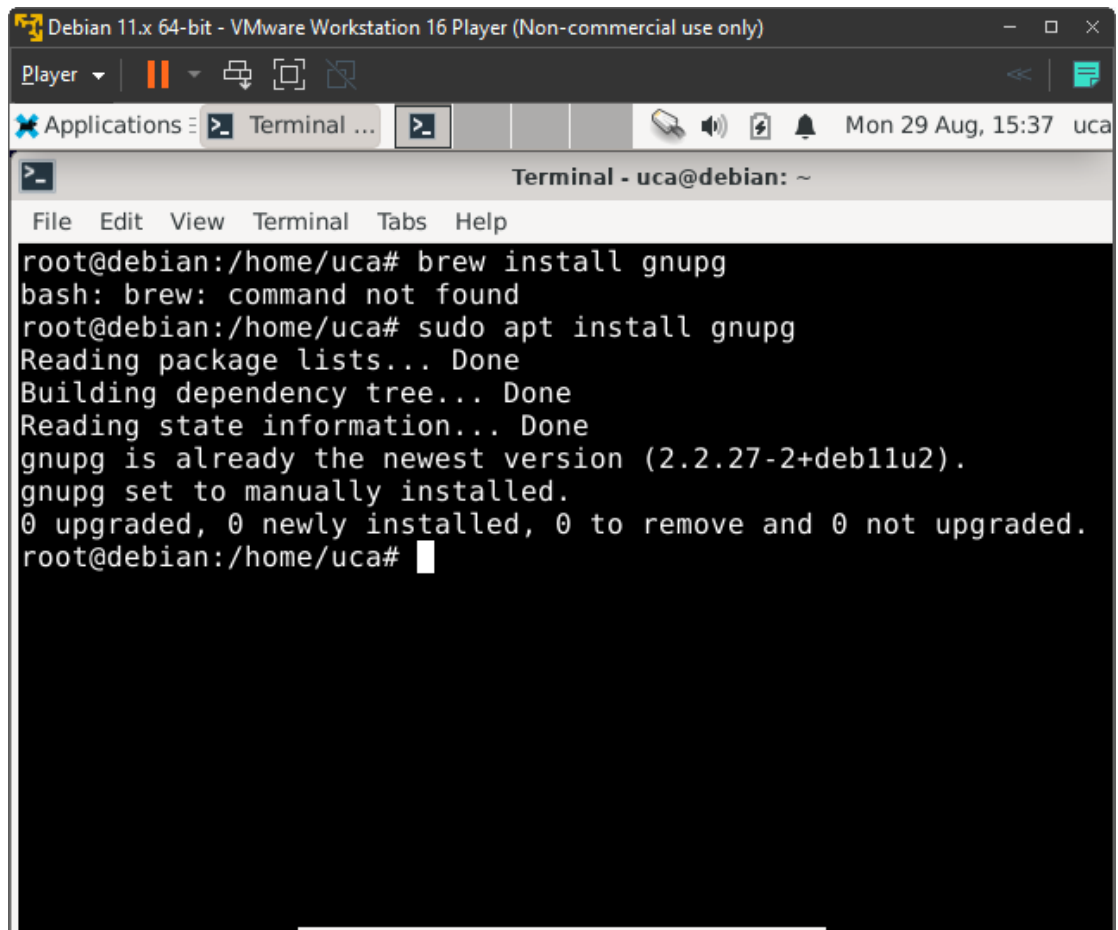
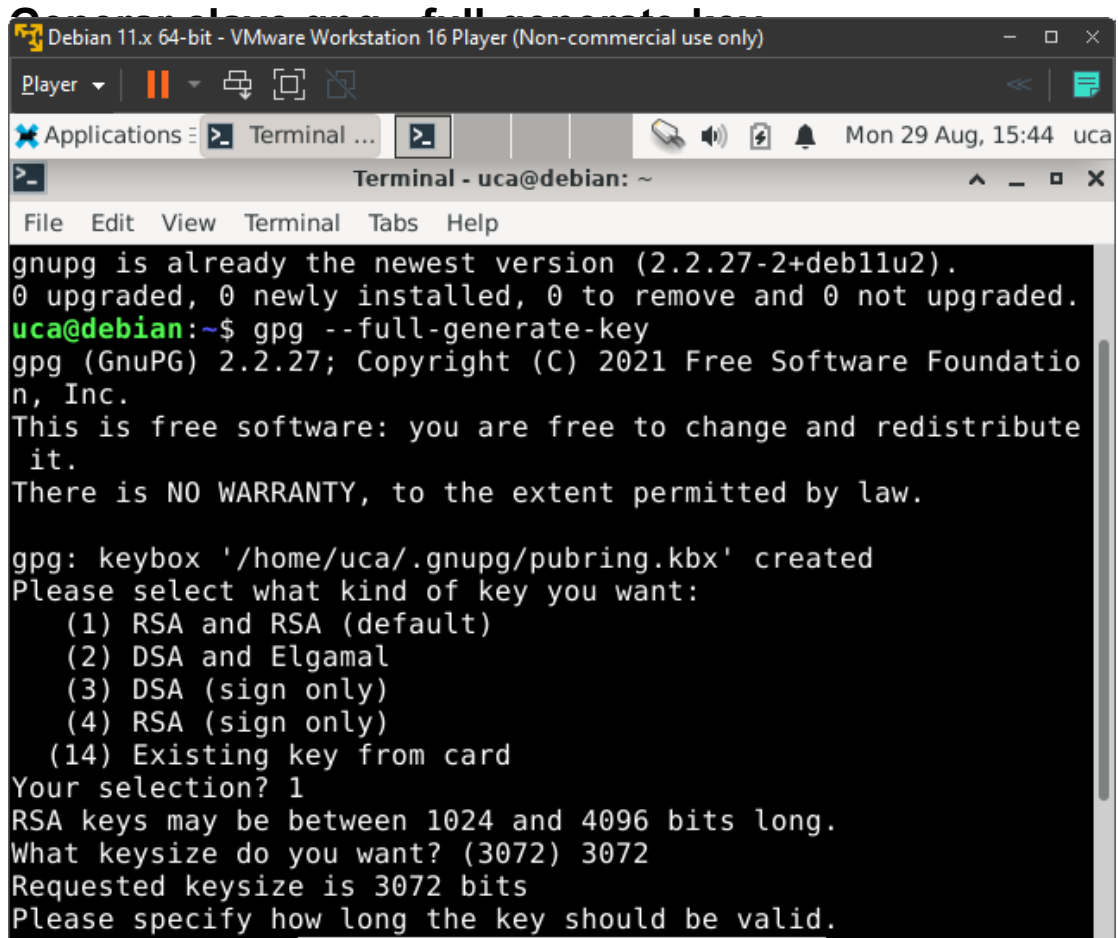


Instalando GPG



```
Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications Terminal ...
Terminal - uca@debian: ~
File Edit View Terminal Tabs Help
root@debian:/home/uca# brew install gnupg
bash: brew: command not found
root@debian:/home/uca# 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:/home/uca#
```



The image shows a terminal window titled "Terminal - uca@debian: ~" within a VMware Workstation 16 Player. The terminal displays the output of the command `gpg --full-generate-key`. The output indicates that gpg is already the newest version (2.2.27-2+deb11u2) and that no packages need to be upgraded, installed, removed, or not upgraded. It then prompts the user to select the type of key to generate. The user selects option 1, "RSA and RSA (default)". The terminal then prompts for the key size, which is set to 3072 bits. The final prompt is "Please specify how long the key should be valid.", which is underlined in the original image.

```
gpg is already the newest version (2.2.27-2+deb11u2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
uca@debian:~$ gpg --full-generate-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundatio
n, 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) 3072
Requested keysize is 3072 bits
Please specify how long the key should be valid.
```

