Московский авиационный институт
(национальный исследовательский университет)

Институт №8 «Информационные технологии и прикладная математика»
Кафедра 806 «Вычислительная математика и программирование»
Дисциплина «Криптография»

Лабораторная работа №2

Тема: Знакомство с PGP

Студент: Глушатов И.С.
Группа: М8О-307Б-19
Преподаватель: Борисов А. В.
Дата:
Оценка:

Москва, 2022

Цель работы: приобретение практических навыков работы с утилитой PGP, шифрования и дешифрования сообщений, проставления электронных подписей.

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:
    1) Прислать собеседнику от своего имени по электронной почте сообщение, во вложении которого поместить свой сертификат открытого ключа.
    2) Дождаться письма, в котором собеседник Вам пришлет сертификат своего открытого ключа.
    3) Выслать сообщение, зашифрованное на открытом ключе собеседника.
    4) Дождаться ответного письма.
    5) Расшифровать ответное письмо своим закрытым ключом.

3. Собрать подписи под своим сертификатом открытого ключа.
    1) Получить сертификат открытого ключа одногруппника.
    2) Убедиться в том, что подписываемый Вами сертификат ключа принадлежит его владельцу - путём сравнения отпечатка ключа или ключа целиком, по доверенным каналам связи.
    3) Подписать сертификат открытого ключа одногруппника.
    4) Передать подписанный Вами сертификат полученный в п.3.2 его владельцу, т. е. одногруппнику.
    5) Повторив п.3.0.-3.3., собрать 10 подписей одногруппников под своим сертификатом.
    6) Прислать преподавателю свой сертификат открытого ключа, с 10-ю или более подписями одногруппников.

4. Подписать сертификат открытого ключа преподавателя и выслать ему.

Листинг

Собранные ключи:

```
C:\Users\Igor>gpg --list-keys
C:\Users\Igor\AppData\Roaming\gnupg\pubring.kbx
------------------------------------------------
pub   brainpoolP512r1 2022-02-18 [SC] [   годен до: 2024-02-18]
      369BF3AC556D76DC6DAA9DBB8C4018F09C2FACB3
uid         [  абсолютно ] Igor Glushatov <igor_743646@mail.ru>
sub   brainpoolP512r1 2022-02-18 [E] [   годен до: 2024-02-18]

pub   rsa3072 2022-02-20 [SC] [   годен до: 2024-02-20]
      3211AE2BD6CCC39572BA33B3922AB26384CDF3D4
uid         [   полное   ] Simon Krassotkin <semen.krassotkin@gmail.com>
sub   rsa3072 2022-02-20 [E] [   годен до: 2024-02-20]

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

pub   rsa3072 2022-02-17 [SC] [   годен до: 2024-02-17]
      8609F1F86DA075F228BD675F01CFA29169E435A7
uid         [   полное   ] Игорь <igor_743646@mail.ru>
sub   rsa3072 2022-02-17 [E] [   годен до: 2024-02-17]

pub   rsa2048 2022-02-15 [SC]
      572D8D13692F3D74EDA0C9ED96B84DE048A15CFA
uid         [   полное   ] Matvey <whitewolf.mot185@gmail.com>
sub   rsa2048 2022-02-15 [E]

pub   rsa3072 2022-02-21 [SC] [   годен до: 2024-02-21]
      A32CB4789DCF616315D6DD9B5EC776B79907F6A0
uid         [   полное   ] dukend-Egor (kek) <workdukend@gmail.com>
sub   rsa3072 2022-02-21 [E] [   годен до: 2024-02-21]

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

pub   rsa2048 2022-02-21 [SC] [   годен до: 2023-02-21]
      9D1E31A6B85ABCC3471D115CE2603F2F4EB312B9
uid         [   полное   ] Ilya Sinitsyn (Hello World!) <iluha.uchiha@mail.ru>
sub   rsa2048 2022-02-21 [E] [   годен до: 2023-02-21]

pub   rsa4096 2022-02-24 [SC]
      4CE7AC5FBD61B36CF2941C5C471CE59C58D00E3A
```

```
uid        [   полное   ] Voronov Kirill (lab) <albert19411380@gmail.com>
sub   rsa4096 2022-02-24 [E]

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

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

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

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

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

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

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

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

Выводы

В ходе работы я научился создавать пару открытого и секретного ключей с помощью утилиты PGP, подписывать сертификаты, а так же смог зашифровать и расшифровать сообщения.