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. В. Тимофеев
Преподаватель: А. В. Борисов
Группа: М8О-307Б-19

Дата:
Оценка:
Подпись:

Москва, 2022

Лабораторная работа №1

Задача:

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.

1 Описание

GNU Privacy Guard (GnuPG, GPG) — свободная программа для шифрования информации и создания электронных цифровых подписей. Разработана как альтернатива PGP и выпущена под свободной лицензией GNU General Public License. GnuPG полностью совместима со стандартом IETF OpenPGP.

Задачей данной лабораторной работы было научиться пользоваться утилитой GPG, а именно освоить создание ключей, установление контактов с другими обладателями ключей, и научиться шифровать сообщения.
Основной сложностью работы было собрать 10 подписей одногруппников, потому что не все быстро реагируют на просьбу подписать сертификат и данный процесс растягивается на несколько дней. Также я попробовал передать зашифрованное сообщение одногруппнику, и успешно получил от него ответ.

2 Сертификаты

```
pub   rsa4096 2022-02-24 [SC] [expires: 2022-08-23]
E9DACAFF174105ECA3F5EC7C56E01C61306BEDA9
uid           [ultimate] Alexey Timofeev (My Key1) <TImofeevAV8f@yandex.ru>
sub   rsa4096 2022-02-24 [E] [expires: 2022-08-23]

pub   rsa4096 2022-02-24 [SC]
4CE7AC5FBD61B36CF2941C5C471CE59C58D00E3A
uid           [  full  ] Voronov Kirill (lab) <albert19411380@gmail.com>
sub   rsa4096 2022-02-24 [E]

pub   rsa3072 2022-02-17 [SC] [expires: 2023-02-17]
CAE1E5990ECBFF7CF8E822191CDCD2FA39B2D588
uid           [  full  ] Dmitry Lyashun <gabn37@gmail.com>
sub   rsa3072 2022-02-17 [E] [expires: 2023-02-17]

pub   rsa4096 2022-02-23 [SC] [expires: 2022-08-22]
D1FA862AB7377B2672C71D1CE954605C1ACB2B6C
uid           [  full  ] Kirill Spiridonov <vo-ro@list.ru>
sub   rsa4096 2022-02-23 [E] [expires: 2022-08-22]

pub   rsa3072 2022-02-25 [SC] [expires: 2024-02-25]
AEA04FC2FDB3EE67FE65AF2C8A0E389A87D49C3D
uid           [  full  ] Nikita <nikita.ejov2012@yandex.ru>
sub   rsa3072 2022-02-25 [E] [expires: 2024-02-25]

pub   rsa2048 2022-02-26 [SC] [expires: 2022-06-26]
8DE1E85F24AEFB7954B55299709A7CABFBA64B69
uid           [  full  ] Tarpanov Daniil <tarpanov01@mail.ru>
sub   rsa2048 2022-02-26 [E] [expires: 2022-06-26]

pub   brainpoolP512r1 2022-02-18 [SC] [expires: 2024-02-18]
369BF3AC556D76DC6DAA9DBB8C4018F09C2FACB3
uid           [  full  ] Igor Glushatov <igor_743646@mail.ru>
sub   brainpoolP512r1 2022-02-18 [E] [expires: 2024-02-18]

pub   rsa4096 2022-02-24 [SC]
0251AC644CC30D2C56CA2AF08252C632C63FBB8B
uid           [  full  ] mainyutin (My RSA key) <mainyutin@gmail.com>
```

```
sub   rsa4096 2022-02-24 [E]

pub   rsa4096 2022-02-22 [SC] [expires: 2023-02-22]
1929D81BD415751548947D4AE0956D04C071BC06
uid           [  full  ] Anton Fedorov (Lab1) <feorov2001@mail.ru>
sub   rsa4096 2022-02-22 [E] [expires: 2023-02-22]

pub   dsa3072 2014-10-29 [SCA] [expired: 2019-10-28]
B573D66D13D8378C4AE156EC18D6F57D532BE542
uid           [ expired] awh <awh@cs.msu.ru>

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   rsa2048 2022-02-24 [SC] [expires: 2022-08-23]
C22CBFE89BBBE18CEFD0C01BB80ED63B140D6E14
uid           [  full  ] Viktor Biryukov <vikvladbir@mail.ru>
sub   rsa2048 2022-02-24 [E] [expires: 2022-08-23]

pub   rsa4096 2022-02-15 [SC] [expires: 2026-02-15]
68BB10DE3E850AB3A4CB143211E5153A290D0EE6
uid           [  full  ] KeyLab1 <bvp.budnikova@gmail.com>
sub   rsa4096 2022-02-15 [E] [expires: 2026-02-15]

pub   rsa2048 2022-03-01 [SC] [expires: 2022-07-29]
889D0A3A9E902538EE2B6113A8C5ED9E05123E58
uid           [  full  ] Vitaliy Yurevich (yuviyu) <vi.yurevich@gmail.com>
sub   rsa2048 2022-03-01 [E] [expires: 2022-07-29]

pub   rsa2048 2022-02-23 [SC] [expires: 2022-08-22]
8D266DB265C7469792872F141B1C62A814884A7B
uid           [  full  ] AFavstova (hello) <sa2040@mail.ru>
sub   rsa2048 2022-02-23 [E] [expires: 2022-08-22]

pub   rsa2048 2022-03-08 [SC] [expires: 2023-03-08]
6ECE4AA957331F534E43C7FFA9749985B2C114D7
uid           [  full  ] Kirill Kalugin <netter2@rambler.ru>
sub   rsa2048 2022-03-08 [E] [expires: 2023-03-08]
```

```
pub   rsa4096 2022-02-27 [SC] [expires: 2026-02-26]
1323D2DA777A9097D79E13CF8EE5B3203149A7AA
uid           [  full  ] Aleksandr <astrumgazer@gmail.com>
sub   rsa4096 2022-02-27 [E] [expires: 2026-02-26]

pub   rsa2048 2022-03-14 [SC] [expires: 2022-07-12]
235C77BA4B88F992B2FE93982ABCECE3345378E1
uid           [  full  ] Masha Yakushkina (lab1) <s19b3_yakushkina@179.ru>
sub   rsa2048 2022-03-14 [E] [expires: 2022-07-12]
```

