

## Generación de una llave pública y privada

```
Terminal - uca@debian: ~/laboratorio1
File Edit View Terminal Tabs Help
uca@debian:~/laboratorio1$ 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
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
```

```
Terminal - uca@debian: ~/laboratorio1
File Edit View Terminal Tabs Help
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) y

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

Real name: Alejandra Villalobos
Email address: 00132820@uca.edu.sv
Comment: labo1
You selected this USER-ID:
    "Alejandra Villalobos (labo1) <00132820@uca.edu.sv>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? 0
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.
```

```
Terminal - uca@debian: ~/laboratorio1
File Edit View Terminal Tabs Help

"Alejandra Villalobos (labo1) <00132820@uca.edu.sv>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? 0
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 D228E99E9BA76299 marked as ultimately trusted
gpg: directory '/home/uca/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/uca/.gnupg/openpgp-revocs.d/EFC529:
81B424932B1BA4539D228E99E9BA76299.rev'
public and secret key created and signed.

pub   rsa3072 2022-09-02 [SC]
      EFC529381B424932B1BA4539D228E99E9BA76299
uid                               Alejandra Villalobos (labo1) <00132820@uca.edu.sv>
sub   rsa3072 2022-09-02 [E]
```

Generación de certificado de revocación

```
Terminal - uca@debian: ~/laboratorio1
File Edit View Terminal Tabs Help

uca@debian:~/laboratorio1$ gpg --output my_revocation_certificate.asc --gen-re
voke D228E99E9BA76299

sec   rsa3072/D228E99E9BA76299 2022-09-02 Alejandra Villalobos (labo1) <0013282
0@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? 1
Enter an optional description; end it with an empty line:
> labo
>
Reason for revocation: Key has been compromised
labo
Is this okay? (y/N) y
ASCII armored output forced.
Revocation certificate created.
```

## Listado de llaves

```
uca@debian:~/laboratorio1$ 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 2022-09-02 [SC]
      EFC529381B424932B1BA4539D228E99E9BA76299
uid   [ultimate] Alejandra Villalobos (labo1) <00132820@uca.edu.sv>
sub   rsa3072 2022-09-02 [E]

uca@debian:~/laboratorio1$
```

## Listado de llaves secretas

```
uca@debian:~/laboratorio1$ gpg --list-secret-keys
/home/uca/.gnupg/pubring.kbx
-----
sec   rsa3072 2022-09-02 [SC]
      EFC529381B424932B1BA4539D228E99E9BA76299
uid   [ultimate] Alejandra Villalobos (labo1) <00132820@uca.edu.sv>
ssb   rsa3072 2022-09-02 [E]

uca@debian:~/laboratorio1$
```