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

```
Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications Terminal ...
Terminal - uca@debian: ~
File Edit View Terminal Tabs Help
    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)
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: Oscar Juarez
Email address: 00126320@uca.edu.sv
Comment: juarezgonzalez
You selected this USER-ID:
    "Oscar Juarez (juarezgonzalez) <00126320@uca.edu.sv>"

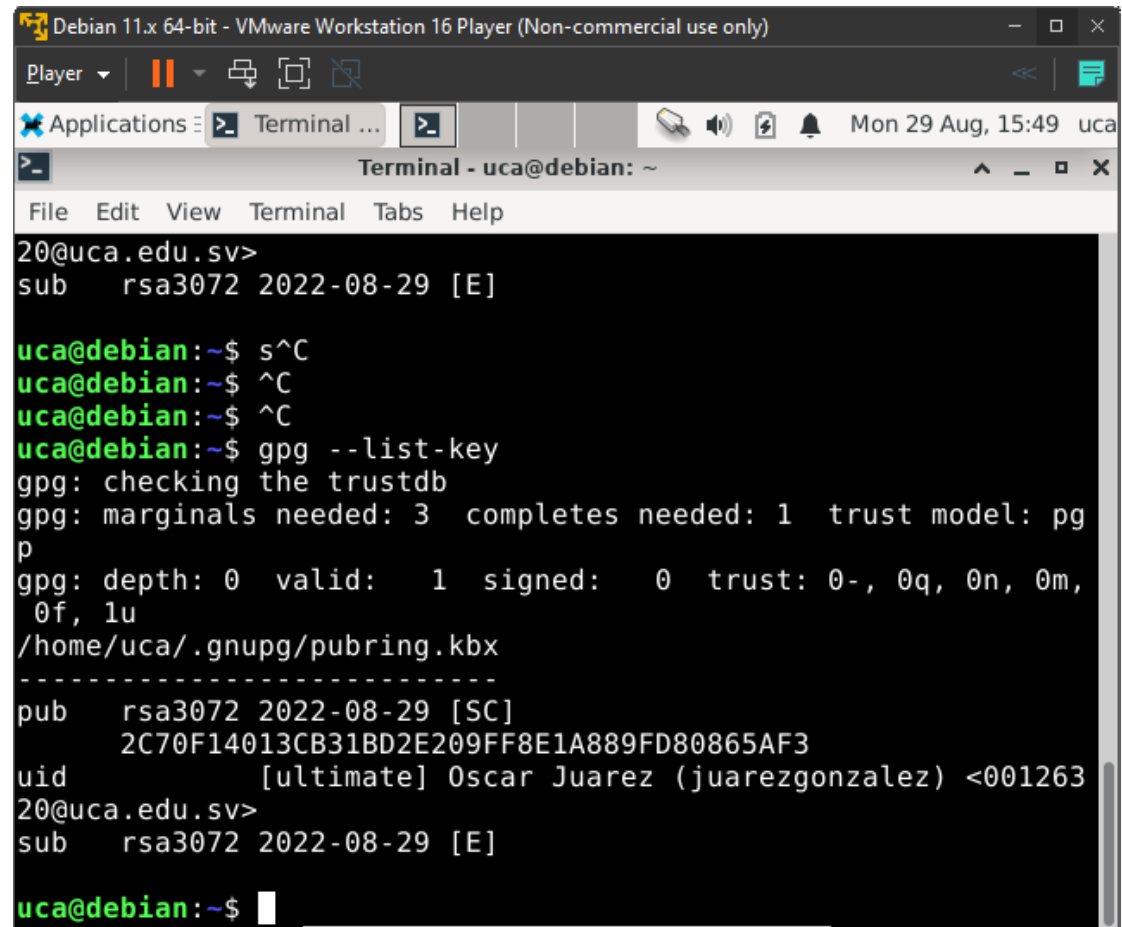
Change (N)ame, (C)omment, (E)mail or (0)key/(Q)uit? 
```

```
Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications Terminal ...
Terminal - uca@debian: ~
File Edit View Terminal Tabs Help
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 E1A889FD80865AF3 marked as ultimately trusted
gpg: directory '/home/uca/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/uca/.gnupg/openpgp-revocs.d/2C70F14013CB31BD2E209FF8E1A889FD80865AF3.rev'
public and secret key created and signed.

pub   rsa3072 2022-08-29 [SC]
       2C70F14013CB31BD2E209FF8E1A889FD80865AF3
uid           Oscar Juarez (juarezgonzalez) <00126320@uca.edu.sv>
sub   rsa3072 2022-08-29 [E]

uca@debian:~$ s
```

USANDO GPG -KEY-LIST



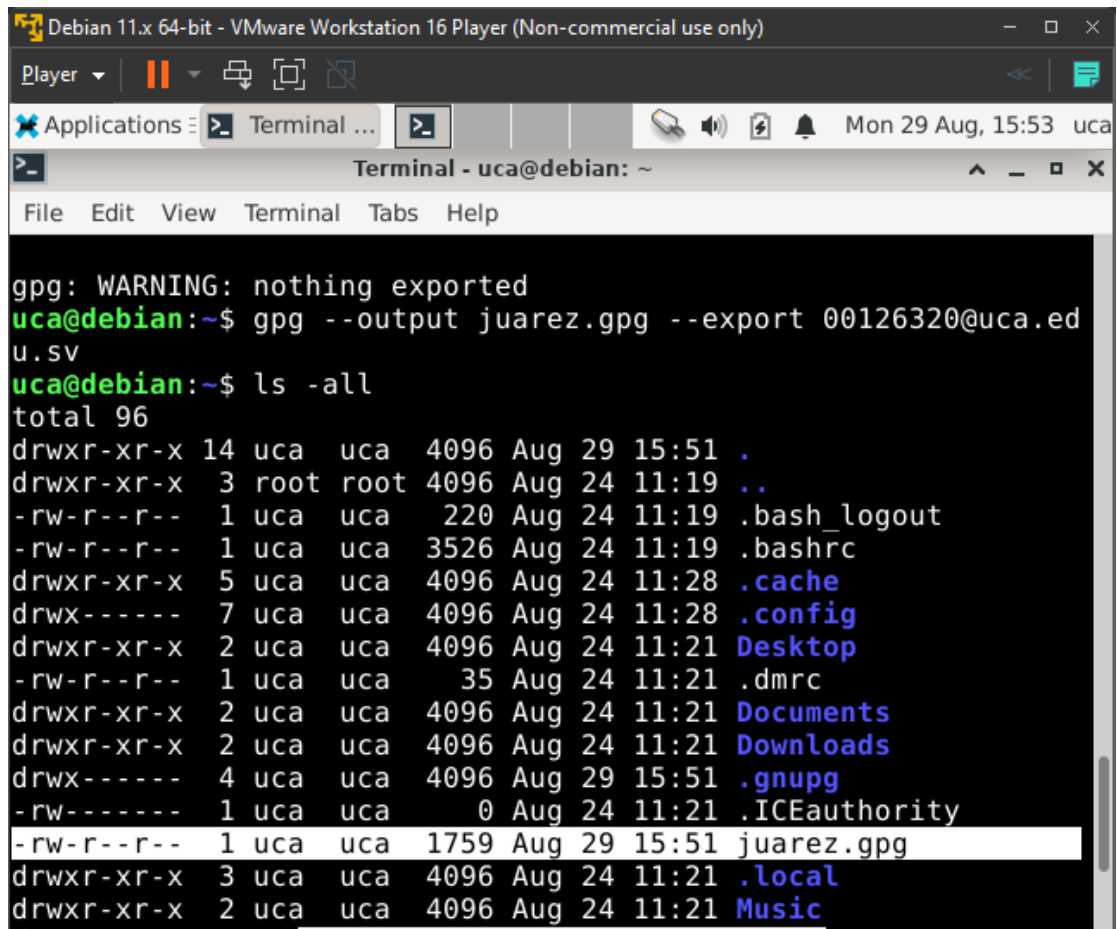
The screenshot shows a terminal window titled "Terminal - uca@debian: ~" within a "Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)" environment. The terminal output shows a user at the prompt "uca@debian:~\$ " typing "gpg --list-key". The output displays key information for a key ID "rsa3072 2022-08-29 [SC]". The key is owned by "Oscar Juarez (juarezgonzalez) <001263...". The terminal also shows the user pressing Ctrl-C three times before the command.

```
Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications Terminal ...
Terminal - uca@debian: ~
File Edit View Terminal Tabs Help
20@uca.edu.sv>
sub  rsa3072 2022-08-29 [E]

uca@debian:~$ s^C
uca@debian:~$ ^C
uca@debian:~$ ^C
uca@debian:~$ gpg --list-key
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pg
p
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]
    2C70F14013CB31BD2E209FF8E1A889FD80865AF3
uid          [ultimate] Oscar Juarez (juarezgonzalez) <001263
20@uca.edu.sv>
sub  rsa3072 2022-08-29 [E]

uca@debian:~$
```

