Московский авиационный институт
(национальный исследовательский университет)

Факультет информационных технологий и прикладной математики

Кафедра вычислительной математики и программирования

# Лабораторная работа №2 по курсу «Криптография»

Студент: А. П. Шорохов
Преподаватель: А. В. Борисов
Группа: М8О-306Б-18
Дата:
Оценка:
Подпись:

Москва, 2021

# Лабораторная работа №2

**Задача:** 1. Создать пару OpenPGP-ключей, указав в сертификате свою почту. Создать её 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.

# 1 Характеристики машины

Lenovo ideapad 700-15ISK
Процессор - Intel Core i7-6700HQ @ 2.6GHz
Оперативная память - 12 Gb
ОС - Windows 10. Все программы были запущены через подсистему Unix в стандартной консоли Windows.

# 2 Описание

Я начал выполнение данной лабораторной работы с изучения работы с pgp. Это оказалось несложным, но очень интересным занятием. После этого я начал собирать подписи своих однокурсников, а так же подписывать их ключи. Ниже покажу процесс подписи:

```
dobriy_alien@LAPTOP-2MM4OK81:/mnt/c/Users/shoro/Downloads$ gpg --import Masha.gpg
gpg: key 8B872365949C66CD: public key "Мария (Алексеева) <alek.maria@yandex.ru>"
imported
gpg: key D349D377B506549D: public key "Masha Alekseeva <alek.maria@yandex.ru>"
imported
gpg: Total number processed: 2
gpg:               imported: 2
dobriy_alien@LAPTOP-2MM4OK81:/mnt/c/Users/shoro/Downloads$ gpg --list-keys
/home/dobriy_alien/.gnupg/pubring.kbx
-------------------------------------
pub   rsa4096 2021-03-16 [SC] [expires: 2031-03-14]
577E3DB1884C37890EDCDB14A50178291B0B48E1
uid           [ultimate] Alexey Shorokhov ($ETH to the moon) <shoroxoff.al@yandex.ru>
sub   rsa4096 2021-03-16 [E] [expires: 2031-03-14]

pub   rsa4096 2021-03-16 [SC] [expires: 2021-09-12]
68B117AEB40C90576C6E0C95C74C1CBB55C71F9C
uid           [  full  ] Kirill Vakhramyan (first try) <kirill.vlg3101@gmail.com>
sub   rsa4096 2021-03-16 [E] [expires: 2021-09-12]

pub   rsa4096 2021-03-14 [SC] [expires: 2024-03-13]
4430FE40F6F4C0C0D6792D69893BD40D95A6735F
uid           [  undef ] Vladislav Kosogorov <vladislav.kosogorov21@gmail.com>
sub   rsa4096 2021-03-14 [E] [expires: 2024-03-13]

pub   rsa4096 2021-03-13 [SC] [expires: 2021-06-11]
2FEC32E585DD54F29B3BF07B6F1E06DE37808B5A
uid           [  full  ] Egor Zhivalev <egorzhivalev@gmail.com>
sub   rsa4096 2021-03-13 [E] [expires: 2021-06-11]

pub   rsa2048 2021-03-10 [SC]
079A3637C573B488E7C3DD9A3D85280D4ED28F41
uid           [  full  ] Dmitriy Artemiev <dmitriiartemev@yandex.ru>
sub   rsa2048 2021-03-10 [E]
```

```
pub   rsa4096 2021-03-13 [SC]
38002364E22F05A6337F6E2A458E964598E5C7E7
uid           [  full  ] Magomed (snaksi) <magomed.kasimov.2000@mail.ru>
sub   rsa4096 2021-03-13 [E]

pub   rsa4096 2021-03-14 [SC]
988B5C1E8E1A0564FA088E59A7061186C229C5EC
uid           [  full  ] Alexander Markov <markov.lifeacc@gmail.com>
sub   rsa4096 2021-03-14 [E]

pub   rsa4096 2021-03-12 [SC]
B0E4B87652960790AC344128CB674CF1E1A66281
uid           [  undef ] Andrew (erophei) <siniavskij.andrei@yandex.ru>
sub   rsa4096 2021-03-12 [E]

pub   rsa4096 2021-03-16 [SC] [expires: 2021-03-30]
25FBEE9A0D9981D1A151AB33AF60E0BC72EF4131
uid           [  full  ] Vladislav (stul) <nikolaev.1407@yandex.ru>
sub   rsa4096 2021-03-16 [E] [expires: 2021-03-30]

pub   rsa4096 2021-03-14 [SC] [expires: 2024-03-13]
A5E2FE7A3BA473DF0EAFA868A841ED4FD71C3BBF
