Московский авиационный институт
(национальный исследовательский университет)

Факультет информационных технологий и прикладной математики

Кафедра вычислительной математики и программирования

Лабораторная работа №2 по курсу «Криптография»

Студент: А. О. Дубинин
Преподаватель: А. В. Борисов
Группа: М8О-306Б
Дата:
Оценка:
Подпись:

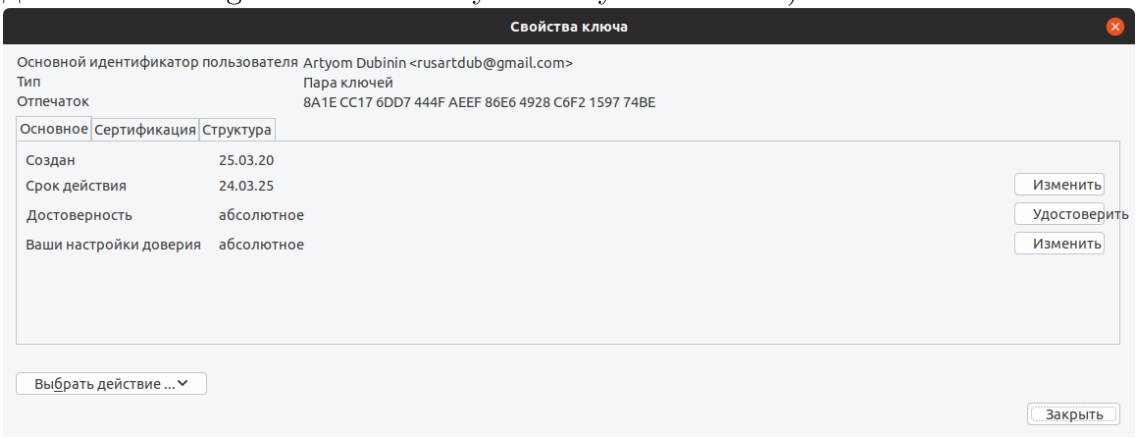
Москва, 2020

Условие

1. Создать пару OpenPGP-ключей, указав в сертификате свою почту(с помощью дополнения Enigmail к почтовому клиенту thunderbird).
2. Установить связь с преподавателем и с хотя бы с одним одногруппником, используя созданный ключ, следующими действиями:
   (a) Прислать собеседнику от своего имени по электронной почте сообщение, во вложении которого поместить свой сертификат открытого ключа и сам открытый ключ.
   (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.3.1.-3.4., 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.

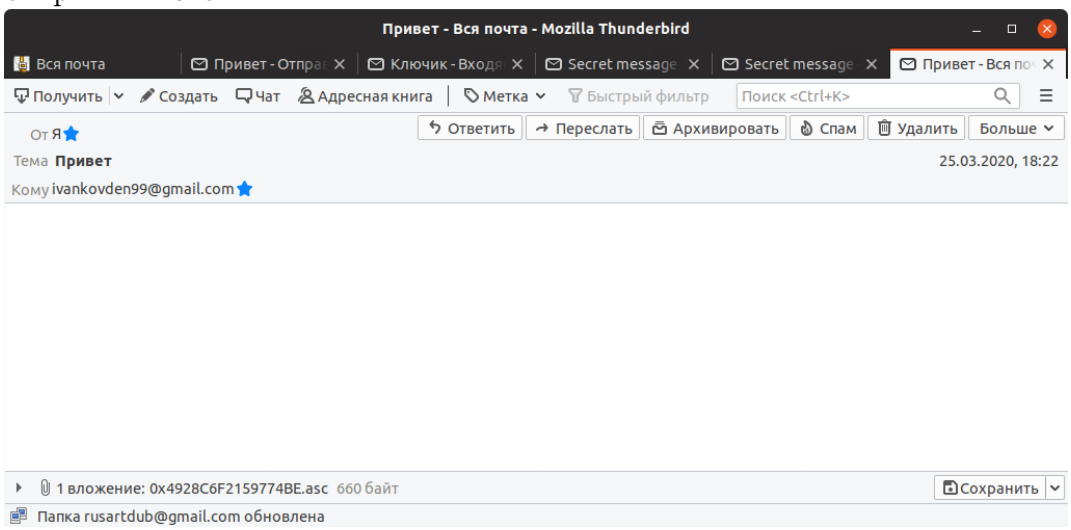
1 Решение

1. Создал пару OpenPGP-ключей, указав в сертификате свою почту(с помощью дополнения Enigmail к почтовому клиенту thunderbird).

