Отчет по лабораторной работе №2 по курсу «Криптография»

Выполнил Моисеенков Илья Павлович, М8О-308Б-19.

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

В работе я пользовался утилитой gpg.

1. Создание ключа

```
gpg --full-gen-key
```

Затем требуется ввести свою почту, имя, фамилию, срок действия ключа и прочую важную информацию.

2. Отправка ключа на подпись

```
gpg -a -o <имя файла> --export <ключ>
```

После этого нужно отправить полученный файл по почте другому человеку для подписания.

3. Подпись ключа

```
gpg --import <полученный файл с ключом>
gpg --sign-key <полученный ключ>
gpg -a -o <файл с подписанным ключом> --export <полученный ключ>
```

Файл с подписанным ключом отправляется обратно, чтобы собеседник импортнул его себе.

Важно сверять отпечаток ключа по надежным источникам перед подписанием.

4. Шифрование сообщения

   `gpg -e -f <ключ получателя> <файл с сообщением>`

После выполнения этой команды появится файл `<файл с сообщением>.gpg`. Его нужно отправить получателю.

5. Дешифрование сообщения

   `gpg -d <файл с сообщением>`

Результаты

В результате выполнения работы я обменялся с преподавателем зашифрованными сообщениями и собрал подписи 10+ одногруппников:

```
ipmoiseenkov-osx:Desktop ipmoiseenkov$ gpg -d 1.txt.gpg
gpg: encrypted with rsa2048 key, ID F2CFEDA5722BB893, created 2022-02-22
      "ilya moiseenkov <moiseenkov_ilya@mail.ru>"
А вдруг, нет?

> Кто прочитал, тот преподаватель криптографии :)

ipmoiseenkov-osx:Desktop ipmoiseenkov$ gpg --list-sigs
/Users/ipmoiseenkov/.gnupg/pubring.kbx
------------------------------------
pub   rsa2048 2022-02-22 [SC] [expires: 2022-06-22]
      B11D1BAE5D365AACF6B968ECA26645706368E1D1
uid           [ultimate] ilya moiseenkov <moiseenkov_ilya@mail.ru>
sig 3        A26645706368E1D1 2022-02-22  ilya moiseenkov
<moiseenkov_ilya@mail.ru>
sig          0ACF2535A20736BD 2022-02-23  Mikhail Gorokhov (Gorkhov M.A. M8O-
308B-19) <magorokhoov@gmail.com>
sig          21B212C9A67F906D 2022-02-23  Anastasiia Nazarova (krypto_key)
<nastya-nazarova-2002@mail.ru>
sig          3442522258CE8D8D 2022-02-24  Angelina <lina.khrennikova@mail.ru>
sig          3C2A309FF20F7528 2022-02-24  Kruglova Maria <krumari01@mail.com>
sig          5A4698A9871B6CE4 2022-02-22  Pavel Mokhliakov
<pmokhliakov@gmail.com>
sig          8E5ABC302DFE7C5E 2022-02-23  Grigoriy Shubin (x)
<garigoriy.gear@gmail.com>
sig          901A4D54DA866A44 2022-02-23  Fedor Shavandrin
<fedshav@rambler.ru>
sig          9FE64CEE5AE4BAF0 2022-02-25  Ivanov Fedor (Key for cripta labs)
<kenola82007@gmail.com>
sig          B57C92DDB797671D 2022-02-23  Oleg Artamonov <eartqk@gmail.com>
sig          CBC55164A04B7F26 2022-03-11  Korotkevich Leonid
<kleonide1@gmail.com>
sig          D87624AA4FF6F826 2022-02-23  Lyubov Ivenkova
<lyubov.iven@mail.ru>
sig          DA5CCD4D3166D000 2022-02-22  Ruslan Gaptulhakov (We have a big
deal) <fynex@mail.ru>
sig          E616813CF1DA9DD1 2022-02-23  saminov (hello there)
<aminovstepan@gmail.com>
sub   rsa2048 2022-02-22 [E] [expires: 2022-06-22]
sig          A26645706368E1D1 2022-02-22  ilya moiseenkov
<moiseenkov_ilya@mail.ru>
```

Выводы

В ходе выполнения данной работы я познакомился с утилитой gpg, которая позволяет обмениваться зашифрованными сообщениями друг с другом. Освоить принцип работы с ней было несложно. Однако ее внутреннее устройство содержит довольно сложные, но интересные математические алгоритмы. Похожие алгоритмы лежат в основе электронной подписи!