Московский авиационный институт
(Национальный исследовательский университет)

Лабораторная работа № 2

по курсу «Криптография»

Студент: Фирфаров А. С.
Группа: 8О-308Б

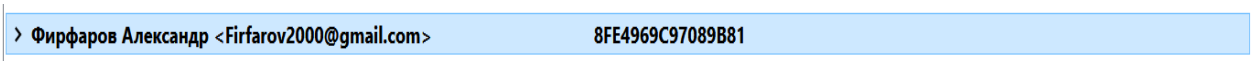
Москва, 2020

Постановка задачи

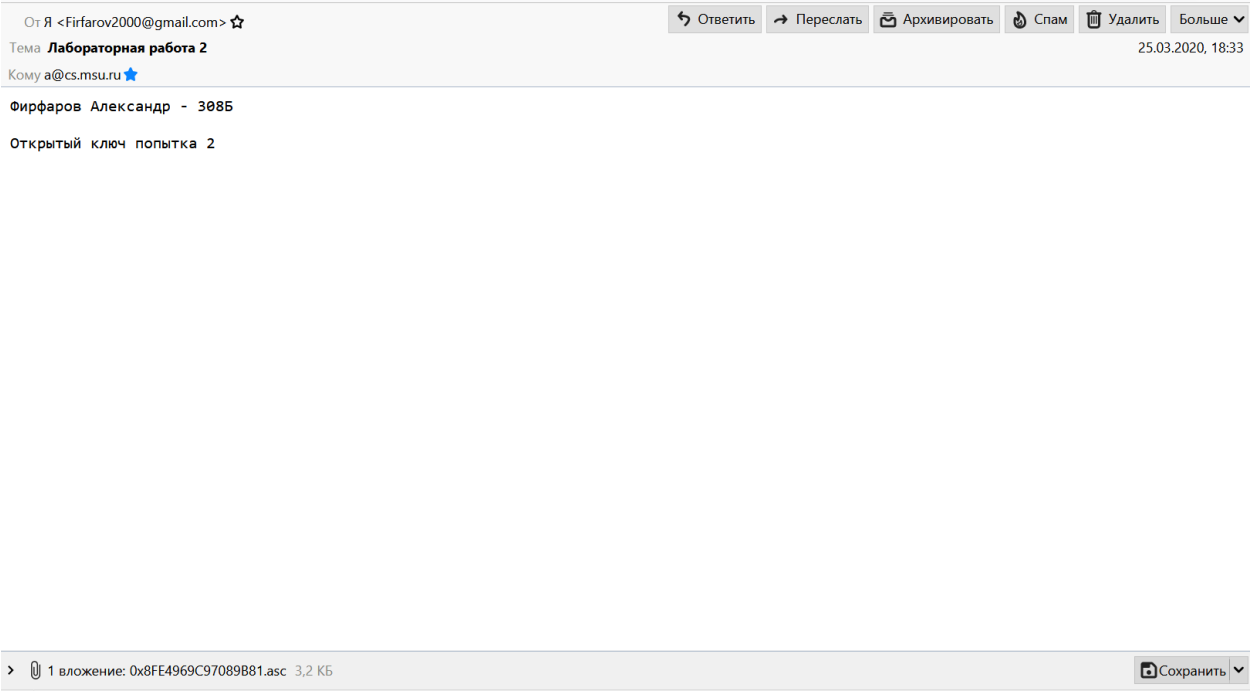
1. Создать пару OpenPGP-ключей, указав в сертификате свою почту. Создать её возможно, например, с помощью дополнения Enigmail к почтовому клиенту thunderbird, или из командной строки терминала ОС семейства linux.
2. Установить связь с преподавателем, используя созданный ключ, следующим образом:
2.1. 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.
4. Подписать сертификат открытого ключа преподавателя и выслать ему

Метод решения:

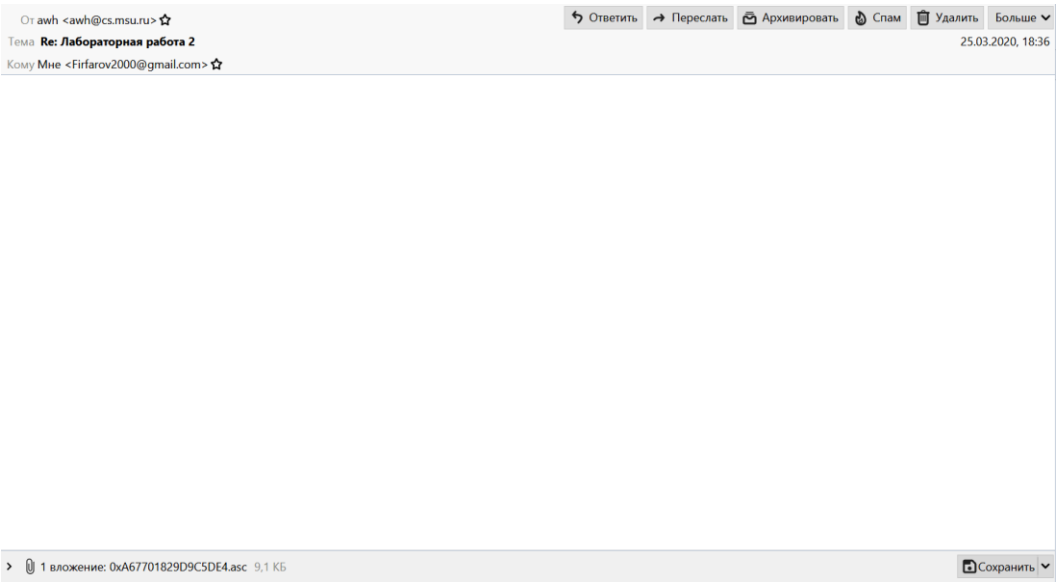
Я создал пару ключей:



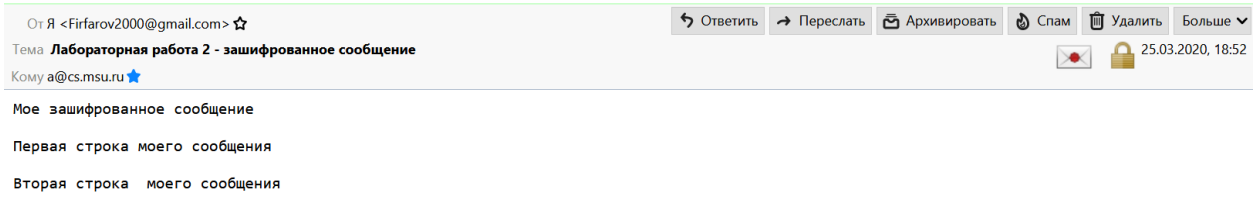
Отправил преподавателю свой открытый ключ:



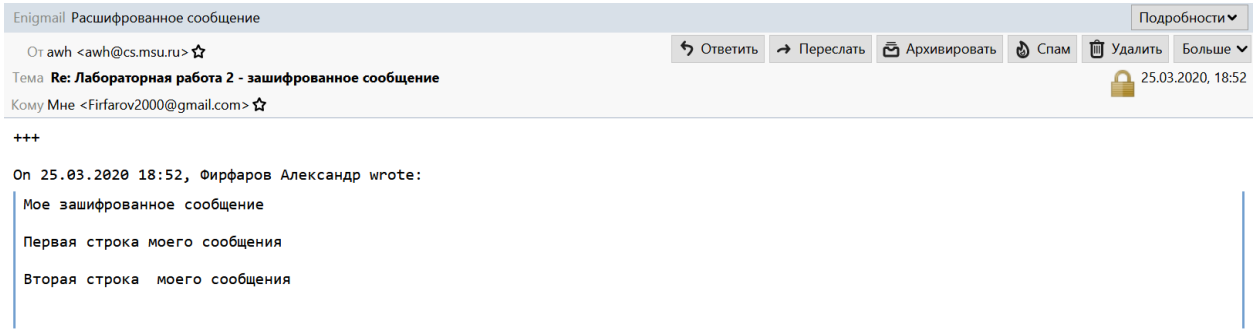
Получил ключ преподавателя:



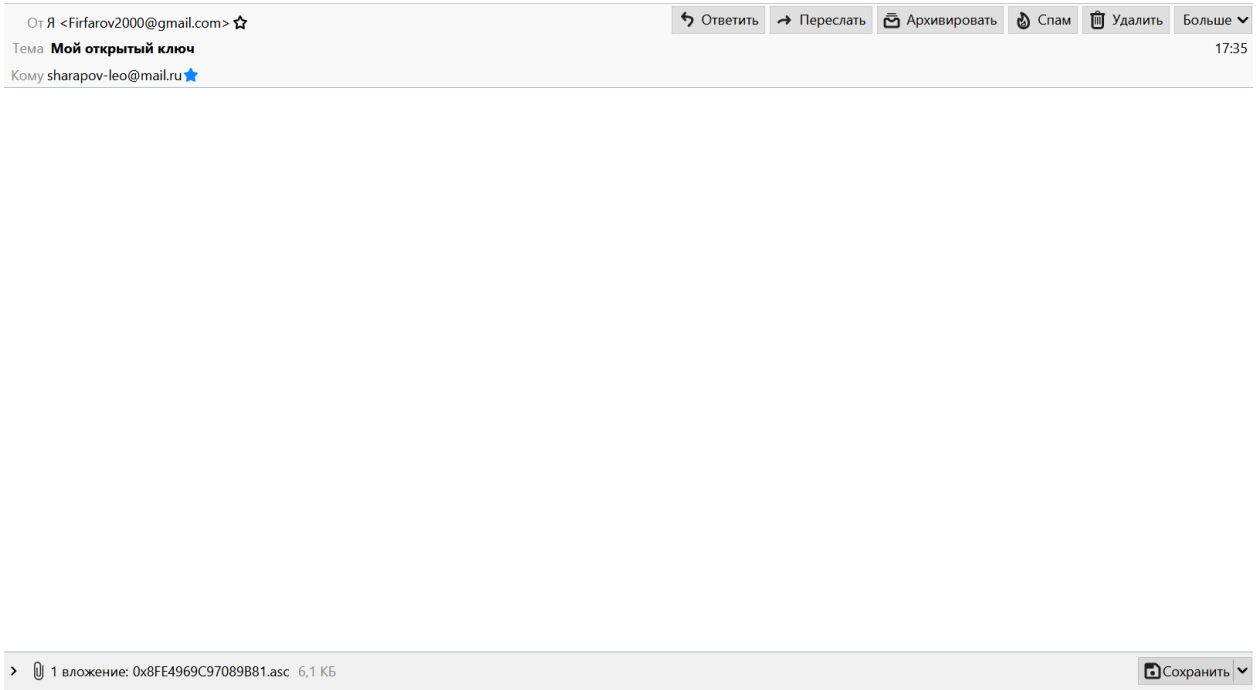
Выслал зашифрованное сообщение:



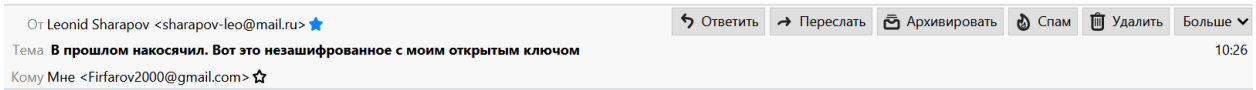
Дождался ответного письма преподавателя и расшифровал его:



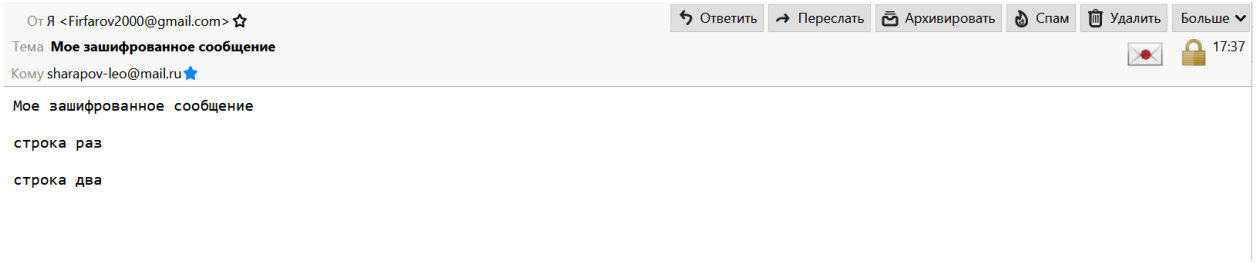
Отправил ключ одногруппнику:



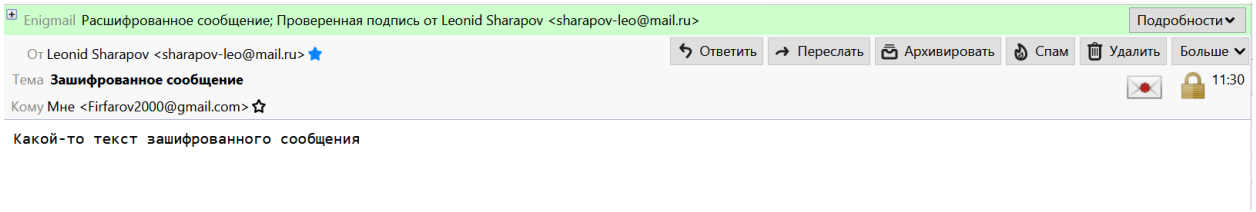
Получил ключ одногруппника:



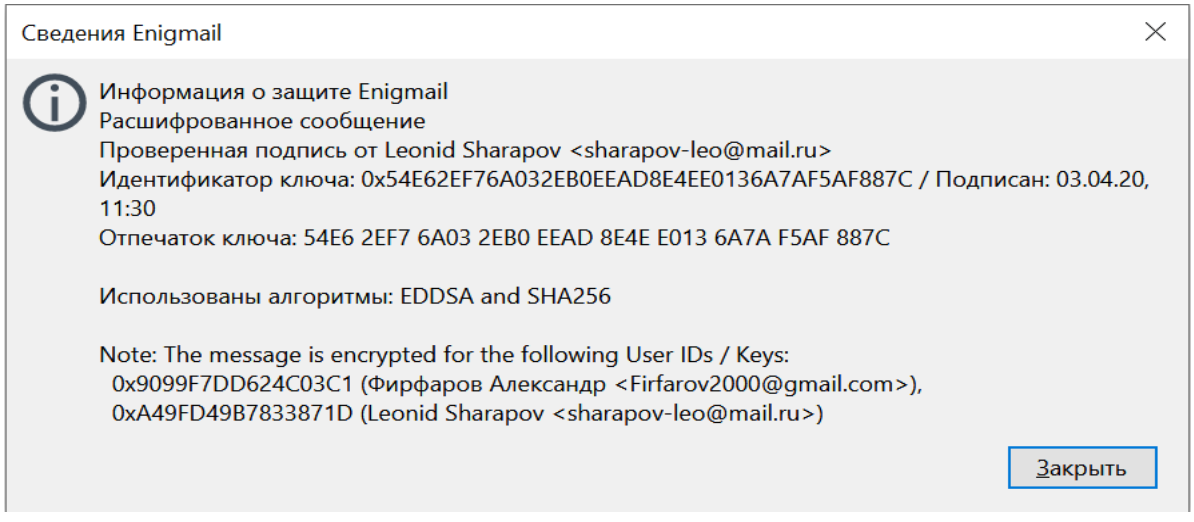
Отправил сообщение, зашифрованное на ключе собеседника:

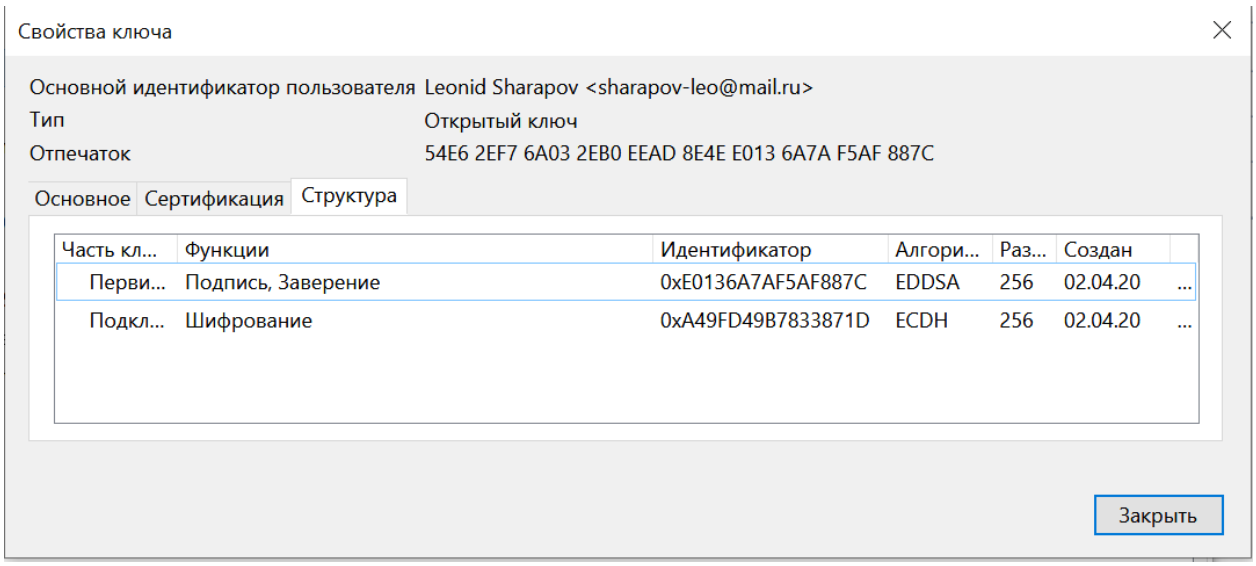


Расшифровал полученное письмо:

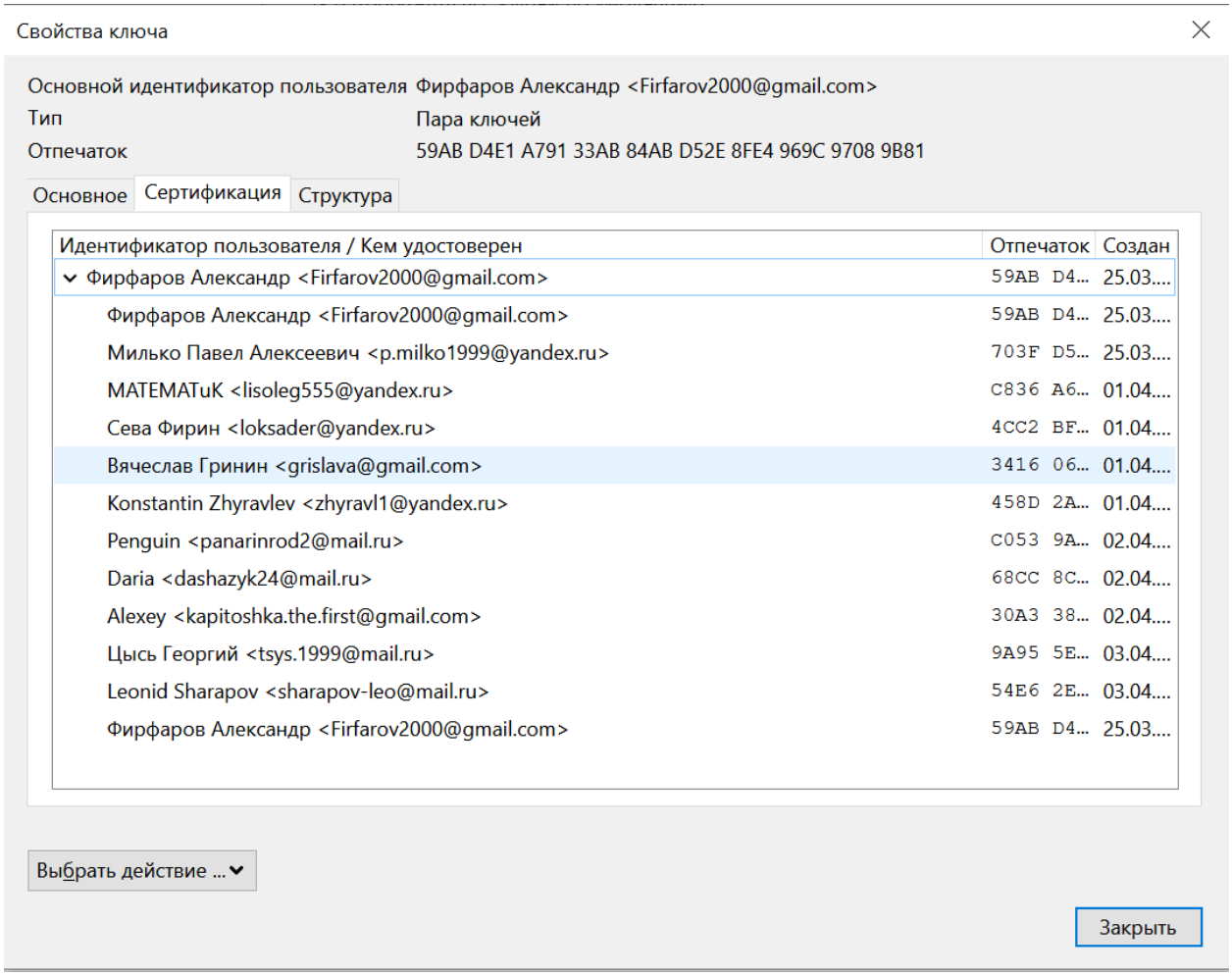


Сравнил ключ в письме и ключ из менеджера ключей:

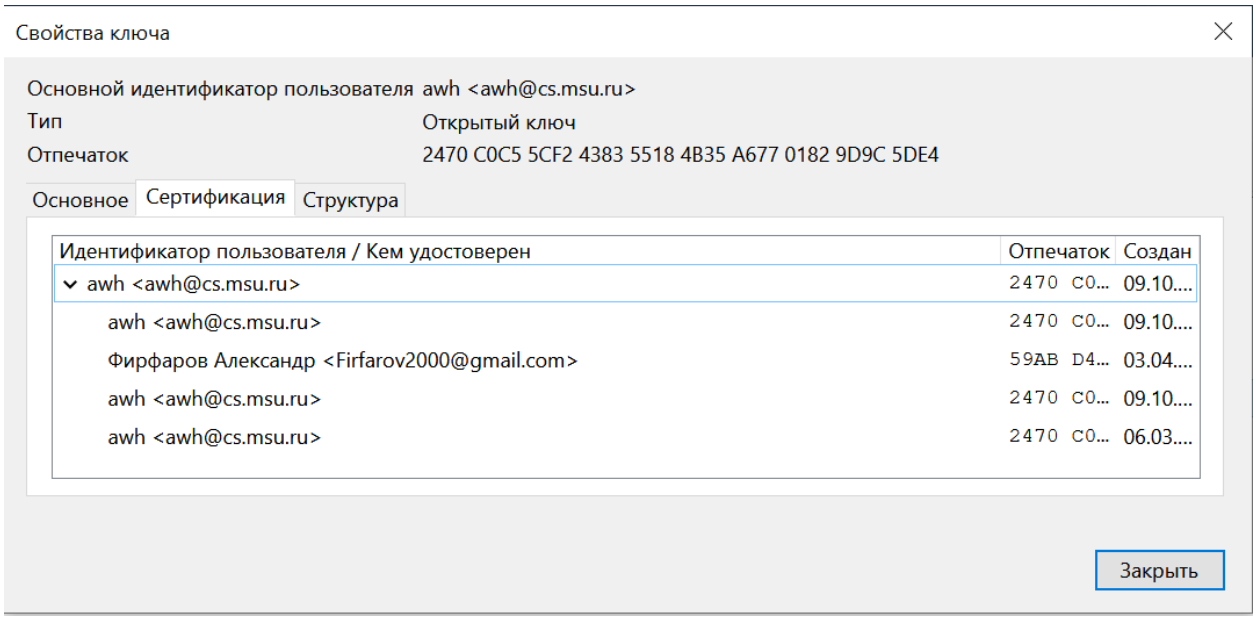




Собрал 10 подписей под своим сертификатом:



Подписал ключ преподавателя:



Выводы

В ходе выполнения данной лабораторной работы я научился работать с OpenPGP-ключами и использовать их для шифрования и подписи. В жизни может быть очень важно иметь возможность отправить письмо, которое нельзя прочитать без наличия ключа. Сложнее всего в лабораторной работе было собрать подписи одногруппников.