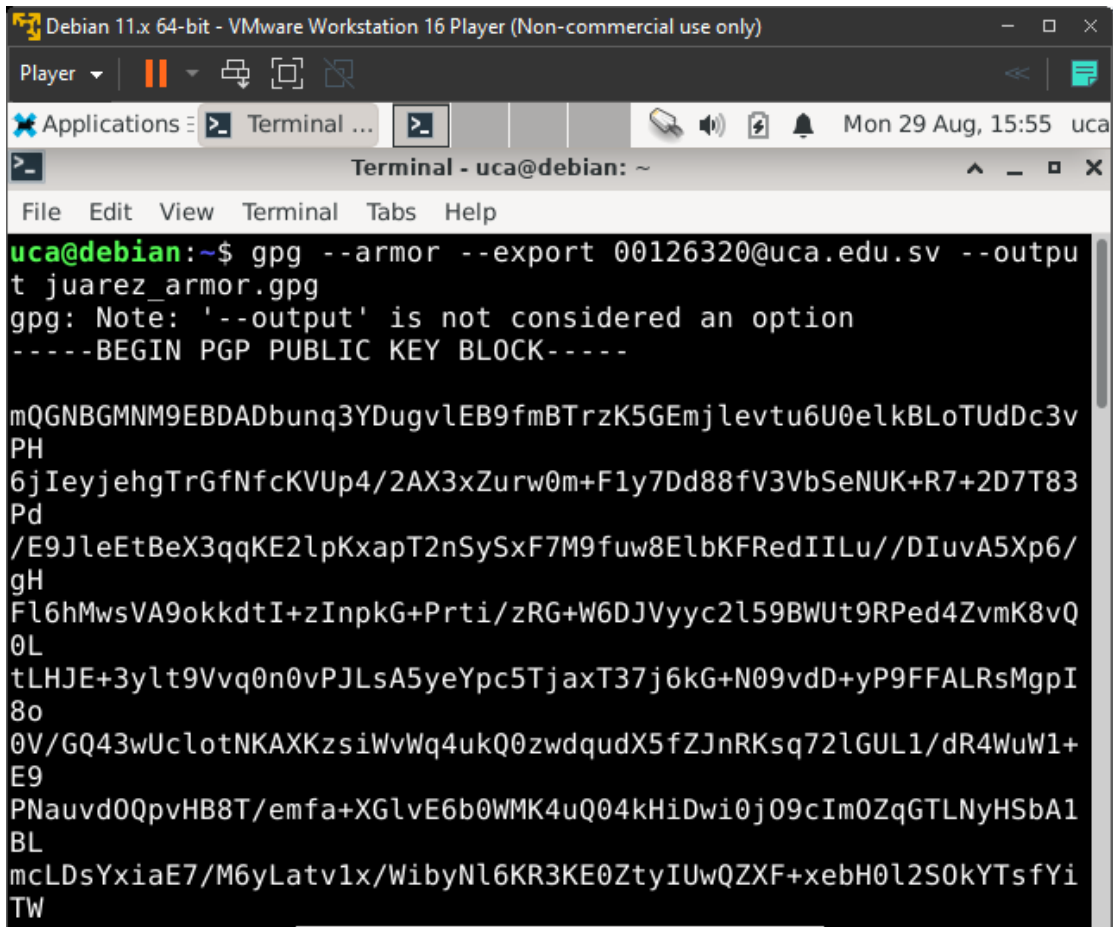
Exportando las claves a binario con gpg --output juarez.gpg --export 00126320@uca.edu.sv



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

gpg: WARNING: nothing exported
uca@debian:~$ gpg --output juarez.gpg --export 00126320@uca.edu.sv
uca@debian:~$ ls -all
total 96
drwxr-xr-x 14 uca uca 4096 Aug 29 15:51 .
drwxr-xr-x  3 root root 4096 Aug 24 11:19 ..
-rw-r--r--  1 uca uca  220 Aug 24 11:19 .bash_logout
-rw-r--r--  1 uca uca 3526 Aug 24 11:19 .bashrc
drwxr-xr-x  5 uca uca 4096 Aug 24 11:28 .cache
drwx-----  7 uca uca 4096 Aug 24 11:28 .config
drwxr-xr-x  2 uca uca 4096 Aug 24 11:21 Desktop
-rw-r--r--  1 uca uca   35 Aug 24 11:21 .dmrc
drwxr-xr-x  2 uca uca 4096 Aug 24 11:21 Documents
drwxr-xr-x  2 uca uca 4096 Aug 24 11:21 Downloads
drwx-----  4 uca uca 4096 Aug 29 15:51 .gnupg
-rw-----  1 uca uca    0 Aug 24 11:21 .ICEauthority
-rw-r--r--  1 uca uca 1759 Aug 29 15:51 juarez.gpg
drwxr-xr-x  3 uca uca 4096 Aug 24 11:21 .local
drwxr-xr-x  2 uca uca 4096 Aug 24 11:21 Music
```

Usando gpg --armor --export 00126320@uca.edu.sv para exportar la clave publica



```
Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications Terminal ...
Terminal - uca@debian: ~
File Edit View Terminal Tabs Help
uca@debian:~$ gpg --armor --export 00126320@uca.edu.sv --output
t juarez_armor.gpg
gpg: Note: '--output' is not considered an option
-----BEGIN PGP PUBLIC KEY BLOCK-----

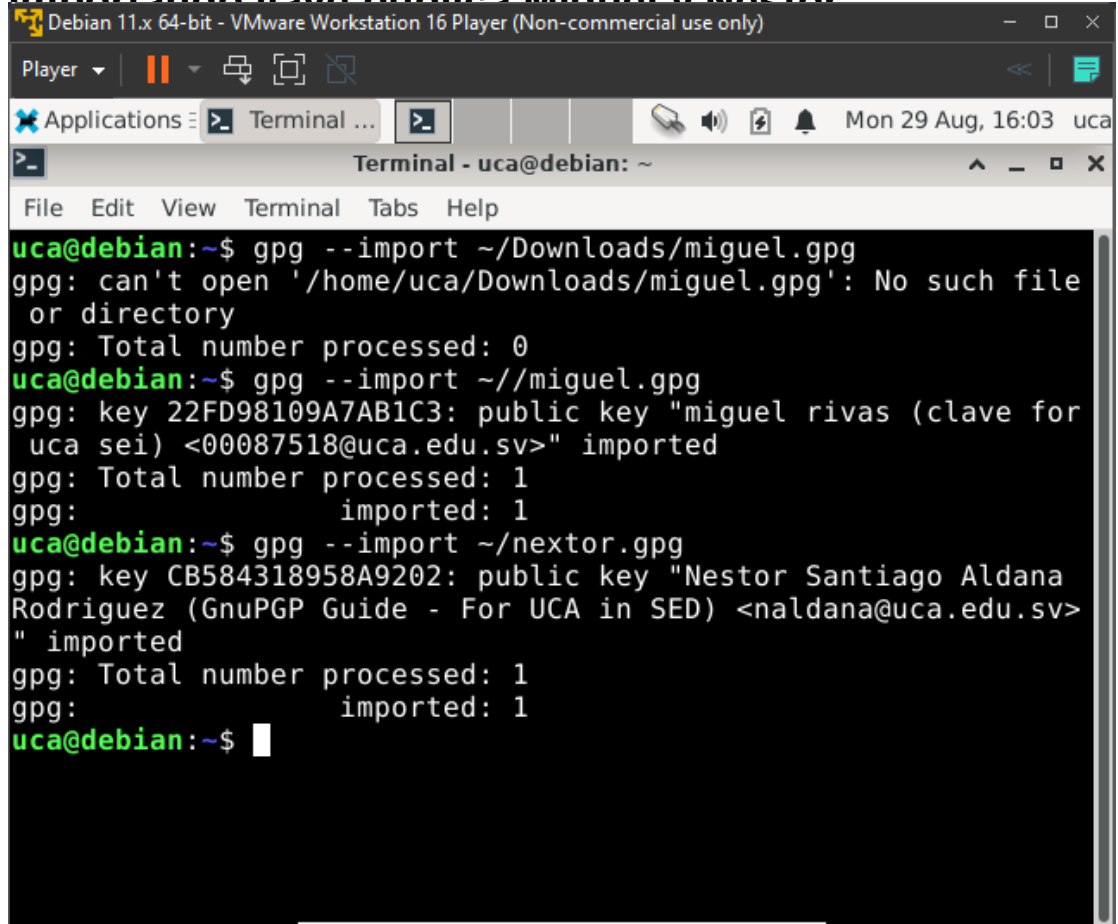
mQGNBGMNM9EBDADBunq3YDugvLEB9fmBTrzK5GEmjlevtu6U0elkBLoTUdDc3v
PH
6jIeyjehgTrGfNfcKVUp4/2AX3xZurw0m+F1y7Dd88fV3VbSeNUK+R7+2D7T83
Pd
/E9JleEtBeX3qqKE2lpKxapT2nSySxF7M9fuw8ElbKfRedIILu//DIuvA5Xp6/
gH
Fl6hMwsVA9okkdtI+zInpkG+Prti/zRG+W6DJVyyc2l59BWUt9RPed4ZvmK8vQ
0L
tLHJE+3ylt9Vvq0n0vPJLsA5yeYpc5TjaxT37j6kG+N09vdD+yP9FFALRsMgpI
8o
0V/GQ43wUclotNKAXKzsiWvWq4ukQ0zwdqudX5fZJnRKsq72lGUL1/dR4WuW1+
E9
PNauvd0QpvHB8T/emfa+XGlvE6b0WMK4uQ04kHiDwi0j09cIm0ZqGTLNyHSbA1
BL
mcLDsYxiaE7/M6yLatv1x/WibyNl6KR3KE0ZtyIUwQZXF+xebH0l2S0kYTsfYi
TW
```



