

1-INSTALAR gnupg

```
Get:4 http://debian.salud.gob.sv/debian bullseye/main amd64 patch amd64 2.7.6-7 [128 kB]
Fetched 7,514 kB in 4s (1,780 kB/s)
Selecting previously unselected package liberror-perl.
(Reading database ... 102620 files and directories currently installed.)
Preparing to unpack .../liberror-perl_0.17029-1_all.deb ...
Unpacking liberror-perl (0.17029-1) ...
Selecting previously unselected package git-man.
Preparing to unpack .../git-man_1%3a2.30.2-1_all.deb ...
Unpacking git-man (1:2.30.2-1) ...
Selecting previously unselected package git.
Preparing to unpack .../git_1%3a2.30.2-1_amd64.deb ...
Unpacking git (1:2.30.2-1) ...
Selecting previously unselected package patch.
Preparing to unpack .../patch_2.7.6-7_amd64.deb ...
Unpacking patch (2.7.6-7) ...
Setting up liberror-perl (0.17029-1) ...
Setting up patch (2.7.6-7) ...
Setting up git-man (1:2.30.2-1) ...
Setting up git (1:2.30.2-1) ...
Processing triggers for man-db (2.9.4-2) ...
root@debian:~# sudo apt install gnupg
```

```
Preparing to unpack .../liberror-perl_0.17029-1_all.deb ...
Unpacking liberror-perl (0.17029-1) ...
Selecting previously unselected package git-man.
Preparing to unpack .../git-man_1%3a2.30.2-1_all.deb ...
Unpacking git-man (1:2.30.2-1) ...
Selecting previously unselected package git.
Preparing to unpack .../git_1%3a2.30.2-1_amd64.deb ...
Unpacking git (1:2.30.2-1) ...
Selecting previously unselected package patch.
Preparing to unpack .../patch_2.7.6-7_amd64.deb ...
Unpacking patch (2.7.6-7) ...
Setting up liberror-perl (0.17029-1) ...
Setting up patch (2.7.6-7) ...
Setting up git-man (1:2.30.2-1) ...
Setting up git (1:2.30.2-1) ...
Processing triggers for man-db (2.9.4-2) ...
root@debian:~# sudo apt install gnupg
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.
root@debian:~#
```

2-Generando claves

The screenshot shows a terminal window titled "Terminal - uca@debian: ~". The window displays the following command-line session:

```
Setting up git-man (1:2.30.2-1) ...
Setting up git (1:2.30.2-1) ...
Processing triggers for man-db (2.9.4-2) ...
root@debian:~# sudo apt install gnupg
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.
root@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: directory '/root/.gnupg' created
gpg: keybox '/root/.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? ■
```

