

CAPTURA DE PANTALLA DE CLAVE GENERADA

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

"Alejandro (GnuPG Guide - For UCA in SED) <00109220@uca.edu.sv>"

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: /root/.gnupg/trustdb.gpg: trustdb created
gpg: key 3B465154DE3989B0 marked as ultimately trusted
gpg: directory '/root/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/root/.gnupg/openpgp-revocs.d/BF8F38E25F37689566F103303B465154DE3989B0.rev'
public and secret key created and signed.

pub   rsa3072 2022-08-24 [SC]
       BF8F38E25F37689566F103303B465154DE3989B0
uid           [ultimate] Alejandro (GnuPG Guide - For UCA in SED) <00109220@uca.edu.sv>
sub   rsa3072 2022-08-24 [E]

root@debian:/home/uca#
```

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

220@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  2 = Key is superseded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? 0
Enter an optional description; end it with an empty line:
>
Reason for revocation: No reason specified
(No description given)
Is this okay? (y/N) y
ASCII armored output forced.
Revocation certificate created.

Please move it to a medium which you can hide away; if Mallory gets
access to this certificate he can use it to make your key unusable.
It is smart to print this certificate and store it away, just in case
your media become unreadable. But have some caution: The print system of
your machine might store the data and make it available to others!
```

LISTA DE CLAVES IMPORTADAS

```
root@debian:/home/uca# 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
/root/.gnupg/pubring.kbx
-----
pub   rsa3072 2022-08-24 [SC]
       BF8F38E25F37689566F103303B465154DE3989B0
uid           [ultimate] Alejandro (GnuPG Guide - For UCA in SED) <00109220@uca.edu.sv>
sub   rsa3072 2022-08-24 [E]

root@debian:/home/uca#
```

