

Laboratorio 1:
Victor Rafael Valenzuela Cortez
00022120

Instalar GPG

```
uca@debian:~$ sudo apt install gnupg
[sudo] password for uca:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
gnupg is already the newest version (2.2.27-2+deb11u2).
gnupg set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Generando llave

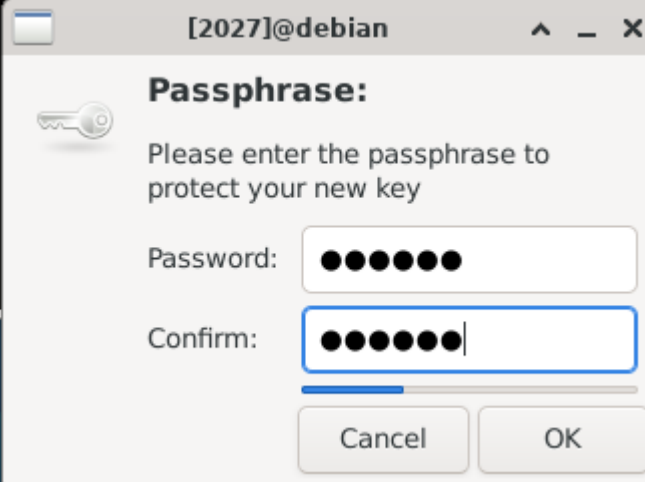
```
uca@debian:~$ gpg --full-generate-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: keybox '/home/uca/.gnupg/pubring.kbx' created
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)
  (14) Existing key from card
Your selection? 1
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (3072)
Requested keysize is 3072 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)
```

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

Real name: Victor Rafael Valenzuela Cortez
Email address: 00022120@uca.edu.sv
Comment: VictorCortez358
You selected this USER-ID:
    "Victor Rafael Valenzuela Cortez (VictorCortez358) <00022120@uca.edu.sv>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? █
```



```
Change (N)ame, (C)omment, (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: /home/uca/.gnupg/trustdb.gpg: trustdb created
gpg: key B19DB1F6312F12CE marked as ultimately trusted
gpg: directory '/home/uca/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/uca/.gnupg/openpgp-revocs.d/04D04EC4BB1FD12B9DEC83E2B19DB1F6312F12CE.rev'
public and secret key created and signed.

pub   rsa3072 2022-08-29 [SC]
       04D04EC4BB1FD12B9DEC83E2B19DB1F6312F12CE
uid
     Victor Rafael Valenzuela Cortez (VictorCortez358) <00022120@uca.edu.sv>
sub   rsa3072 2022-08-29 [E]
```

Remover el certificado a la llave

```
uca@debian:~$ gpg --output my_revocation_certificate.asc --gen-revoke 04D04EC4BB1FD12B9DEC83E2B19DB1F6312F12CE

sec  rsa3072/B19DB1F6312F12CE 2022-08-29 Victor Rafael Valenzuela Cortez (VictorCortez358) <00022120@uca.edu.sv>

Create a revocation certificate for this key? (y/N) y
Please select the reason for the revocation:
  0 = No reason specified
  1 = Key has been compromised
  2 = Key is superseded
  3 = Key is no longer used
  Q = Cancel
(Probably you want to select 1 here)
Your decision? Q
```

Lista de claves que hay

```
uca@debian:~$ gpg --list-keys
gpg: checking the trustdb
gpg: marginals needed: 3 completes needed: 1 trust model: pgp
gpg: depth: 0 valid: 1 signed: 0 trust: 0-, 0q, 0n, 0m, 0f, 1u
/home/uca/.gnupg/pubring.kbx
-----
pub   rsa3072 2022-08-29 [SC]
      04D04EC4BB1FD12B9DEC83E2B19DB1F6312F12CE
uid   [ultimate] Victor Rafael Valenzuela Cortez (VictorCortez358) <0002
2120@uca.edu.sv>
sub   rsa3072 2022-08-29 [E]
```

