Московский Авиационный Институт
(Национальный Исследовательский Университет)

Факультет информационных технологий и прикладной математики
Кафедра вычислительной математики и программирования

Лабораторная работа №2 по курсу «Криптография»

Группа: М80 – 306Б-18
Студентка: Макаренкова В.М.
Преподаватель: Борисов А. В.
Оценка: _____
Дата: _____

Москва, 2021.

Задача:

1. Создать пару OpenPGP-ключей, указав в сертификате свою почту. Создать ее возможно, например, с помощью дополнения Enigmail к почтовому клиенту thunderbird, или из командной строки терминала ОС семейства linux.

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 и сам открытый ключ (как правило, они умещаются в одном файле).

2.2. Дождаться письма, в котором собеседник Вам пришлет сертификат своего открытого ключа.
2.4. Выслать сообщение, зашифрованное на 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

Создание ключа:

% gpg --full-generate-key

gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.

This is free software: you are free to change and redistribute it.

There is NO WARRANTY, to the extent permitted by law.

Выберите тип ключа:

(1) RSA и RSA (по умолчанию)

(2) DSA и Elgamal

(3) DSA (только для подписи)

(4) RSA (только для подписи)

(14) Имеющийся на карте ключ

Ваш выбор? 1

длина ключей RSA может быть от 1024 до 4096.

Какой размер ключа Вам необходим? (3072) 4096

Запрошенный размер ключа - 4096 бит

Выберите срок действия ключа.

0 = не ограничен

<n> = срок действия ключа - n дней

<n>w = срок действия ключа - n недель

<n>m = срок действия ключа - n месяцев

<n>y = срок действия ключа - n лет

Срок действия ключа? (0) 2y

Ключ действителен до среда, 12 апреля 2023 г. 13:51:44 MSK

Все верно? (y/N) y

GnuPG должен составить идентификатор пользователя для идентификации ключа.

Ваше полное имя: Vera Makarenkova

Адрес электронной почты: vmmak.post@gmail.com

Примечание:

Вы выбрали следующий идентификатор пользователя:

"Vera Makarenkova <vmmak.post@gmail.com>"

Сменить (N)Имя, (C)Примечание, (E)Адрес; (O)Принять/(Q)Выход? O

gpg: /Users/iamverk/.gnupg/trustdb.gpg: создана таблица доверия

gpg: ключ F8835CDCB707586F помечен как абсолютно доверенный

gpg: создан каталог '/Users/iamverk/.gnupg/openpgp-revocs.d'

gpg: сертификат отзыва записан в '/Users/iamverk/.gnupg/openpgp-revocs.d/1AD707A00ABDF2291A74D631F8835CDCB707586F.rev'.

открытый и секретный ключи созданы и подписаны.

pub rsa4096 2021-04-12 [SC] [годен до: 2023-04-12]

1AD707A00ABDF2291A74D631F8835CDCB707586F

uid Vera Makarenkova <vmmak.post@gmail.com>

sub rsa4096 2021-04-12 [E] [годен до: 2023-04-12]

Процедура подписания ключа друга:

% gpg --import katermin.gpg

gpg: ключ 55D520EB3CC73A32: импортирован открытый ключ "Катермин Всеволод Сергеевич (BlahBlahBruh) <katermin.vsevolod@yandex.ru>"

gpg: Всего обработано: 1

gpg: импортировано: 1

% gpg --import vera_signed.pgp

gpg: ключ F8835CDCB707586F: "Vera Makarenkova <vmmak.post@gmail.com>" 1 новая подпись

gpg: Всего обработано: 1

gpg: новых подписей: 1

gpg: marginals needed: 3 completes needed: 1 trust model: pgp

gpg: глубина: 0 достоверных: 1 подписанных: 0 доверие: 0-, 0q, 0n, 0m, 0f, 1u

gpg: срок следующей проверки таблицы доверия 2023-04-12

% gpg -u 1AD707A00ABDF2291A74D631F8835CDCB707586F --sign-key 1976C11B48A82905AD9E335F55D520EB3CC73A32

pub rsa4096/55D520EB3CC73A32

  создан: 2021-03-12 годен до: 2021-09-08 назначение: SC

 доверие: неизвестно достоверность: неизвестно

sub rsa4096/92C5F5DAD9E4148B

  создан: 2021-03-12 годен до: 2021-09-08 назначение: E

[неизвестно] (1). Катермин Всеволод Сергеевич (BlahBlahBruh) <katermin.vsevolod@yandex.ru>

pub rsa4096/55D520EB3CC73A32

  создан: 2021-03-12 годен до: 2021-09-08 назначение: SC

 доверие: неизвестно достоверность: неизвестно

Отпечаток первичного ключа: 1976 C11B 48A8 2905 AD9E 335F 55D5 20EB 3CC7 3A32

 Катермин Всеволод Сергеевич (BlahBlahBruh) <katermin.vsevolod@yandex.ru>

Срок действия данного ключа истекает 2021-09-08.

