Лабораторная работа № 2 по курсу: криптография

Выполнил студент группы М8О-308Б-17 МАИ *Милько Павел.*

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.

   2.3. Выслать сообщение, зашифрованное на ключе собеседника.

   2.4. Дождаться ответного письма.

   2.5. Расшифровать ответное письмо своим закрытым ключом.

3. Собрать подписи под своим сертификатом открытого ключа.

   3.1. Получить сертификат открытого ключа одногруппника.

   3.2. Убедиться в том, что подписываемый Вами сертификат ключа принадлежит его владельцу — путём сравнения отпечатка ключа или ключа целиком, по доверенным каналам связи.

   3.3. Подписать сертификат открытого ключа одногруппника.

   3.4. Передать подписанный Вами сертификат полученный в п.3.2 его владельцу, т.е.одногруппнику.

   3.5. Повторив п.3.0.-3.3., собрать 10 подписей одногруппников под своим сертификатом.

   3.6. Прислать преподавателю свой сертификат открытого ключа, с 10-ю или более подписями одногруппников.

4. Подписать сертификат открытого ключа преподавателя и выслать ему.

Часть 1: генерация ключа

gpg −−generate−key

```
gpg (GnuPG) 2.2.19; Copyright (C) 2019 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.

Note: Use "gpg −−full−generate−key" for a full featured key generation dialog.

GnuPG needs to construct a user ID to identify your key.

Real name: Милько Павел Алексеевич
Email address: p.milko1999@yandex.ru
You are using the 'iso−8859−1' character set.
You selected this USER−ID:
    "Милько Павел Алексеевич <p.milko1999@yandex.ru>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit? O
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: key 4DF7496E16FD3CBC marked as ultimately trusted
gpg: revocation certificate stored as '/home/lol/.gnupg/openpgp−revocs.d/703
    FD5D038947C5B57CCE5A64DF7496E16FD3CBC.rev'
public and secret key created and signed.

pub   rsa2048 2020−03−10 [SC] [expires: 2022−03−10]
      703FD5D038947C5B57CCE5A64DF7496E16FD3CBC
uid                      Милько Павел Алексеевич <p.milko1999@yandex.ru>
sub   rsa2048 2020−03−10 [E] [expires: 2022−03−10]
```

Экспорт сертификата ключа в файл:

gpg −−armor −−export −−output key.asc p.milko1999@yandex.ru

key.asc

−−−−−BEGIN PGP PUBLIC KEY BLOCK−−−−−

mQENBF5nkU8BCAC9zdYG0TMymaXlgTGcJ9kOANYFiZMNSmgJnKvDWukaH0XM+Jhz
xpxqYMBjLMLDNYLJQKCEd9Oyw9orxjFFKwYmUhScF2PPJ1ii6PsMV8WSdp243mSn
TK1kP/z2oIJ4/EVqiUkIDIaeGakAElSV6BvhQjN15ZaCkcXSf4bTbbvT83aLzUd0
hPKvpznA9mJ418xwy6dH9Brjx9OQywIiyDFDL10moU6rfOAkRni5RettxYZJ57cw
OipIAyKV1dQB1CEot3zZ1vpEqFoJ3C5vx4xleA3GWI0DqsZFIw/XRJ1Sj+M6alOA
dH6G17J1RGggC3NInwz2S2h8RIaMR9UGIp0/ABEBAAG0RNCc0LjQu9GM0LrQviDQ
n9Cw0LLQtdC7INCQ0LvQtdC60YHQtdC10LLQuNGHIDxwLm1pbGtvMTk5OUB5YW5k
ZXgucnU+iQFUBBMBCAA+FiEEcD/V0DiUfFtXzOWmTfdJbhb9PLwFAl5nkU8CGwMF
CQPCZwAFCwkIBwIGFQoJCAsCBBYCAwECHgECF4AACgkQTfdJbhb9PLyhyQf/RQvD
cf6r6t6nkaHrdWr2vM4V2AQRol2g3QTJcL7DZyb1jVrHINdIUw2mMoGAZemWPmpg
f9QpQ0vmg42q5Mi4z47On74b7LZgt5M7p64aZKhR97hcuB4r+8CQoV40nA5hD1j5
86gg9uk+B7Hvs7E2sFYEwLNfFhBwhUAXDYyJa8wuUYH+BGRnGg8GQ1Bj61JbqlP1
1ujsCZx9sgfLk+jD3OcSOenA8DI6bTFO6fv4SV+DeUAYIoHnTuyltAiNoWMouWYU