COPIA DE SEGURIDAD DE CLAVE PUBLICA EN ASCII

```
root@debian:/home/uca# gpg --output alejandro.gpg --export 00109220@uca.edu.sv
root@debian:/home/uca# gpg --armor --export 00109220@uca.edu.sv
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGMGgRoBDADWkY56esNVzkma49rLNNFrGfXhB3biD5+wsN+i2LPdM8W/MvWU
2GIeP088Yj63CzGAvg0sJRIfJ3LoRUh/Vu8XwUyPdlt+aE1wiTw/aqsdgB5VboTk
mvRtNEZeNln4JCwIibVJ9FdQs4IJ6lKZGhckb16fPR6Je48Ns953fhX045+Ny3Pf
4XXyFCMGDc+zDf+bq7SFwTWKSOUViGHAmB/LJuCTP//rYRVs0JlchjzW20BtCala
AncMu20kWPeSUH3YWy2YGh1GLofxo0dP13EGb/vev6n/Zz5K3dKaWuD3qbM4nac/
H1FhEIJQa178HVeJA/0EGhNZX+aCF5De2aTtePu9Y3WFAxN0xg6oYxl0t00Wel0N
fUmgydwdlAco0ZA0UW1cDgGUUGeDASGNK9iKfTkIkL6qo0Kbu+VTIiYSloZVqd8h
vp+q9ML7w7o19//27rfNhbaTKAlnBx6d+5x73h464se1GzML2kjpna4hhgEkmkGV
DZwQIGlqBZbhqtEAEQEAAAbQ/QWxlamFuZHZJvIChHbnVQR1AgR3VpZGUgLSBGb3Ig
VUNBIGluIFNFRCKgPDAMTA5MjIwOHVjYS5lZHUuc3Y+iQHOBMBBCgA4FiEEv484
4l83aJvM8QMw00ZRVN45ibAFAMGgRoCGwMFCwkIBwIGFQoJCAsCBBYCAwECHgEC
F4AACgkQ00ZRVN45ibBBEwv+IzdadI7NJ5sX+B2oc2ZDyP4ntvg9FBpAWNGWRFyn
HYxhnmFK0wR+Wy3AlAg+TY8UJyWFLiZ4FeNNZcy7D1QqGb1zicAueWwXtwxKyK/
ODVHUHF151Vy2TnYRwCFQsLujyNl4j1o64yIiVKpgQVBlC49XLM69pQ+kDmUxh6s
Uv3sLGaFfU3sH0gMS+pCtll37Si3t8WlpwMuZhV8e6yLqX1gpKqK0h3Ii0b05rGG
io1aRGUJkPwIwgxrxdqTX+Pb0Sz0dpa79m8VEEU3YCY1UsNhGwMbNncNc7+3ESl
137sbd528VJJfGHH9Hc8PNLctNSuoEuTIJntN3EGScQ8Pr8GHbw0CuP0fAhTz84Q
5XS+SEAUxNxi+CPuXh6U71CYJct+mDHsVDFfVTr0Gxe2YZ/W/Jm2XAFHJVD1NZp6
9rQfCN6FKihJiQ/LoUDwdewIzgQffjH30babXtYUSrXrqomzCrqGrE87nLnw+HxF
HEjYZNXq2bH8Umdr652H4zXjuQGNBGMGgRoBDAC+JqVden5vPpwwT6hYRR7NW7V
+DaN86FuGPBncdpdlxHgfkq4SloqVU7fC9NQNXKYr6g8y43s1Ji9HLdLk0n5Zvrj
04lE1KN3+TXfu9YPRWMSgoXTPxpkEuV2kMw12rC8uGPT4YbQX39nUbnxgjk82EFD
/iC4c1JnVapUj1t9HZdyc0HAv7djhfSg1qtC9f33T0g8Ent70g77T/0DzxP78pr4
k67vLm3BcdlqPtN6AT8K74LZ4edesux+Wq1x/LHA4qs8Nq0Wf0bx61AeLbgke6pj
T3fepz8S3DNG50P85bDo6U5SKTUhf5+HWynDf3U8szJ+Xw0YG417Q52D2uG+PmCS
+4LKgspszN3HDD0cEpD1e9Qt609YXtwQSAoSLmIt1Ks8ZYKsFwuWSj7EZ3FxHyFy
DN0K4PyA4FyaBZj6KCKrizWtZN0aJTVdvWsuNec6VLlXu0RK906GB0djy+8LPuRI
4wChYfm18UrnA7UGM7cEyajEoyF1gBgJgGCXcraEAEQEAAYkBTgQYAAQoAIBYhBL+P
00JfN2iVZvEDMDtGUVTe0YmwBQJjBoEaAhsMAAoJEDtGUVTe0YmwafkL/0U/i+0G
nI4+ykRE0rtAqUJLwgr0FxcocUw7BMf4Qh+xddggko/tzCEcwmBbzjVK0dwFpRNq
+vP2IkyhrWwc9vklUuf+1U6b7+gyaBBokiWskDJC2asP0ZKm6TlzzqN1raF2CmiY
K0J+6wmZ6RfGquleBLr8Lu+ELtkkb8NofduFXyghUHCtqfygrFEE2bRnHd3enAMK
6wEdU4nlWILUeBDETS0pJSfgCMawbQBRApVgrLvmjW2Kj0L5smEqjt78FkVvGLHg
pgkiQzExZF1X8LZswYSkxAWgT0zesTUedhvf8JmLRuIT0V2y07FflmwyYNedr77ZF
kCC/zqs850EMoFhSFwvse6/KlGfcbgq00HnbhuaiXFY3vZ7kfS0WvbjXCtSZwFmN
D1MI8cg5JukxpP8aDHg6t0QHUT8ydB6BvHV/xFq3Aadx+e6dIeYe+4QVHWZUt8V4
YTr0/wzj58YNxy7ckD0LrwQ0df4QizZEXv0JsfG0Z0NcTNQ0g2zR5007FA==
=IUBC
-----END PGP PUBLIC KEY BLOCK-----
root@debian:/home/uca#

gpg: Total number processed: 0
root@debian:/home/uca# gpg --import 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
root@debian:/home/uca#
```

