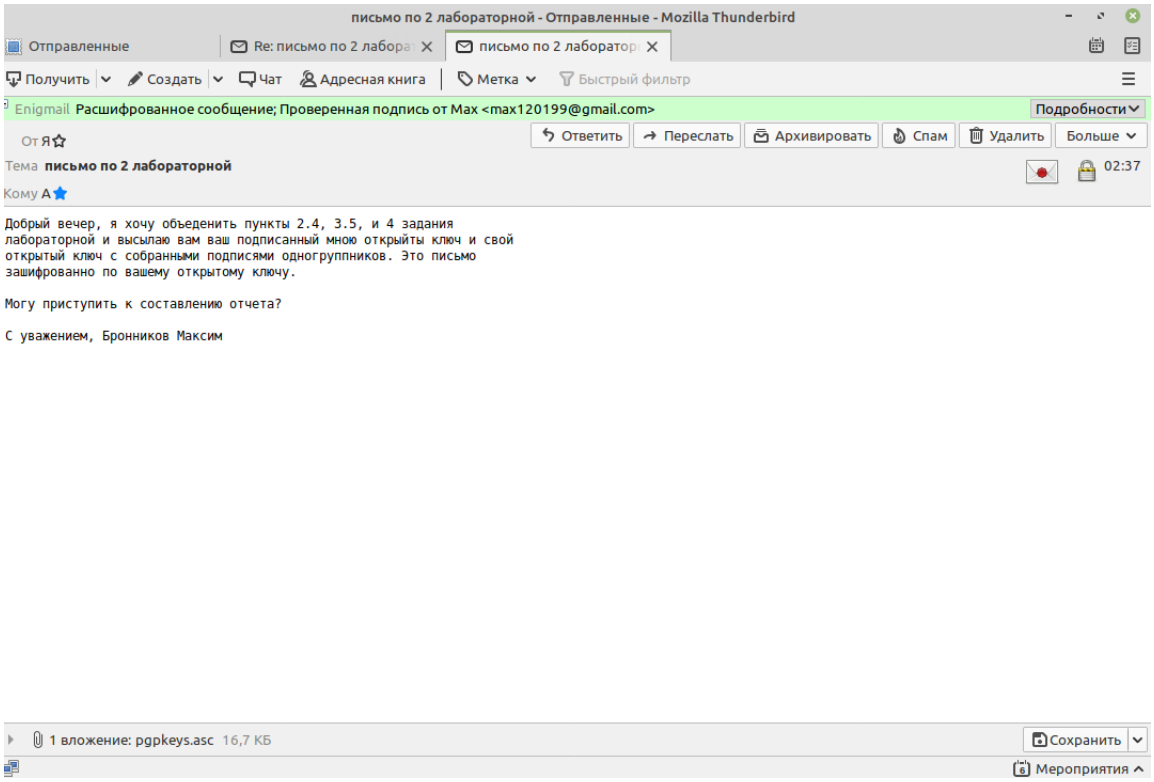
(e) Получил письмо со своим подписанным сертификатом, который импортировал к себе в менеджер ключей:



После выполнения этой последовательности действий я получил 12 подписей одногруппников под своим сертификатом:



4. Я подписал сертификат преподавателя своим ключом и выслал ему на его адрес электронной почты вместе со своим открытым ключом, содержащим необходимое количество подписей одногруппников, после чего приступил к выполнению отчета по лабораторной работе:



2 Выводы

Выполнив вторую лабораторную работу по курсу «Криптография», я получил представление о том, что такое электронная подпись и зачем она нужна.

В процессе решения задачи мне довелось заняться интересной задачей: создать свой электронный сертификат, при помощи которого стало возможно обменивается с собеседником посредством зашифрованных сообщений. Несмотря на то, что это не первый мой опыт работы с *RSA* шифрованием, мне было интересно посмотреть как это реализуется и работает на почтовых клиентах.

Я уверен, что полученные мной навыки не пропадут даром и я буду использовать созданный мной электронный сертифиат в будущем для обмена защищенными сообщениями.