**Отчет по лабораторной работе №1 по курсу «Криптография»**

Выполнил Лисин Роман Сергеевич, М8О-306Б-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***

В работе я пользовался утилитой gpg.

1. Создание ключа

gpg --gen-key

Затем требуется ввести свои имя, фамилию и почту.

1. Отправка ключа на подпись

gpg -a --export <ключ> > <имя файла>

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

1. Подпись ключа

gpg -–import <полученный файл с ключом>

gpg --sign-key <полученный ключ>

gpg -a --export <полученный ключ> > <файл с подписанным ключом>

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

Важно сверять отпечаток ключа по надежным источникам перед подписанием.

1. Шифрование сообщения

gpg -e -s -r <имя получателя> <файл с сообщением>

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

1. Дешифрование сообщения

gpg -d <файл с сообщением>

***Результаты***

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

roma@roma-Inspiron-5415:~$ echo "0JrQu9GO0Ycg0L/QvtC70YPRh9C40LsuDQoNCjExLjAyLjIwMjMgMTM6NTEsINCg0L7QvNCw

0L0g0JvQuNGB0LjQvSDQv9C40YjQtdGCOg0KPiDQoSDRg9Cy0LDQttC10L3QuNC10LwsINCb

0LjRgdC40L0g0KDQvtC80LDQvSwg0Jw40J4tMzA20JEtMjANCg==" | base64 --decode

Ключ получил.

11.02.2023 13:51, Роман Лисин пишет:

> С уважением, Лисин Роман, М8О-306Б-20

roma@roma-Inspiron-5415:~$ cat message.txt

Зашифровал секретное сообщение вашим ключом.

>Ключ получил.

11.02.2023 13:51, Роман Лисин пишет:

>> С уважением, Лисин Роман, М8О-306Б-20

roma@roma-Inspiron-5415:~$ gpg --list-sigs

/home/roma/.gnupg/pubring.kbx

-----------------------------

pub rsa3072 2023-02-11 [SC] [годен до: 2025-02-10]

A95DBF6A7A0765DABD1E9C363E8CED25ED4704D8

uid [ абсолютно ] Roman Lisin <roma.lisin123@mail.ru>

sig 3 3E8CED25ED4704D8 2023-02-11 Roman Lisin <roma.lisin123@mail.ru>

sig EEC99770CA1930DF 2023-02-11 Michael <frolov\_mika@mail.ru>

sig 72DE711729F7B4A9 2023-02-11 Артём Гаврилов <aagavrilov03@gmail.com>

sig CA73BDBA1AA006CE 2023-02-11 Ivan Maltsev <ivan.malz@yandex.ru>

sig 568235EF833FC126 2023-02-11 Aleksandr Semin <semin.alex222@yandex.ru>

sig 8A64D7880F9E0098 2023-02-12 Danila Gudynin (306) <ddgudynin@mai.education>

sig 72C6B9D0E76CE153 2023-02-12 Гапонов Никита <nikitychgaponov1990@gmail.com>

sig D47BE9256A42F227 2023-02-12 Alexey Fedorov <darcalexis@gmail.com>

sig 26FB6DE9CC432789 2023-02-12 Andrey Cherkashin <andrey@cherkashin.su>

sig 9AC8280183676A26 2023-02-12 Angelina Rechinskaya <operativnosty@gmail.com>

sig 064A5D1375B430FB 2023-02-12 Lunidep <ilya151102@yandex.ru>

sig 6E78FB2D26AEED39 2023-02-12 Rodions Safuanovs <rararadij@yandex.ru>

sig 19CA5DCDB9694228 2023-02-13 Vladimir Bakharev (М8О-307Б-20) <vdbakharev@mai.education>

sig 190DA7980C706ED6 2023-02-13 Sophie Mokeeva <mokeso@mail.ru>

sub rsa3072 2023-02-11 [E] [годен до: 2025-02-10]

sig 3E8CED25ED4704D8 2023-02-11 Roman Lisin <roma.lisin123@mail.ru>

***Выводы***

В ходе выполнения данной работы я познакомился с утилитой gpg, которая позволяет обмениваться зашифрованными сообщениями друг с другом. Данная утилита помогает легко работать с OpenPGP-ключами из терминала.