The screenshot shows a terminal window titled "Terminal - uca@debian: ~". The window displays the following command-line session, continuing from the previous one:

```
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: directory '/root/.gnupg' created
gpg: keybox '/root/.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) 0
Key does not expire at all
Is this correct? (y/N) y■
```

```
Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player | Terminal - uca@debian: ~ | File Edit View Terminal Tabs Help | Terminal - uca@debian: ~ | Wed 24 Aug, 16:03 uca

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) 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: Tania Michelle Delgado Vasquez
Email address: 00190918@uca.edu.sv
Comment: GnuPG Guide - For UCA in SED
You selected this USER-ID:
    "Tania Michelle Delgado Vasquez (GnuPG Guide - For UCA in SED) <00190918@u
a.edu.sv>"

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

Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)

Player | Terminal - uca@debian: ~

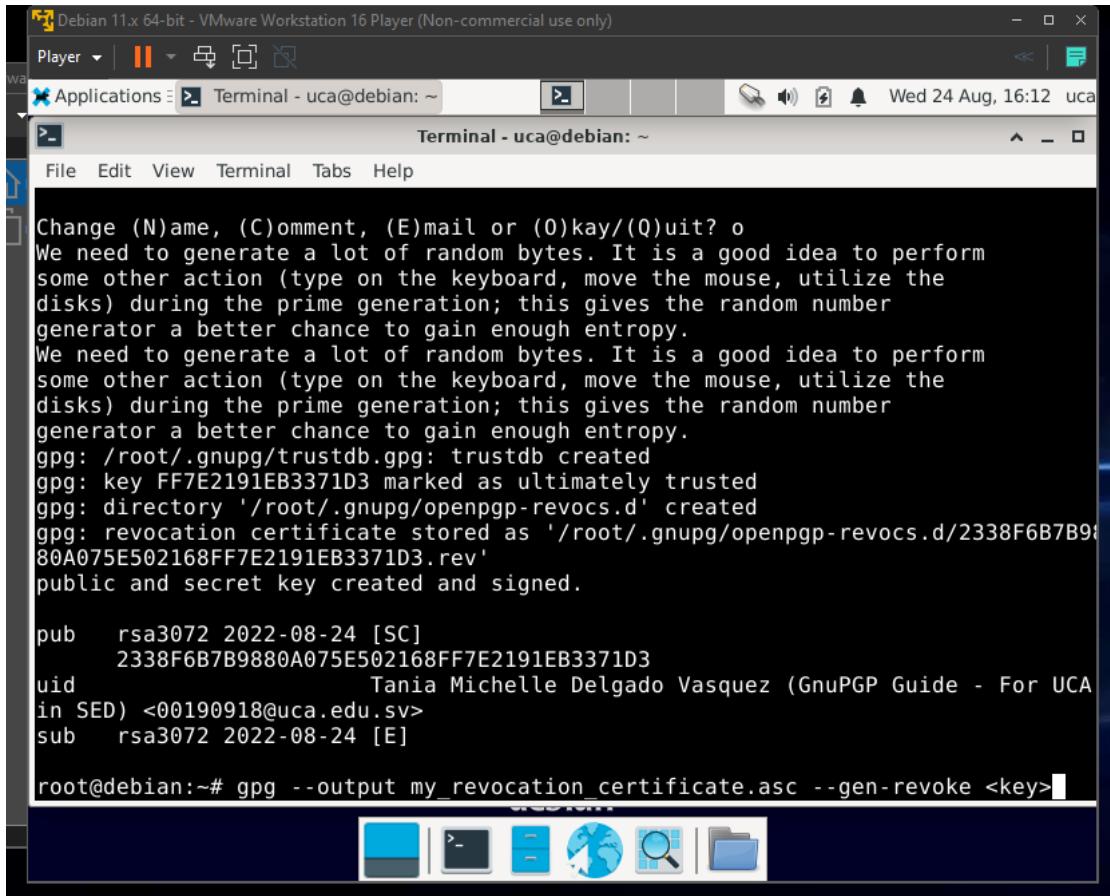
File Edit View Terminal Tabs Help

```
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 FF7E2191EB3371D3 marked as ultimately trusted
gpg: directory '/root/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/root/.gnupg/openpgp-revocs.d/2338F6B7B980A075E502168FF7E2191EB3371D3.rev'
public and secret key created and signed.

pub    rsa3072 2022-08-24 [SC]
      2338F6B7B9880A075E502168FF7E2191EB3371D3
uid          Tania Michelle Delgado Vasquez (GnuPG Guide - For UCA
in SED) <00190918@uca.edu.sv>
sub    rsa3072 2022-08-24 [E]

root@debian:~#
```

3 CERTIFICADO DE REVOCACIÓN



Debian 11x 64-bit - VMware Workstation 16 Player (Non-commercial use only)

Player Applications Terminal - uca@debian: ~

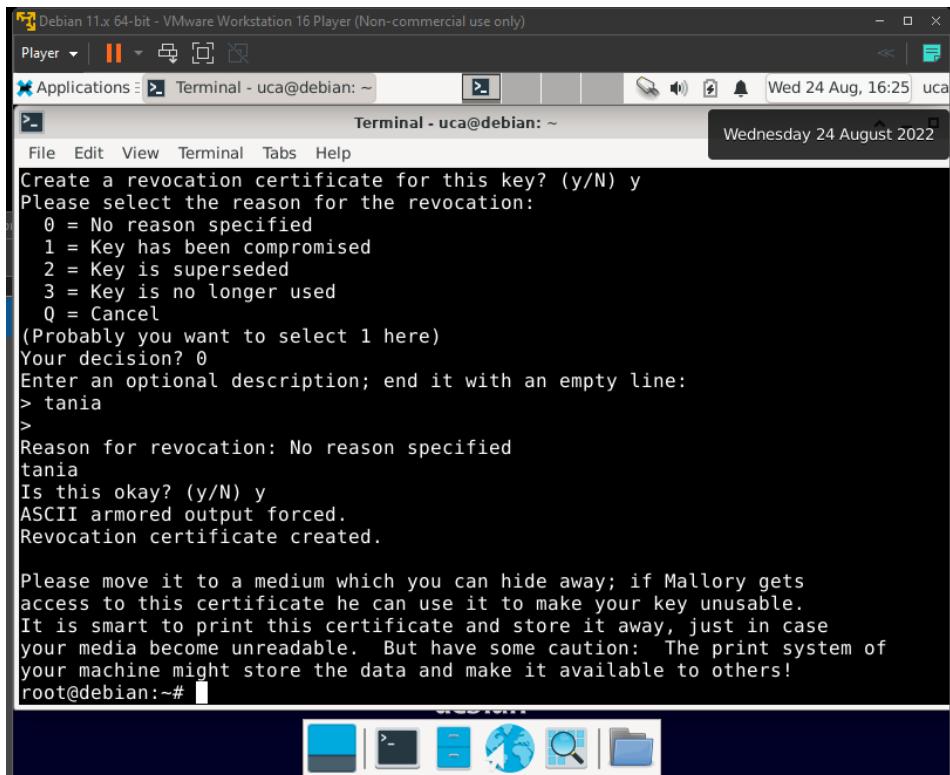
File Edit View Terminal Tabs Help

