

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

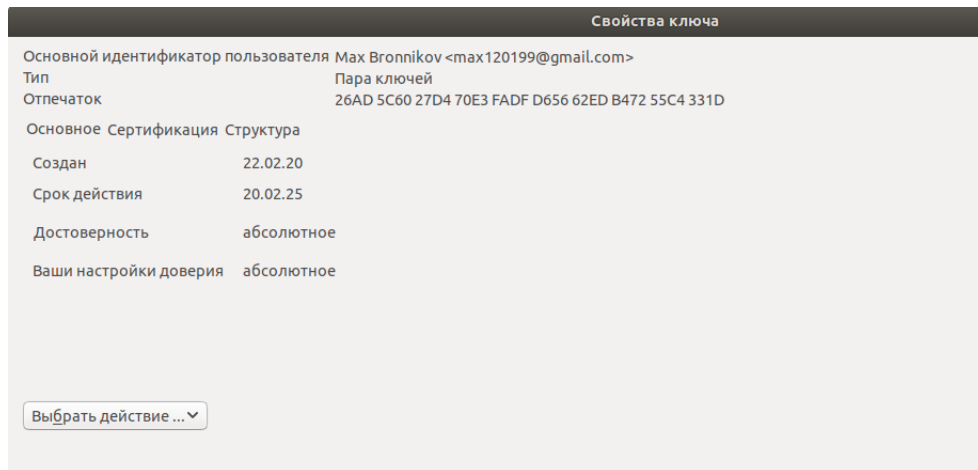
Задание

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 одноклассника.
 - (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 одноклассника.
 - (d) Передать подписанный Вами сертификат полученный в п.3.2 его владельцу, т.е. однокласснику.
 - (e) Повторив п.3.0.-3.3., собрать 10 подписей одноклассников под своим сертификатом.
 - (f) Прислать преподавателю свой сертификат открытого ключа, с 10-ю или более подписями одноклассников.
4. Подписать сертификат открытого ключа преподавателя и выслать ему.

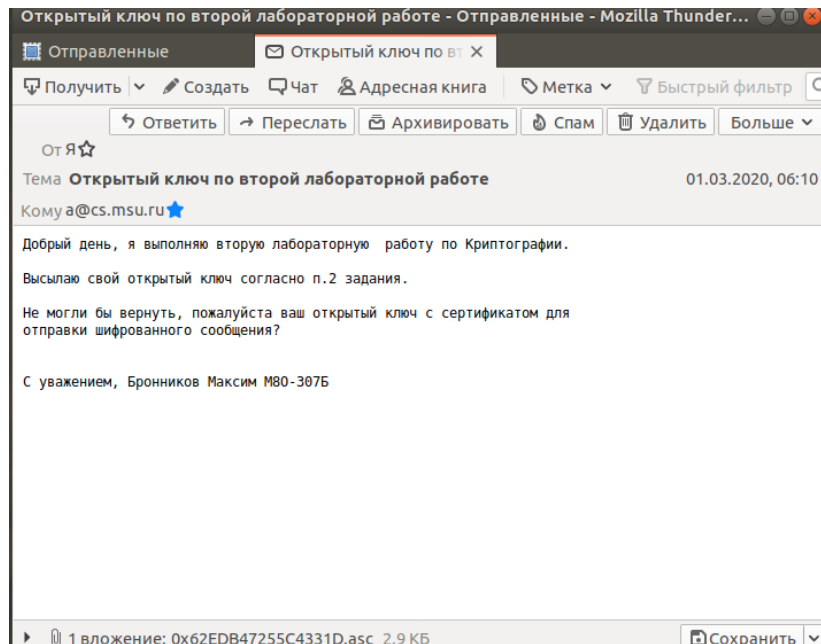
1 Описание

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:

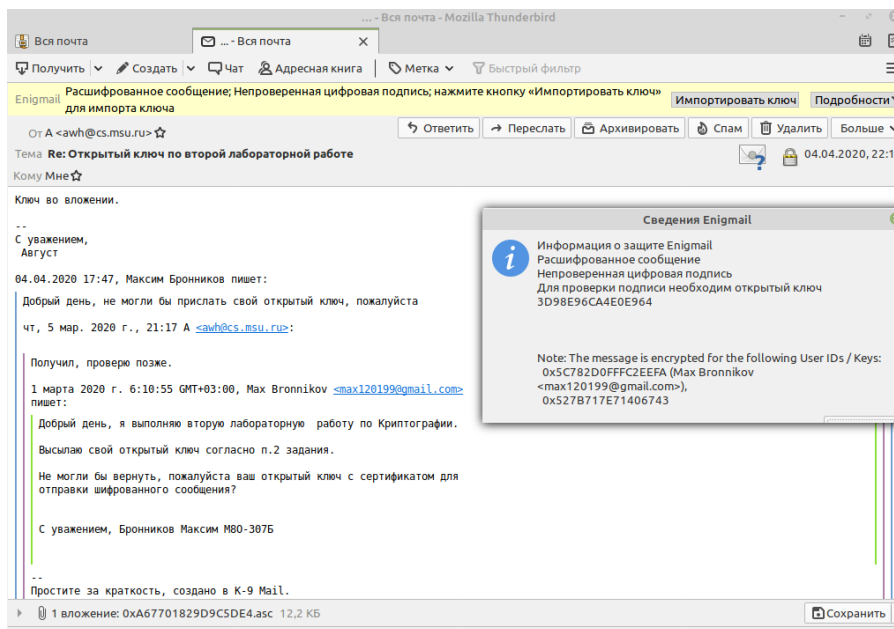


2. Я установил связь с преподавателем следующим образом:

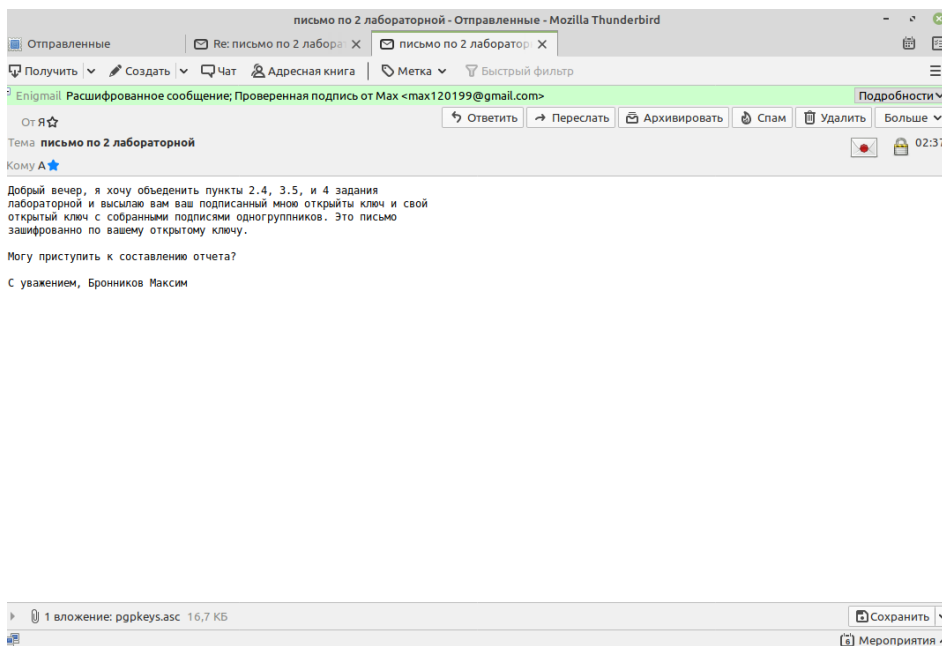
- (а) Отправил на его адрес электронной почты **a@cs.msu.ru** сообщение, во вложении которого лежит сертификат с моим открытым ключом:



- (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*:

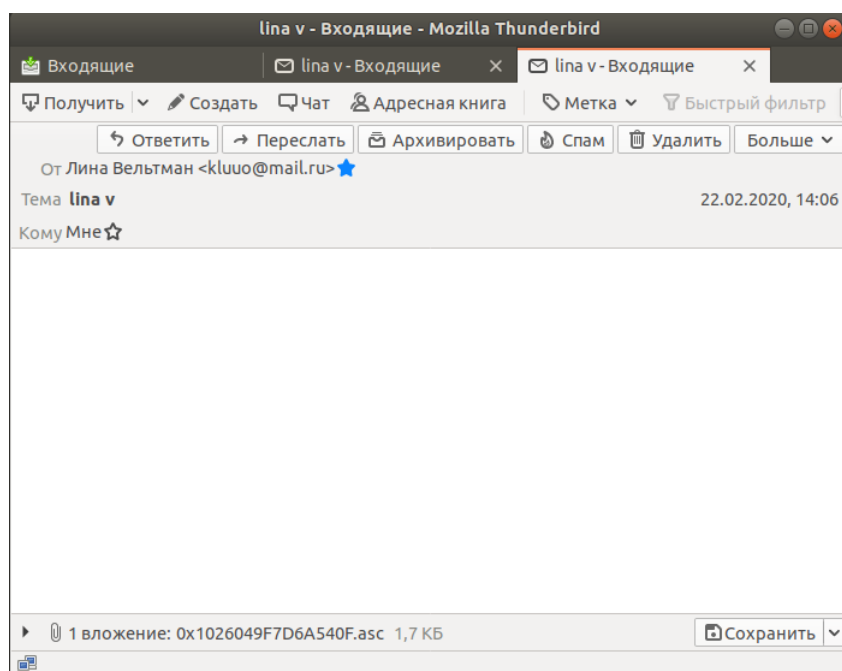


- (c) При помощи клиента *Enigmail* и импортированного открытого ключа получателя я отправил ему на почту зашифрованное письмо:

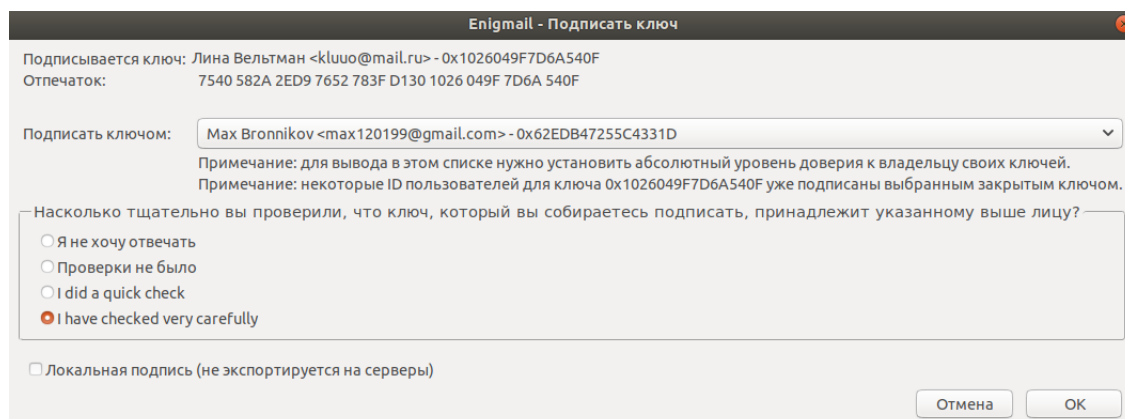


3. Я выполнял следующую последовательность действий для получения необходимого количества подписей одноклассников:

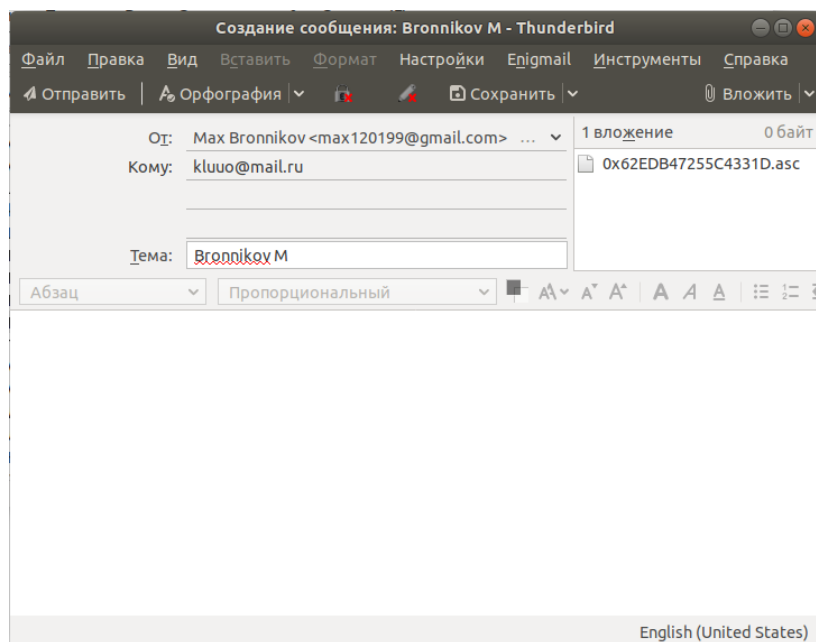
(а) Получил письмо с открытым ключом одноклассницы и импортировал этот ключ в менеджер ключей:



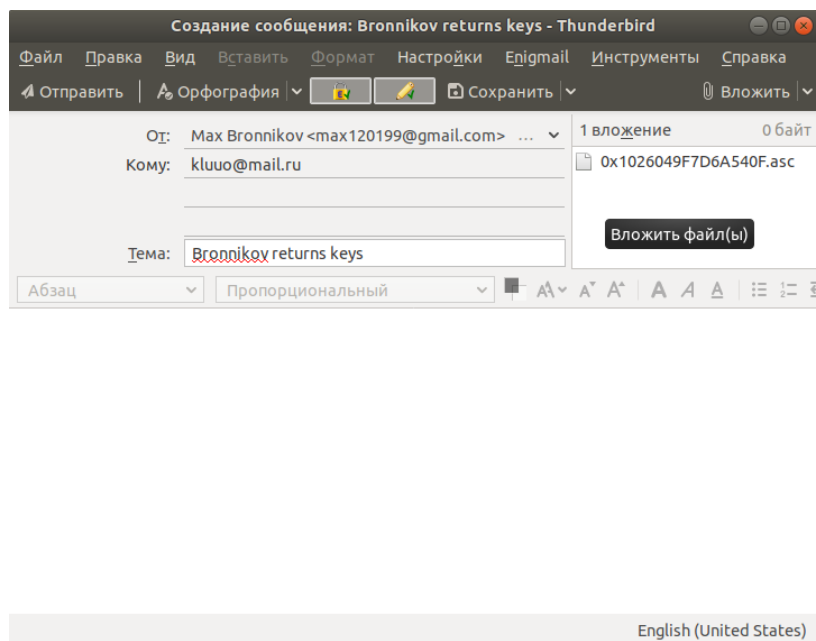
(б) Я убедился в том, что полученный мною ключ действительно принадлежит однокласснице, сравнив отпечаток полученного ключа с открытым ключом отправителя в ходе личной беседы, и подписал ключ своим ключом, используя *Enigmail*:



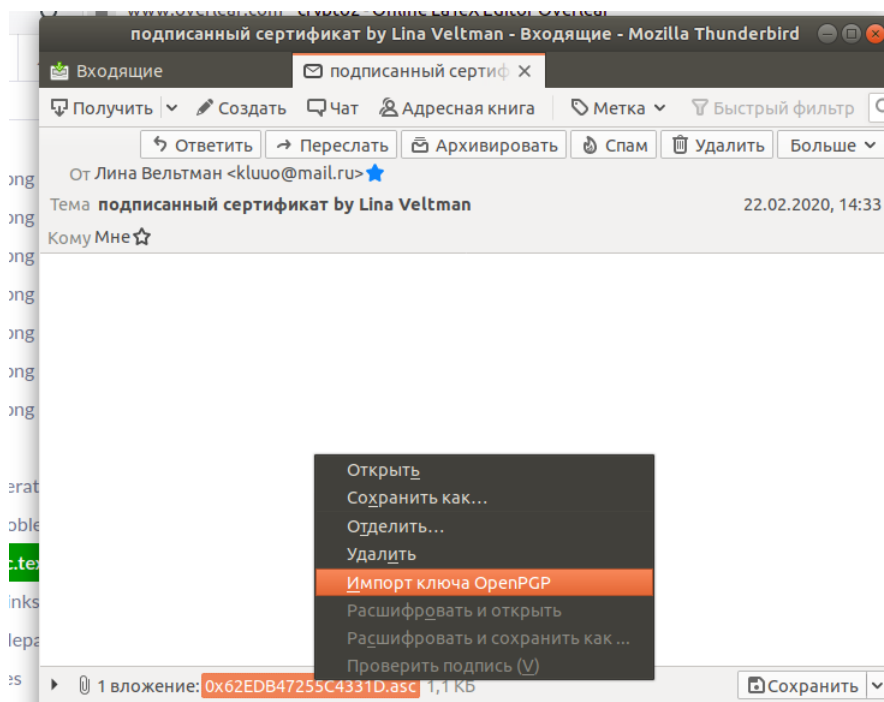
- (с) Отправил письмо со своим сертификатом открытого ключа ей на почту для подписи:



- (d) Зашифрованным на её ключе письмом я отправил подписанный ключ од-ногруппницы ей обратно:



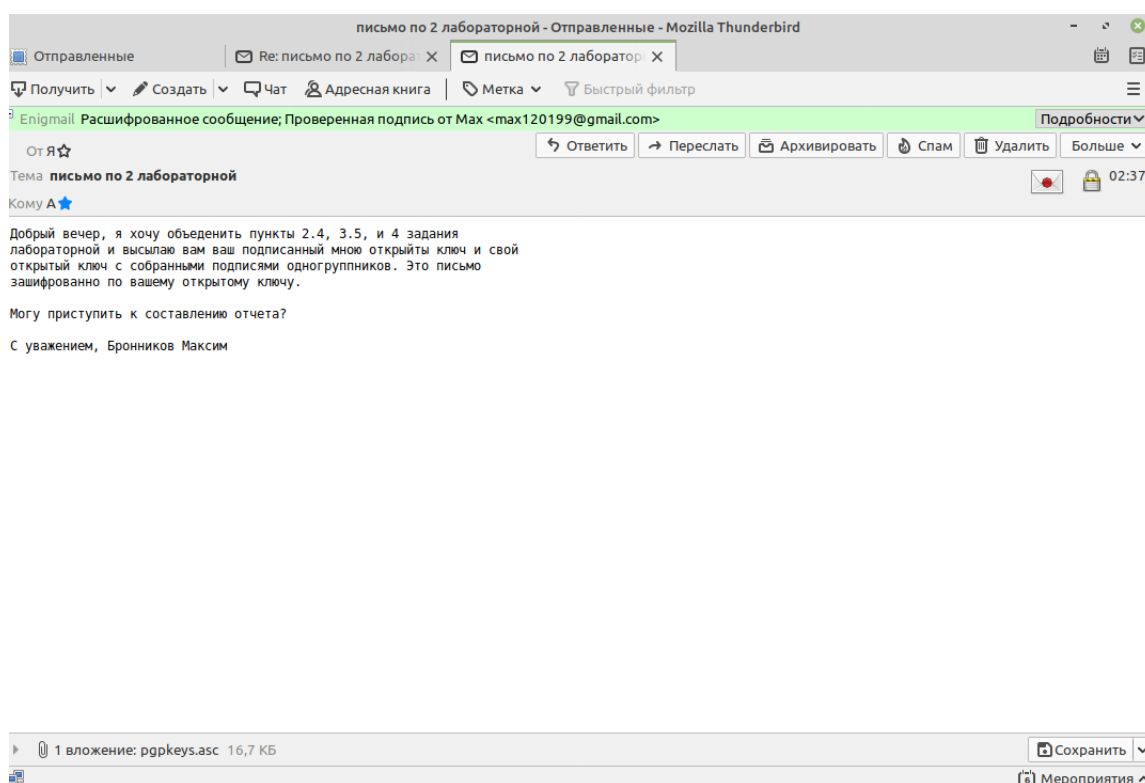
- (е) Получил письмо со своим подписанным сертификатом, который импортировал к себе в менеджер ключей:



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

Основной идентификатор пользователя Max Bronnikov <max120199@gmail.com>	
Тип	Пара ключей
Отпечаток	26AD 5C60 27D4 70E3 FADF D656 62ED B472 55C4 331D
Основное Сертификация Структура	
Идентификатор пользователя / Кем удостоверяется	Отпечаток
Max Bronnikov <max120199@gmail.com>	26AD 5C60 27D4 70E3 FADF D656 62ED B472 55C4 331D
Max Bronnikov <max120199@gmail.com>	26AD 5C60 27D4 70E3 FADF D656 62ED B472 55C4 331D
Лина Вельтман <kluu@mail.ru>	7540 582A 2ED9 7652 783F D130 1026 049F 7D6A 540F
235=89 1B8D552 <stifeev99@mail.ru>	D5ED 9D0B E947 BA35 87E7 87E2 A6DF 611D C1FE 9963
Alex Lopatin <minelabory@gmail.com>	303C 534B 1B4A 8BB7 DBC5 F076 2E1B FC24 D3E3 076C
Tururu Era <maksik1xd@gmail.com>	BC47 3422 6DC0 3832 D38C 50ED 41B4 DA30 AFDA 8099
ksuxich <ksenshaaa@gmail.com>	B08E 8E55 0BB9 C661 5D00 523E 1425 FE57 50B3 AF50
Норгаев Дамир <curlysilks53@yandex.ru>	9021 C503 72CD 0823 4AF0 5253 2EEE 2213 2A89 3CE4
Alexey Uskov <pardus@yandex-team.ru>	7593 F20A 8309 42F9 9FFF 9C9D 1060 D77E DC91 AE7A
Ярослав Поскрывков <yaroslavposkryakov@gmail.com>	9A4C FCA7 D032 1624 BBBD F135 B7D4 8A07 4644 1035
Victor <viko2000@mail.ru>	E977 D270 6D76 98B3 8EB2 2F37 2BD7 2DBF 8A90 D76A
Vanya Dneprov <vanya.dneprov@gmail.com>	FA74 5DFE 3DBD 16C2 5385 E093 0CF8 6A94 6FA5 C5B0
Денис Ваньков <ivankovden99@gmail.com>	B2FB 1A70 DF00 2C33 326A 890F 0989 80D4 45CF 5271
Ju Vysotina <juvyjuli@gmail.com>	3761 8A30 52A5 9725 5CDB D1A5 1B33 C8C3 6073 E185
Max Bronnikov <max120199@gmail.com>	26AD 5C60 27D4 70E3 FADF D656 62ED B472 55C4 331D

4. Я подписал сертификат преподавателя своим ключом и выслал ему на его адрес электронной почты вместе со своим открытым ключом, содержащим необходимое количество подписей одноклассников, 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 обмениваться 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 сертификат в будущем для обмена защищенными сообщениями.