```
Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications Terminal ...
Terminal - uca@debian: ~
File Edit View Terminal Tabs Help
uca@debian:~$ gpg --export-secret-keys --armor 00126320@uca.edu
u.sv > ./my-priv-gpg-key.asc
uca@debian:~$ cat my-priv-gpg-key.asc
-----BEGIN PGP PRIVATE KEY BLOCK-----

lQWGBGMNM9EBDADbunq3YDugvLEB9fmBTzK5GEmjlevtu6U0elkBLoTUdDc3v
PH
6jIeyjehgTrGfNfcKVUp4/2AX3xZurw0m+F1y7Dd88fV3VbSeNUK+R7+2D7T83
Pd
/E9JleEtBeX3qqKE2lpKxapT2nSySxF7M9fuw8ElbKFRedIILu//DIuvA5Xp6/
gH
Fl6hMwsVA9okkdtI+zInpkG+Prti/zRG+W6DJVyyc2l59BWUt9RPed4ZvmK8vQ
0L
tLHJE+3ylt9Vvq0n0vPJLsA5yeYpc5TjaxT37j6kG+N09vdD+yP9FFALRsMgpI
8o
0V/GQ43wUclotNKAXKzsiWvWq4ukQ0zwdqudX5fZJnRKsq72lGUL1/dR4WuW1+
E9
PNauvd0QpvHB8T/emfa+XGlV6b0WMK4uQ04kHiDwi0j09cIm0ZqGTLNyHSbA1
BL
mcLDsYxiaE7/M6yLatv1x/WibyNl6KR3KE0ZtyIUwQZXF+xebH0l2S0kYTsfYi
TW
```

Importando llave publica Miguel y Nestor



The screenshot shows a terminal window titled "Terminal - uca@debian: ~" within a "Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)" environment. The terminal displays the following commands and output:

```
uca@debian:~$ gpg --import ~/Downloads/miguel.gpg
gpg: can't open '/home/uca/Downloads/miguel.gpg': No such file
or directory
gpg: Total number processed: 0
uca@debian:~$ 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
uca@debian:~$ gpg --import ~/nextor.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:~$
```

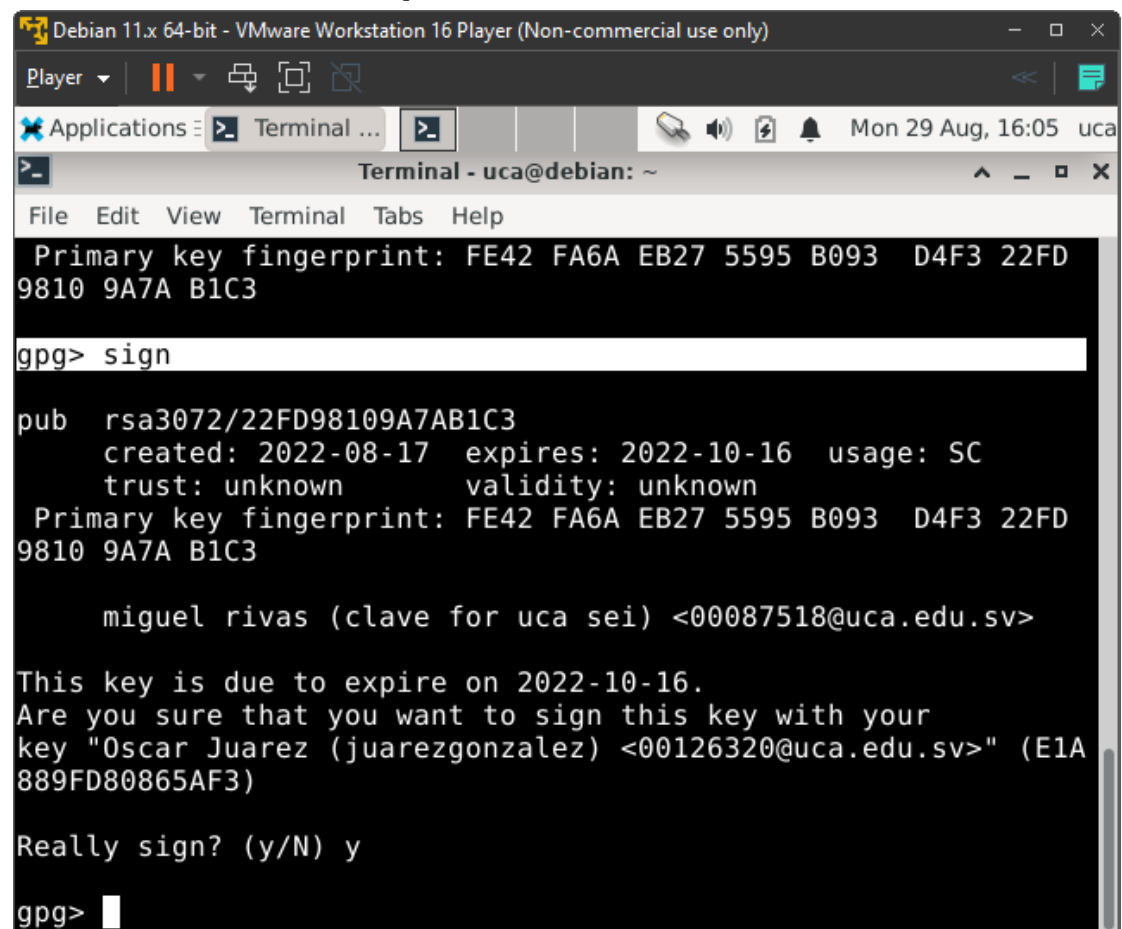
```
Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications Terminal ...
Terminal - uca@debian: ~
File Edit View Terminal Tabs Help
/home/uca/.gnupg/pubring.kbx
-----
pub  rsa3072 2022-08-29 [SC]
    2C70F14013CB31BD2E209FF8E1A889FD80865AF3
uid          [ultimate] Oscar Juarez (juarezgonzalez) <001263
20@uca.edu.sv>
sub  rsa3072 2022-08-29 [E]

pub  rsa3072 2022-08-17 [SC] [expires: 2022-10-16]
    FE42FA6AEB275595B093D4F322FD98109A7AB1C3
uid          [ unknown] miguel rivas (clave for uca sei) <000
87518@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 (Gnu
PGP Guide - For UCA in SED) <naldana@uca.edu.sv>
sub  rsa3072 2022-08-17 [E]

uca@debian:~$
```

Firmando llaves importadas



The screenshot shows a terminal window titled "Terminal - uca@debian: ~" within a "Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)" environment. The terminal displays the output of the 'gpg --list-keys' command, showing a key for 'miguel rivas (clave for uca sei) <00087518@uca.edu.sv>' with a primary fingerprint of FE42 FA6A EB27 5595 B093 D4F3 22FD 9810 9A7A B1C3. The user then enters 'gpg> sign' at the prompt. The terminal shows the key's details, including its creation and expiration dates, and asks for confirmation to sign the key with the user's own key. The user responds with 'y' to confirm the signature.

```
Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications Terminal ...
Terminal - uca@debian: ~
File Edit View Terminal Tabs Help
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 "Oscar Juarez (juarezgonzalez) <00126320@uca.edu.sv>" (E1A
889FD80865AF3)
Really sign? (y/N) y
gpg>
```

```
Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications Terminal ...
Terminal - uca@debian: ~
File Edit View Terminal Tabs Help
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 (GnuPGP Guide - For UCA
in SED) <naldana@uca.edu.sv>

Are you sure that you want to sign this key with your
key "Oscar Juarez (juarezgonzalez) <00126320@uca.edu.sv>" (E1A
889FD80865AF3)