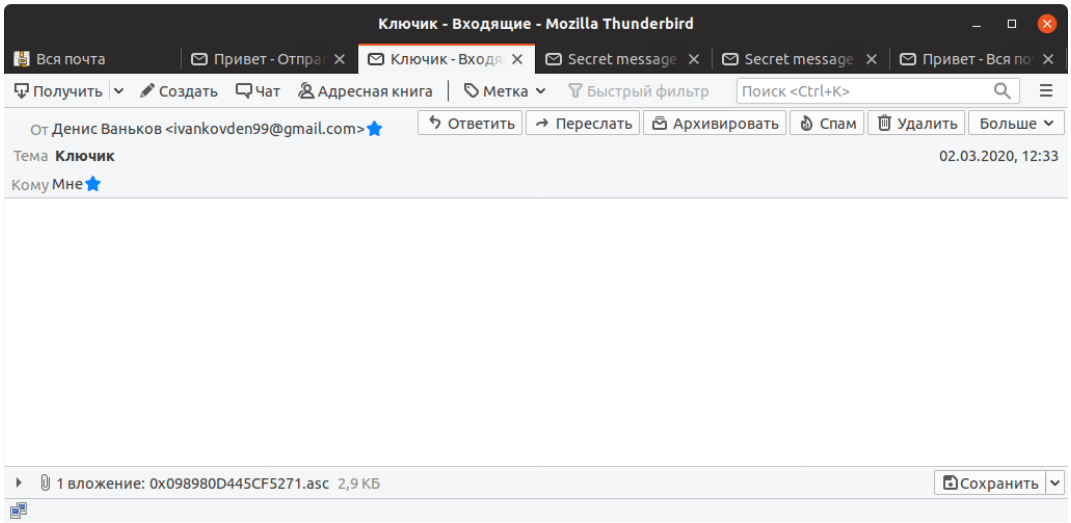


2. Установить связь с преподавателем и с хотя бы с одним одногруппником, используя созданный ключ, следующими действиями:

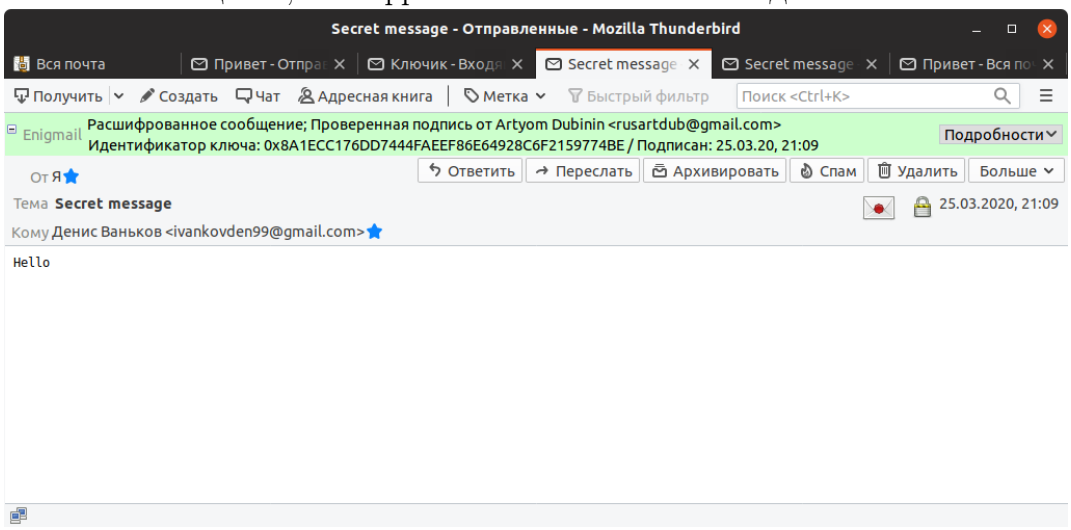
   (a) Прислать собеседнику от своего имени по электронной почте сообщение, во вложении которого поместить свой сертификат открытого ключа и сам открытый ключ.



