# Лабораторная работа № 2 по курсу Криптография

Выполнила студентка группы 08-307 МАИ *Усачева Елизавета*.

## Задание

- Создать пару OpenPGP-ключей, указав в сертификате свою почту.
- Установить связь с преподавателем, используя созданный ключ.
- Собрать подписи под своим сертификатом открытого ключа.

## Введение

OpenPGP – это открытый протокол шифрования электронной почты с использованием криптографии с открытым ключом. Он основан на оригинальном программном обеспечении PGP (Pretty Good Privacy). Протокол OpenPGP определяет стандартные форматы для зашифрованных сообщений, подписей и сертификатов для обмена открытыми ключами.

Шифрование OpenPGP может обеспечить безопасную доставку файлов и сообщений, а также обеспечить подтверждение того, кто создал или отправил сообщение, используя процесс, называемый цифровой подписью. Использование OpenPGP для связи требует участия как отправителя, так и получателя. OpenPGP также может использоваться для защиты конфиденциальных файлов, когда они хранятся в уязвимых местах, таких как мобильные устройства или в облаке.

## Метод решения

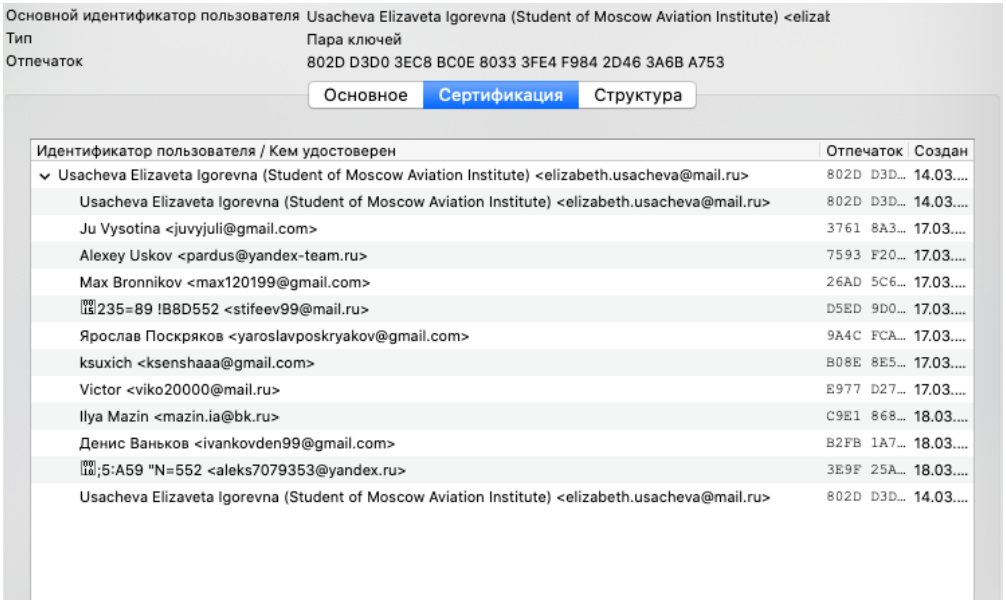
Для генерации публичного и приватного ключей и для подписания публичных ключей собеседников я использовала дополнение Enigmail для почтового клиента Thunderbird. Дополнение поддерживает шифрование, расшифровку и подпись электронных писем с использованием криптосистемы с открытым ключом PGP.

- Установила связь с преподавателем и получила зашифрованное сообщение.
- Обменялась открытыми ключами с одногруппниками и собрала подпись.

## Выводы

В данной лабораторной работе я познакомилась с практическим шифрованием данных, предназначенным для безопасного обмена информацией и в качестве цифровой подписи. Однако, OpenPGP требует для связи участие обоих собеседников и личный контроль подлинности ключа шифрования собеседника, что является уязвимостью.


Enigmail Расшифрованное сообщение
Подробности
От awh <awh@cs.msu.ru>
Ответить
Переслать
Архивировать
Спам
Удалить
Больше
Тема Re: Криптография. Лабораторная работа №2.
16.03.2020, 17:45
Кому Мне
Добрый день, Елизавета!
Получил ключ.
--
С уважением,
Август
On 3/16/20 2:08 PM, Елизавета Усачева wrote:
Добрый день, Август Валерьевич! Выполняю пункт 2.1 – устанавливаю с Вами связь и высылаю свой открытый ключ во вложении.
С уважением,
Усачева Елизавета,
80-307Б.


Основной идентификатор пользователя Usacheva Elizaveta Igorevna (Student of Moscow Aviation Institute) <elizat
Тип Пара ключей
Отпечаток 802D D3D0 3EC8 BC0E 8033 3FE4 F984 2D46 3A6B A753
Основное
Сертификация
Структура
Идентификатор пользователя / Кем удостоверен
Отпечаток
Создан
Usacheva Elizaveta Igorevna (Student of Moscow Aviation Institute) <elizabeth.usacheva@mail.ru> 802D D3D… 14.03....
Usacheva Elizaveta Igorevna (Student of Moscow Aviation Institute) <elizabeth.usacheva@mail.ru> 802D D3D… 14.03....
Ju Vysotina <juvyjuli@gmail.com> 3761 8A3… 17.03....
Alexey Uskov <pardus@yandex-team.ru> 7593 F20… 17.03....
Max Bronnikov <max120199@gmail.com> 26AD 5C6… 17.03....
235=89 !B8D552 <stifeev99@mail.ru> D5ED 9D0… 17.03....
Ярослав Поскряков <yaroslavposkryakov@gmail.com> 9A4C FCA… 17.03....
ksuxich <ksenshaaa@gmail.com> B08E 8E5… 17.03....
Victor <viko20000@mail.ru> E977 D27… 17.03....
Ilya Mazin <mazin.ia@bk.ru> C9E1 868… 18.03....
Денис Ваньков <ivankovden99@gmail.com> B2FB 1A7… 18.03....
;5:A59 "N=552 <aleks7079353@yandex.ru> 3E9F 25A… 18.03....
Usacheva Elizaveta Igorevna (Student of Moscow Aviation Institute) <elizabeth.usacheva@mail.ru> 802D D3D… 14.03....