

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

Метод решения:

Я создал пару ключей:

> Фирфаров Александр <Firfarov2000@gmail.com>

8FE4969C97089B81

Отправил преподавателю свой открытый ключ:

От Я <Firfarov2000@gmail.com> ☆

↩ Ответить

➡ Переслать

📁 Архивировать

🔥 Спам

🗑 Удалить

Больше ▼

Тема **Лабораторная работа 2**

25.03.2020, 18:33

Кому a@cs.msu.ru ★

Фирфаров Александр - 3085

Открытый ключ попытка 2

> 📎 1 вложение: 0x8FE4969C97089B81.asc 3,2 КБ

📁 Сохранить ▼

Получил ключ преподавателя:

От awh <awh@cs.msu.ru> ☆

↩ Ответить

➡ Переслать

📁 Архивировать

🔥 Спам

🗑 Удалить

Больше ▼

Тема **Re: Лабораторная работа 2**

25.03.2020, 18:36

Кому Мне <Firfarov2000@gmail.com> ☆

> 📎 1 вложение: 0xA67701829D9C5DE4.asc 9,1 КБ

📁 Сохранить ▼

Выслал зашифрованное сообщение:

От Я <Firfarov2000@gmail.com> ☆

Тема **Лабораторная работа 2 - зашифрованное сообщение**

Кому a@cs.msu.ru ★

ОтвечитьПереслатьАрхивироватьСпамУдалитьБольше

25.03.2020, 18:52

Мое зашифрованное сообщение

Первая строка моего сообщения

Вторая строка моего сообщения

Дождался ответного письма преподавателя и расшифровал его:

Enigmail Расшифрованное сообщение

Подробнее

От awh <awh@cs.msu.ru> ☆

Тема **Re: Лабораторная работа 2 - зашифрованное сообщение**

Кому Мне <Firfarov2000@gmail.com> ☆

ОтвечитьПереслатьАрхивироватьСпамУдалитьБольше

25.03.2020, 18:52

+++

On 25.03.2020 18:52, Фирфаров Александр wrote:

Мое зашифрованное сообщение

Первая строка моего сообщения

Вторая строка моего сообщения

Отправил ключ однокласснику:

От Я <Firfarov2000@gmail.com> ☆

Тема **Мой открытый ключ**

Кому sharapov-leo@mail.ru ★

ОтвечитьПереслатьАрхивироватьСпамУдалитьБольше

17:35

1 вложение: 0x8FE4969C97089B81.asc 6,1 КБ

Сохранить

Получил ключ одnogруппника:

От Leonid Sharapov <sharapov-leo@mail.ru> ★

Тема В прошлом накосячил. Вот это незашифрованное с моим открытым ключом

Кому Мне <Firfarov2000@gmail.com> ☆

Ответить

Переслать

Архивировать

Спам

Удалить

Больше

10:26

1 вложение: 0xE0136A7AF5AF887C.asc 677 байт

Сохранить

Отправил сообщение, зашифрованное на ключе собеседника:

От Я <Firfarov2000@gmail.com> ☆

Тема **Мое зашифрованное сообщение**

Кому sharapov-leo@mail.ru ★

Ответить

Переслать

Архивировать

Спам

Удалить

Больше

17:37

Мое зашифрованное сообщение

строка раз

строка два

Расшифровал полученное письмо:

Enigmail Расшифрованное сообщение; Проверенная подпись от Leonid Sharapov <sharapov-leo@mail.ru>

От Leonid Sharapov <sharapov-leo@mail.ru> ★

Тема **Зашифрованное сообщение**

Кому Мне <Firfarov2000@gmail.com> ☆

Какой-то текст зашифрованного сообщения

Ответить

Переслать

Архивировать

Спам

Удалить

Больше

11:30

Сравнил ключ в письме и ключ из менеджера ключей:

Сведения Enigmail

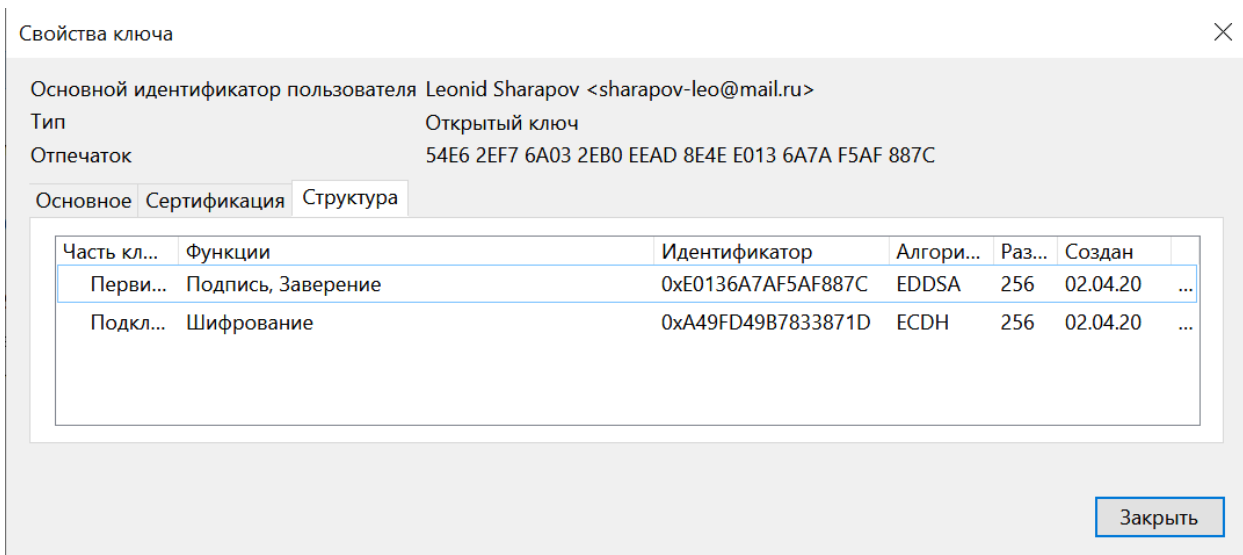
И

Информация о защите Enigmail
Расшифрованное сообщение
Проверенная подпись от Leonid Sharapov <sharapov-leo@mail.ru>
Идентификатор ключа: 0x54E62EF76A032EB0EEAD8E4EE0136A7AF5AF887C / Подписан: 03.04.20, 11:30
Отпечаток ключа: 54E6 2EF7 6A03 2EB0 EEAD 8E4E E013 6A7A F5AF 887C

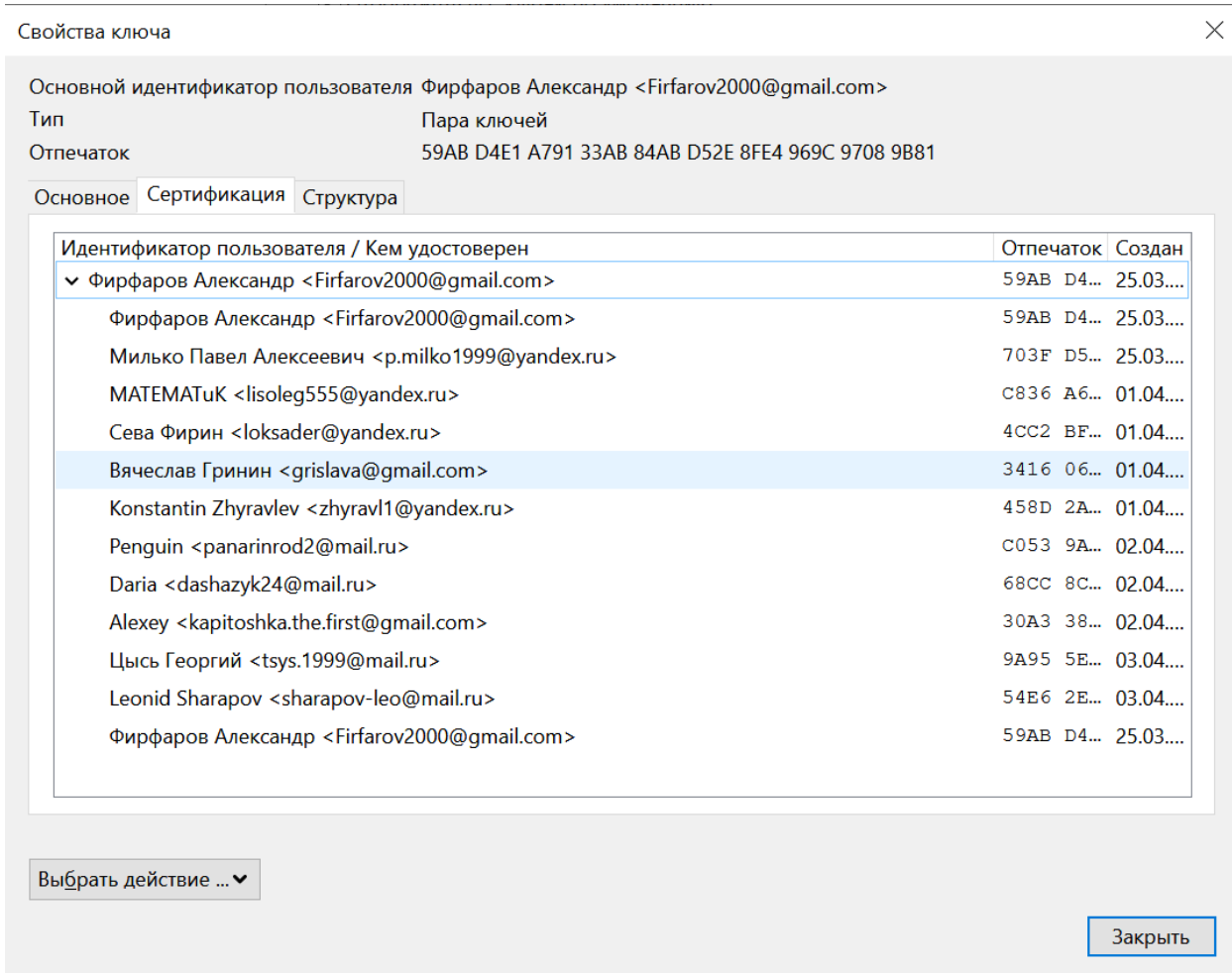
Использованы алгоритмы: EDDSA and SHA256