j2DHMn0WeN9qNi2R+wi0/phmztYNGoaRUNccoiiONvAaD3ZPnQR6+xcbJs7/FFMC
2n/OdGMRUJpHEWYZfrkBDQReZ5FPAQgA0syxTUzJ63N3VwQeNs3SrM9k1LTRP2kF
hLS3q44gHMgS5C6pi4ILjzpjx0Lu1NDLXOcfzxTt2mdbxrKTLrYo+1BCLZNhOci0
JZfaXRpOSDKTLIgfqTe5Z9/5BvysIxJGuVWi1xZHS4AB7g3fL2vIDkNm2f1uCTUc
DyBwrTqAR+yMPIKwErn7WJpulWYHl97C8EG6g8RdIBgF9PwwkZP853e/T4jecxJ2
nVbO4FqMpg10f+EUsRL1BbRyc4OxUbZaVdQF8yQDkgIwB1HYjtPh+66snC5D0GLQ
s3GEXi/Fx3RTFpPTQPr3EsXCI1ZK1DkDmw0v2jAkmy4hy4qx07TziwARAQABiQE8
BBgBCAAmFiEEcD/V0DiUfFtXzOWmTfdJbhb9PLwFAl5nkU8CGwwFCQPCZwAACgkQ
TfdJbhb9PLyvRgf/QRnkiAatZHKxhSFsqrkFFgpuK44L2blU6wJdr+R6wxBGRz3P
R+dyk3vpHpFJ/p97Hy9fTQUuzTW4EJ39m+6DljT75/SmJzA7tFVHHHUuc+RXc7O4
AJaa2FXXAxJiEIzbf3fzLvEi8NKgYg6mhSBEgyc+r0s8lSihDewvrMM02+TsAeDk
fI8P3oumlBAnhALnZpkXNV1/0+dzAO7h8hPmGdfGfRiKEjz9B9PDQGnNB0Zlg0Wt
GSSbuOtDo8fbdCG2bJzmQIT1Ksd3V6KC9bU99YjpTUY3vw0ajXZo/PmHT3q6v2J9
GG04BMCAio09TBPJ0nzsJnKHxb+VxyuGELkwTw==
=Tr5Q
-----END PGP PUBLIC KEY BLOCK-----

Часть 2: расшифровка полученного сообщения с помощью ключа преподавателя

Зашифрованный файл:

t3/encrypted.asc

-----BEGIN PGP MESSAGE-----
Version: GnuPG v2

hQEMA1j+AFwiJ3GGAQgAmmwV1CRm3AzQGkaXGWmFGbDsZ07Ad0JeU1CZs3s7+cmj
CknhpJusxgLz0S6DSrvDd+F8mb2732Sr9U60xHkbqXUxoAvNZIWD5KOgpZvSjAVY
jaVcGQ3J20cfeA8NiYIYUDdAnaYc0ak1NRI3w41cHKyv713rzjwMn822DJEeY/ju
rMdCeV6IZW3kr3ARsvaHGBB9vaYWSTjZ4EwOImXfiuc1Pa6MdbYvLtxQ6wTlBhFf
zuh95BEpHeFOSRZYvRnkaU1+DAoKQmG6ZUuhSe1R72PaxNQSt4fJgwKmDzWifwi1
KOcivVNaqcUj0K2kUZYUxEMFKaxpRenxIP4nSxbz9IUCDANSe3F+cUBnQwEP/13L
ZkM8E5/bTMPiG0Mns/tFbL9FK64QZuXRN2VOV/CQ2+S6yNHjhxEOd/W9cJLRXLvj
bIBORIdoP8yOcBXJG7ag6/KZDgtE+7SbvwCQu9kxg9torJt2q9mtmuQjj/YImtim
NYStne5In0LNPr5ZNjOabWoXgPPwOSrhkMqANyHz+WEcioD8CZMRwZaF5HoC+OtR
P07KGRm33TCzg5wX6iTLWHkRBuDradBRxQEY/MRsu2Hc/01hzQeLpq3qysXKEcbJ
VYZ6SnRHkDtcWXvPjBNgeEEhSMM3jr2n/D6RTjepySLXGfCxTNjTqCAxDvvoiWmS
6RmTQFaLtQQszvZ2PYUom0h8jlZO4jDoSjgYEtCYb6XDwZoxSPQnbdSwumiNYH8R
B6dHxkmGLeRrpuLQDTnZhIi9OCLx7CIiKhyDvf08gFwD72az4ofeTPx/boASxtAH
ZcdOM+jk9jJTWpDP/3HZCwYE5ppCfmsBNn5LyzoUZG3B486v2nNJDrBRf8vtGEF9
1uk7upGmn3jyVAIejGtxtbnD4+ffNca+ovOAqni8HNRhou0M2OMAwdnnyyir4QWo
MFCoZ56rqYaGe4066O7JlNsaCHi4d7mhWfY0LVdAANCHYgNMPuMSAT8Qw6Hb/NE/
Rs6NS62cUka316DPO6pkcribhGX92AhWxbMhS1cT0ukBi4D00bQInZK2TT2k90tv
G8i2ssRWAIxGrvvqrlzFxZKkvJoD4K/oBCxiKmZv9MgoXXetHt+D+FyUgwDkWYC9
gH0MBzDYbm8Cor/DHVJOOYw2w21DI9Xf7HYsuIfUM4tYB6q/tUGawhhTA7ICv161
qnXZJI8MhAgOyK3Z4kJYZKww1/XvG0tH6U3hqfK0HDoDA6Xv+9ilsZwtmgZERgTc
DeYMlayzhoKT4RLbJwctvAkGkiQY420+AFQMZtZG1eH/lkrGwjkHUyZfI0HeZknY
Y7ZMcwIEfTpG2XdmQ+FJcFWdk+8E38QDk78rcsdELVnISLHEiPgGNr/dl9pURYoI
ayw+fc7w+hguiny8CMf3Aa5owO+RJUk3L7AogVKCIrQhw3Pr676cIdf7XOpIeTKf
khJXKfkkUSZBWRXTgxHuAX6j3pIgaqAywSb5lJVvGsQGER85aFB4l0bOd6e7kPcx
Gw4E2Ea1p3P4NJKMjlhc7aG6keGJFG+LWi7awP+kLtbhIgwE6wEd41sHBoArM/LY
woSqShi04pZqb4TuPDCnfGxFZH7+uzdoL5drGRdV0pDCVn06P2DYP+tn7g2r6hXZ
cwx6ac/l+BhDKSU9IvZZF6QpTkEatp96AptzJKBtADKYJPbT4sp1qJLQUMWlzbfE
+nt5hlh4+afxmRKOTfcehVLT5br93l0PNPqaETMgr8aIAP9IB0C2X03RCU1nDkvZ
KKqqE+2Wg5oaVmMN/8HcqG1xRfimE+x7qhTTEr0QHL2QzwsnLASamiaUxmza02lo

```
LSRS
=kmVp
-----END PGP MESSAGE-----
```

