

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

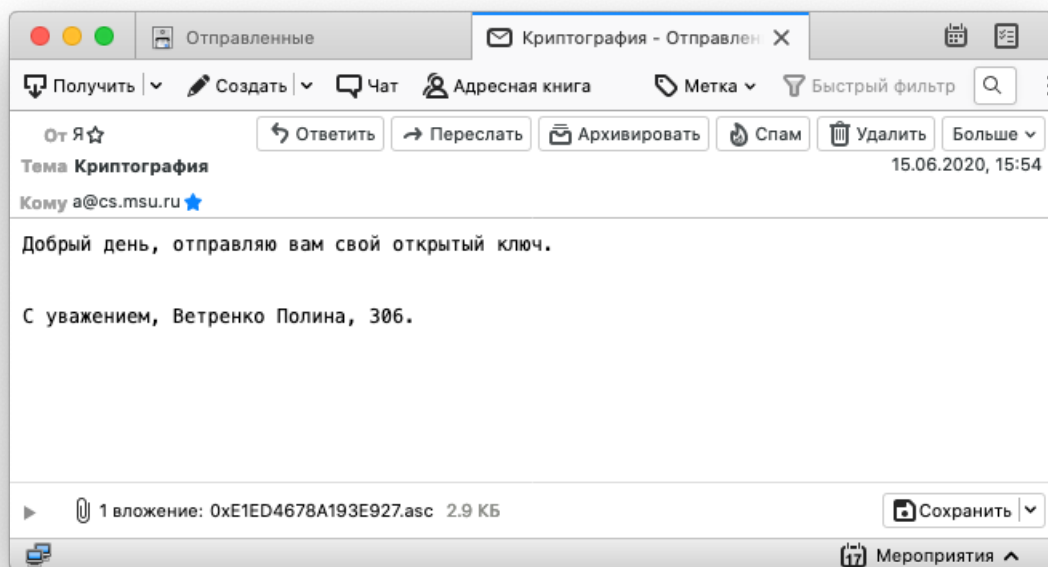
OpenPGP – это открытый протокол шифрования электронной почты с использованием криптографии с открытым ключом. Он основан на оригинальном программном обеспечении PGP (Pretty Good Privacy). Протокол OpenPGP определяет стандартные форматы для зашифрованных сообщений, подписей и сертификатов для обмена открытыми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



Основной идентификатор пользователя Полина Ветренко <psvetrenko@mail.ru>
Тип Пара ключей
Отпечаток D73F 8C60 5BEF 07D1 4A18 6744 E1ED 4678 A193 E927

Основное Сертификация Структура

Идентификатор пользователя / Кем удостоверен	Отпечаток	Создан
Полина Ветренко <psvetrenko@mail.ru>	D73F 8C6...	15.06...
Полина Ветренко <psvetrenko@mail.ru>	D73F 8C6...	15.06...
Eugene <leo.efremenko@gmail.com>	683C FCF...	15.06...
C1>28F:89 !5@359 <wrtwegf@yandex.ru>	4258 67B...	15.06...
0;5@80 <vlrlskv@gmail.com>	3EF8 77A...	15.06...
Alexey Maximov <lex201207@yandex.ru>	4E07 CC2...	15.06...
andrew <andrejrozdestvenskih@gmail.com>	038F 41B...	15.06...
Dima Naumov <dandachok@gmail.com>	F1AE BC0...	15.06...
Анастасия Литвина <litvina_anastasiya@bk.ru>	7BDC CBA...	15.06...
denis <semenov-dv-mai@mail.ru>	C756 FE2...	15.06...
Sergey Starcheus <toorbosd@gmail.com>	8FA3 419...	15.06...
Svetlana Vlasova <vlasovasm_1999@mail.ru>	AACE 722...	15.06...
Эльдар Нурмаммедов <eldar.leki@yandex.ru>	C307 E41...	15.06...
Руслан Градский <ruslan0399@gmail.com>	2322 F2B...	15.06...
Полина Ветренко <psvetrenko@mail.ru>	D73F 8C6...	15.06...

Выбрать действие ...

Заккрыть

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.