Exportar clave

```
uca@debian:~$ gpg --armor --export naldana@uca.edu.sv
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
```

```
mQGNBGL9PsYBDADwGye3bdKckImLEiC8PZ5PF2z9x3J2VH5DaPtJrcwxDN7g5DC7
TTR2hHXmKcmpgkAPhDo/Hz1kIpJgKgiCfuquxdQ0wxXCeHrtv004sAzzPa/utGLf
+iRgKto9y0EI4W9IMzkluzp0fN4JBr/08hwLRNfcr5wu5ZCgDliZSDK3vDop16LM
k+yGvQzcp/gGt35fBbx9acdYHEaRTUhegKz3mIMEErfsf6qYj/NuLszqKCJH8edV
c+FqNjD2A/RB/8H3IVB+5VSBnggF50+UIHzejzrFLPi0W+qvJ0Eb0wq0rMRLAYs
5IfCpsC4WnruvY6rgHBfUKuPnXg5J+WFMM3nJjJQd8PP9oyodnrVa09W/lGn0Qzj
gn7RwmlHKn+VHVR9f7BIEBZ4CRHHE3+4Dr19+V6B7EeBT7S3xgHbLsd2qg/1BK
XxhjSZsmgsSYwrX2H0FM+RwYpBsmUJgXrG7sxJzL5eyB3w9+gdUvXMaapCM6vIiV
PhBJnLPwR5wv4/MAEQEAABRVtmVzdG9yIFNhbnpYwYdIEFsZGFuYSB2RyaWd1
ZXogKEduVBUHUCBhdWlkZSAteIEZvciBVQ0EgaW4uU0VEKSA8bmFsZGFuYUB1Y2Eu
ZWR1LnN2PokBzGQTAQoA0BYhBJ7ma0RsDnvBt05t6ctYQxiVipICBQJi/T7GAhsD
BQsJCACCBhUKCQgLAGQWAgMBAh4BAheAAAJEMTYQxiVipIC2fAMAKrYhMjLhq8C
iewmqzV3cym1fd5+4D2oH2bpRxPEICge3y0A0EmFZWjNWybJSWL7VncTuU9wbrUZ
IxMAqH9xINiY0Gopf0JZ2dVj5KpVH7gmCLGU35WPBWvafsaC5rvexkDHptx92x+
Sm03Nl7biNyiG8gSz/1jVP6Sns3Nfv9N2/xjkhcgI5f5DUiAYIUUSVR6I407YIBN
i5TNfFzglm9v+TY0K7JkFxCgdqgB7CkxXQrWlwojps0xhJulc2Y0dzY9qnofn3Jw
tw0K8xSYCK9N4oUCLLD+zD1zJfkefc8ziWhEM93+I4K/oD3P0zhJM0+wQo1QE1p
uAQ9+YEcAz2hKDrT+2zJhFSK384FUSD/uuVg3Ddg6M5QsalwC/fwBLE/50SqtL71
ndZc8JB+kt5tvTBn6F3XZ/mssypN1nEuWyIfiHiFZa8PVJ1+M9KRWY4gITsZjbrv
e0DRP83lc2/rnhavT4aD8i5Coscj0sM9sKzDYoc/ZoZ8x2ICFuOGPbkBjQRi/T7G
AQwAxaPyFumXp65qJ0Qm0W6urCD9v47AHMY6zWZvx7cq6y/jwNh8foUd8pV9qm3
LRFNmtVNPd/WYB7su/449IJ80Ca/Tx/GpQjnFMvIVYfjyWfDsFYLy1DBI0bft5RT
2QyJd03EKxKVSj9tthwi2oZp0TLsta+Qpb/e/CLIXDzaXImfbkYVP8mtvIXGnrja
GE6ZWXLMEv6r1T5pe/jqEP2E89Y1S0sY7Jvrpg5JF5rCWmAPT+yJIzY7ckA/0eoq
siAigb3h4CtMDWV6gQWh8skln2tL9GsQj6xDrNqvDwpQryLLRTtIIPB8VfFawcAK
MHfrJrn0KtBUASmHkVxhhCgzWfogctaPlyA9r094bzbLkIDj5EX6LPRzmu60gfmw
jFNs3z0S3UBAzIse5IcgU6xssFI451Vg52pAEERS7g9+0Vy2E3C6Ppfv2kuqbtV
crC0Vrv3mth30iycM3g4Z3+0/ljeRmzltPZ98gbhfeMrTQ7v+b1MMTVR3lqIC+5K
LtanABEBAAGJAbYEGAeKACAWIQSe5mtEbA57wbd0benLWEMYLYqSAGUCYv0+XgIb
DAAKCRDLWEMYLYqSAu+MC/9vucDaVN8QU/HAZIFp06PuTOcZ26RsGca/qs5A+W6x
XM3Qeqj+00Hv/eNZAKd/6KMXtdddrldDxwA6M0+qM5bFNzxGUmztXHIxy86pjcW
8dRZCqa/3b+Gnr1QYy0Pvyd0D0+Eh1CHWFBswKBZY7Czxim0QZoJ/+BlhLpjQxcw
Mb0sM//C+uqXpi3R0Ez0F2CmTF7d+8yzeqm3K0LgA3A44GEzdUL2ICYw7d6hVBAA
p2Da8HA1jW4PvyQIXLT0UfAPgZyz8Tdxz8I0Poc3/5sDKl+gx8wmW/RtmqZzCoK
eqoPVgyZ6fCc3RJhG6902agYpxqr1RiSCkqAAzSxqXd6RpD4+AqmuAYMtLvBNBbp
bgxl/RsXA5WT9vqRwXt6C/TTFNy7xVEQqL7Vpz6xL3wDv+pWX1dq5WbYNUkgscpb
vvfVs93l1HwOXWiuKSJt1VhKFalXPu092JTZtdTdE33+/bc46BuDY17LR6wxIMJp
tvDMzd9ydpLWzgygQZfb0vo=
=Y5zo
```

```
-----END PGP PUBLIC KEY BLOCK-----
```

