

Лабораторная работа №2

Задание

1. Сгенерировать OpenPGP-ключ и самоподписанный сертификат.
2. Установить связь с преподавателем и одногруппником, используя созданный ключ.
3. Собрать подписи под ключом.

Решение

Для генерации ключа, а так же шифрования/расшифровки писем буду использовать Дополнение к почтовому клиенту Thunderbird — Enigmail.

Чтобы установить связь с использованием ключа, отправим публичный ключ адресату, в ответ получим открытый ключ собеседника. Теперь используя полученный публичный ключ зашифруем письмо и отправим его, для этого достаточно поставить галочку Encryption. Примем в ответ зашифрованное письмо, расшифровка происходит автоматически, необходимо только ввести пароль от своего ключа.

Что бы подписать чужой ключ зайдём в раздел Key management и выберем опцию Sign key. Далее отправим подписанный ключ и в ответ получим свой публичный ключ с подписью собеседника, его необходимо импортировать. Повторяя данную операцию несколько раз соберём необходимое число подписей.