```
Change (N)ame, (C)oмment, (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 FF7E2191EB3371D3 marked as ultimately trusted
gpg: directory '/root/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/root/.gnupg/openpgp-revocs.d/2338F6B7B980A075E502168FF7E2191EB3371D3.rev'
public and secret key created and signed.

pub    rsa3072 2022-08-24 [SC]
      2338F6B7B9880A075E502168FF7E2191EB3371D3
uid          Tania Michelle Delgado Vasquez (GnuPG Guide - For UCA
in SED) <00190918@uca.edu.sv>
sub    rsa3072 2022-08-24 [E]

root@debian:~# gpg --output my_revocation_certificate.asc --gen-revoke <key>
```

The screenshot shows a terminal window on a Debian 11 desktop environment. The user has run the command `gpg --output my_revocation_certificate.asc --gen-revoke <key>`. The terminal displays the process of generating a revocation certificate, including prompts for a name, comment, and email, and a list of existing keys. The user's key is selected for revocation.



Debian 11x 64-bit - VMware Workstation 16 Player (Non-commercial use only)

Player Applications Terminal - uca@debian: ~

File Edit View Terminal Tabs Help

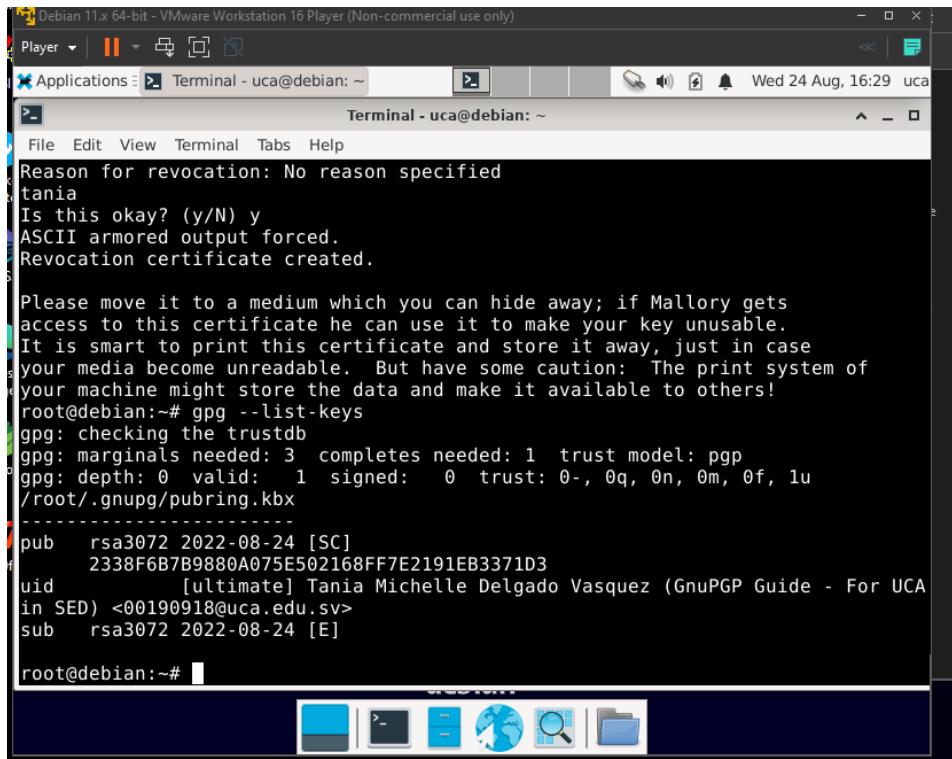
Wednesday 24 August 2022

