Московский авиационный институт (национальный исследовательский университет)

Факультет информационных технологий и прикладной математики

Кафедра вычислительной математики и программирования

Лабораторная работа №2 по курсу «Криптография»

Студент: Л. Я. Вельтман
Преподаватель: А. В. Борисов
Группа: М8О-307Б

Дата: 9.03.2020
Оценка:
Подпись:

Москва, 2020

Лабораторная работа №2

Вариант 7:

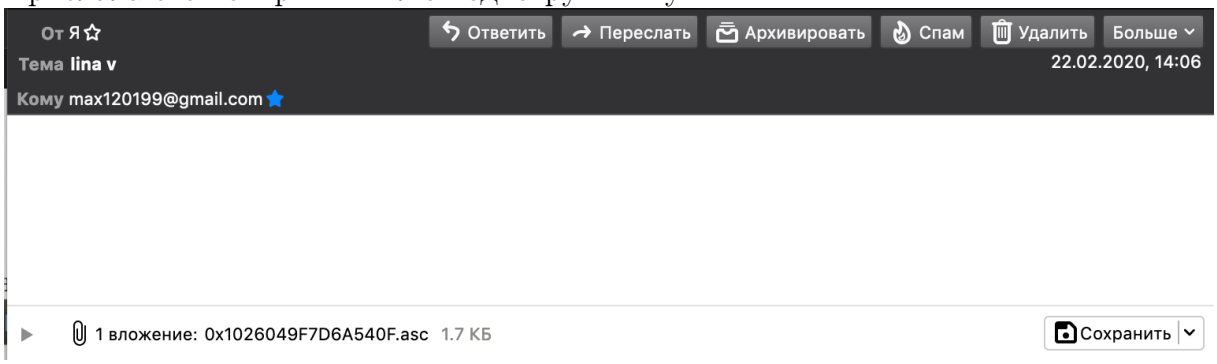
1. Создать пару OpenPGP-ключей, указав в сертификате свою почту. Создать её возможно, например, с помощью дополнения Enigmail к почтовому клиенту thunderbird, или из командной строки терминала ОС семейства linux.
2. Установить связь с преподавателем, используя созданный ключ, следующим образом:
   (a) Прислать от своего имени по электронной почте сообщение, во вложении которого поместить свой открытый ключ.
   (b) Дождаться письма, в котором отправитель вам пришлёт свой сертификат открытого ключа.
   (c) Выслать сообщение, зашифрованное на ключе собеседника.
   (d) Дождаться ответного письма.
   (e) Расшифровать письмо своим закрытым ключом.
3. Собрать подписи под своим сертификатом открытого ключа.
   (a) Получить сертификат открытого ключа одногруппника.
   (b) Убедиться, что ключу абонента можно доверять путём сравнения отпечатка ключа или ключа целиком, по доверенным каналам связи.
   (c) Подписать сертификат открытого ключа одногруппника.
   (d) Передать подписанный Вами сертификат почтой п.3(c) его владельцу.
   (e) Собрать 10 подписей одногруппников под своим сертификатом.
   (f) Прислать преподавателю (желательно почтой) свой сертификат, с 10-ю или более подписями одногруппников.
4. Подписать сертификат открытого ключа преподавателя и выслать ему.

1 Метод решения

Файлы:
0x1026049F7D6A540F.asc – мой ключ.
0xA67701829D9C5DE4.asc – подписанный ключ преподавателя.

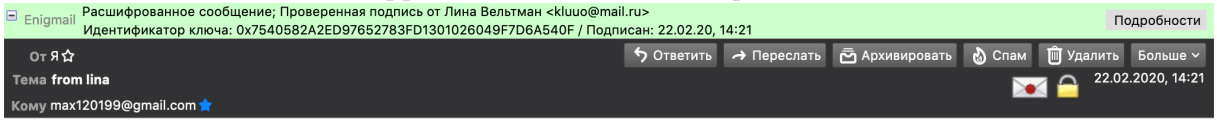
Я сгенерировала ключ:

Прислала свой открытый ключ одногруппнику:



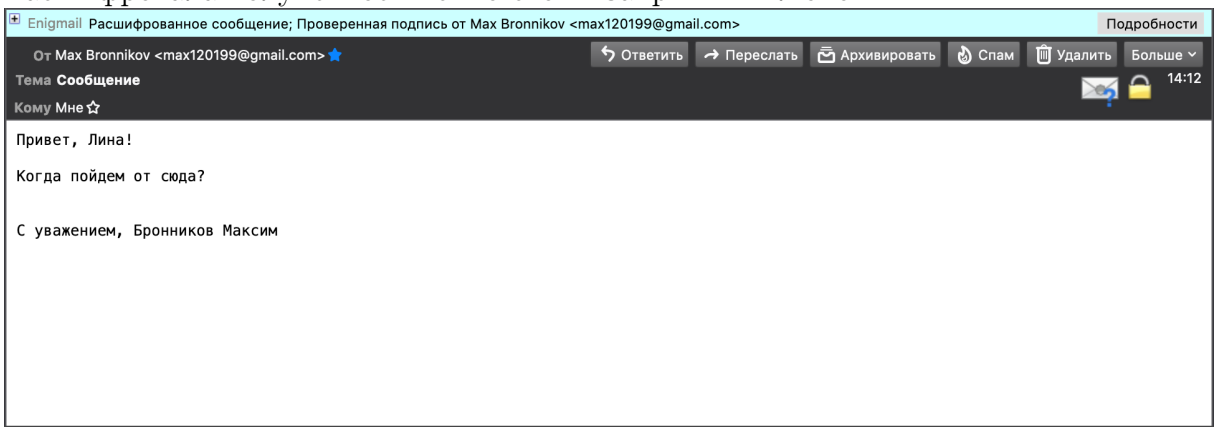
Дождалась письма, в котором одногруппник прислал мне свой сертификат:

Выслала сообщение, зашифрованное на ключе отправителя:

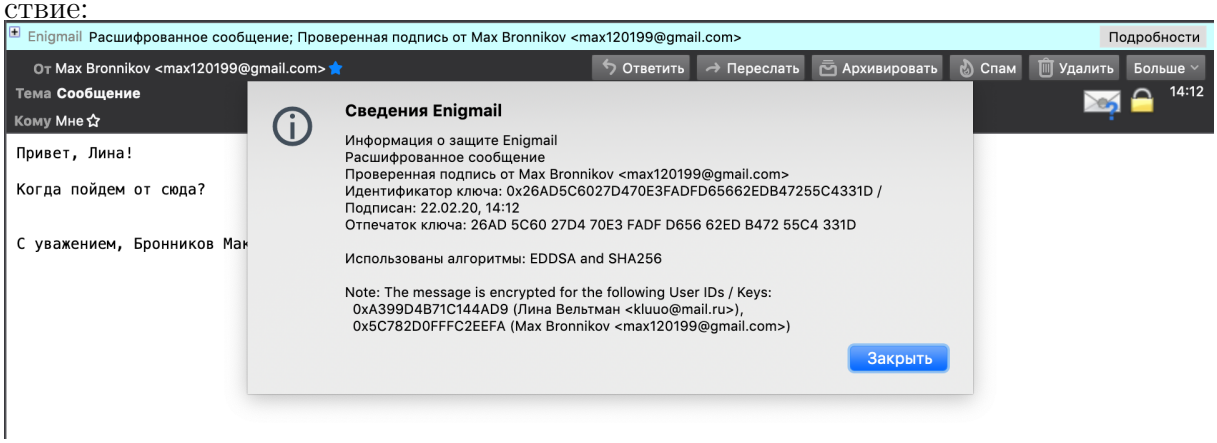


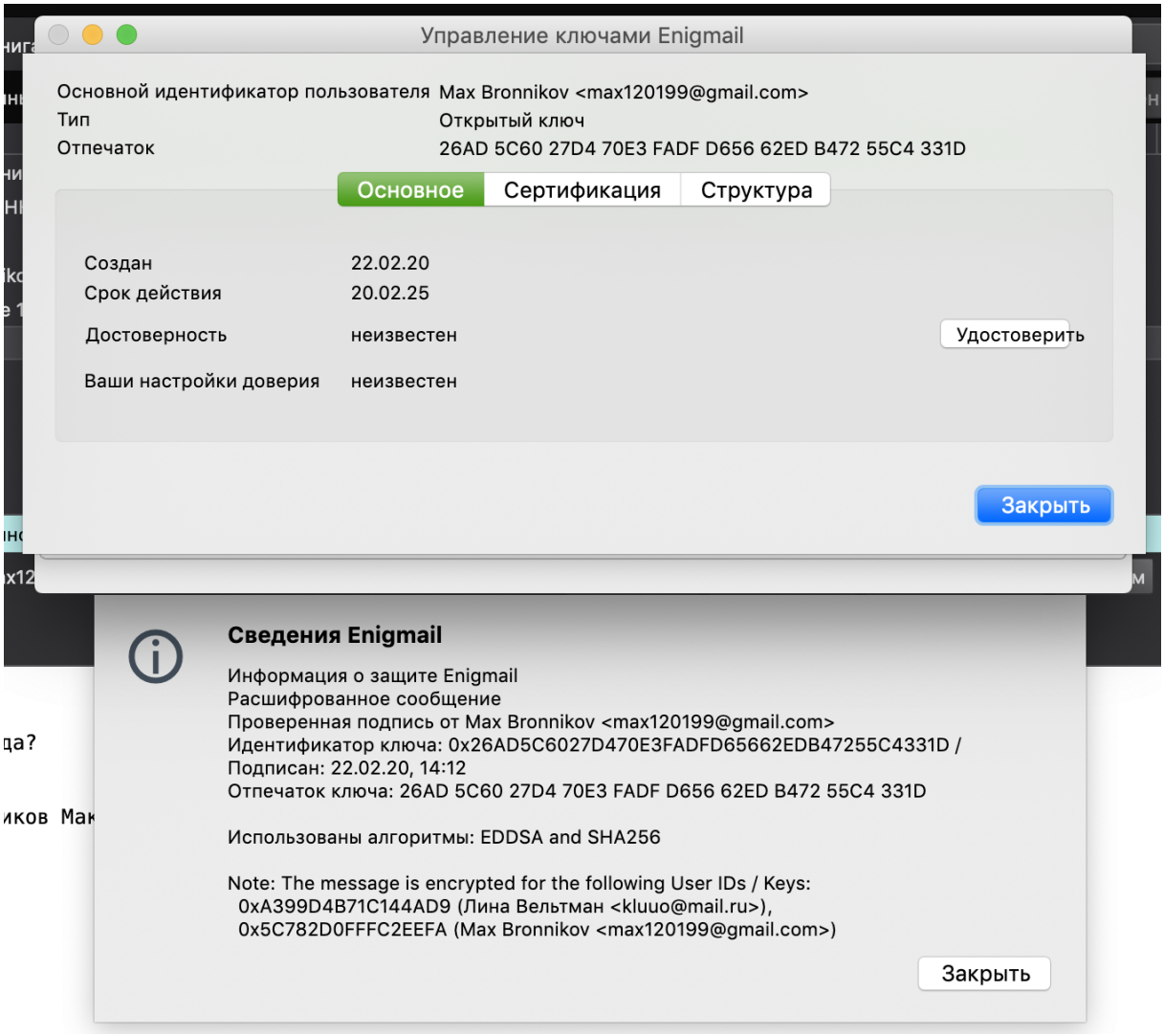
LU-разложение — это представление матрицы A в виде A=L•U, где L — нижнетреугольная матрица с еденичной диагональю, а U — верхнетреугольная матрица. LU-разложение является модификациеё метода Гаусса. Основные применения данного алгоритма — решение систем алгебраических уравнений, вычисление определителя, вычисление обратной матрицы и др.