## Exportación de la llave que generamos

```
uca@debian:~/laboratorio1$ gpg --output alejandra.gpg --export 00132820@uca.edu.sv
uca@debian:~/laboratorio1$

uca@debian:~/laboratorio1$ gpg --armor --export 00132820@uca.edu.sv
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGMSCfQBDADGtnDSTRbxzKckyefyo5IgH+jRgui6UUlezs+cEo3MhyWf7QJL
thRjqujKdoJ7jLRxs3QqF9eFVmx6tR76ITNkEdBBFlh4YZzuSvPMe2Ks0LfGujd3
28Txw/2jhGfNCU08umteWbm0oR1GK07iDnSxaysBLQZg+NqrMz+/B6BsL3ijJy5p
mQWVvh97ziaQALVGaxgcvZ2w4r2TyZYXr7eyE9JobfCU099XPiB0HzzmXq5v6DxY
egR/fB0a10qEGmPspQo8YoXIENI9ECUfrn8JWUVdTGDLB11FQ266zzM7AxLHmTZl
gRkw2I0tatzm0qcp1+uXeHuhIr5o90LKswIvsHS2/8iv30p1xoB3j7LjtD5FRpkA
GSClljCsL9TSDb1M4t+DjeTSAfvY6im84JqteCRahixjAb1t09YtC6y5nLN0nKRF
3Bc9T8lSiSxcYQERiyd3NIb1cGmLR6ZQ+BN2crCENTuyGW+a4DPgkGELDPM3SG1A
JjSIRoDVojwVRV0AEQEAAbQyQWxlamFuZHZHhIFZpbGxhbG9ib3MgKGxhYm8xKSA8
MDAxMzI4MjBAdWNhLmVkdS5zdj6JAc4EEwEKADgWIQTvxSk4G0JJMrG6RTnSK0me
m6dimQUCYxIJ9AIbAwULCQgHAgYVCgkICwIEFgIDAQIEAQIXgAAKCRDSK0mem6di
mdRJDAC7af9H9foPYsWQgy00L3JPtLpkjLjCpEQTwIthqltPyPT0yMpJsGcJGDii
c6INH6/BRdM3hUNyrJCUNAgdliJbb70oJ4VhAIukHF8MjesbWNXQByLYPB3GwZXA
/e5i4Fad8dlHurlGdAFSjX4XasTpW7vnMEyPSd0CSi64LIRhhLT6fCSUR02IRAcN
o9A2JzG1CiucflsipkRrwpI8Lb2iSB0+gMb0MB5m0SfpckiwyLmP69qWJ7MGWnXp
7jnDE14Pr07+rKdKNXzf6Gu2Lkw/N8cTkfGikdywrQl07GIXHpd3yriRv3fpHgVA
lUoncPyp22k6FxxMxRGQrF0Bvz+MP/K9rB4r/+vWxGY/T0YnFydDw5Vxvk7crllG
rhw2LR0D9vtYyzANu7wum0l7/SM+fVxhbavHj0fCeEQPtstbZUZMv3c4v+JdrQix
9aaB5nmqXhYtUsUaDDt7tVRa1oqoYHnSUurKM24HYjmkfpJ95YiSkMaLwnGtM8zF
vroZhna5AY0EYxIJ9AEMAMonZ1XeKgXCjV09++3ic/HU9scLoLI+Fx0tKanCfxFK
6V1l8fistGyKnMxGJGUZUJD0cv0MTprg9h7FuDQkGWzUW1md0RJu/TUuysSf/pYhF
PHb03Q/MnYTK3nbc6jVaYC4sMj9z3+6YjIyI2kW5q80FeZz/mvP+GWS63KFtKtuo
uQJ8u0E0+vT/99CTnY63zZtFE7siArN6tKX+Ez1YMgZb9mxDf3xmYXj9k9uqe8HC
PxyJEIq5gu5R08vpYgEh2jFjQMtJqmH3ZCfoBhZWh0AxNJcDQ8WH/Vy/kBYtMMq/
```

```

/e5i4Fad8dlHurlGdAFSjX4XasTpW7vnMEyPSd0CSi64LIRhhLT6fCSUR02IRAcN
o9A2JzG1Ciucfls1pkRrwpI8Lb2iSB0+gMb0MB5m0SfpcikiwyLmp69qWJ7MGWnXp
7jnDE14Pr07+rKdKNXzf6Gu2Lkw/N8cTkfGikdywrQl07GIXHpd3yriRv3fpHgVA
lUoncPyp22k6FxxMxRGQRf0Bvz+MP/K9rB4r/+vWxGY/T0YnFydDw5Vxvk7crllG
rhW2LR0D9vtYyzANu7wum0L7/SM+fVxhbavHj0fCeEQPtstbZUZMv3c4v+JdrQix
9aaB5nmqXhYtUsUaDDt7tVRa1oqoYHnSUurKM24HYjmkfpJ95YiSkMaLwnGtM8zF
vroZhna5AY0EYxIJ9AEMAMonZ1XeKgXCjV09++3ic/HU9scLoLi+Fx0tKanCfxFK
6V1l8fistGyKnMxGJGZUJD0cv0MTrpg9h7FuDQkGWzUWlmd0RJu/TUuysSf/pYhF
PHb03Q/MnYTK3nbc6jVaYC4sMj9z3+6YjIyI2kW5q80FeZz/mvP+GWS63KFtKtuo
uQJ8u0E0+vT/99CTnY63zZtFE7siArN6tKX+Ez1YmgZb9mxDf3xmYXj9k9uqe8HC
PxyJEIq5gu5R08vpYgEh2jfjQMtJqmH3ZCfoBhZWh0AxNJcDQ8WH/Vy/kBYtMMq/
lUkFRZhgSfgJiAB3B8nnLY3ohD2K2DaKopGeJy16Kb29hy+CgS0Rq7HixlVPiUqg
CtYAK4CEDsX98AAWYP3k0Y6v03t/twbYXTvBuZ7X+bcZlouIG2wwidBCCi3apG1W
S+CFZdmQ1NPR6SV++CvgairymqMDh/Fp6Mib4jG30niTi5Mc3AF+yEvXIcD2hWcy
9oq8LPLeQDvc/TYS1HqFeQARAQABiQG2BBgBCAgFiEE78Up0BtCSTKxukU50ijp
npunYpkFAMMSCfQCgWwACgkQ0ijpnpunYpmQlgwAiAdkzsYfm7nhg0gMZ2LevRNP
BSBfAO+G2a9HEJWnlUKua1lqM2dHgTvKYYX16Fq3G0tbPHJtAmCQTS6u3CaT5gW3
bAa2gcc0pqfBNq38iS9IFhwLudCOWRB5y3TnqcbuIE3dqj7wMut/7EFEheWSfpeY
Jw4fLUDECD+IRdWZ7hcCzpMo8vAUp6qaIGNJudmkf94cGFRj28LX6fgKl3sR2hjd
ZxGDJ0ya61u5nwlYQbCxXoY61PP0d3gHWKqBU2os8JkFo1reLlBSXYgUtAc/G4RW
pS2LSUXZAWsjpJwJFgm0raeoyLZjTv6YATXenY/7Gq3zxy68CzzipxLfPtEfoKzo
ZN1NHgzg3/peQXYa6mX5lhQE1RJ2D0mY2UZD3CUT219z0sNisMiCTAlw99viR6jn
gHMZ4WJkaeJiMwQvoNqa5yztR6Gk+P0JPjpYbLyFGzJtnnxDeVI3aAphKCd05sqf
dNGb7ePEgLP/nxY+vjaob+2xEYhJZKnVcLYcIj0c
=ViUT
-----END PGP PUBLIC KEY BLOCK-----
uca@debian:~/laboratorio1$