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

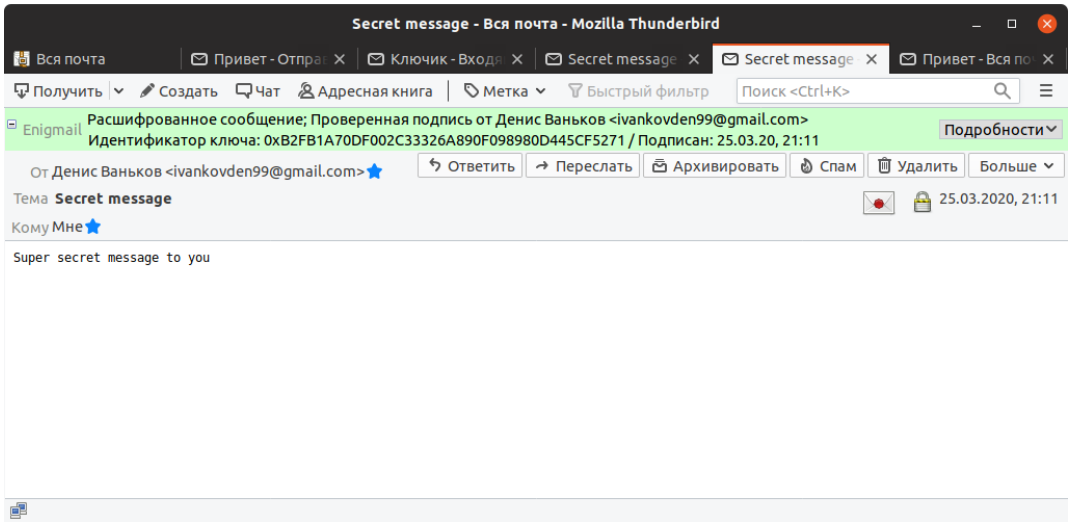


(c) Выслать сообщение, зашифрованное на ключе собеседника.

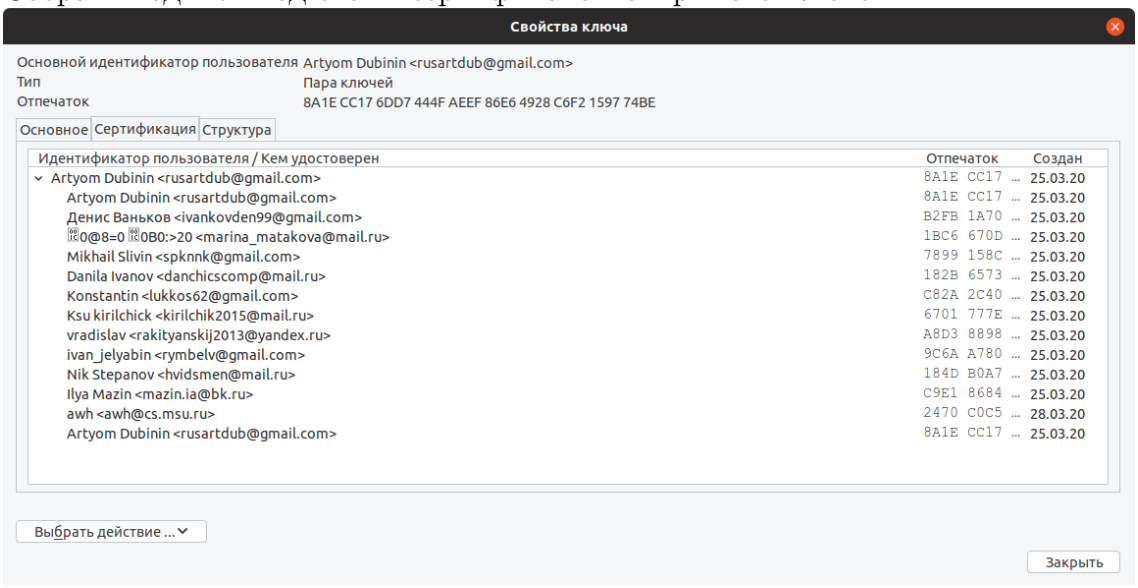


(d) Дождаться ответного письма.