3 Сообщения

```
dude@DESKTOP-545VSUH:/mnt/d/education/education/Cripta$ cat message.txt

Lorem ipsum dolor sit amet,consectetur adipiscing elit,sed do eiusmod tempor
incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam,quis nostrud
exercitation ullamco laboris nisi
ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit
in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint
occaecat cupidatat non proident,sunt in culpa qui officia deserunt mollit anim
id est laborum.

dude@DESKTOP-545VSUH:/mnt/d/education/education/Cripta$ cat message.txt.asc

-----BEGIN PGP MESSAGE-----


hQIMAzrdNYKOVHRjAQ//WuFdtqyRxEsAjmn7fGTPOSRe+WDgvZSLchE9y7WXPhf/
jFiV/lGkYx0/cxHCBkJoMdknhObB+3FoGIMd7hSKzMGlDP7Wch5PQXnDXglck1+7
T2iNOB7xbrDhnyO/aqjQza5oOwxLT3gEcGPoMtMbdssxNG+UQx/NgygOzrYRNSWo
helRaS+XY/emOF1DZTp46wM4o2dyzPMkZpNr+tYzguqIcGxWhxtCvvqqxAQ6fSYT
dEpDidALF73RDxVjlOS0DZoD2ohbKd2KJJ/8aaj/QvpLXNQI9vDDyxLN6gPMfErB
pa8KZ2pVXnqjj4+aZOoOevft6jJFkuo5mW6qdPR+wWl3VlsD2x3d1z4dYMFuZV4s
Dh+gM6daadOzeM+XW70yqb7LLlqO2XozsfFBkVALZMMECfbPDEc8v7n+cP0yC/c9
J0FBYSiyfSszMq75gz00MbOBiWACy4C5lQ9APitNJMQtGbtmmXE21ndTpzM7ycuK
B92MmzUV01Yrfkon0YZezpktBA6QGYNbgAemkavkEZQR7TDLOl/1pRPl2ruvPvAn
WDwlZbQjPa7s/porPI9zFTCDSIbVE4Wv73X07vMKbDUSgqsLxVaDnV8H95YSkaIH
G4MZNrgqwcpYAkJ1dyBdFD92MDZf0ErzKtPS3WX0ml2geyLmSEZw9Um7K5vLxv/S
VgEMTioxnaKeuA2Y55ZQ5cfG8NH2Fr7AtI99/TQNzWYVSvvpqPRoRkEcfsVKahp3
bDMkwXWlelfhKKR5Hxs6GNInXMn+SMsks0JA3eJPfTp7ybtz6h6i
=OjTS

-----END PGP MESSAGE-----

dude@DESKTOP-545VSUH:/mnt/d/education/education/Cripta$ cat 1.txt

Ух,какой текст.


>Lorem ipsum dolor sit amet,consectetur adipiscing elit,sed do eiusmod tempor
incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam,quis nostrud
```

```
exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis
aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu
fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident,sunt
in culpa qui officia deserunt mollit anim id est laborum.

dude@DESKTOP-545VSUH:/mnt/d/education/education/Cripta$ cat 1.txt.gpg


:5Ttc_gc!<&N|"BY
/>~elW>uS5j7SX      v]'cHSX{N"s‘*uQY  vMg@cN@S(XK*aUČw}7y

DA7az(eqt@

qNHLmwUG%=8  ~#s6u?u/cCeL|u=<*P%<38cL<!g+RGJa-VbV<_W%M|tOIn/{        ‘;vc;G;W<6

!+K qBc2n):Bq3++hgRu?)vO7l

Vvp~Q̂4i]3<%P;

*$D‘JK<‘[lgXO>=h#{iG"%A       _C}7!ITjV_<|p        Gz-k5}wKb


$HYzyn0:&TF>‘cyFMPD sVNsXWGhvL)hh/YGK>N1‘Zarv;S9fC3U‘-:lTj;?n;_L2Lj!VJ;@P{c)9|Evf0(jXn

#1hŜdude@DESKTOP-545VSUH:/mnt/d/education/education/Cripta$
```

4 Выводы

Выполнив первую лабораторную работу по курсу «Криптография», я познакомился с утилитой GPG, а также понял основы ведения деловой переписки с использованием электронных цифровых подписей. За несколько дней я собрал 10 подписей, но помогая одногруппникам делать лабораторную работу мне удалось перевыполнить норму и собрать около 14 подписей.