

Отчёт по лабораторной работе №1 по курсу «Криптография»

Выполнил Попов Николай, группа М8О-308Б-21

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 gpg на свою систему.
2. Создал пару приватный-публичный ключ.
3. Экспортировал его и отправил 11 одноклассникам на подпись, взамен импортировал их сертификаты и подписывал их сертификаты.

```
helio@MacBook-Pro-helio ~ -- -zsh
[~ > gpg --list-sigs nikolay.p998@gmail.com Py base 22:26:12]
pub   rsa4096 2024-03-10 [SC]
      28AC45E8547728656F0B682D6E880FD46434FFC5
uid       [ undef ] Nikolay Popov (hey) <nikolay.p998@gmail.com>
sig 3      6E880FD46434FFC5 2024-03-10 [self-signature]
sig        03A7AC6194F0F7DB 2024-03-14 Danya Shangin <shangin.daniil2018@yandex.ru>
sig        14B9772F84B3764B 2024-03-12 [User ID not found]
sig        2D459E6010E168DD 2024-03-12 Kaloev George <caloev.georgy@yandex.ru>
sig        3E9FA9D7B73DF1ED 2024-03-14 kirill <kirillmedvedev23@gmail.com>
sig        6CA2AEDDB4EF2089 2024-03-13 Nikita Shaposhnik <shaposhnik.8668@mail.ru>
sig        6CCEE9E6331AD1E2 2024-03-14 [User ID not found]
sig        6CCEE9E6331AD1E2 2024-03-14 [User ID not found]
sig        BDE994BEE6C7D283 2024-03-12 Алина Суляева <darersth@gmail.com>
sig        C0FC4DC8FC262DA9 2024-03-13 [User ID not found]
sig        D15C5089A548D39B 2024-03-12 Alina Polzikova <polzikova.alina@icloud.com>
sig        DBAC53B8758EA3E0 2024-03-13 Armishev Kirill <armishev@yandex.ru>
sub   rsa4096 2024-03-10 [E]
sig      6E880FD46434FFC5 2024-03-10 [self-signature]

[~ > Py base 22:26:19]
```

4. Получив нужное количество подписей на сертификате, отправил его преподавателю.
5. Получил зашифрованное сообщение от преподавателя, расшифровал его с помощью своего приватного ключа через утилиту gpg. Сообщение представляло собой текст в кодировке base64, декодировав которое я получил следующий результат:

```
helio@MacBook-Pro-helio ~/Desktop -- -zsh
[~/Desktop > base64 -d --input decrypted.asc Py base 22:37:16]
Здравствуйте, Николай.

10.03.2024 23:01, Николай Попов пишет:
>

--
С уважением,
Август
~/Desktop > Py base 22:37:19
```

6. Зашифровал публичным ключом преподавателя текстовый файл сообщения и отправил его преподавателю.
7. Получил зашифрованный ответ преподавателя на мое сообщение. Расшифровал и декодировал:

```
helio@MacBook-Pro-helio — -zsh
~/Desktop
Last login: Sat Mar 23 22:45:34 on ttys006
~ > cd Desktop
~/Desktop > base64 -d --input decrypted2.asc
Расшифровал : "Hello, August."

14.03.2024 21:20, Николай Попов пишет:
>
>
> чт, 14 мар. 2024 г. в 20:50, awh <awh@cs.msu.ru <mailto:awh@cs.msu.ru>>:
>
--
С уважением,
Август
~/Desktop >
```

8. Подписал и отправил публичный ключ преподавателя

9. Написал отчет к данной лабораторной работе

Вывод

В ходе выполнения лабораторной работы были изучены и практически применены механизмы шифрования и цифровой подписи с использованием стандарта OpenPGP. Был получен опыт работы с инструментом GnuPG для создания ключевых пар, шифрования / дешифрования сообщений и управления цифровыми подписями.