uid           [  full  ] Sergei Simonov (123) <wqsadfak@yandex.ru>
sub   rsa4096 2021-03-14 [E] [expires: 2024-03-13]

pub   rsa4096 2021-03-13 [SC]
722CC4345CE7E025398C2591711FA949D66AD665
uid           [  full  ] Александр (Zaycev806) <aksyonow2015@yandex.ru>
sub   rsa4096 2021-03-13 [E]

pub   rsa4096 2021-03-12 [SC] [expires: 2021-09-08]
1976C11B48A82905AD9E335F55D520EB3CC73A32
uid           [ unknown] Катермин Всеволод Сергеевич (BlahBlahBruh) <katermin.vsevolo
sub   rsa4096 2021-03-12 [E] [expires: 2021-09-08]

pub   rsa4096 2019-10-09 [SCA] [expires: 2024-10-07]
2470C0C55CF2438355184B35A67701829D9C5DE4
uid           [ unknown] awh <awh@cs.msu.ru>
sub   rsa4096 2019-10-09 [E] [expires: 2024-10-07]
sub   rsa4096 2020-03-06 [S] [expires: 2029-03-04]
```

```
pub   rsa4096 2021-03-14 [SC]
60DCCF116C7941C7D4367E49A3B0C96698F937D3
uid           [  full  ] Andrew Dubov (DragonKeker) <eldbv80@gmail.com>
sub   rsa4096 2021-03-14 [E]

pub   rsa4096 2021-03-17 [SCA] [expires: 2023-03-17]
E85E484C0518AD70AA69AFA92AD5D75943E8C8BE
uid           [  full  ] Sergey Kudinov <enstein225@gmail.com>
sub   rsa4096 2021-03-17 [E] [expires: 2023-03-17]

pub   rsa3072 2021-03-02 [SC] [expires: 2023-03-02]
F8E33F918926C243FD0DEB9760A0A1801FA258C7
uid           [  undef ] Ilya Chernenko <ilya.chernenko.2012@gmail.com>
sub   rsa3072 2021-03-02 [E] [expires: 2023-03-02]

pub   rsa4096 2021-03-15 [SC]
93897E8370D076EB0008A644A0E962D87E41D1DE
uid           [  undef ] Nikita (kek kripta) <trol53.nek@gmail.com>
sub   rsa4096 2021-03-15 [E]

pub   rsa4096 2021-03-15 [SC]
70AF6901165A6510F3FCA7BFDA09107605A08098
uid           [  undef ] Lidia Patrikeeva <lida.patrikeyeva@inbox.ru>
sub   rsa4096 2021-03-15 [E] [expires: 2021-04-14]

pub   rsa3072 2021-03-15 [SC] [expires: 2023-03-15]
AEA2228AF8FC74F88147A4C1F926448F3E286B1D
uid           [  undef ] Sergey Kudinov <redpixelforce@gmail.com>
sub   rsa3072 2021-03-15 [E] [expires: 2023-03-15]

pub   rsa4096 2021-03-14 [SC]
E0471A8CB8906289AF7597C18B872365949C66CD
uid           [ unknown] Мария (Алексеева) <alek.maria@yandex.ru>
sub   rsa4096 2021-03-14 [E]

pub   rsa4096 2021-03-14 [SC]
67EEA90655FCED5C30C5556CD349D377B506549D
uid           [ unknown] Masha Alekseeva <alek.maria@yandex.ru>
sub   rsa4096 2021-03-14 [E]
```

```
dobriy_alien@LAPTOP-2MM4OK81:/mnt/c/Users/shoro/Downloads$ gpg -u 577E3DB1884C37890ED
--sign-key 67EEA90655FCED5C30C5556CD349D377B506549D

pub  rsa4096/D349D377B506549D
created: 2021-03-14  expires: never       usage: SC
trust: unknown       validity: unknown
sub  rsa4096/877A91C98D9630D5
created: 2021-03-14  expires: never       usage: E
[ unknown] (1). Masha Alekseeva <alek.maria@yandex.ru>


pub  rsa4096/D349D377B506549D
created: 2021-03-14  expires: never       usage: SC
trust: unknown       validity: unknown
Primary key fingerprint: 67EE A906 55FC ED5C 30C5  556C D349 D377 B506 549D

Masha Alekseeva <alek.maria@yandex.ru>

Are you sure that you want to sign this key with your
key "Alexey Shorokhov ($ETH to the moon) <shoroxoff.al@yandex.ru>" (A50178291B0B48E1)

Really sign? (y/N) y

dobriy_alien@LAPTOP-2MM4OK81:/mnt/c/Users/shoro/Downloads$ gpg --export 577E3DB1884C37
>alien.gpg
dobriy_alien@LAPTOP-2MM4OK81:/mnt/c/Users/shoro/Downloads$ gpg --export E85E484C0518AD
>masha_signed.gpg
dobriy_alien@LAPTOP-2MM4OK81:/mnt/c/Users/shoro/Downloads$
```

