Guilherme Sbrolini Mazzariol - RA 138466
Computer Security - 2017s2 - EXP04

All commands used in Exp04

1. Create a key pair (pubkeyRA and prikeyRA) in GnuPG.

```
$ gpg --gen-key
gpg (GnuPG) 1.4.16; Copyright (C) 2013 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.
Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 2048
Requested keysize is 2048 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0)
Key does not expire at all
Is this correct? (y/N) y
You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"
Real name: Guilherme Mazzariol
Email address: g138466@g.unicamp.br
Comment: SEGC - EXP04
You selected this USER-ID:
    "Guilherme Mazzariol (SEGC - EXP04) <g138466@g.unicamp.br>"
Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
You need a Passphrase to protect your secret key.
can't connect to server: ec=255.16777215
gpg: problem with the agent - disabling agent use
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 6E91697A marked as ultimately trusted
public and secret key created and signed.
gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
pub   2048R/6E91697A 2017-10-21
      Key fingerprint = DB46 4994 ACEE F85B 1D3D  51DA 0F2A FC20 6E91 697A
```

```
uid              Guilherme Mazzariol (SEGC - EXP04) <g138466@g.unicamp.br>
sub   2048R/E61BF562 2017-10-21
```

2. Add a photo in the public key.

```
$ gpg --edit-key 6E91697A
gpg (GnuPG) 1.4.16; Copyright (C) 2013 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.

Secret key is available.

pub  2048R/6E91697A  created: 2017-10-21  expires: never       usage: SC
                     trust: ultimate      validity: ultimate
sub  2048R/E61BF562  created: 2017-10-21  expires: never       usage: E
[ultimate] (1). Guilherme Mazzariol (SEGC - EXP04) <g138466@g.unicamp.br>

gpg> addphoto

Pick an image to use for your photo ID.  The image must be a JPEG file.
Remember that the image is stored within your public key.  If you use a
very large picture, your key will become very large as well!
Keeping the image close to 240x288 is a good size to use.

Enter JPEG filename for photo ID: GSM.jpeg
Is this photo correct (y/N/q)? y

You need a passphrase to unlock the secret key for
user: "Guilherme Mazzariol (SEGC - EXP04) <g138466@g.unicamp.br>"
2048-bit RSA key, ID 6E91697A, created 2017-10-21

pub  2048R/6E91697A  created: 2017-10-21  expires: never       usage: SC
                     trust: ultimate      validity: ultimate
sub  2048R/E61BF562  created: 2017-10-21  expires: never       usage: E
[ultimate] (1). Guilherme Mazzariol (SEGC - EXP04) <g138466@g.unicamp.br>
[ unknown] (2)  [jpeg image of size 5073]
gpg> quit
Save changes? (y/N) y
```

3. Sign your partner's public key (pubkeyRA_validatedRA) in ASCII armor format.

```
$ gpg --import pubkey140604.pub
$ gpg --list-keys
/home/guilherme/.gnupg/pubring.gpg
----------------------------------
pub   2048R/6E91697A 2017-10-21
uid                  Guilherme Mazzariol (SEGC - EXP04) <g138466@g.unicamp.br>
uid                  [jpeg image of size 5073]
sub   2048R/E61BF562 2017-10-21

pub   2048R/47196AED 2017-10-20
uid                  Felipe Caminada (Encrypted key for the segc class on UNICAMP) <caminadaf@gmail.com>
sub   2048R/53617163 2017-10-20

pub   2048R/316B9ECA 2017-10-19
uid                  Marcelo Pinheiro Machado <marcelopmachado@gmail.com>
uid                  [jpeg image of size 23629]
sub   2048R/F390606F 2017-10-19

$ gpg --edit-key caminadaf@gmail.com
gpg (GnuPG) 1.4.16; Copyright (C) 2013 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.

pub  2048R/47196AED  created: 2017-10-20  expires: never       usage: SC
                     trust: unknown       validity: unknown
sub  2048R/53617163  created: 2017-10-20  expires: never       usage: E
[ unknown] (1). Felipe Caminada (Encrypted key for the segc class on UNICAMP) <caminadaf@gmail.com>
gpg> sign
pub  2048R/47196AED  created: 2017-10-20  expires: never       usage: SC
                     trust: unknown       validity: unknown
 Primary key fingerprint: C7EF DEB7 BC21 C4F4 869D  D772 8B09 0EE9 4719 6AED

     Felipe Caminada (Encrypted key for the segc class on UNICAMP) <caminadaf@gmail.com>

Are you sure that you want to sign this key with your
key "Guilherme Mazzariol (SEGC - EXP04) <g138466@g.unicamp.br>" (6E91697A)

Really sign? (y/N) y

You need a passphrase to unlock the secret key for
user: "Guilherme Mazzariol (SEGC - EXP04) <g138466@g.unicamp.br>"
2048-bit RSA key, ID 6E91697A, created 2017-10-21

gpg> trust
pub  2048R/47196AED  created: 2017-10-20  expires: never       usage: SC
                     trust: unknown       validity: unknown
sub  2048R/53617163  created: 2017-10-20  expires: never       usage: E
[ unknown] (1). Felipe Caminada (Encrypted key for the segc class on UNICAMP) <caminadaf@gmail.com>
```

```
Please decide how far you trust this user to correctly verify other users' keys
(by looking at passports, checking fingerprints from different sources, etc.)

  1 = I don't know or won't say
  2 = I do NOT trust
  3 = I trust marginally
  4 = I trust fully
  5 = I trust ultimately
  m = back to the main menu

Your decision? 4

pub  2048R/47196AED  created: 2017-10-20  expires: never       usage: SC
                     trust: full          validity: unknown
sub  2048R/53617163  created: 2017-10-20  expires: never       usage: E
[ unknown] (1). Felipe Caminada (Encrypted key for the segc class on UNICAMP) <caminadaf@gmail.com>
Please note that the shown key validity is not necessarily correct
unless you restart the program.

gpg> quit
Save changes? (y/N) y
```

