

## 1. Clave generada

```
labo-miranda@debian-labo:/$ gpg --list-key
/home/labo-miranda/.gnupg/pubring.kbx
-----
pub   rsa3072 2022-08-25 [SC]
      EEFEEFCF19FC2D792FB1BE066F573C831873A124E
uid    [ultimate] Marisol Abigail Miranda Flores (Laboratorio01 S
ED - Miranda) <00086320@uca.edu.sv>
sub    rsa3072 2022-08-25 [E]
```

## 2. Clave pública en ASCII

```
labo-miranda@debian-labo:~$ gpg --output miranda.gpg --export 00086320@uca.edu.sv
labo-miranda@debian-labo:~$ gpg --armor --export 00086320@uca.edu.sv
-----BEGIN PGP PUBLIC KEY BLOCK-----
```

```
mQGNBGM8YyBDAC4Yu/pZt/QUseLGrehrSegu3wIGFjk0JH5odJPsbHHQMKIEibJr
COTBgFIMjlcFBZow5tooaXxLpFHjKRGiI6LQ7+i66SPYwJksUivw7C5RBXHC0Xc
5wYGI01hkX+YNapUpFtg61u1gmMvid2ACuquFQ2DHHJ3qBKSnbQI5hk04efRLE/L
NiNUmATIHVjWbYeg22XhMRfrf4i5Zz0R1vr4t2d18pu0RaJGZLTHp/K1drk01bN
tDYKt/b3Bb0Uwalc9FwdjA17X0QLw0BGcPLNe0iS3o94bCI0p+tjv0fS8sWtRMH
gzb3/GqWLRXoFD71086yngluHkrdKgtug0lsFnHGIWXBpzEBonjeJLnW04aeJZ
qMr5UtgiSCqBVoRQGNwNoeNhmap7c4DT9EhayJ6JLF3I3W6DaASvdLIAAKJBEGTZx
v6rJtkIMNRDR02nPN3PxEKbLog8JEsQn7oqZ/azfsXL0tyf9IIsRwz024x+5S4J85
FvPB0teaJX6CkgAEQEAABRSTWfYaXNvbCBBymlnYWlsIElpcmFuZGEgRmxvcmlvZy
IChMYWVvcmlFb3JpbzAxIFNFRCAtIElpcmFuZGEpIDwwMDA4NjMyMEB1Y2EuZWRL
LnN2PokBzgQTAQoA0BYhB07+/PGfwteS+xvgZvVzyDGH0hJ0BQJjBvGGAhsDBQsJ
CAcCBhUKCQgLAQQAQwMBAAh4BAheAAAOJEPVzyDGH0hJ06FYl/0r4gauK/I08Bjqv
+P2BpQ0/HLWARjU0wUDDktNf84uI9L5318BRB7yi+fV5dgkhpKtCtVfYBv+Mknam
I2VNkg12/6bauuFJ1iPLFhy/+ngufjH8I3PhLFX/49xmA6T0u4AFYA0fNbKDdLTP
+bbDbHczdVlVec0k9XF8mk0QfFY5Qi38N1Ve+wDMYzVXW4Q08UqvieDmwvVwzGEw
YqAxMpItQ64EkoD+kq7PclVsXfGBDBrlzzppRSUcBfQtKwZLlqV6mNYy/REOE7z
vGBEGf8a514wzBA0+ZAQX0buwzgi4Y6dFwWJundGELI4MUQKEamVvcp157gdEfKn
k90tpURik4Y1QFMQGaAwgn5pK/ubckMpu145/rDU4w9MCddi0aE0ulegp+xeaD4E
Phnb/Z1QrmomFoaUhsz+mSgnRL3/05+Xr/vE0uTR4/pWNX6JWKKqNXS1HwmKT5JM
969pj5Y09txtLZNZqSkVu5o0G3RPmnowUBSX/XRTme1bIw70rkBjQRjBvGGAQwA
qRwPDK2nps5Ng7LL2V3VELuK8Iag7zcz99ya63m/bAfTPReZpd1q91dcX+ADY6Fn
sMjahDLycRWCi6aLaow9Qr6aMBtU90+LY+CC3PzNTKxD5uY73xm1EbWEWKFCcNQ
hNTF9IsVdcrrFbrzIdcikhE4I/8G9xYALANpdNVmgY6acNLGy/EHVPy/Z33z9AR
gRd2jQ2nXp96osPEZvd4KGVu5ipulJG1035mPM0qLRTXsB2LlVbYXj8P08spm6h
2gunELPo+a+mZ3VEy6sD4oRe+9i9YNZP7mzRgRWn6D2SBA0PBf1dLCHGMVibfKnX
C5RobSr9bS9P58M9+W2KU6fiVeMoSAxWLWIZ0AjmW892k3jPeZVmwZNKsXpbh5sv
i+VfCW6eVn06EenAQKx/cv2VNs2YJmj3eUCR0wv7cpdjZwiHohdtfebQB8wvWYr
kwNLEJdhzRwVRzluGHJ4ujqZCpUybja2tS4eokCfrgFCTq3FG+ImKg0jC5CdL17
ABEBAAGJAbYEGAEEKACAWITu/vzxn8LXkvsb4Gb1c8gxhzoSTgUCYwbxhgIbDAAK
CRD1c8gxhzoSTuRCC/9wiWEuJE91FM00PCHY3th2UKWASMGp2vWk+hnGwdfapNBm
3FpHx6NIaXhtZXqDR1x0EYaq6oW0J70Totix735coyElJl3lu1T1bcNd0qVvRHR
VL64GUovgilzYXs+mJunbip/luKBKV+wmPboKC7YELmfHYwomg61qv2t4aQqP/6Y
LbZPAwNq6cGnftKSvW3LNX8/5bHxW6kco0b/fQQXxgJmh64LQn0vGybcLZu0xPqV
BIvo09y8prN04aUBJ0HP3bI4MXm5hkbILz91PuXRQgTwACfNRGb6EgofKwczq/se
CgToYKVs3WAIIdnYS+8CJYc3l77dDWUiclz/9pTgU0y5qSi9+kAiPDmkDRd4ct5bE
CBjzWL25rCehq4jdDjH204Z/NLwGbJK0iSVFXzt5D53hTklKU5S0VDNRAYKN06fu
jMz8aaWu6KX7nnK32qpnCFr6NhmXdfKltr5YpdAUy0K7y6svWAFIzbGLow8AZwPt
kighCwyVC2s6x7KKnQ=
```

```
=t6Q9
-----END PGP PUBLIC KEY BLOCK-----
```

```
labo-miranda@debian-labo:~$ █
```

```
labo-miranda@debian-labo:~$ gpg --export-secret-keys --armor marisol > ./my-priv-gpg-key.asc
```

```
labo-miranda@debian-labo:~$ █
```