Таким образом, я подписал 14 ключей однокурсников и получил от них 12 подписей.
Вот список людей, подписавших мой ключ:

```
dobriy_alien@LAPTOP-2MM4OK81:/mnt/c/Users/shoro/Downloads$ gpg --list-sign
577E3DB1884C37890EDCDB14A50178291B0B48E1
pub   rsa4096 2021-03-16 [SC] [expires: 2031-03-14]
577E3DB1884C37890EDCDB14A50178291B0B48E1
uid           [ultimate] Alexey Shorokhov ($ETH to the moon) <shoroxoff.al@yandex.ru>
sig 3        A50178291B0B48E1 2021-03-16  Alexey Shorokhov ($ETH to the moon)
<shoroxoff.al@yandex.ru>
sig          893BD40D95A6735F 2021-03-16  Vladislav Kosogorov <vladislav.kosogorov21@g
sig          6F1E06DE37808B5A 2021-03-16  Egor Zhivalev <egorzhivalev@gmail.com>
sig          3D85280D4ED28F41 2021-03-16  Dmitriy Artemiev <dmitriiartemev@yandex.ru>
```

```
sig          C74C1CBB55C71F9C 2021-03-16  Kirill Vakhramyan (first try) <kirill.vlg31
sig          458E964598E5C7E7 2021-03-16  Magomed (snaksi) <magomed.kasimov.2000@mail
sig          CB674CF1E1A66281 2021-03-16  Andrew (erophei) <siniavskij.andrei@yandex.
sig          AF60E0BC72EF4131 2021-03-16  Vladislav (stul) <nikolaev.1407@yandex.ru>
sig          A841ED4FD71C3BBF 2021-03-16  Sergei Simonov (123) <wqsadfak@yandex.ru>
sig          A7061186C229C5EC 2021-03-16  Alexander Markov <markov.lifeacc@gmail.com>
sig          55D520EB3CC73A32 2021-03-16  Катермин Всеволод Сергеевич (BlahBlahBruh)
<katermin.vsevolod@yandex.ru>
sig          711FA949D66AD665 2021-03-16  Александр (Zaycev806) <aksyonow2015@yandex.
sig          2AD5D75943E8C8BE 2021-03-17  Sergey Kudinov <enstein225@gmail.com>
sub   rsa4096 2021-03-16 [E] [expires: 2031-03-14]
sig          A50178291B0B48E1 2021-03-16  Alexey Shorokhov ($ETH to the moon)
<shoroxoff.al@yandex.ru>

dobriy_alien@LAPTOP-2MM4OK81:/mnt/c/Users/shoro/Downloads$
```

Затем я написал Августу Валерьевичу Борисову и в письме приложил свой публичный ключ. В ответ получил публичный ключ Августа Валерьевича. Я создал файлик file.txt, содержащий 1 строку "$ETH is the best cryptocurrency!"После этого я зашифровал его, используя ключ Августа Валерьевича. После небольших проблем и поисков итогового файла, был найден и отправлен file.txt.gpg. Вместе с одноргуппником Владом Косогоровым мы успешно проделали такую же операцию. Август Валерьевич тоже подтвердил, что этот файл правильный, и его получается расшифровать.

# 3 Выводы

Мне очень понравилась эта лабораторная, ибо она включает в себя не только работу с ключами и подписями, но еще и учит уговаривать других людей(в данном случе одногруппников) делать то, что им лень в данный момент времени.
Я поглубже познакомился с ключами и подписями, что поможет мне в будущем с работой в нише криптовалют.