gpg --decrypt --output decrypted.txt encrypted.asc

Расшифрованный файл:

t3/decrypted.txt

```
Content-Type: multipart/mixed; boundary="dtihBuymNvhVuYZSzhhTPmvnYDttovhj6";
 protected-headers="v1"
From: awh <awh@cs.msu.ru>
To: p.milko1999@yandex.ru
Message-ID: <1b1593f6-051a-b1b0-1678-bce15ccb8c53@cs.msu.ru>
Subject: =?UTF-8?B?UmU6INCe0YLQutGA0YvRgtGL0Lkg0LrQu9GO0Ycg0L/QviDQstGC0L4=?=
 =?UTF-8?B?0YDQvtC5INC70LDQsdC+0YDQsNGC0L7RgNC90L7QuSDRgNCw0LHQvtGC0LU=?=
References: <7398811583869376@vla4-d1c3bcedfacb.qloud-c.yandex.net>
In-Reply-To: <7398811583869376@vla4-d1c3bcedfacb.qloud-c.yandex.net>

--dtihBuymNvhVuYZSzhhTPmvnYDttovhj6
Content-Type: text/plain; charset=utf-8
Content-Language: ru
Content-Transfer-Encoding: quoted-printable

=D0=97=D0=B0=D1=88=D0=B8=D1=84=D1=80=D0=BE=D0=B2=D0=B0=D0=BD=D0=BD=D0=BE=D0=
=B5 =D1=81=D0=BE=D0=BE=D0=B1=D1=89=D0=B5=D0=BD=D0=B8=D0=B5 3.

On 3/10/20 10:43 PM, p.milko1999@yandex.ru wrote:


--dtihBuymNvhVuYZSzhhTPmvnYDttovhj6--
```

Сначала я подумал, что мне по ошибке пришёл дамп http-запроса, но потом я заметил строчку “Content-Transfer-Encoding: quoted-printable”.

После перекодирования тела сообщения из этой кодировки я получил следующее:

“Зашифрованное сообщение 3.”

Часть 3: сбор подписей одногруппников

В качестве пробного одногруппника был выбран Алексей Куликов. Мы обменялись открытыми ключами и подписали их друг другу.

Теперь мой ключ выглядит так:

```
pub    rsa2048 2020-03-10 [SC] [expires: 2022-03-10]
       703FD5D038947C5B57CCE5A64DF7496E16FD3CBC
uid             [ultimate] Милько Павел Алексеевич <p.milko1999@yandex.ru>
sig 3        4DF7496E16FD3CBC 2020-03-10   Милько Павел Алексеевич <p.milko1999@yandex.ru>
sig 3        B104CF5F4D4DE318 2020-03-13   Alexey <kapitoshka.the.first@gmail.com>
sub    rsa2048 2020-03-10 [E] [expires: 2022-03-10]
sig          4DF7496E16FD3CBC 2020-03-10   Милько Павел Алексеевич <p.milko1999@yandex.ru>
```