Really sign? (y/N) y
gpg> S
```

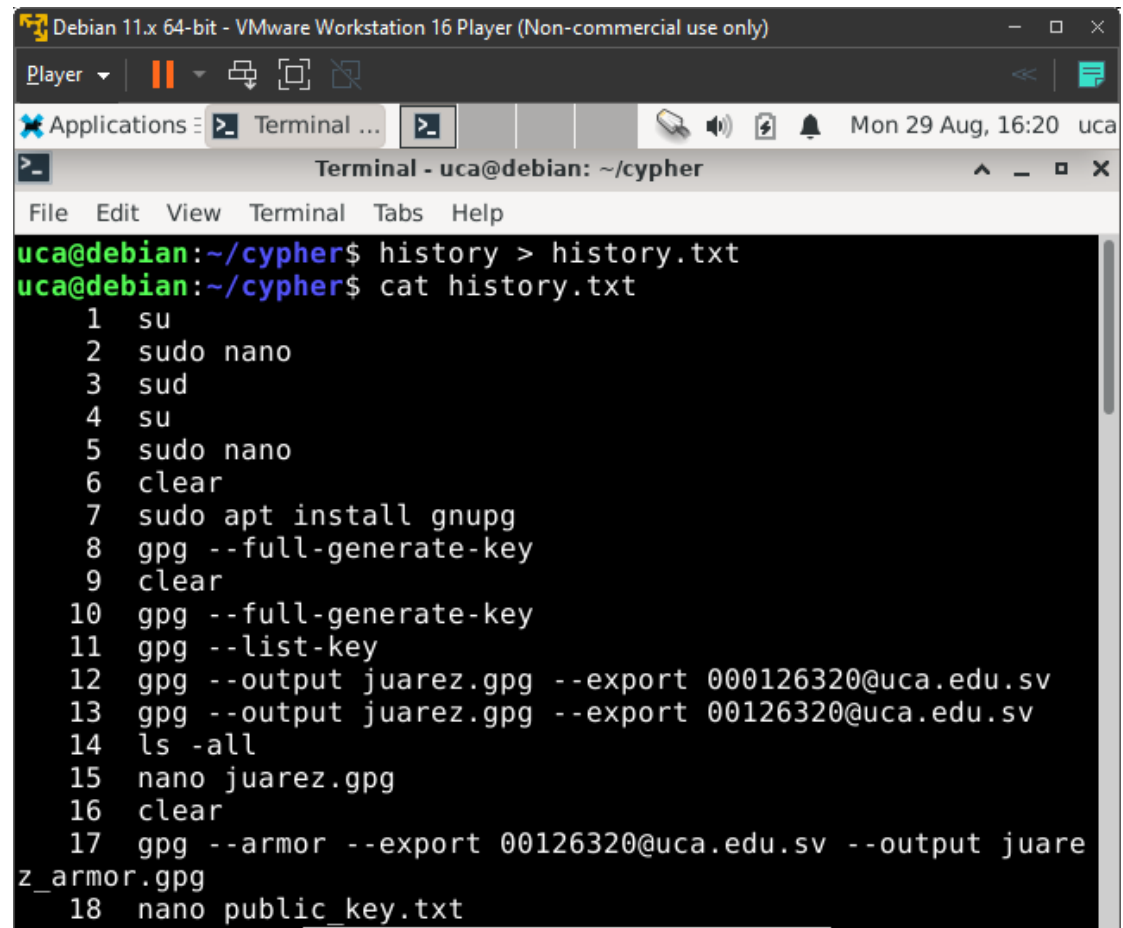
```
Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications Terminal ...
Terminal - uca@debian: ~
File Edit View Terminal Tabs Help
/home/uca/.gnupg/pubring.kbx
-----
pub  rsa3072 2022-08-29 [SC]
    2C70F14013CB31BD2E209FF8E1A889FD80865AF3
uid          [ultimate] Oscar Juarez (juarezgonzalez) <001263
20@uca.edu.sv>
sub  rsa3072 2022-08-29 [E]

pub  rsa3072 2022-08-17 [SC] [expires: 2022-10-16]
    FE42FA6AEB275595B093D4F322FD98109A7AB1C3
uid          [ full ] miguel rivas (clave for uca sei) <000
87518@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 (Gnu
PGP Guide - For UCA in SED) <naldana@uca.edu.sv>
sub  rsa3072 2022-08-17 [E]

uca@debian:~$
```

Cifrado simétrico

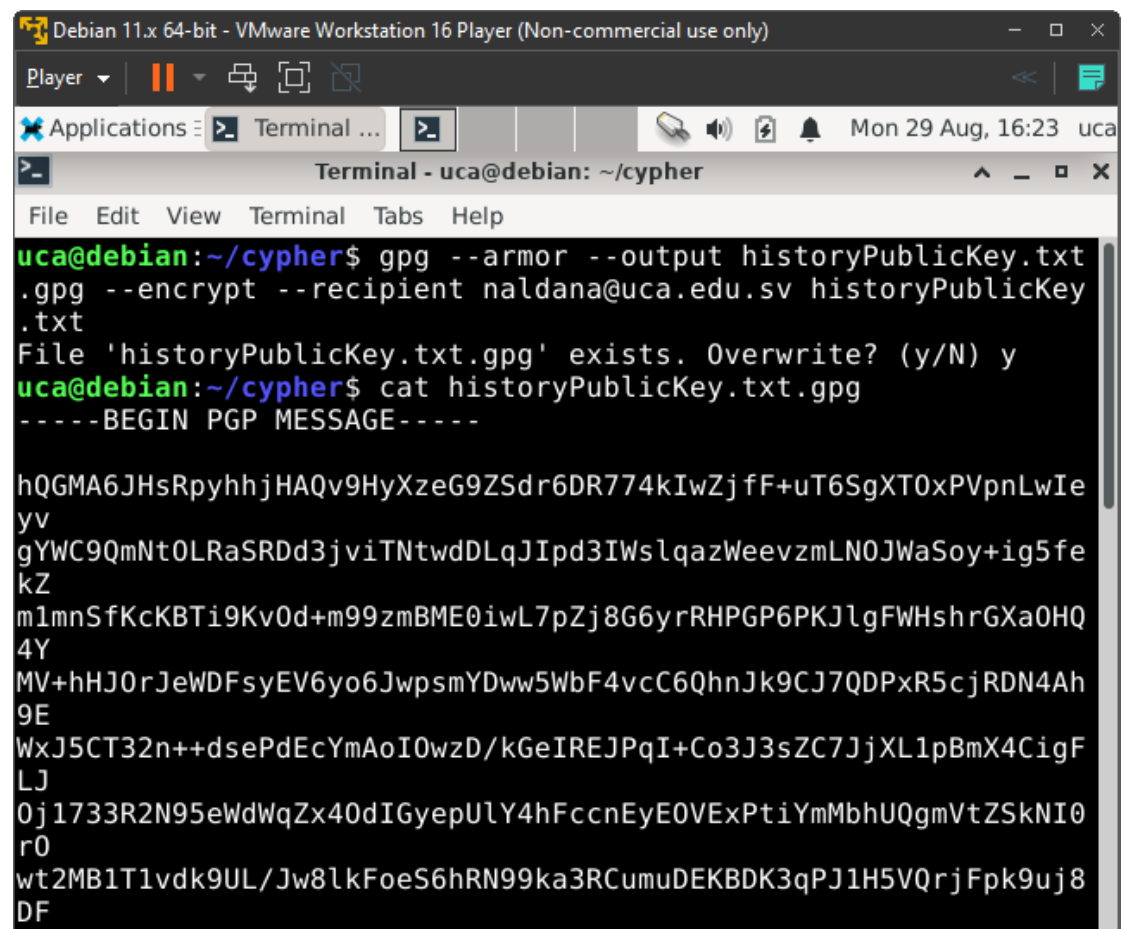


```
Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications
Terminal ...
Terminal - uca@debian: ~/cypher
File Edit View Terminal Tabs Help
uca@debian:~/cypher$ history > history.txt
uca@debian:~/cypher$ cat history.txt
1 su
2 sudo nano
3 sud
4 su
5 sudo nano
6 clear
7 sudo apt install gnupg
8 gpg --full-generate-key
9 clear
10 gpg --full-generate-key
11 gpg --list-key
12 gpg --output juarez.gpg --export 000126320@uca.edu.sv
13 gpg --output juarez.gpg --export 00126320@uca.edu.sv
14 ls -all
15 nano juarez.gpg
16 clear
17 gpg --armor --export 00126320@uca.edu.sv --output juare
z_armor.gpg
18 nano public_key.txt
```

```
Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications Terminal ...
Terminal - uca@debian: ~/cypher
File Edit View Terminal Tabs Help
uca@debian:~/cypher$ gpg --armor --output history.txt.gpg --symmetric history.txt
File 'history.txt.gpg' exists. Overwrite? (y/N) Y
uca@debian:~/cypher$ cat history.txt.gpg
-----BEGIN PGP MESSAGE-----