4. Export pubkey:

```
$ gpg --armor --export caminadaf@gmail.com > pubkey140604_validate138466.gpg
$ gpg --armor --export g138466@g.unicamp.br > pubring138466.gpg
```

5. Sign and Encrypt a File:

```
$ gpg --clearsign -o msg138466.txt.asc msg138466.txt
You need a passphrase to unlock the secret key for
user: "Guilherme Mazzariol (SEGC - EXP04) <g138466@g.unicamp.br>"
2048-bit RSA key, ID 6E91697A, created 2017-10-21
$ cat msg138466.txt.asc
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Guilherme Sbrolini Mazzariol
ra138466
Ciência da Computação
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1

iQEcBAEBAgAGBQJZ7OuAAAoJEA8q/CBukWl6re4IAJbj+IJIKuTMHaioFpcAtHLA
09CJAjRpWLlR9PQJv4VtNDMWF2Dh4GQwv2LBmoSwHVIDzVNR7JK+4wVWrsPnN3Yj
gzgWLCjEMF5z6V9GKNamhFkmtjUWL6DBv/0pUqAnhgvsACZuhofAVILHHLiGc2vZ
jvfkPtol8DijO7YXfk5/sFtdtWSiqg1Us500DT3KSx1hZMHXKuD1vhABvd0Ro1te
6rVf1rpTaXHtVTwEcOZiZSbV4SWicjrn0sVPVN6OyeK4jkWqqVkKT9HJhkiRpaqy
bO6Un/NAdLQ9mbUR6VJE6TCS+qiS0mEA9ynSeRisZdkrP6dw0Mox11en97sx/VA=
=H0fc
-----END PGP SIGNATURE-----
```

6. Import key:

```
$ gpg --import mo639-pub.txt
gpg: key 462BFA2C: public key "MO639A_2017
          (sistema seguro e aquele que nao esta
          inseguro) <ic-segc-staff-l@g.unicamp.br>"
          imported
gpg: Total number processed: 1
gpg:          imported: 1  (RSA: 1)
$ gpg --list-keys
/home/guilherme/.gnupg/pubring.gpg
----------------------------------
pub   2048R/6E91697A 2017-10-21
uid                  Guilherme Mazzariol (SEGC - EXP04)
<g138466@g.unicamp.br>
uid                  [jpeg image of size 5073]
sub   2048R/E61BF562 2017-10-21

pub   2048R/47196AED 2017-10-20
uid                  Felipe Caminada (Encrypted key for the
segc class on UNICAMP) <caminadaf@gmail.com>
sub   2048R/53617163 2017-10-20

pub   2048R/316B9ECA 2017-10-19
uid                  Marcelo Pinheiro Machado
<marcelopmachado@gmail.com>
uid                  [jpeg image of size 23629]
sub   2048R/F390606F 2017-10-19

pub   1024R/462BFA2C 2017-10-05 [expires:
2017-12-14]
uid                  MO639A_2017 (sistema seguro e aquele
          que nao esta inseguro)
          <ic-segc-staff-l@g.unicamp.br>
sub   1024R/D084404D 2017-10-05 [expires:
2017-12-14]

$ gpg --encrypt --armor --recipient
ic-segc-staff-l@g.unicamp.br msg138466.txt.asc
```