Note: The message is encrypted for the following User IDs / Keys:
0x9099F7DD624C03C1 (Фирфаров Александр <Firfarov2000@gmail.com>),
0xA49FD49B7833871D (Leonid Sharapov <sharapov-leo@mail.ru>)

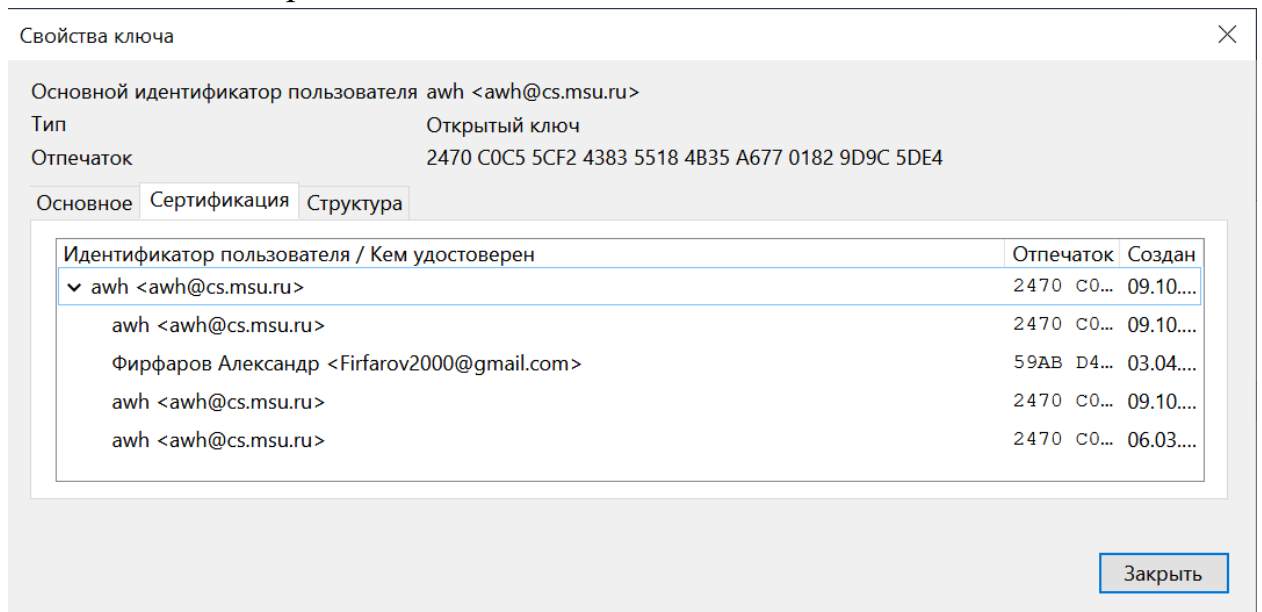
Заккрыть



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 одноклассников.