Importar claves

```
uca@debian:~$ gpg --output victorcortez.gpg --armor --export 00022120@uca.edu.sv
```

```
uca@debian:~$ gpg --export-secret-keys --armor 00022120@uca.edu.sv > ./my-priv-gpg-key.asc
```

```
uca@debian:~$
```

```
uca@debian:~$ nano miguel.gpg
```

```
uca@debian:~$ nano miguel.gpg
```

```
uca@debian:~$ gpg --import ~/miguel2.gpg
gpg: key 22FD98109A7AB1C3: public key "miguel rivas (clave for uca sei) <00087518@uca.edu.sv>" imported
gpg: Total number processed: 1
gpg: imported: 1
```

```
uca@debian:~$ gpg --list-keys
/home/uca/.gnupg/pubring.kbx
-----
pub   rsa3072 2022-08-29 [SC]
      04D04EC4BB1FD12B9DEC83E2B19DB1F6312F12CE
uid   [ultimate] Victor Rafael Valenzuela Cortez (VictorCortez358) <00022120@uca.edu.sv>
sub   rsa3072 2022-08-29 [E]

pub   rsa3072 2022-08-17 [SC]
      9EE66B446C0E7BC1B74E6DE9CB584318958A9202
uid   [ unknown] Nestor Santiago Aldana Rodriguez (GnuPG Guide - For UCA in SED) <naldana@uca.edu.sv>
sub   rsa3072 2022-08-17 [E]

pub   rsa3072 2022-08-17 [SC] [expires: 2022-10-16]
      FE42FA6AEB275595B093D4F322FD98109A7AB1C3
uid   [ unknown] miguel rivas (clave for uca sei) <00087518@uca.edu.sv>
sub   rsa3072 2022-08-17 [E] [expires: 2022-10-16]

uca@debian:~$ gpg --edit-key 00087518@uca.edu.sv
gpg (GnuPG) 2.2.27; Copyright (C) 2021 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   rsa3072/22FD98109A7AB1C3
      created: 2022-08-17 expires: 2022-10-16 usage: SC
      trust: unknown validity: unknown
sub   rsa3072/04C91A3A0839EA12
      created: 2022-08-17 expires: 2022-10-16 usage: E
[ unknown] (1). miguel rivas (clave for uca sei) <00087518@uca.edu.sv>

gpg> fpr
pub   rsa3072/22FD98109A7AB1C3 2022-08-17 miguel rivas (clave for uca sei) <00087518@uca.edu.sv>
      Primary key fingerprint: FE42 FA6A EB27 5595 B093 D4F3 22FD 9810 9A7A B1C3

gpg> sign

pub   rsa3072/22FD98109A7AB1C3
      created: 2022-08-17 expires: 2022-10-16 usage: SC
      trust: unknown validity: unknown
      Primary key fingerprint: FE42 FA6A EB27 5595 B093 D4F3 22FD 9810 9A7A B1C3

      miguel rivas (clave for uca sei) <00087518@uca.edu.sv>

This key is due to expire on 2022-10-16.
Are you sure that you want to sign this key with your
key "Victor Rafael Valenzuela Cortez (VictorCortez358) <00022120@uca.edu.sv>" (B19DB1F6312F12CE)

Really sign? (y/N) y

gpg> check

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

uca@debian:~$ gpg --list-keys
gpg: checking the trustdb
gpg: marginals needed: 3 completes needed: 1 trust model: pgp
gpg: depth: 0 valid: 1 signed: 1 trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: depth: 1 valid: 1 signed: 0 trust: 1-, 0q, 0n, 0m, 0f, 0u
gpg: next trustdb check due at 2022-10-16
/home/uca/.gnupg/pubring.kbx
-----
pub   rsa3072 2022-08-29 [SC]
      04D04EC4BB1FD12B9DEC83E2B19DB1F6312F12CE
uid   [ultimate] Victor Rafael Valenzuela Cortez (VictorCortez358) <00022120@uca.edu.sv>
sub   rsa3072 2022-08-29 [E]

pub   rsa3072 2022-08-17 [SC]
      9EE66B446C0E7BC1B74E6DE9CB584318958A9202
uid   [ unknown] Nestor Santiago Aldana Rodriguez (GnuPG Guide - For UCA in SED) <naldana@uca.edu.sv>
sub   rsa3072 2022-08-17 [E]

pub   rsa3072 2022-08-17 [SC] [expires: 2022-10-16]
      FE42FA6AEB275595B093D4F322FD98109A7AB1C3
uid   [ full ] miguel rivas (clave for uca sei) <00087518@uca.edu.sv>
sub   rsa3072 2022-08-17 [E] [expires: 2022-10-16]
```