```

```

uca@debian:~/laboratorio1$ gpg --export-secret-keys --armor 00132820@uca.edu.s
v > ./my-priv-gpg-key.asc

```

Creación del archivo miguel.gpg con su llave pública

```

Terminal - uca@debian: ~/laboratorio1
GNU nano 5.4                                miguel.gpg *
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGL9UfkbDACL5f/WNANYgFzsyv2pWu0QM85jwW/v0Hc4/3ZPl1+v3r/gjWJ
nGJBg7Ttp0Gi13ZoucAVkzUFqcR6m9d5ovf0h1TVGs7/yW21u0oXsENduA6Sul01
HPGMH5F/AwR32CuqjDcR8U81aL53cYp069Ygh76JJcLwXZvhtXRRHi+Gy413DZJC
XdXtx/bX4lmlZ5ItjjkEpLfd2d7TViPgCflBVgblX4LtrRtBfIxyv1iYp6tVbGfl
0xMH7IkHLY5cFKAT/WQ+Yp9f+lKEDOML59qN0UDqYJsyCY0svPYLMxXZT0HIi1FB
+Dy0YTxovTTaJz4NCrPK2ljLU3NLLktGfbRumeJfTLl/mwkyPUFBjh846D0WCoza
kzx/TS3Zj4qZyqTvV4AjU++HeK9LzaFvT+zKPuHZsfscnSF3p1AnswbYmVCu7Ad+
6hYcbWuV0IPWxnM8v+dszjZDl9vjeJJQw3eynT9p5RLVL4XhQa+taigilIqPjBjg
qouZQBeW2G076ZUAEEAAbQ2bWlndWVsIHJpdmFzIChjbGF2ZSBmb3IgdWNhIHNL
aSkpPDAwMDg3NTE4QHVjYS5lZHUuc3Y+IQHUBBMBGCA+FiEE/kL6ausnVZWwk9Tz
Iv2YEJp6scMFamL9UfkcGwMFCQBPgGAFcWkIBwIGF0oJCAsCBBYCAwECHgECF4AA
CgkQIv2YEJp6scMnSgv/U6EQ0wk20dwjkPaLkwXXWuAu7oysq+0TTbhNuqSpun3Z
l12pQnlg1W90+XqrFze1k6+a4RodLUs6IQjRXINrcuqpGwEZ028bUgyvzzB0D0el
r+tPwpGKS80d+9xEvQqnMaxhWS5ddRRLCgJoNybXMeZ3svtX4wKWzPqHUPfj+WoW
QodmDuGELhE1Fgh2m0PPclIGZ3pJn3dxY+u0bB7E2fnhhrpk22rqP0wb8U53K2DV
B06367bggZAWFU4JRjevzTVxo4sJcjWTFal7fIiJcWwfjwUiqx1Z3GD3UzHt400N
3uuKLvYLLsG3uZ9dE1J8EKn5DdgcYimiX3o2xAfzrAKcY3SbkKXXD+4CP/fj5xfs
GSml7YYjvm5LJYu8gy/pbP/kiF7x2ca9dYEUzu9vq3+u1uPW/xIFXNJf2UaLGiUL

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line