```
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
  0 = Cancel
(Probably you want to select 1 here)
Your decision? 0
Enter an optional description; end it with an empty line:
> tania
>
Reason for revocation: No reason specified
tania
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!
root@debian:~#
```

This screenshot shows the continuation of the revocation process. The user has confirmed the creation of the revocation certificate and provided an optional description ('tania'). The terminal then prompts for confirmation and provides instructions for secure storage of the certificate.

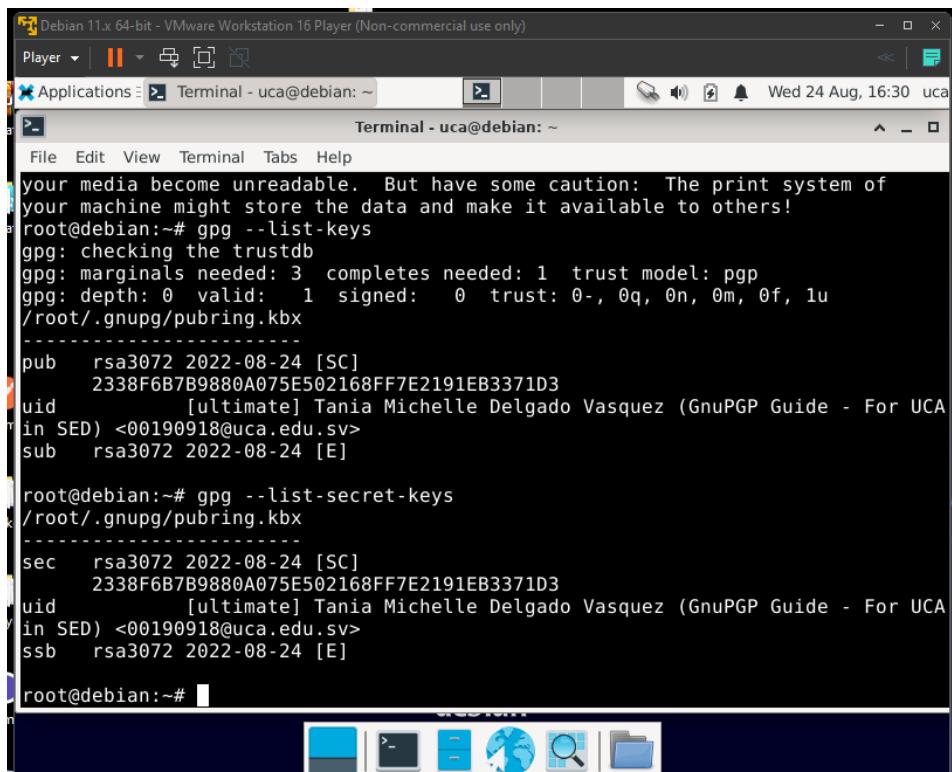
5- ADMINISTRACIÓN DE CLAVES



```
Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player | || | Applications Terminal - uca@debian: ~
File Edit View Terminal Tabs Help
Reason for revocation: No reason specified
tania
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!
root@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
/root/.gnupg/pubring.kbx
-----
pub    rsa3072 2022-08-24 [SC]
      2338F6B7B9880A075E502168FF7E2191EB3371D3
uid          [ultimate] Tania Michelle Delgado Vasquez (GnuPG Guide - For UCA
in SED) <00190918@uca.edu.sv>
sub    rsa3072 2022-08-24 [E]

root@debian:~#
```



```
Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player | || | Applications Terminal - uca@debian: ~
File Edit View Terminal Tabs Help
your media become unreadable. But have some caution: The print system of
your machine might store the data and make it available to others!
root@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
/root/.gnupg/pubring.kbx
-----
pub    rsa3072 2022-08-24 [SC]
      2338F6B7B9880A075E502168FF7E2191EB3371D3
uid          [ultimate] Tania Michelle Delgado Vasquez (GnuPG Guide - For UCA
in SED) <00190918@uca.edu.sv>
sub    rsa3072 2022-08-24 [E]

