Отчёт по лабораторной работе №1 по курсу «Криптография»

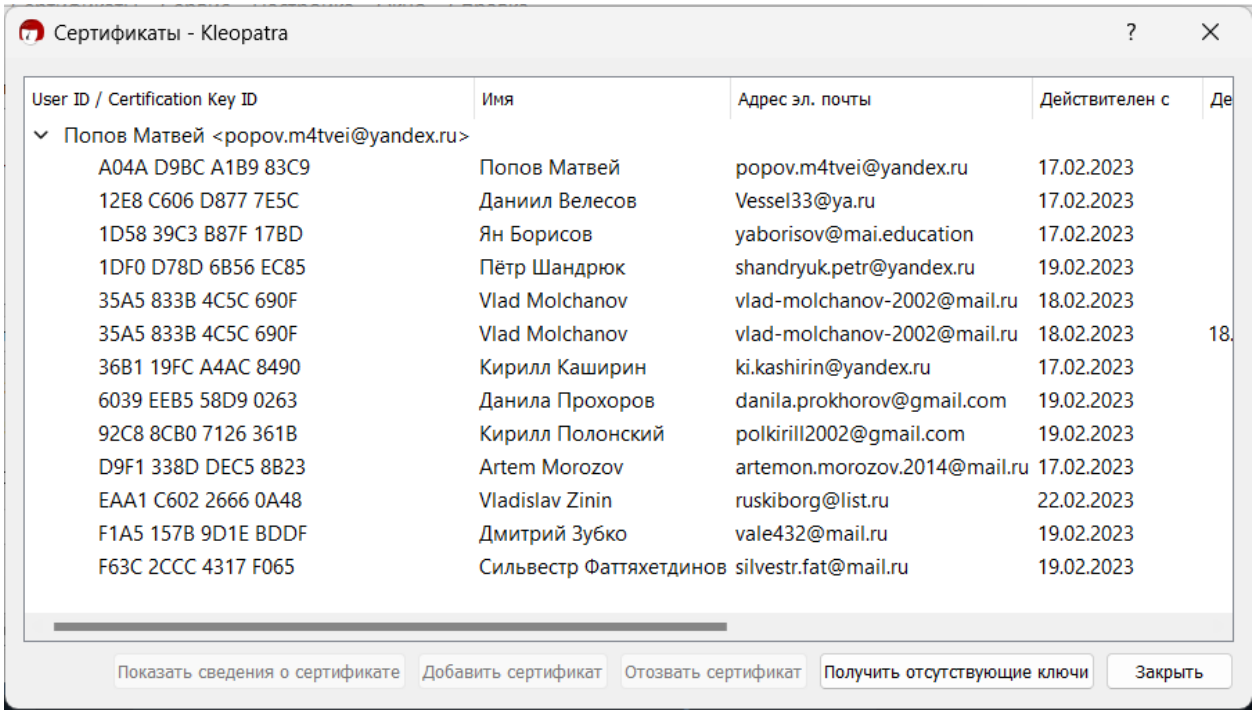
Выполнил Попов Матвей, группа М8О-308Б-20

Задание

1. Создать пару OpenPGP-ключей, указав в сертификате свою почту. Создать её возможно, например, с помощью почтового клиента thunderbird, или из командной строки терминала ОС семейства linux, или иным способом.
2. Установить связь с преподавателем, используя созданный ключ, следующим образом:
2.1. Прислать собеседнику от своего имени по электронной почте сообщение, во вложении которого поместить свой сертификат открытого ключа.
2.2. Дождаться письма, в котором собеседник Вам пришлет сертификат своего открытого ключа.
2.4. Выслать сообщение, зашифрованное на открытом ключе собеседника.
2.5. Дождаться ответного письма.
2.6. Расшифровать ответное письмо своим закрытым ключом.
3. Собрать подписи под своим сертификатом открытого ключа.
3.0. Получить сертификат открытого ключа одногруппника.
3.1. Убедиться в том, что подписываемый Вами сертификат ключа принадлежит его владельцу - путём сравнения отпечатка ключа или ключа целиком, по доверенным каналам связи.
3.2. Подписать сертификат открытого ключа одногруппника.
3.3. Передать подписанный Вами сертификат полученный в п.3.2 его владельцу, т.е. одногруппнику.
3.4. Повторив п.3.0.-3.3., собрать 10 подписей одногруппников под своим сертификатом.
3.5. Прислать преподавателю свой сертификат открытого ключа, с 10-ю или более подписями одногруппников.
3. Подписать сертификат открытого ключа преподавателя и выслать ему.

Ход работы

1. Установил Kleopatra на свою систему
2. Создал в ней свой сертификат
3. Экспортировал его и отправил 11 одногруппникам на подпись, взамен импортировал их сертификаты и подписывал их
4. Получив нужное количество подписей на сертификате, отправил его преподавателю



5. Получил зашифрованное сообщение от преподавателя, расшифровал его с помощью почтового клиента Mozilla Thunderbird.
6. С помощью того же почтового клиента отправил преподавателю своё зашифрованное сообщение.

Вывод

Проделав лабораторную работу, я познакомился с ПО Kleopatra, с новыми возможностями Mozilla Thunderbird, а также с новой концепцией шифрования почтовых писем с помощью сертификатов. Помимо этого, я улучшил свои коммуникативные навыки (т.н. Soft Skills), так как сбор подписей подразумевает общение с людьми.