```



## Creación del archivo nestor.gpg con su llave pública

```
Terminal - uca@debian: ~/laboratorio1
File Edit View Terminal Tabs Help
GNU nano 5.4 nestor.gpg *
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQGNBGL9PsYBDADwGye3bdKckImLEiC8PZ5PF2z9x3J2VH5DaPtJrcwDN7g5DC7
TTR2hHXmKcmpgkAPhDo/Hz1kIpJgKgiCfuquxdQ0wxxCeHrtv004sAzxPa/utGLf
+iRgKto9y0EI4W9IMzkluzp0fN4JBr/08hwLRNfcR5wu5ZCgDliZSDK3vDop16LM
k+yGVqzcp/gGt35fBbx9acdYHEaRTUheqKz3mIMEErfsf6qYj/NuLszqKCJH8edV
c+FqNjD2A/RB/8H3IVB+5VSBnggF50+UIHzejzrFLpI0wQ+qvJ0Eb0wq0rMRLAYs
5IfCpsC4WnruvY6rgHBfUKuPnXg5J+WFMM3nJjJQd8PP9oyodnrVa09W/lGn0Qzj
gn7RwmlHKn+VHVR9f9c7BIEBZ4CRHHE3+4Dr19+V6B7EeBT7S3xgHbLsd2qg/1BK
XxhjSZsmgsSYwrX2H0FM+RwYpBsmUJgXrG7sxJzL5eyB3w9+gdUvXMaapCM6vIiV
PhBjNLPwR5wv4/MAEQEAAbRVTmVzdG9yIFNhbnRpYWdvIEFsZGFuYSBSb2RyaWd1
ZXogKEduVHUCBHdWlkZSAteEZvciBVQ0EgaW4gU0VEKSA8bmFsZGFuYUB1Y2Eu
ZWR1LnN2PokBzgQTAQoA0BYhBJ7ma0RsDnvBt05t6ctYQxiVipICBQJi/T7GAhsD
BQsJCAcCBhUKCQgLAQWAgMBAh4BAheAAAJEMtYQxiVipIC2fAMAKrYhMjLhq8C
iewmzqV3cym1fd5+4D2oH2bpRxPEICge3y0A0EmFZWjNWybJSWL7VncTuU9wbRUZ
IxMAqH9xINiY0Gopf0JZ2dVj5KpVH7gmCllGU35WPBWvafsaC5rvexkDHptx92x+
Sm03Nl7biNyiG8gSz/1jVP6SnS3Nfv9N2/xjkhcgI5f5DUIaYIUUSVR6I407YIBN
i5TNfFzglm9V+TY0K7JkFxCgdqgB7CkxXQrWlwojps0xhJulc2Y0dzY9qnofn3Jw
tw0K8xSYCK9N4oUCLLD+zD1zJFjkefc8ziWhEM93+I4K/oD3P0zhJMQ+wQo1QE1p
uAQ9+YEcAz2hKDrT+2zJhFSK384FUSD/uuVg3Ddg6M5QsalwC/fwBLE/50SqtL71
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

## Importación de la llave de Miguel