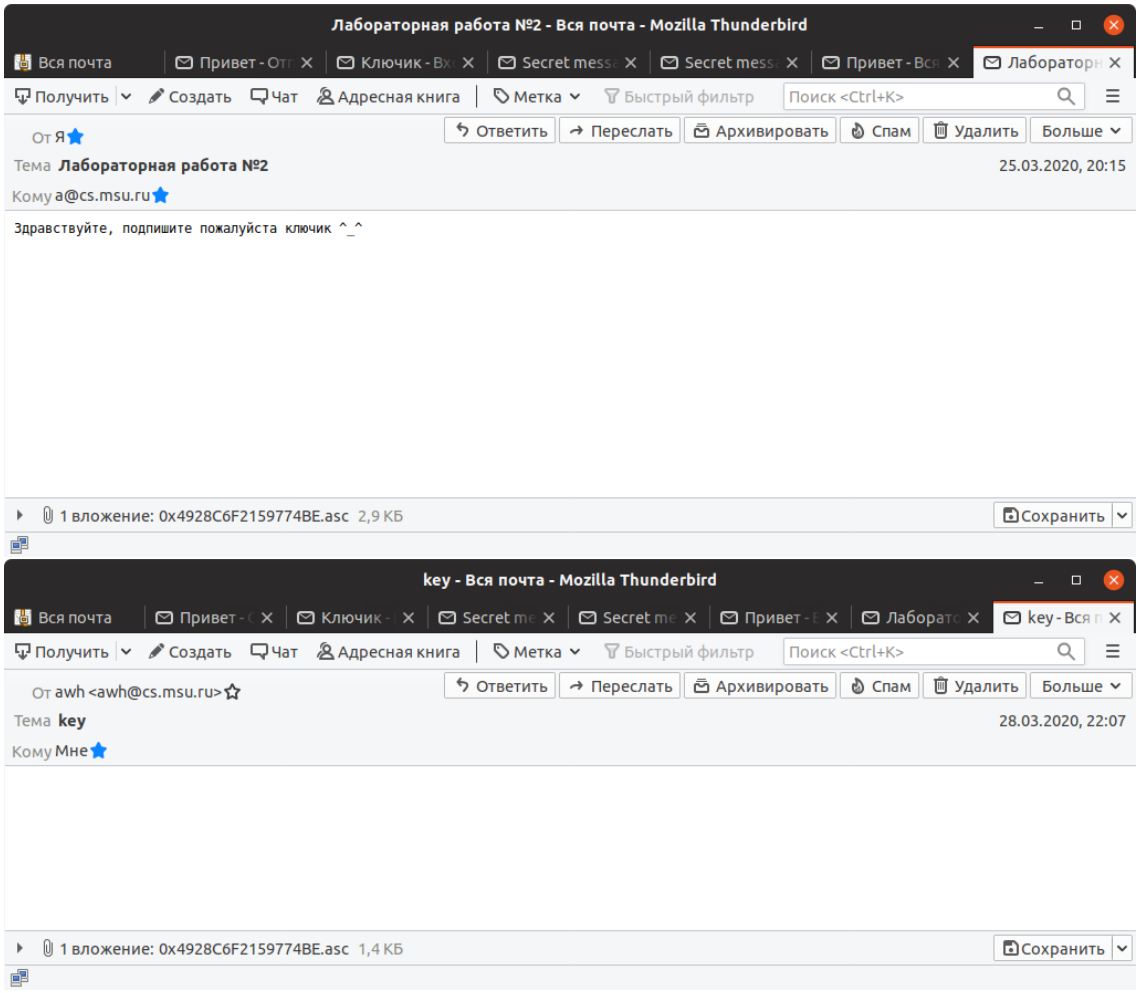
(e) Расшифровать ответное письмо своим закрытым ключом.



3. Собрать подписи под своим сертификатом открытого ключа.



4. Подписать сертификат открытого ключа преподавателя и выслать ему.


Лабораторная работа №2 - Вся почта - Mozilla Thunderbird
Вся почта
Получить
Создать
Чат
Адресная книга
Метка
Быстрый фильтр
Поиск <Ctrl+K>
Ответить
Переслать
Архивировать
Спам
Удалить
Больше
От Я
Тема Лабораторная работа №2
25.03.2020, 20:15
Кому a@cs.msu.ru
Здравствуйте, подпишите пожалуйста ключик ^_^
1 вложение: 0x4928C6F2159774BE.asc 2,9 КБ
Сохранить
key - Вся почта - Mozilla Thunderbird
Вся почта
Получить
Создать
Чат
Адресная книга
Метка
Быстрый фильтр
Поиск <Ctrl+K>
Ответить
Переслать
Архивировать
Спам
Удалить
Больше
От awh <awh@cs.msu.ru>
Тема key
28.03.2020, 22:07
Кому Мне
1 вложение: 0x4928C6F2159774BE.asc 1,4 КБ
Сохранить

2 Выводы

Я решил лабораторную с помощью thunderbird + enigmail, понял, как работают pgp keys и насколько надежна защита сообщений по почте. Так же я узнал, что можно выбрать криптографический алгоритм, либо эллиптические кривые, либо RSA.