Лабораторная работа № 2 по курсу Криптография

Выполнила студентка группы М8О-306Б-17 *Ветренко Полина*.

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

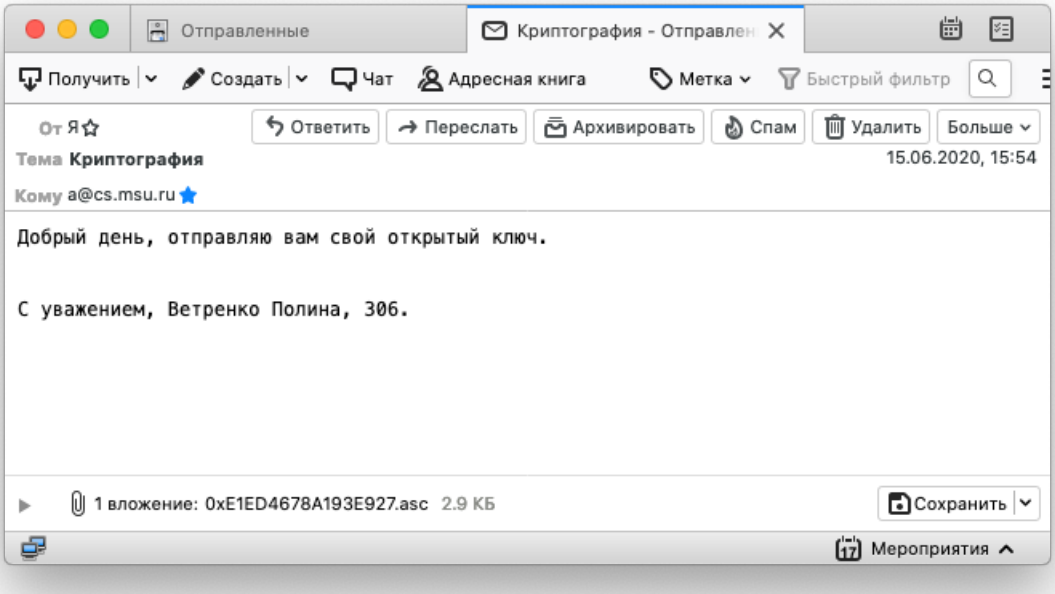
OpenPGP – это открытый протокол шифрования электронной почты с использованием криптографии с открытым ключом. Он основан на оригинальном программном обеспечении PGP (Pretty Good Privacy). Протокол OpenPGP определяет стандартные форматы для зашифрованных сообщений, подписей и сертификатов для обмена открытыми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

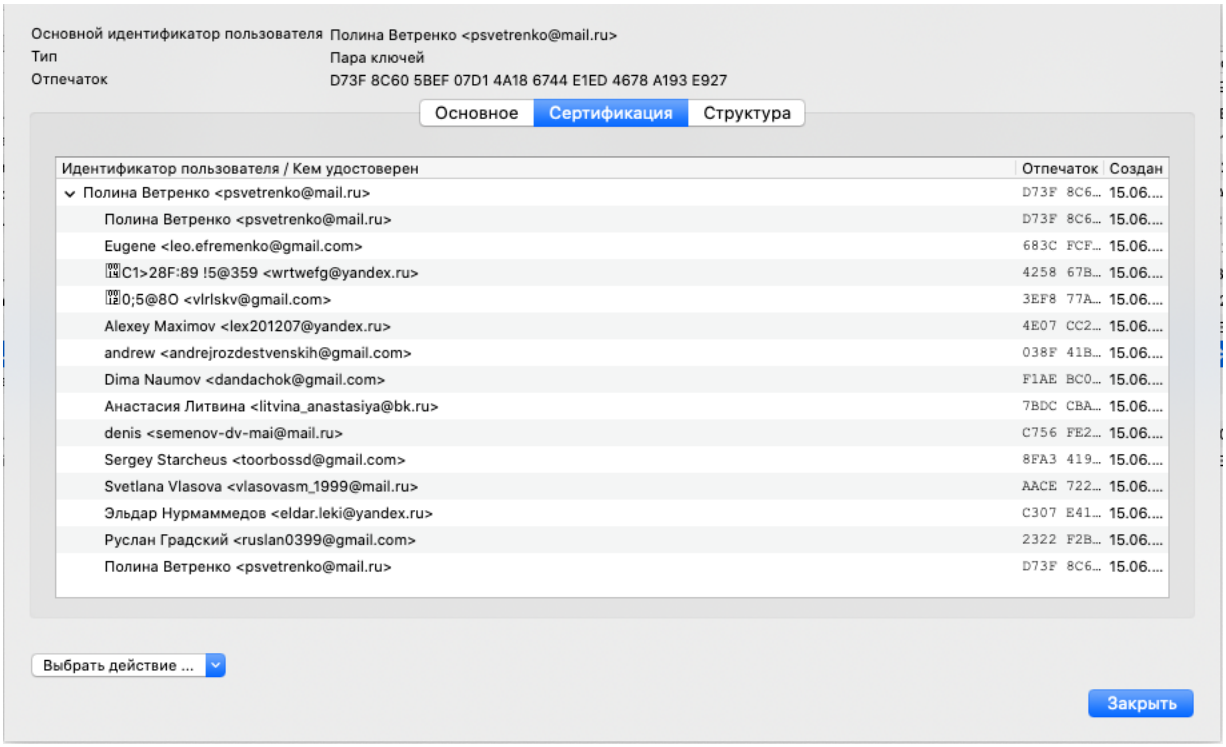
Шифрование OpenPGP может обеспечить безопасную доставку файлов и сообщений, а также обеспечить подтверждение того, кто создал или отправил сообщение, используя процесс, называемый цифровой подписью. Использование OpenPGP для связи требует участия как отправителя, так и получателя. OpenPGP также может 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.

Результаты работы





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.