```
uca@debian:~/laboratorio1$ gpg --import ~/laboratorio1/miguel.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:~/laboratorio1$
```

## Importación de la llave de Nestor

```
uca@debian:~/laboratorio1$ gpg --import ~/laboratorio1/nestor.gpg
gpg: key CB584318958A9202: public key "Nestor Santiago Aldana Rodriguez (GnuPG Guide - For UCA in SED) <naldana@uca.edu.sv>" imported
gpg: Total number processed: 1
gpg:      imported: 1
uca@debian:~/laboratorio1$
```

Se muestran todas las llaves que se tienen

```
uca@debian:~/laboratorio1$ gpg --list-keys
/home/uca/.gnupg/pubring.kbx
-----
pub   rsa3072 2022-09-02 [SC]
      EFC529381B424932B1BA4539D228E99E9BA76299
uid   [ultimate] Alejandra Villalobos (labo1) <00132820@uca.edu.sv>
sub   rsa3072 2022-09-02 [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]

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

uca@debian:~/laboratorio1$
```

Se edita la clave de Miguel para ver su fingerprint y se firma

```
uca@debian:~/laboratorio1$ 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) <0008
7518@uca.edu.sv>
      Primary key fingerprint: FE42 FA6A EB27 5595 B093  D4F3 22FD 9810 9A7A B1C3

gpg>
```

```
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 "Alejandra Villalobos (labo1) <00132820@uca.edu.sv>" (D228E99E9BA76299)

Really sign? (y/N) y

gpg> quit
Save changes? (y/N) y
uca@debian:~/laboratorio1$
```

Se edita la clave de Néstor para ver su fingerprint y se firma

```
uca@debian:~/laboratorio1$ gpg --edit-key naldana@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.

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
pub rsa3072/CB584318958A9202
   created: 2022-08-17 expires: never usage: SC
   trust: unknown validity: unknown
sub rsa3072/A247B11A728618C7
   created: 2022-08-17 expires: never usage: E
[ unknown] (1). Nestor Santiago Aldana Rodriguez (GnuPG Guide - For UCA in SED)
<naldana@uca.edu.sv>

gpg> fpr
pub rsa3072/CB584318958A9202 2022-08-17 Nestor Santiago Aldana Rodriguez (GnuPG
GP Guide - For UCA in SED) <naldana@uca.edu.sv>
Primary key fingerprint: 9EE6 6B44 6C0E 7BC1 B74E 6DE9 CB58 4318 958A 9202

gpg> sign

pub rsa3072/CB584318958A9202
   created: 2022-08-17 expires: never usage: SC
   trust: unknown validity: unknown
Primary key fingerprint: 9EE6 6B44 6C0E 7BC1 B74E 6DE9 CB58 4318 958A 9202

Nestor Santiago Aldana Rodriguez (GnuPG Guide - For UCA in SED) <naldana@uca.edu.sv>

Are you sure that you want to sign this key with your
key "Alejandra Villalobos (labo1) <00132820@uca.edu.sv>" (D228E99E9BA76299)

Really sign? (y/N) y

gpg> quit
Save changes? (y/N) y
uca@debian:~/laboratorio1$
```

Ahora se muestran las llaves públicas con su valor en "full"

```
uca@debian:~/laboratorio1$ gpg --list-keys
gpg: checking the trustdb
gpg: marginals needed: 3 completes needed: 1 trust model: pgp
gpg: depth: 0 valid: 1 signed: 2 trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: depth: 1 valid: 2 signed: 0 trust: 2-, 0q, 0n, 0m, 0f, 0u
gpg: next trustdb check due at 2022-10-16
/home/uca/.gnupg/pubring.kbx
-----
pub   rsa3072 2022-09-02 [SC]
      EFC529381B424932B1BA4539D228E99E9BA76299
uid   [ultimate] Alejandra Villalobos (labo1) <00132820@uca.edu.sv>
sub   rsa3072 2022-09-02 [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]