CAPTURA Y ARCHIVO DE CIFRADO SIMÉTRICO

```

root@debian:/home/uca# gpg --output history.txt.gpg --symmetric history.txt
root@debian:/home/uca# cat history.txt.gpg
0xGD00000000000000
x:Bv000000Y0000Wi2000X00000IzK0,hVx0~[0]u<"000G0W05Ww10^0:00U00c0.0bb0|0gk00000k@f0_gVD0.
#0I00(c00e0 0b0A00CG000l]0,05k00000.0Pc00RY0AK00N0s0"-2t0)5\'00$$dKə0M0j0z08000U0(,, D000
gh00TX-0{Z00d,G0000:00u0\00000B0000;qfH'\:E0W00_0B00_\00c00"00n00g00 P0
005ku0000MuP0BE
05顚 r200g00T%
00IZM0000BW000E0Hj00GBDj0h00/u;0
0Z000o0Údl0sb
Q0?0K0a0000R_9000"ijU]Fv;:0 {00d
Y0#G00(I000,0\000g0
[00004[çTRWUyiU0`@0@0'0/0M00J
ã000rJ'j0770((u>70l'y00000Sn00000n0)[0~%0pS7X0000'root@debia
n:/home/uca# --armor
bash: --armor: command not found
root@debian:/home/uca#
root@debian:/home/uca#

```

CAPTURA Y ARCHIVO DE CIFRADO ASIMÉTRICO

```

root@debian:/home/uca# cat historyPublicKey.txt.gpg
00[0]00%
007000[0]Q!0E0A~3s^a0M000Dl00&000j=0:
y06e00002?0HP\ 00:0S0r0G0sTwG0{0000=50^L
0}000>00>0u%00Z|0_0;0[0]FS00b04R00iA0%D000UA0(0T0*00g00+0v00H000@0
06U'000&000s00r_>00&~3}0
000ll020h0000|d0
V0^000\N30K,00 0Ja00 fB.ÇN
cD040W0u000Y`l00H+G0S0[t00#<g000W00090a8/~0&K00\0cD00{0~0j000}00融<0j00004qñ,G0
)@K+00)0a0x000 0000^0k00sp00kd00-z0#m/RL>I0zL0005ag0%0G0^0xF04h000.U000000000A 0('0¥80?i
f0(00b02000*)q003ynW+G00H00R0007000@0A'E'00`0Lw00S+p
00z000700upRQ0,/00f;000
00ju00s0A000;J000^0}00Di0-000'DS;{0 `0[0]00g00w0004xW0Ui
yc000.00500 o*0000M0|0}00+0493
u00000Y000t$0t 4000E0XZ0000l0G6f0000£m^00v00000000000000
0 LDN 00x0s"J0D 00L0000k090u
[ 000<^VL4]00400F0#00>0a00*&!z`a000000000500
000\K]0B400I0K0]0[0]0/u000u00069p0000?4é1l00w0
300qaN0g0p>0kI3UQ00root@debian:/home/uca#

```

CAPTURA DE PROCESO DE FIRMAS

```

root@debian:/home/uca# gpg --output history.sig --sign history.txt
root@debian:/home/uca# gpg --output history.txt --decrypt history.sig
File 'history.txt' exists. Overwrite? (y/N) y
gpg: Signature made Wed 24 Aug 2022 02:46:10 PM CST
gpg: using RSA key BF8F38E25F37689566F103303B465154DE3989B0
gpg: Good signature from "Alejandro (GnuPG Guide - For UCA in SED) <00109220@uca.edu.sv>" [ultimate]
root@debian:/home/uca# gpg --clear-sign history.txt
root@debian:/home/uca# gpg --output history.sig --detach-sig history
gpg: can't open 'history': No such file or directory
gpg: signing failed: No such file or directory
root@debian:/home/uca# gpg --output history.sig --detach-sig history.txt
File 'history.sig' exists. Overwrite? (y/N) y
root@debian:/home/uca# gpg --verify history.sig history.txt
gpg: Signature made Wed 24 Aug 2022 02:48:04 PM CST
gpg: using RSA key BF8F38E25F37689566F103303B465154DE3989B0
gpg: Good signature from "Alejandro (GnuPG Guide - For UCA in SED) <00109220@uca.edu.sv>" [ultimate]
root@debian:/home/uca#

```