### 3. Lista de claves importadas (Miguel y Nestor)

```
labo-miranda@debian-labo:~$ gpg --list-key
/home/labo-miranda/.gnupg/pubring.kbx
-----
pub   rsa3072 2022-08-25 [SC]
      EEEFECF19FC2D792FB1BE066F573C831873A124E
uid     [ultimate] Marisol Abigail Miranda Flores (Laboratorio01 SED - Miranda) <00086320@uca.edu.sv>
sub   rsa3072 2022-08-25 [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 (GnuPGP Guide - For UCA in SED) <naldana@uca.edu.sv>
sub   rsa3072 2022-08-17 [E]

labo-miranda@debian-labo:~$
```

### 4. Archivo cifrado simétrico

```
labo-miranda@debian-labo:~$ cat history.txt.gpg
0      v00^fK0000Po      0080M008e0q0000003pH00K070*0N005000(00#0V0
000?000f9p0^00002f00
00,-00;@00Y000a0qnc000u20K000Qz_00Kc_C0s00C!c300i000H?0<0h0060v0
NF2h02040oJ0(L0V0z000
      00050000200Dbw0*00000000_0*00)F0aX0Лo<0v0000000@
o000R0A}*00000S0)000Lo0!400.0c1040Iu0?0H0m0000d00扭00&@1^A0/~M0000000
80cV000d000$0YaI-0I000t0006e00Y00><0"
sb0t[S=00p000[0;000w0200c00
!
      000#000?000H0T0
      00$>"0(0[0'00000*0*0000I0
0
0000*0i y0%.B000f0*3U00z04qp0600Ce00000000s0jFk($x0k]0000000+9008+mF
p/a00G0?0000G0100R0.000000Ng0zG000000!0"00.>000[00 0000:0a00C+F00
0000j000X.i=<000000[0^0lo0?x000t0000
      0000i00Y00
      0P_000030%0000)00B0000

labo-miranda@debian-labo:~$
```

### 5. Archivo cifrado Asimétrico

```
labo-miranda@debian-labo:~$ gpg --output historyPublicKey.txt.gpg --
encrypt --recipient 00086320@uca.edu.sv historyPublicKey.txt
```