Cifrado simétrico

```
uca@debian:~$ history > history.txt
uca@debian:~$ cat history.txt
1 su
2 sudo apt install gnupg
3 sudo -
4 sudo nano
5 su
6 sudo apt install gnupg
7 gpg --full-generate-key
8 gpg --output my_revocation_certificate.asc --gen-revoke 04D04EC4BB1FD12B9DEC83E2B19DB1F631
9 gpg --list-keys
10 gpg --armor --export naldana@uca.edu.sv
11 gpg --armor --export naldana@uca.edu.sv
12 gpg --armor --export naldana@uca.edu.sv
13 gpg --output nextor.gpg --export naldana@uca.edu.sv
14 gpg --output nextor.gpg --export 00022120@uca.edu.sv
15 gpg --armor --export 00022120@uca.edu.sv
16 gpg --output nextor.gpg --armor --export 00022120@uca.edu.sv
17 gpg --output victorcortez.gpg --armor --export 00022120@uca.edu.sv
18 gpg --export-secret-keys --armor 00022120@uca.edu.sv > ./my-priv-gpg-key.asc
19 nano miguel.gpg
20 nano victor.gpg
21 gpg --import ~/Downloads/miguel.gpg
22 gpg --import ~/miguel.gpg
23 gpg --armor --export naldana@uca.edu.sv
24 gpg --output nextor.gpg --armor --export naldana@uca.edu.sv
25 gpg --list-keys
26 gpg --import ~/miguel.gpg
27 nano miguel.gpg
28 nano miguel2.gpg
29 gpg --import ~/miguel2.gpg
30 gpg --list-keys
31 gpg --edit-key 00087518@uca.edu.sv
32 gpg --list-keys
33 history > history.txt
uca@debian:~$ gpg --output history.txt.gpg --symmetric history.txt
uca@debian:~$ cat history.txt.gpg
Yz00007a0YA:000YXj1002hl00-0000mC0XKR)00%000oD00000*i0000=000#q00f00000,00-00(pZaR00M0)0T0030#0w000Vy003600X0V00c0p|I0000
00"0000
G0
(00"kJ00:0vU900kxg:a000+ 000 r0BA00s0] 0w0Jk0?0M00Bn0]0+000S0nx00uF_008[s0mtc-100V!%(0v00/0092g00Y0fSm
0/0#s00:0I000000"nc0V08x0 0:E0d9,0(U
:00c0B0tA"0000 0i0A00n/0)0"00000"=uca@debian:~$
```