root@debian:~# gpg --list-secret-keys
/root/.gnupg/pubring.kbx
-----
sec    rsa3072 2022-08-24 [SC]
      2338F6B7B9880A075E502168FF7E2191EB3371D3
uid          [ultimate] Tania Michelle Delgado Vasquez (GnuPG Guide - For UCA
in SED) <00190918@uca.edu.sv>
ssb    rsa3072 2022-08-24 [E]

root@debian:~#
```

The screenshot shows a terminal window titled "Terminal - uca@debian: ~". The terminal displays the following command-line session:

```
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]
      2338F6B7B9880A075E502168FF7E2191EB3371D3
uid          [ultimate] Tania Michelle Delgado Vasquez (GnuPG Guide - For UCA
in SED) <00190918@uca.edu.sv>
sub    rsa3072 2022-08-24 [E]

root@debian:~# gpg --list-secret-keys
/root/.gnupg/pubring.kbx
-----
sec    rsa3072 2022-08-24 [SC]
      2338F6B7B9880A075E502168FF7E2191EB3371D3
uid          [ultimate] Tania Michelle Delgado Vasquez (GnuPG Guide - For UCA
in SED) <00190918@uca.edu.sv>
ssb    rsa3072 2022-08-24 [E]

root@debian:~# gpg --output tania.gpg --export 00190918@uca.edu.sv
root@debian:~# ls
my_revocation_certificate.asc  tania.gpg
root@debian:~#
```

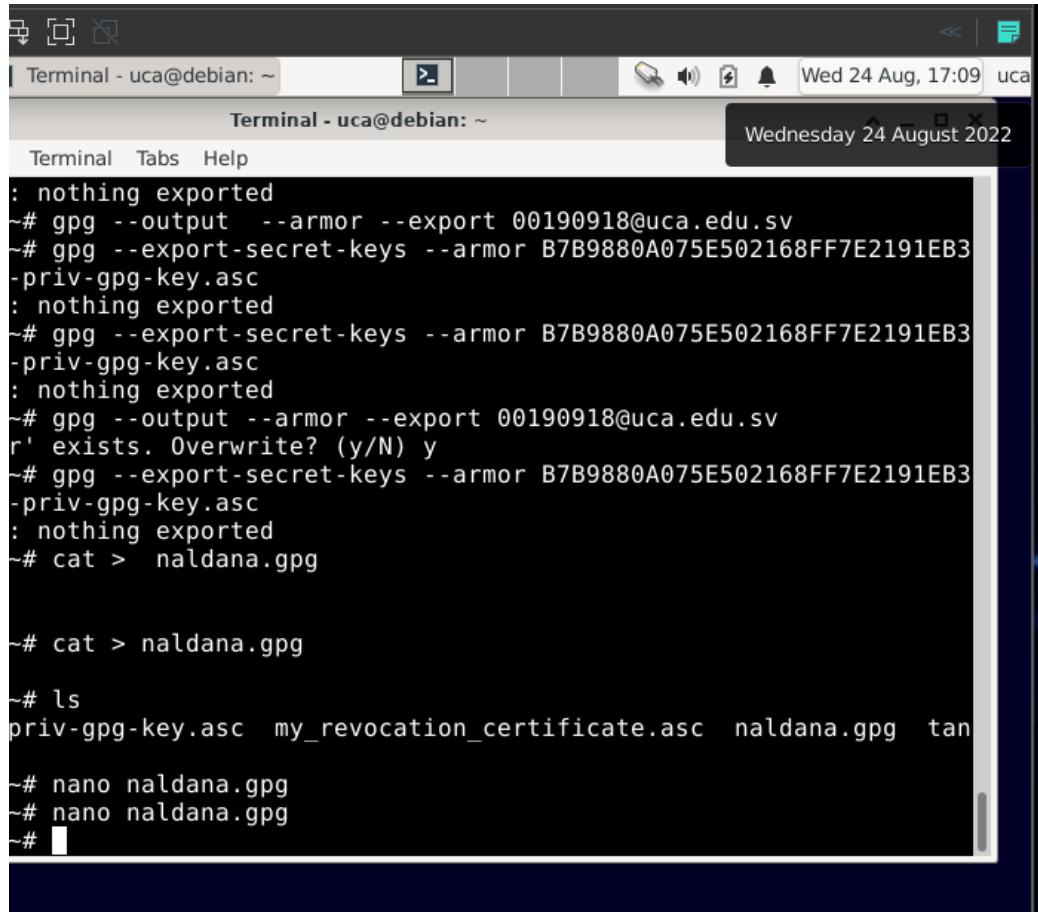
PUBLIC KEY

PGP PUBLIC KEY BLOCK-----

mQGNBGMGoWUBDACuA1kY7Z70sghnsoZiLWtRvBPtUzpiOpmwCfb44yJ5e2+lyk84
MuFGj+MTxOIIExel0wSE0AeMYyj+QVEkFp16SawuYn4T2ME6XId+oVjqeL66OVG
it0ne1kV2WhTuGFYhXxf4GzdxP62TEEcdbX0soUecp775X1kfz95Wb8yCkLAZIIQ
iucDGNr88/qwxJl4VJ0JBnRCVqNJ8sql0dn4BNMB5XuXD7tXLqT+pahixcjsb1mh
FrCw6JcZe2l1VitGP404/GSWsZNdB4+pUogGiGEPfaoQYv5xtFJZYRB7IKDbISv6
tJh8yp8UC5YKfaiMS7ekNCMmICYyG68fxIra8Xd004rkE+q5qJ0wg4fUrfJyMUN+
f0vqXBOEyLbz2Yhrmqbd768ax4cvYINsU2xHSL1i7CLpZ/fOr2adu/pceBbHUrW
KT5UcKJhgPqX+n2ixLRaanaFQMOp+85K17FOaSgzR0GHQaVewhfedSQfsJbE92V2
pMLqfgnP2tJKCk8AEQEAbRUVGFuaWEgTWIjaGVsbGUgRGVsZ2FkbyBWYXNxdWV6
IChHbnVQR1AgR3VpZGUgLSBGb3lgVUNBIGluIFNFRCkgPDAwMTkwOTE4QHVjYS5I
ZHUuc3Y+iQHOBBMBCgA4FiEEIzj2t7mlCgdeUCFo/34hkeszcdMFAmMGoWUCGwMF
