

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 одноклассника.
 - 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 одноклассника.
 - 3.3. Передать подписанный Вами сертификат полученный в п.3.2 его владельцу, т.е. однокласснику.
 - 3.4. Повторив п.3.0.-3.3., собрать 10 подписей одноклассников под своим сертификатом.
 - 3.5. Прислать преподавателю свой сертификат открытого ключа, с 10-ю или более подписями одноклассников.
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 одноклассникам на подпись, взамен импортировал их сертификаты и подписывал их
4. Получив нужное количество подписей на сертификате, отправил его преподавателю

Сертификаты - Kleopatra				
User ID / Certification Key ID	Имя	Адрес эл. почты	Действителен с	До
▼ Попов Матвей <popov.m4tvei@yandex.ru>				
A04A D9BC A1B9 83C9	Попов Матвей	popov.m4tvei@yandex.ru	17.02.2023	
12E8 C606 D877 7E5C	Даниил Велесов	Vessel33@ya.ru	17.02.2023	
1D58 39C3 B87F 17BD	Ян Борисов	yaborisov@mai.education	17.02.2023	
1DF0 D78D 6B56 EC85	Пётр Шандрюк	shandryuk.petr@yandex.ru	19.02.2023	
35A5 833B 4C5C 690F	Vlad Molchanov	vlad-molchanov-2002@mail.ru	18.02.2023	
35A5 833B 4C5C 690F	Vlad Molchanov	vlad-molchanov-2002@mail.ru	18.02.2023	18.02.2023
36B1 19FC A4AC 8490	Кирилл Каширин	ki.kashirin@yandex.ru	17.02.2023	
6039 EEB5 58D9 0263	Данила Прохоров	danila.prokhorov@gmail.com	19.02.2023	
92C8 8CB0 7126 361B	Кирилл Полонский	polkirill2002@gmail.com	19.02.2023	
D9F1 338D DEC5 8B23	Artem Morozov	artemon.morozov.2014@mail.ru	17.02.2023	
EAA1 C602 2666 0A48	Vladislav Zinin	ruskiborg@list.ru	22.02.2023	
F1A5 157B 9D1E BDDF	Дмитрий Зубко	vale432@mail.ru	19.02.2023	
F63C 2CCC 4317 F065	Сильвестр Фатяхетдинов	silvestr.fat@mail.ru	19.02.2023	

- Получил зашифрованное сообщение от преподавателя, расшифровал его с помощью почтового клиента Mozilla Thunderbird.
- 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.