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

Se crea un archivo history.txt con el historial de la consola

```
uca@debian:~/laboratorio1$ history > history.txt
uca@debian:~/laboratorio1$ cat history.txt
 1 mkdir laboratorio1
 2 cd laboratorio1
 3 touch saludo
 4 nano saludo
 5 cat saludo
 6 file saludo
 7 md5sum saludo
 8 shasum saludo
 9 sha256 saludo
10 sha256sum saludo
11 sha512sum saludo
12 shasum saludo
13 sha512sum saludo
14 sha512sum saludo > checksaludo
15 ls
16 cat saludo
17 cat checksaludo
18 sha512sum -c checksaludo
19 nano saludo
20 sha512sum -c checksaludo
21 gnupg
```

Se cifra el contenido del archivo de manera simétrica

```
uca@debian:~/laboratorio1$ gpg --output history.txt.gpg --symmetric history.txt
uca@debian:~/laboratorio1$ cat history.txt
```



Se muestra el archivo cifrado

```
uca@debian:~/laboratorio1$ cat history.txt.gpg
00W[00r000000$00000Y;TGv0
.Fa060e0QR08[0]bk00!0yE000CAY|0D
0&00^ 0D00U00000:_0GL000)cI;0000|0 X00~003{000[0A0!|0VW0}yk000D{000030 °fo0f
Z000$000000
0|q0*L0Ip0000Ää"frb2070A 00D04o00}000y0?h7.c000h%0-000x0Md0S&0i0+ {
0000vz0$h$D000DG010 05
{y^0
+k_q0 PbSU[00
B000R[000zE)0000P
00
0.n000000-C#}x0{0000;00@00000mr\t0LR2b000(*0(0ij0R0P0a00=0L-0b0%N]0.(10^=0
^
06000uca@debian:~/laboratorio1$
```

Se crea otro archivo con el historial

```
06000uca@debian:~/laboratorio1$ history > historyPublicKey.txt
uca@debian:~/laboratorio1$ cat historyPublicKey.txt
1 mkdir laboratorio1
2 cd laboratorio1
3 touch saludo
4 nano saludo
5 cat saludo
6 file saludo
7 md5sum saludo
8 shasum saludo
9 sha256 saludo
10 sha256sum saludo
11 sha512sum saludo
12 shasum saludo
13 sha512sum saludo
14 sha512sum saludo > checksaludo
15 ls
16 cat saludo
17 cat checksaludo
18 sha512sum -c checksaludo
19 nano saludo
20 sha512sum -c checksaludo
21 gnupg
22 sudo apt install gnupg
```

Se cifra el contenido del archivo de manera simétrica con la clave pública del receptor

```
uca@debian:~/laboratorio1$ gpg --output historyPublicKey.txt.gpg --encrypt --recipient naldana@uca.edu.sv historyPublicKey.txt
uca@debian:~/laboratorio1$ cat historyPublicKey.txt
1 mkdir laboratorio1
2 cd laboratorio1
3 touch saludo
4 nano saludo
5 cat saludo
6 file saludo
7 md5sum saludo
8 shasum saludo
9 sha256 saludo
10 sha256sum saludo
11 sha512sum saludo
12 shasum saludo
13 sha512sum saludo
14 sha512sum saludo > checksaludo
15 ls
16 cat saludo
17 cat checksaludo
18 sha512sum -c checksaludo
19 nano saludo
```