Расшифровала полученное письмо своим закрытым ключом:

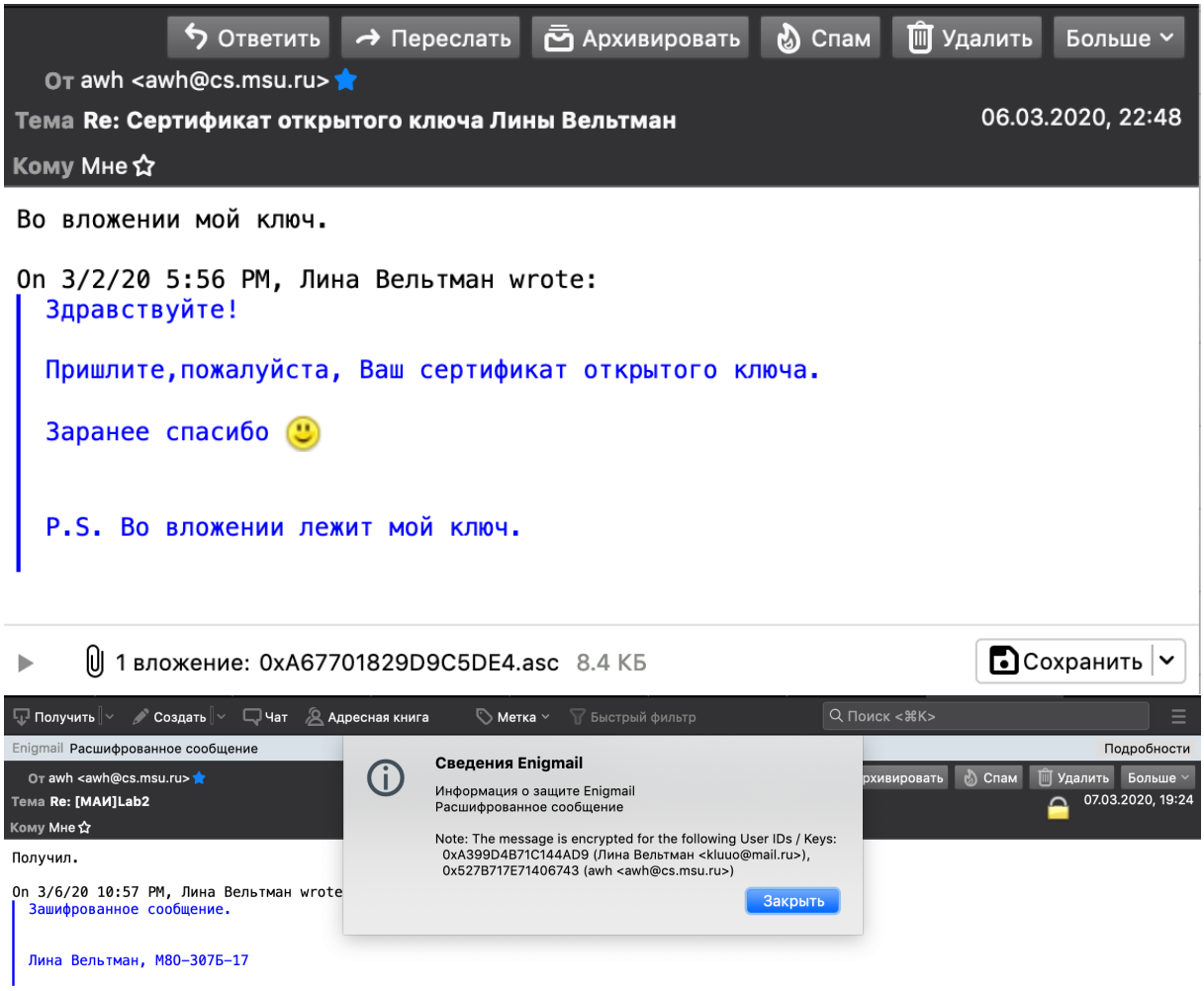


Дальше я сравнила ключ в письме и ключ в менеджере ключей и нашла соответствие:

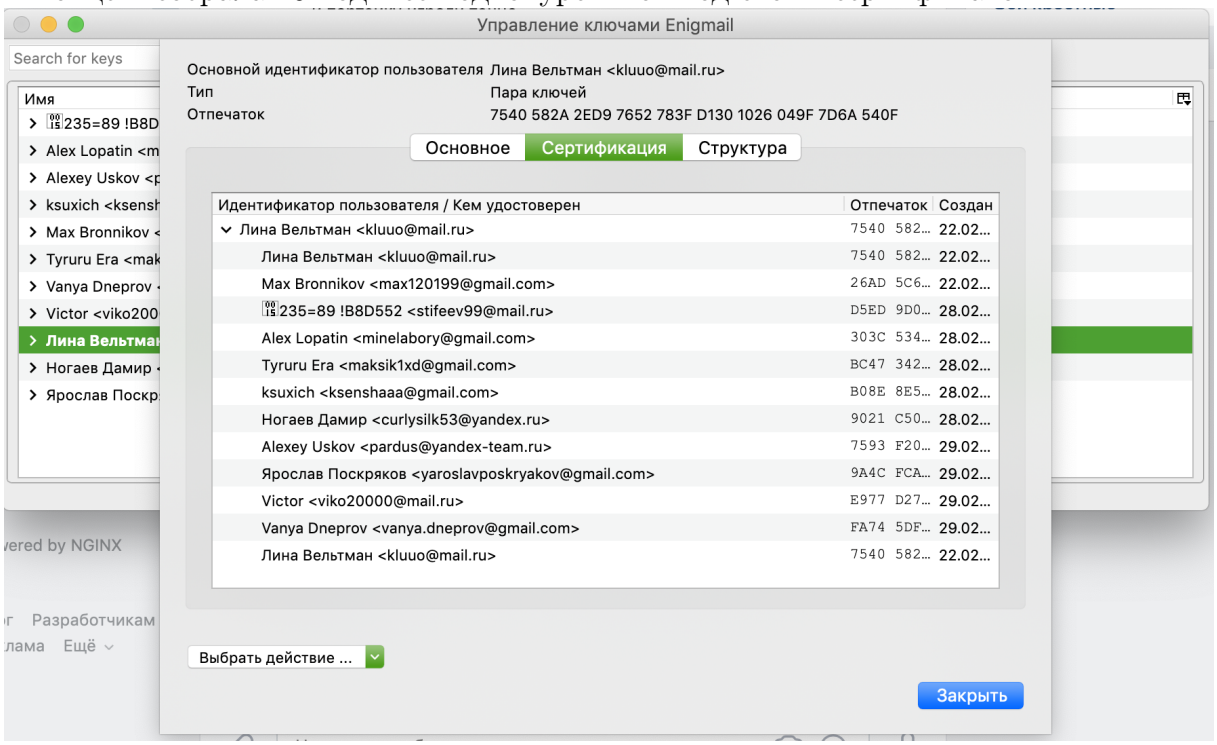




Также я отправила свой открытый ключ и зашифрованное сообщение преподавателю:


Ответить
Переслать
Архивировать
Спам
Удалить
Больше
От awh <awh@cs.msu.ru>
Тема Re: Сертификат открытого ключа Лины Вельтман
06.03.2020, 22:48
Кому Мне
Во вложении мой ключ.
On 3/2/20 5:56 PM, Лина Вельтман wrote:
Здравствуйте!
Пришлите,пожалуйста, Ваш сертификат открытого ключа.
Заранее спасибо
P.S. Во вложении лежит мой ключ.
1 вложение: 0xA67701829D9C5DE4.asc 8.4 КБ
Сохранить
Получить
Создать
Чат
Адресная книга
Метка
Быстрый фильтр
Поиск <⌘K>
Enigmail Расшифрованное сообщение
Подробности
От awh <awh@cs.msu.ru>
Тема Re: [МАИ]Lab2
Кому Мне
Спам
Удалить
Больше
07.03.2020, 19:24
Сведения Enigmail
Информация о защите Enigmail
Расшифрованное сообщение
Note: The message is encrypted for the following User IDs / Keys:
0xA399D4B71C144AD9 (Лина Вельтман <kluuo@mail.ru>),
0x527B717E71406743 (awh <awh@cs.msu.ru>)
Закрыть
Получил.
On 3/6/20 10:57 PM, Лина Вельтман wrote
Зашифрованное сообщение.
Лина Вельтман, М8О-307Б-17

В конце я собрала 10 подписей однокурсников под своим сертификатом:



2 Выводы

С данными технологиями я столкнулась впервые, механизм работы pgp показался мне очень интересным. Основные сложности при выполнении работы были связаны с организационной частью. Решив все коммуникационные проблемы, далее были проделаны все действия по заданному алгоритму по несколько раз. Как итог, научилась пользоваться шифрованием и подписью на примере pgp и почты.