Вы уверены, что хотите подписать этот ключ

своим ключом "Vera Makarenkova <vmmak.post@gmail.com>" (F8835CDCB707586F)?

Действительно подписать? (y/N) y

Подписи на моём ключе:

% gpg --list-sign
gpg: проверка таблицы доверия
gpg: marginals needed: 3 completes needed: 1 trust model: pgp
gpg: глубина: 0 достоверных: 1 подписанных: 9 доверие: 0-, 0q, 0n, 0m, 0f, 1u
gpg: глубина: 1 достоверных: 9 подписанных: 22 доверие: 9-, 0q, 0n, 0m, 0f, 0u
gpg: срок следующей проверки таблицы доверия 2021-06-11
/Users/iamverk/.gnupg/pubring.kbx
---
pub rsa4096 2021-04-12 [SC] [годен до: 2023-04-12]
     1AD707A00ABDF2291A74D631F8835CDCB707586F
uid   [абсолютно] Vera Makarenkova <vmmak.post@gmail.com>
sig 3   F8835CDCB707586F 2021-04-12 Vera Makarenkova <vmmak.post@gmail.com>
sig   55D520EB3CC73A32 2021-04-17 Катермин Всеволод Сергеевич (BlahBlahBruh) <katermin.vsevolod@yandex.ru>
sig   C4E95DC7F65F315E 2021-04-17 Pavel (crypto lab) <pagamov@gmail.com>
sig   9AF10323BD7BCCD6 2021-04-18 Timofey (Dixi) <timofey.1234@mail.ru>
sig   C74C1CBB55C71F9C 2021-04-18 Kirill Vakhramyan (first try) <kirill.vlg3101@gmail.com>
sig   893BD40D95A6735F 2021-04-18 Vladislav Kosogorov <vladislav.kosogorov21@gmail.com>
sig   458E964598E5C7E7 2021-04-18 Magomed (snaksi) <magomed.kasimov.2000@mail.ru>
sig   F8645C48C4C9A6DC 2021-04-18 Ilya Semenov (crypto labs) <ilya.semenov89099@yandex.ru>
sig   374A7F04410D2D88 2021-04-18 Max T (first pair) <qwerty65k@mail.ru>
sig   60A0A1801FA258C7 2021-04-18 Ilya Chernenko <ilya.chernenko.2012@gmail.com>
sig   DA45A9AC78F0DB72 2021-04-18 Gennadii Khrenov <khrenov.gena@yandex.ru>
sig   CB674CF1E1A66281 2021-04-18 Andrew (erophei) <siniavskij.andrei@yandex.ru>
sub rsa4096 2021-04-12 [E] [годен до: 2023-04-12]
sig   F8835CDCB707586F 2021-04-12 Vera Makarenkova <vmmak.post@gmail.com>

Расшифровка сообщения преподавателя:

% gpg -d encr_.txt.pgp > decrypted.txt

gpg: зашифровано 4096-битным ключом RSA с идентификатором 527B717E71406743, созданным 2019-10-09

"awh <awh@cs.msu.ru>"

gpg: зашифровано 4096-битным ключом RSA с идентификатором 274CC1DFC185695D, созданным 2021-04-12

"Vera Makarenkova <vmmak.post@gmail.com>"

gpg: Подпись сделана суббота, 24 апреля 2021 г. 10:13:21 MSK

gpg: ключом RSA с идентификатором E56F1BEAB34472C1D78ED9B43D98E96CA4E0E964

gpg: Действительная подпись пользователя "awh <awh@cs.msu.ru>" [неопределено]

gpg: Внимание: Данный ключ не заверен доверенной подписью!

gpg: Нет указаний на то, что подпись принадлежит владельцу.

Отпечаток первичного ключа: 2470 C0C5 5CF2 4383 5518 4B35 A677 0182 9D9C 5DE4

Отпечаток подключа: E56F 1BEA B344 72C1 D78E D9B4 3D98 E96C A4E0 E964

Шифрование сообщения для преподавателя:

% gpg -r 2470C0C55CF2438355184B35A67701829D9C5DE4 -e filik.rtf > fil_encrypted.gpg

gpg: 527B717E71406743: Нет свидетельств того, что данный ключ принадлежит названному пользователю

sub rsa4096/527B717E71406743 2019-10-09 awh <awh@cs.msu.ru>

Отпечаток первичного ключа: 2470 C0C5 5CF2 4383 5518 4B35 A677 0182 9D9C 5DE4

Отпечаток подключа: 6BBB BE76 0528 F7AC B843 9537 527B 717E 7140 6743

НЕТ уверенности в том, что ключ принадлежит человеку, указанному

в идентификаторе пользователя. Если Вы ТОЧНО знаете, что делаете,

можете ответить на следующий вопрос утвердительно.

Все равно использовать данный ключ? (y/N) y

Выводы

Выполнив вторую лабораторную работу по курсу «Криптография», я познакомилась с утилитой gpg, научилась подписывать ключи других пользователей, шифровать и расшифровывать сообщения.