jA0ECQMCUbZ2KxXIJUn/0ukBK00Lx35n0jw8ApYb7Bk4anjfPp0mNiF0MmxI0p
WN
hYvp1bSHtega3lFUzPxxBIWTt3+CA9jR9A+g6xECBiZHCTo586xVixrtM/wSr/
If
IYIXG+bLZ5shGyo0EzIx9sc7Nn/Q2tGut0C0H3lMbyWa5hNjDIcxQv3Q1MA9aH
dX
UNzdoKXtagPj+iRGyoqjY7XZt27lx2f1sicQ/jXUhLCLGQHof0uYX9sU0ptWpJ
Zb
vgVnQw2DSIUzxBnqLMNujb7X80Kg8cGttAulx50cj1izFSh+7SJ656EJ692V8A
lH
XiLQsw6l+CAGXFKpaCjGAiu78uuVll0ee/XQGQ1lKLYV3hMzqb9vymTYCC93XI
XK
GUvA1fsflSdfC7Q9mZbtd1nTfynGhT5oK0R25NYnkppLGZwMrNzRgH0ZtNYmr2
tm
Gq4vCCEueEkTWX0nbCPsrGRyfBKhgZrDJnmsiyiS3IjYtZu2MWzmrDkt0a1Hys
```


Cifrado asimétrico

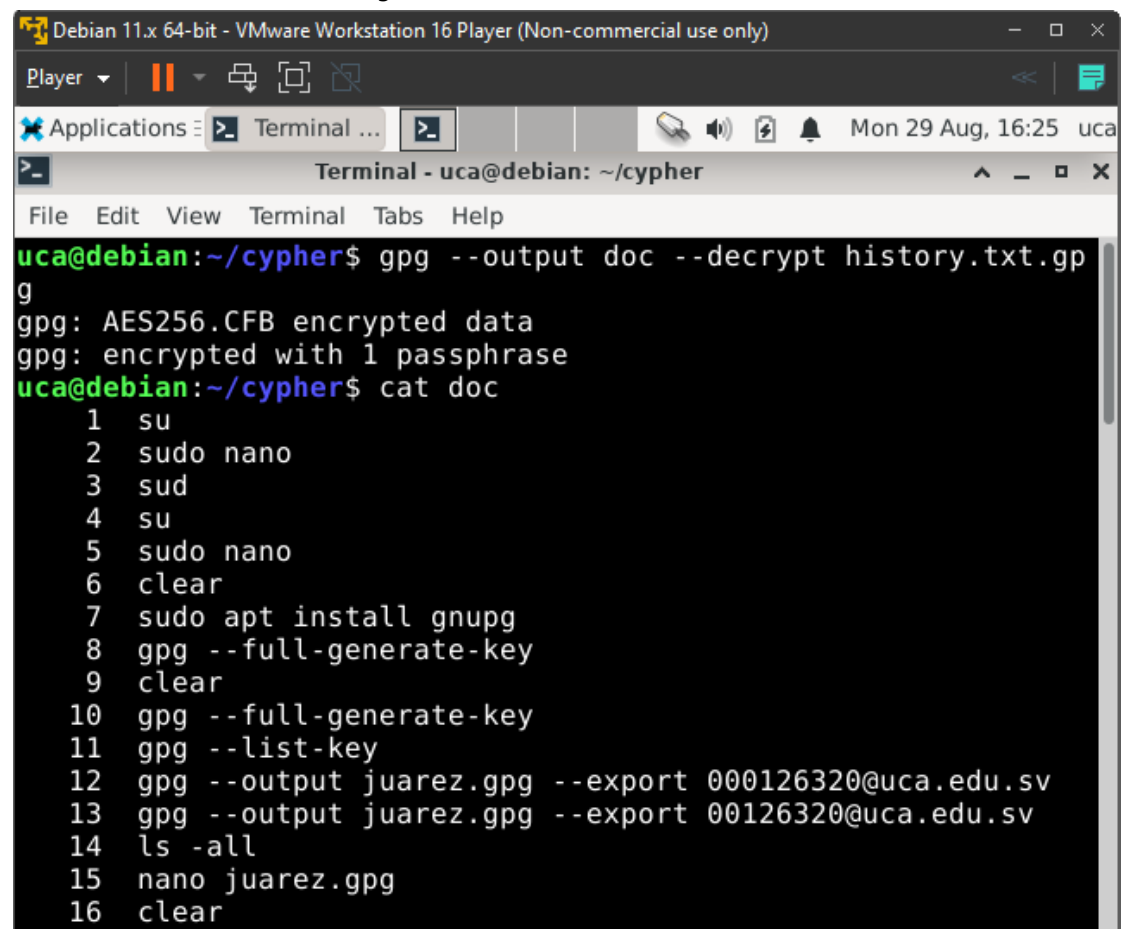


The screenshot shows a terminal window titled "Terminal - uca@debian: ~/cypher" within a "Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)" environment. The terminal displays the following commands and output:

```
uca@debian:~/cypher$ gpg --armor --output historyPublicKey.txt
.gpg --encrypt --recipient naldana@uca.edu.sv historyPublicKey
.txt
File 'historyPublicKey.txt.gpg' exists. Overwrite? (y/N) y
uca@debian:~/cypher$ cat historyPublicKey.txt.gpg
-----BEGIN PGP MESSAGE-----

hQGMA6JHsRpyhhjHAQv9HyXzeG9ZSdr6DR774kIwZj fF+uT6SgXT0xPVpnLwIe
yv
gYWC9QmNt0LRaSRDd3jviTNtwDLqJIpd3IWslqazWeevzmLN0JWaSoy+ig5fe
kZ
m1mnSfKcKBTi9Kv0d+m99zmBME0iwL7pZj8G6yrRHPGP6PKJlgFWHshrGXa0HQ
4Y
MV+hHJ0rJeWDFsyEV6yo6JwpsmYDww5WbF4vcC6QhnJk9CJ7QDPxR5cjRDN4Ah
9E
WxJ5CT32n++dsePdEcYmAoIOwzD/kGeIREJPqI+Co3J3sZC7JjXL1pBmX4CigF
LJ
Oj1733R2N95eWdWqZx40dIGyepULY4hFccnEyEOVExPtYmMbhUQgmVtZSkNI0
r0
wt2MB1T1vdk9UL/Jw8lkFoeS6hRN99ka3RCumuDEKBDK3qPJ1H5VQrjFpk9uj8
DF
```

Descifrado mensaje con cifrado simétrico



The screenshot shows a terminal window titled "Terminal - uca@debian: ~/cypher" within a "Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)" environment. The terminal displays the following commands and output:

```
uca@debian:~/cypher$ gpg --output doc --decrypt history.txt.gpg
gpg: AES256.CFB encrypted data
gpg: encrypted with 1 passphrase
uca@debian:~/cypher$ cat doc
1  su
2  sudo nano
3  sud
4  su
5  sudo nano
6  clear
7  sudo apt install gnupg
8  gpg --full-generate-key
9  clear
10 gpg --full-generate-key
11 gpg --list-key
12 gpg --output juarez.gpg --export 000126320@uca.edu.sv
13 gpg --output juarez.gpg --export 00126320@uca.edu.sv
14 ls -all
15 nano juarez.gpg
16 clear
```

¿Cuál es el punto más débil de PGP?

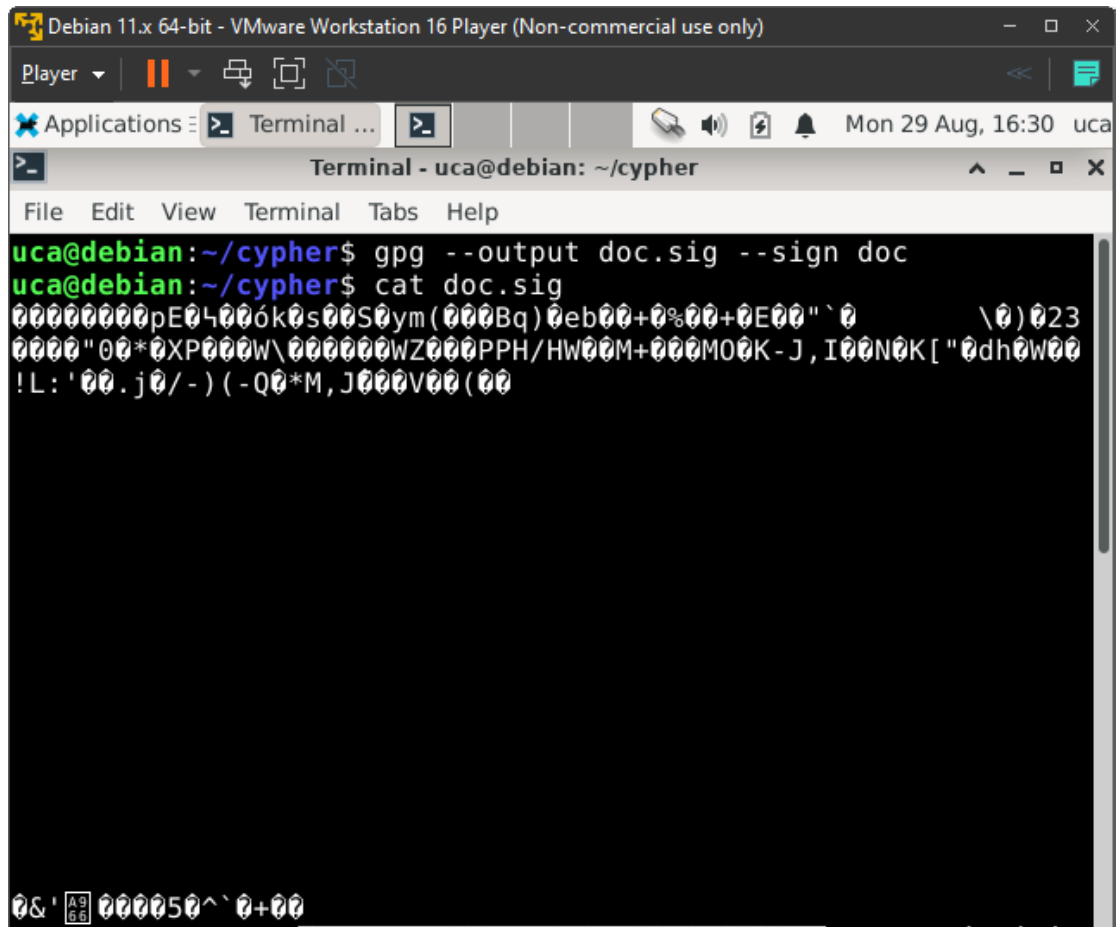
Compartir las claves entre personas

¿Cuándo es conveniente utilizar solamente cifrado simétrico?

Es necesario una única llave, puede ser muy eficaz porque no experimenta ningún retraso de tiempo significativo como resultado del cifrado y descifrado.

Firmando documento

Firmando documento

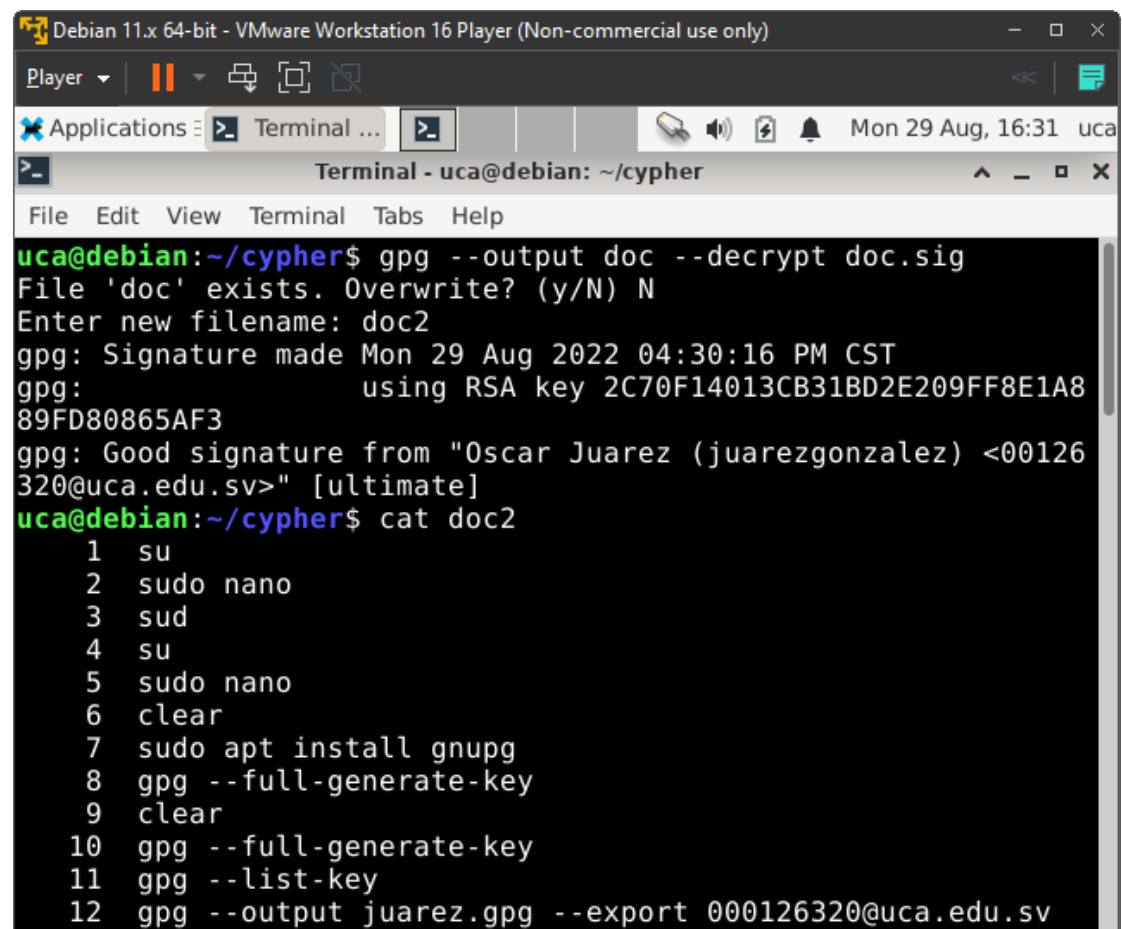


The screenshot shows a terminal window titled "Terminal - uca@debian: ~/cypher" within a VMware Workstation 16 Player. The terminal displays the following commands and output:

```
uca@debian:~/cypher$ gpg --output doc.sig --sign doc
uca@debian:~/cypher$ cat doc.sig
00000000pE04006k0s00S0ym(000Bq)0eb00+0%00+0E00"0
\0)023
0000"00*0XP000W\000000WZ000PPH/HW00M+000M00K-J,I00N0K["0dh0W00
!L:'00.j0/-)(-Q0*M,J000V00(00
```

The terminal window includes a menu bar with "File", "Edit", "View", "Terminal", "Tabs", and "Help". The status bar at the bottom shows the time as "Mon 29 Aug, 16:30" and the user as "uca".

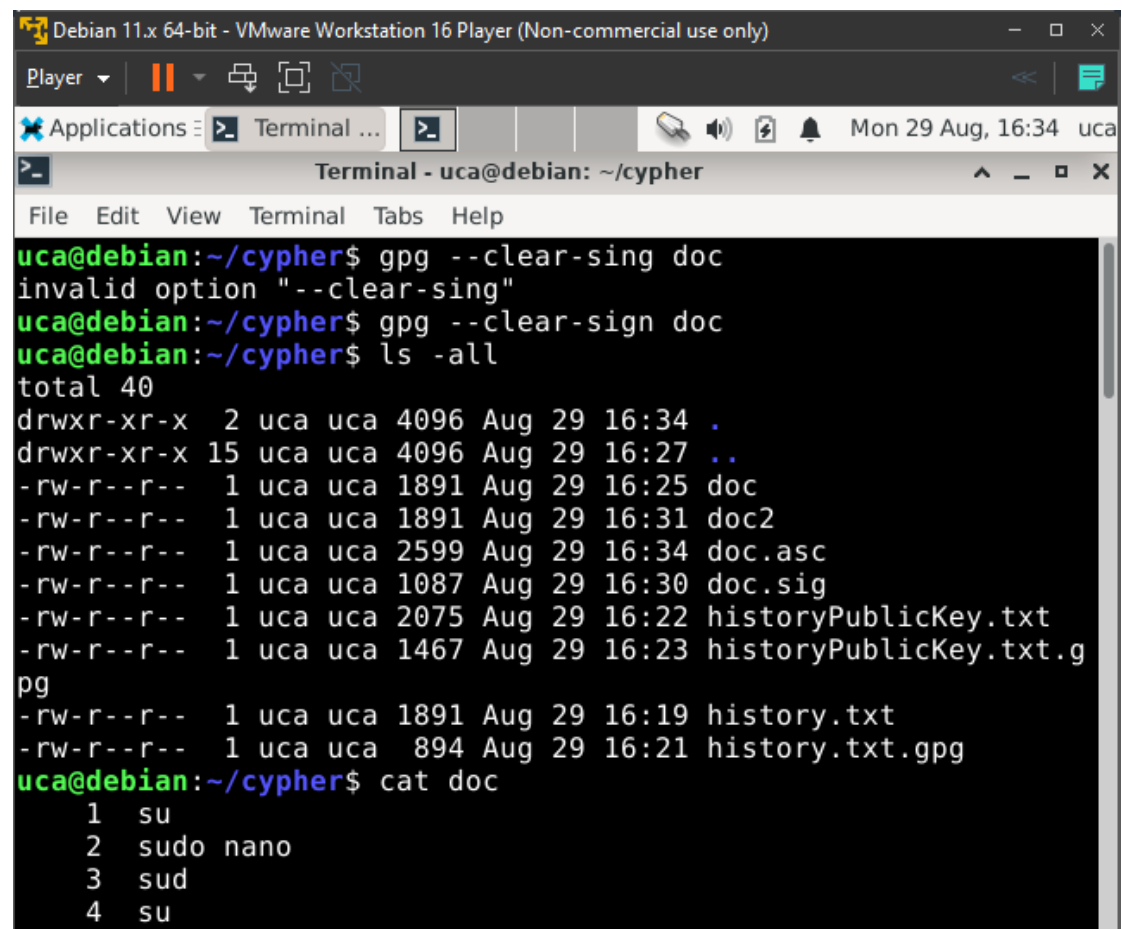
Descifrado documento firmado



The screenshot shows a terminal window titled "Terminal - uca@debian: ~/cypher" within a "Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)" environment. The terminal displays the following commands and output:

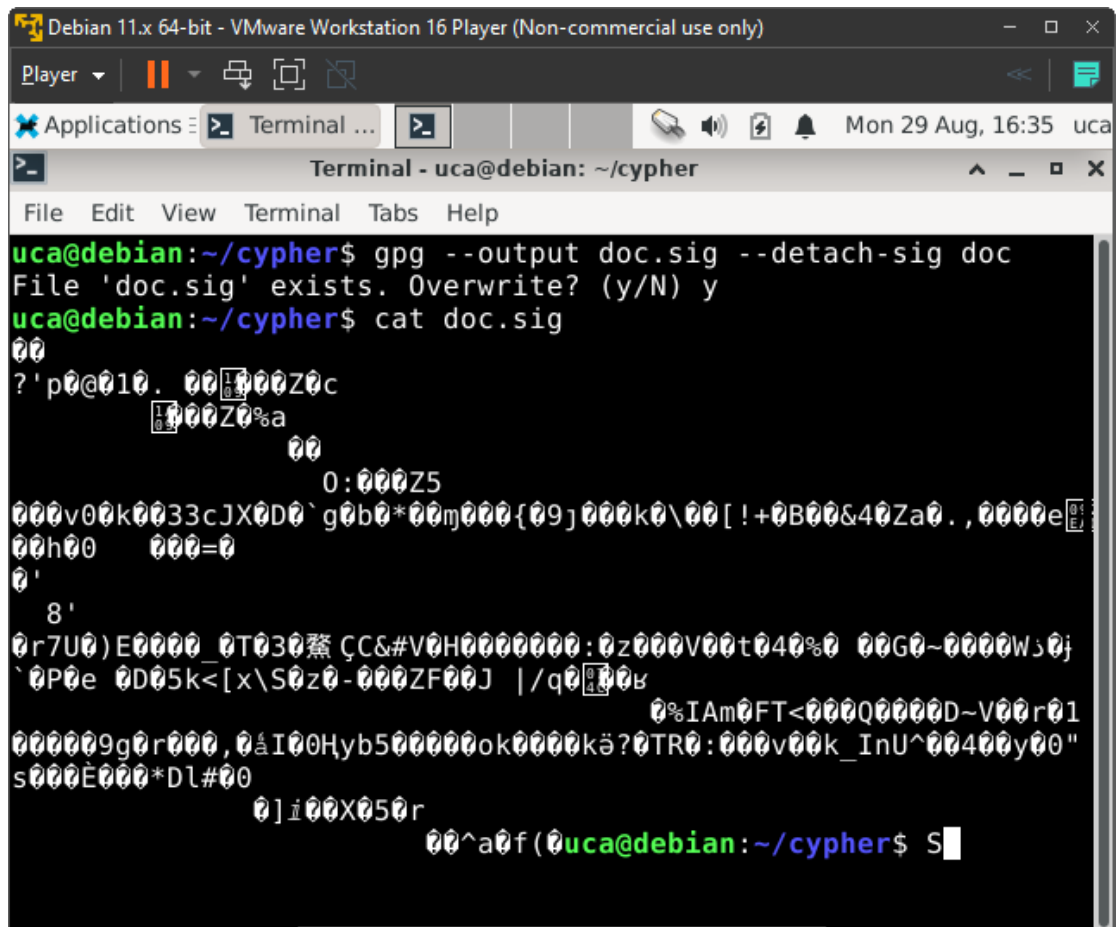
```
uca@debian:~/cypher$ gpg --output doc --decrypt doc.sig
File 'doc' exists. Overwrite? (y/N) N
Enter new filename: doc2
gpg: Signature made Mon 29 Aug 2022 04:30:16 PM CST
gpg:                using RSA key 2C70F14013CB31BD2E209FF8E1A8
89FD80865AF3
gpg: Good signature from "Oscar Juarez (juarezgonzalez) <00126
320@uca.edu.sv>" [ultimate]
uca@debian:~/cypher$ cat doc2
1  su
2  sudo nano
3  sud
4  su
5  sudo nano
6  clear
7  sudo apt install gnupg
8  gpg --full-generate-key
9  clear
10 gpg --full-generate-key
11 gpg --list-key
12 gpg --output juarez.gpg --export 000126320@uca.edu.sv
```

Quitando la firma al documento



