Московский авиационный институт (национальный исследовательский университет)

Факультет информационных технологий и прикладной математики

Кафедра вычислительной математики и программирования

Лабораторная работа №2 по курсу «Криптография»

Студент: И. Т. Батяновский
Преподаватель: А. В. Борисов
Группа: М8О-307Б

Дата:
Оценка:
Подпись:

Москва, 2020

Лабораторная работа №2

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:

   - 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).
   - Дождаться письма, в котором собеседник Вам пришлет сертификат своего открытого ключа.
   - Выслать сообщение, зашифрованное на ключе собеседника.
   - Дождаться ответного письма.
   - Расшифровать ответное письмо своим закрытым ключом.

3. Собрать подписи под своим сертификатом открытого ключа.

   - Получить сертификат открытого ключа одногруппника.
   - Убедиться в том, что подписываемый Вами сертификат ключа принадлежит его владельцу - путём сравнения отпечатка ключа или ключа целиком, по доверенным каналам связи.
   - Подписать сертификат открытого ключа одногруппника.
   - Передать подписанный Вами сертификат полученный в п.3.2 его владельцу, т.е. одногруппнику.
   - Повторив п.3.0.-3.3., собрать 10 подписей одногруппников под своим сертификатом.
   - Прислать преподавателю свой сертификат открытого ключа, с 10-ю или более подписями одногруппников.

4. Подписать сертификат открытого ключа преподавателя и выслать ему.

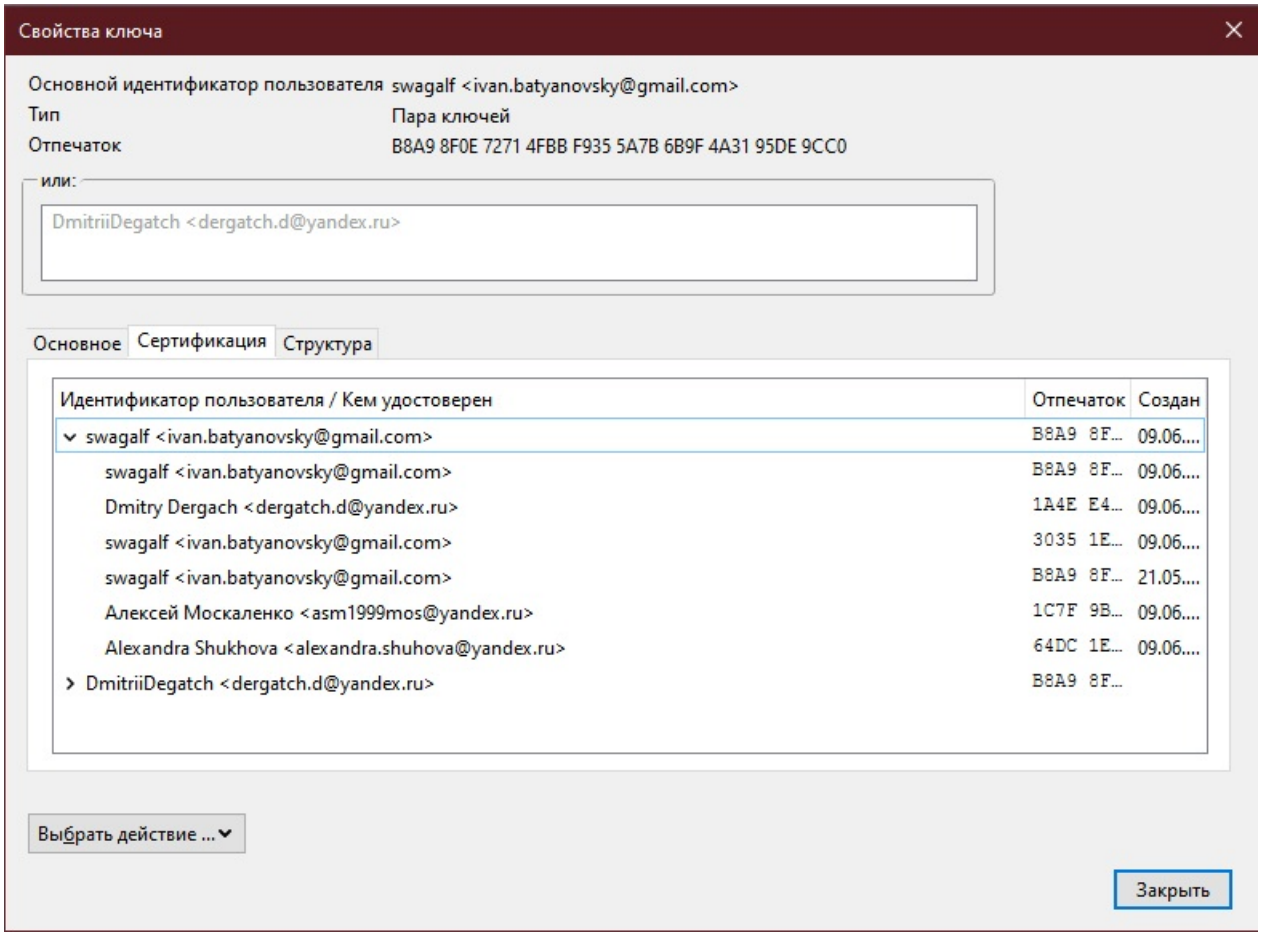
1 Решение

Для решения данной работы я использовал *Thunder bird*. Я установил дополнение *Enigmail*, которое позволяет удобно работать с PGP-ключами.

После установки дополнение предлагает сгенерировать пару ключей (public, private). Публичный ключ нужно отослать одногруппникам, которое используя его шифруют сообщения. Присылают его обратно, где я его могу расшифровать его используя второй ключ. Смысл в том, что даже при утечке публичного ключа злоумышленник не сможет расшифровать зашифрованное сообщение.

Получая сообщения со вложенными публичными ключами, *Enigmail* предлагает импортировать его в свой список ключей. Нужно отметить, что зайдя во вкладку подробнее можно подписать полученный ключ. Это нужно в дальнейшем, чтобы собрать подписи сертификации.

Подписанный чужой публичный ключ нужно отправить обратно владельцу, что список сертификации пополнялся.



Список подписей одногруппников

2 Выводы

В этой работе я получил навыки работы с ключами шифрования. Понял как в *Thunder Bird* шифровать открытым ключом сообщения, разшифровывать закрытым, подписывать сертификаты ключей и отправлять другие ключи.