Se muestra el archivo cifrado

```
uca@debian:~/laboratorio1$ cat historyPublicKey.txt.gpg
000G00r00
00$0E [000y'0000~000:0T|n}0Γ`00500æ00Wg0Q000008050,Y0000wH2wL$700B
U0t)
0/0t000weH
N
R0 /0j00u0 00v?0.(J0Zu00q0}t1m|0C00B000~00]v000C00
00||0hHJ!000N000900{0000b
M0A0000#00易D9 /V00)0,0s=000ri N0'0z000000@L0I q#G00,000000JXD000jr000N000r0Z~0
P00]C00E0>00000b0}0;)0io0C0\00W00糖3040=0g0(00+000S0$00n0C00B0B0t00Vp00z0v A
#(00'000L4R0eo00R000u0030/hp0[f030.$d0000Q0q&0}00J0$b0
g0010
0000000V0j000=a05|V00
K00U0000c;0Ns00o[&0cmx0[~ 05000g100
t[A00@G0T^ognT 0
0 0rp0;0n00'0'0050iH00\g0(I0LP0X00(z0.x0s#00a200400A0W0)G9000a0
0V00n0@>000-,0K^N 000Y0500V0006(000c0b
iYo0k0
>0J00\;0y0A00}N00#000r0i.0,0c0300@00-T0D000c0S000k@G0]Z00f0[70J00Dl0!
```

## Ejercicio:

Creación del archivo con la llave pública

```
uca@debian:~/laboratorio1$ gpg --armor --export 00132820@uca.edu.sv > alejandra.asc
uca@debian:~/laboratorio1$ ls
alejandra.asc          historyPublicKey.txt.gpg  my-priv-gpg-key.asc
alejandra.gpg          history.txt               my_revocation_certificate.asc
checksaludo            history.txt.gpg           nector.gpg
historyPublicKey.txt    miguel.gpg               saludo
uca@debian:~/laboratorio1$ cat alejandra.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGMSCfQBDADGtnDSTRbxzKckyefyo5IgH+jRgui6UUlezs+cEo3MhyWf7QJL
thRjqujKdoJ7jLRXs3QqF9eFVmx6tR76ITNkEdBBFlh4YZzuSvPMe2Ks0LfGujd3
28Txw/2jhGfNCUQ8umteWbm0oR1GK07iDnSxaysBLQZg+NqrMz+/B6BsL3ijJy5p
mQWVvh97ziAQALVGaxgcvZ2w4r2TyZYXr7eyE9JobfCU099XPiBQHzzmXq5v6DxY
egR/fB0a10qEGmPsqPo8YoXIENI9ECUfrn8JWUVdTGDLB11FQ266zzM7Ax1HmTZl
gRkw2I0tatzm0qcp1+uXeHuhIr5o90LKswIvsHS2/8iv30p1xoB3j7LjtD5FRpkA
GSClljCsL9TSDB1M4t+DjeTSAfvY6im84JqteCRahixjAb1t09YtC6y5nLN0nKRF
3Bc9T8lsiSxcYQERiyd3NIb1cGmLR6ZQ+BN2crCENTuyGW+a4DPgkGELDPM3SG1A
JjSIRoDVoJwVRV0AEQEAAbQYQWxlamFuZlJhIFZpbGxhbG9ib3MgKGxhYm8xKSA8
MDAxMzI4MjBAdWNhLmVkdS5zdj6JAc4EEwEKADgWIQTvxSk4G0JJMrG6RTnSK0me
m6dimQUCYxIJ9AIbAwULCQgHAgYVCgkICwIEFgIDAQIeAQIXgAAKCRDSK0mem6di
mdRJDAC7af9H9foPYsWQgy00L3JPtLpkjLjCPEQTWItHqltPyPT0yMpJsGcJGDii
c6INH6/BRdM3hUNyrJCUNAgdliJbb70oJ4VhAIukHF8MjesbWNNQByLYPB3GwZXA
```

Se firma el archivo con 3 métodos

```
uca@debian:~/laboratorio1$ gpg --output alejandra.sig --sign alejandra.asc
uca@debian:~/laboratorio1$ gpg --output alejandradetach.sig --detach-sig alejandra.asc
Invalid option -c
uca@debian:~/laboratorio1$ gpg --clear-sign alejandra.asc
uca@debian:~/laboratorio1$
```

Se cifra el documento para que pueda ser descifrado por Miguel y Nestor

```
uca@debian:~/laboratorio1$ gpg -e -r naldana@uca.edu.sv -r 00087518@uca.edu.sv alejandra.asc
```