## 6. Proceso de firma y archivos firmados

```
labo-miranda@debian-labo: ~
GNU nano 5.4 pk-marisol.gpg
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGMG8YyBDAC4Yu/pZt/QUseLGrehrSegu3wIGFjk0JH5odJPsbHHQMKEIbJr
COTBgFlMjlcFBZow5tooaXxLpFHjjKRGiI6LQ7+i66SPYwJksUivW7C5RBXHC0Xc
5wYGI0lhkX+YNapUpFlg61ulgmMvid2ACuquFQ2DHHJ3qBKSnbQI5hk04efRLE/L
NiNUmATIHhvjWbYeg22XhMRfrf4i5Zz0R1vr4t2dl8pu0RaJGZLTHp/K1drk01bN
tDYKt/b3Bb0Uwalc9FwdjAl7X0QLw0BGcPLNE0iS3o94bCI0p+tjv0fS8sWTtRMH
gzb3/GqwLxRXoFD7l086yngluHkrdKgtugg0lsFnHGIWXBpzEBonjeJLnW04aeJZ
qMr5UtgiSCqBVoRQGWNoeNhmaP7c4DT9EhayJ6JLF3I3W6DaASvdLIAaKJBEgTZX
v6rJtk1MNRDR02nPN3PxEKbLog8JEsQn7oqZ/azfsXL0tyf9IsRwz024x+5S4J85
FvPB0teaJX6CkkgAEQEAABRSTWFyaXNvbCBBymlnYWlsIElpcmFuZGEgRmxvcmVz
IChmYWJvcml0b3JpbzAxIFNFRCAtIElpcmFuZGEpIDwwMDA4NjMyMEB1Y2EuZWRI
LnN2PokBzgQTAQoA0BYhB07+/PGfwteS+xvgZvVzyDGH0hJ0BQJjBvGGAhsDBQsJ
CACCBhUKCQgLAQWAgMBAh4BAheAAoJEPVzyDGH0hJ06FYl/0r4gauK/I08Bjqv
+P2BpQ0/HlWARjU0wUDdktNf84uI9L5318BRB7yi+fV5dgkhpKtCtVfYBv+Mknam
I2VNkg12/6bauuFJliPLFhy/+ngufjH8I3PhLFX/49xmA6T0u4AFYA0fNbKDDlTP
+bbDbHczdvLVec0k9XF8mk0QfFY5QI38N1Ve+wDMYzVXW4QQ8UqvieDmwvVwzGEw
YqAxMpItQ646EkoD+kq7PclVsXFgBDBrlzzppRSUCBfQtkWzLlqV6mNYy/RE0E7z
vGBEGf8a514wzBA0+ZAQXQbuwzgi4Y6dFwwUundGELI4MUQKEamVvcpl57gdEfKn
k90tpURik4Y1QFmQGaAwgn5pK/ubckMpui45/rDU4w9MCddi0aE0ulegp+xeAD4E
Phnb/Z1QrmomFoaUhsz+mSgnRL3/05+Xr/vE0uTR4/pWNX6JWKKqNXS1HwmkT5JM
969Pj5Y09txtLZNZqSkVu5o0G3RPwmnowUBSX/XRTme1bIw70rkBjQRjBvGGAQwA
qRwPDK2nps5Ng7LL2V3VELuK8Iag7zcz99yA63m/bAfTPREzpdLq91dcX+ADY6Fn
sMjahDLycRWCi6aLAow9Qr6aMBtU90+LY+CC3PzNTKxDb5uY73xm1EbWEWKFCcNQ
hNTF9IsVdclrrFbrzIdcikhE4I/8G9xYALANpdNVmgYe6acNlGy/EHVPy/Z33z9AR

[ Read 42 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justifv
```

Primer forma de firmar

```
labo-miranda@debian-labo:~$ nano pk-marisol.gpg
labo-miranda@debian-labo:~$ gpg --output pk-marisol.sig --sign pk-marisol.gpg
labo-miranda@debian-labo:~$
```

Otra forma de firmar

```
labo-miranda@debian-labo:~$ gpg --output pk-marisolm.sig --detach-sig pk-marisol.gpg
labo-miranda@debian-labo:~$ gpg --verify pk-marisolm.sig pk-marisol.gpg
gpg: Signature made Thu 25 Aug 2022 12:59:50 AM CDT
gpg:          using RSA key EEFECF19FC2D792FB1BE066F573C831873A124E
gpg: Good signature from "Marisol Abigail Miranda Flores (Laboratorio01 SED - Miranda)
<00086320@uca.edu.sv>" [ultimate]
```

Puede ser descifrado por Miguel y Néstor

```
labo-miranda@debian-labo:~$ gpg -e -r "naldana@uca.edu.sv" -r "00087518@uca.edu.sv"
pk-marisol.txt
gpg: can't open 'pk-marisol.txt': No such file or directory
gpg: pk-marisol.txt: encryption failed: No such file or directory
labo-miranda@debian-labo:~$ ls
Desktop          history.txt      Pictures         Public
Documents        history.txt.gpg  pk-marisol.gpg  Templates
Downloads        miranda.gpg     pk-marisolm.sig Videos
historyPublicKey.txt  Music
historyPublicKey.txt.gpg  my-priv-gpg-key.asc  pk-marisol.sig
pk-marisol.txt.gpg      pk-marisol.txt.gpg
labo-miranda@debian-labo:~$
```

## 7. Configuración de GitHub

Git y la verificación


```
labo-miranda@debian-labo:~$ gpg --armor --export EEFECF19FC2D792FB1BE066F3A124E
-----BEGIN PGP PUBLIC KEY BLOCK-----
```

Agregando una clave GPG

### GPG keys

[New GPG key](#)

This is a list of GPG keys associated with your account. Remove any keys that you do not recognize.




**Public Key SED**

**Email address:** 00086320@uca.edu.sv

**Key ID:** F573C831873A124E

**Subkeys:** AD8050235EB67213

Added on Aug 25, 2022



[Delete](#)