CwkIBwIGFQoJCAsCBBYCAwECHgECF4AACgkQ/34hkeszcdMu3wv/YWNnv85QBm78
oMzpYYU88jhx8NOg2Hu9LodxErcL0ZXCEQUXLaM8jWnPDkWjnW6qNegpmI3HS62
HRnZt3QzcF8hG4NrDac1m7ExGiYy3dm0m127bB8mDr5bM38nNIIB1S2sNTfiudtM
1EsMygFrPW9EEA7N6ydYL5TeIZQ/VXXzrxmasI0UfTE/o7RKPSI947YwdxUQptir
wSO9oFIHFUHJs7KTmJ7TflJWB/FkOmMERJcbvj/R9N1r3KdIFTn6bdJYkRJJOMz
BNQSYMI/2cjFhPawp8IH6busbwDX1o6dirIWYs4aRXL7achFrhiAMauf5ioLKG5
d/l0WzSA7IWsb0NSXt+eWw774prS7RhOsNjlsjjG10bDe7LkxtyXAhQTEzDBYr3p
MP9tiM+MoLCVeY5XiEUoGTjjhWOiEWup/WZgMUpYcP7JpoXML6WdMnUX+JDI0b/G
DPEt/URbyseCM8oHf7vjmA+J15CLBiY/LPTv4SFOuct/KmswbJEHuQGNBGMGoWUB
DADyWTHhsA63rtUVmqZjCgusJh2jE2lbd6J1gxCqpHT9wrhtBc4javb6joYJ+mEB
AjOTbtDfUGZoGKfqIne4d8hvOE5lv+Oh44DNzCrszUqDa9jmwt3WYgg4q7whbDAC

b+2/PrI0J60MXyBUENBBy2C/3u6dwaTWiQDH1DQH5yaFVwlew+lAtaojo/a0lY49
tlMaSvKPgi7m0i81Sf3NXT2EjRq+jyPTU0MLxHT6He08G11DmtevVaEdZSP7lJE1
W4FqPrw/hYgU7TXfz1esDqO45PSsq269xD+q1ohpKBSS/yz28/A7lrwo57WAuhq/
+c3FTu7LVnq5mLzd2bG2UjaKmsdhkJVsD7Lxuzawza3xHzHZRmCplLhAEKxep6Lu
E5wr1fpq4szg+JOBavskfLYW9SJexAQG40VJX40xJwSCE5s3XtSihQyg1389MBB
rLcA3DPf1+6Cpi1VsXbgbhgnwEuA9refcvJ9A1F6SUB+iAPsYAHBiYNpK0ll6eT1
XYcAEQEAYkBtgQYAQoAIBYhBCM49re5iAoHXIAhaP9+IZhrM3HTBQJbqFIahsM
AAoJEP9+IZhrM3HT+JQMAJLalsABifCstFWKM7a+XnNhnUfB/0bJxllwsRmwk6pu
a9d2LYwEF7OG+T0ARBohilPt7geCK+1zKW6z43SRFetmf0gnizrJnLVSEzWEGkLF
g0nCaeSODpveMbrJ2KJuF5QfmlReGBssHVwkaAx1Zlap+sAMat3FTZOOD9ZS2PmM
qvJ6MWq3VrmXdHeu9yURoofP8/MXNPrjIMIUEhUSfJml7+csZY8PX0ltwqoddtn
9Y+jjv2tly3XQem4fFp7gJHCcRhIHLA77Pr9cvhbuZYTAvQSbKILc5qJMbkLxV6x
jPOiuZGiJvKPgXpcAQFOaV4M9b3fhojojBUz4pAe2BtdUbuWPoCgc1+0jjE5E8yT
VH6tel44uxsGZplwkS+mu70w3Yu35H7Zn3RssFT6TTCqluBQ7jJOz7HyI3VDEDAJ
DtgvHa8K3kXLBY7m7faAPz1AWPfVcosKjMhsVeEqkzx/dilvg2QAbhXO/PhdO9Zg
2tST60vn7ujcSMY9D03snA==
=tPkY

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



The screenshot shows a terminal window titled "Terminal - uca@debian: ~". The window has a dark theme and displays the following command history:

```
: nothing exported
~# gpg --output --armor --export 00190918@uca.edu.sv
~# gpg --export-secret-keys --armor B7B9880A075E502168FF7E2191EB3
-priv-gpg-key.asc
: nothing exported
~# gpg --export-secret-keys --armor B7B9880A075E502168FF7E2191EB3
-priv-gpg-key.asc
: nothing exported
~# gpg --output --armor --export 00190918@uca.edu.sv
r' exists. Overwrite? (y/N) y
~# gpg --export-secret-keys --armor B7B9880A075E502168FF7E2191EB3
-priv-gpg-key.asc
: nothing exported
~# cat > naldana.gpg

~# cat > naldana.gpg

~# ls
priv-gpg-key.asc  my_revocation_certificate.asc  naldana.gpg  tan

~# nano naldana.gpg
~# nano naldana.gpg
~#
```

Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)

Player | || |

Applications Terminal - uca@debian: ~

File Edit View Terminal Tabs Help

```
root@debian:~# gpg --import ~/Downloads/naldana.gpg
gpg: can't open '/root/Downloads/naldana.gpg': No such file or directory
gpg: Total number processed: 0
root@debian:~# gpg --import ~/Downloads/naldana.gpg
gpg: can't open '/root/Downloads/naldana.gpg': No such file or directory
gpg: Total number processed: 0
root@debian:~# gpg --import Downloads/naldana.gpg
gpg: can't open 'Downloads/naldana.gpg': No such file or directory
gpg: Total number processed: 0
root@debian:~# gpg --import Downloads/naldana.gpg
gpg: can't open 'Downloads/naldana.gpg': No such file or directory
gpg: Total number processed: 0
root@debian:~# nano naldana.gpg
root@debian:~# nano naldana.gpg
root@debian:~# gpg --import Downloads/naldana.gpg
gpg: can't open 'Downloads/naldana.gpg': No such file or directory
gpg: Total number processed: 0
root@debian:~# gpg --import Downloads/naldana.gpg
gpg: can't open 'Downloads/naldana.gpg': No such file or directory
gpg: Total number processed: 0
root@debian:~# gpg --import Downloads/naldana.gpg
gpg: can't open 'Downloads/naldana.gpg': No such file or directory
gpg: Total number processed: 0
root@debian:~#
```