Cifrado

asimétrico:

```
uca@debian:~$ history > historyPublicKey.txt
uca@debian:~$ cat historyPublicKey.txt
1 su
2 sudo apt install gnupg
3 sudo -
4 sudo nano
5 su
6 sudo apt install gnupg
7 gpg --full-generate-key
8 gpg --output my_revocation_certificate.asc --gen-revoke 04D04EC4BB1FD12B9DEC83E2B19DB1F6312F12CE
9 gpg --list-keys
10 gpg --armor --export naldana@uca.edu.sv
11 gpg --armor --export naldana@uca.edu.sv
12 gpg --armor --export naldana@uca.edu.sv
13 gpg --output nextor.gpg --export naldana@uca.edu.sv
14 gpg --output nextor.gpg --export 00022120@uca.edu.sv
15 gpg --armor --export 00022120@uca.edu.sv
16 gpg --output nextor.gpg --armor --export 00022120@uca.edu.sv
17 gpg --output victorcortez.gpg --armor --export 00022120@uca.edu.sv
18 gpg --export-secret-keys --armor 00022120@uca.edu.sv > ./my-priv-gpg-key.asc
19 nano miguel.gpg
20 nano victor.gpg
21 gpg --import ~/Downloads/miguel.gpg
22 gpg --import ~/miguel.gpg
23 gpg --armor --export naldana@uca.edu.sv
24 gpg --output nextor.gpg --armor --export naldana@uca.edu.sv
25 gpg --list-keys
26 gpg --import ~/miguel.gpg
27 nano miguel.gpg
28 nano miguel2.gpg
29 gpg --import ~/miguel2.gpg
30 gpg --list-keys
31 gpg --edit-key 00087518@uca.edu.sv
32 gpg --list-keys
33 history > history.txt
34 cat history.txt
35 gpg --output history.txt.gpg --symmetric history.txt
36 cat history.txt.gpg
37 history > historyPublicKey.txt
```

```
uca@debian:~$ gpg --output historyPublicKey.txt.gpg --encrypt --recipient naldana@uca.edu.sv historyPublicKey.txt
gpg: A247B11A728618C7: There is no assurance this key belongs to the named user

sub   rsa3072/A247B11A728618C7 2022-08-17 Nestor Santiago Aldana Rodriguez (GnuPG Guide - For UCA in SED) <naldana@uca.edu.sv>
Primary key fingerprint: 9EE6 6B44 6C0E 7BC1 B74E 6DE9 CB58 4318 958A 9202
Subkey fingerprint: 13FF A121 FBA4 DB9B BCE8 EC75 A247 B11A 7286 18C7

It is NOT certain that the key belongs to the person named
in the user ID. If you *really* know what you are doing,
you may answer the next question with yes.

Use this key anyway? (y/N) y
```

- *¿Cuál es el punto más débil de PGP?*

Phong Nguyen identifico un error grave en la manera en la que GnuPG creaba y usaba claves ElGamal para firmar. Éste es un fallo de seguridad significativo, ya que podría provocar un compromiso de casi todas las claves ElGamal que se usaran para firmar.

- *¿Cuándo es conveniente utilizar solamente cifrado simétrico?*

Por que se puede adivinar la clave de alguna manera.

Creación y verificación de firmas digitales

```
uca@debian:~$ gpg --output doc.sig --sign victor.gpg
uca@debian:~$ gpg --output doc --decrypt doc.sig
gpg: Signature made Mon 29 Aug 2022 04:39:52 PM CST
gpg:                using RSA key 04D04EC4BB1FD12B9DEC83E2B19DB1F6312F12CE
gpg: Good signature from "Victor Rafael Valenzuela Cortez (VictorCortez358) <00022120@uca.edu.sv>" [ultimate]
```