```
Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications Terminal ...
Terminal - uca@debian: ~/cypher
File Edit View Terminal Tabs Help
uca@debian:~/cypher$ gpg --clear-sing doc
invalid option "--clear-sing"
uca@debian:~/cypher$ gpg --clear-sign doc
uca@debian:~/cypher$ ls -all
total 40
drwxr-xr-x  2 uca uca 4096 Aug 29 16:34 .
drwxr-xr-x 15 uca uca 4096 Aug 29 16:27 ..
-rw-r--r--  1 uca uca 1891 Aug 29 16:25 doc
-rw-r--r--  1 uca uca 1891 Aug 29 16:31 doc2
-rw-r--r--  1 uca uca 2599 Aug 29 16:34 doc.asc
-rw-r--r--  1 uca uca 1087 Aug 29 16:30 doc.sig
-rw-r--r--  1 uca uca 2075 Aug 29 16:22 historyPublicKey.txt
-rw-r--r--  1 uca uca 1467 Aug 29 16:23 historyPublicKey.txt.g
pg
-rw-r--r--  1 uca uca 1891 Aug 29 16:19 history.txt
-rw-r--r--  1 uca uca  894 Aug 29 16:21 history.txt.gpg
uca@debian:~/cypher$ cat doc
1 su
2 sudo nano
3 sud
4 su
```

Usando firmas desacopladas

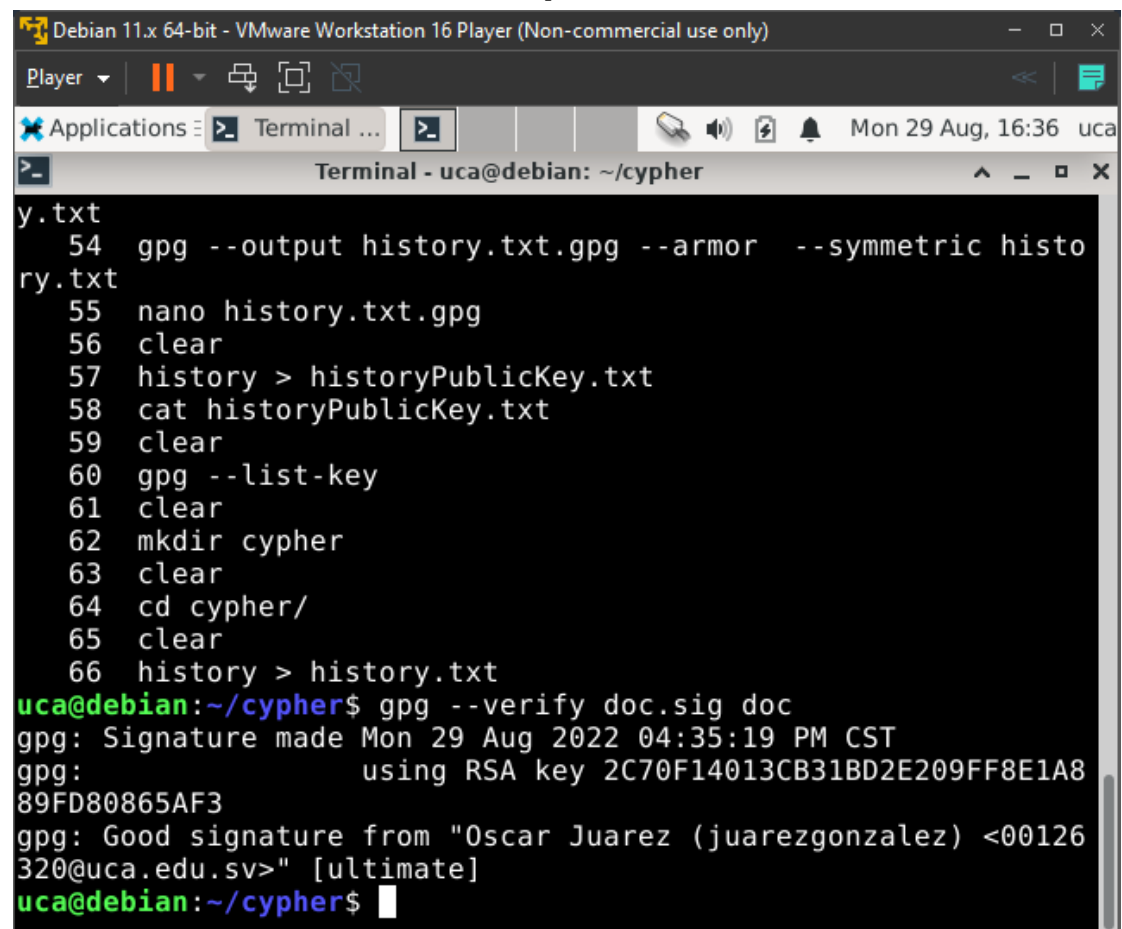


The screenshot shows a terminal window titled "Terminal - uca@debian: ~/cypher" within a "Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)" environment. The terminal output shows the execution of the following commands:

```
uca@debian:~/cypher$ gpg --output doc.sig --detach-sig doc
File 'doc.sig' exists. Overwrite? (y/N) y
uca@debian:~/cypher$ cat doc.sig
```

The output of the `cat doc.sig` command is a detached signature, represented as a block of Base64-encoded text. The signature begins with the ASCII armor header `?p0010. 000000Z0c` and ends with the ASCII armor trailer `00^a0f(uca@debian:~/cypher$ S`.

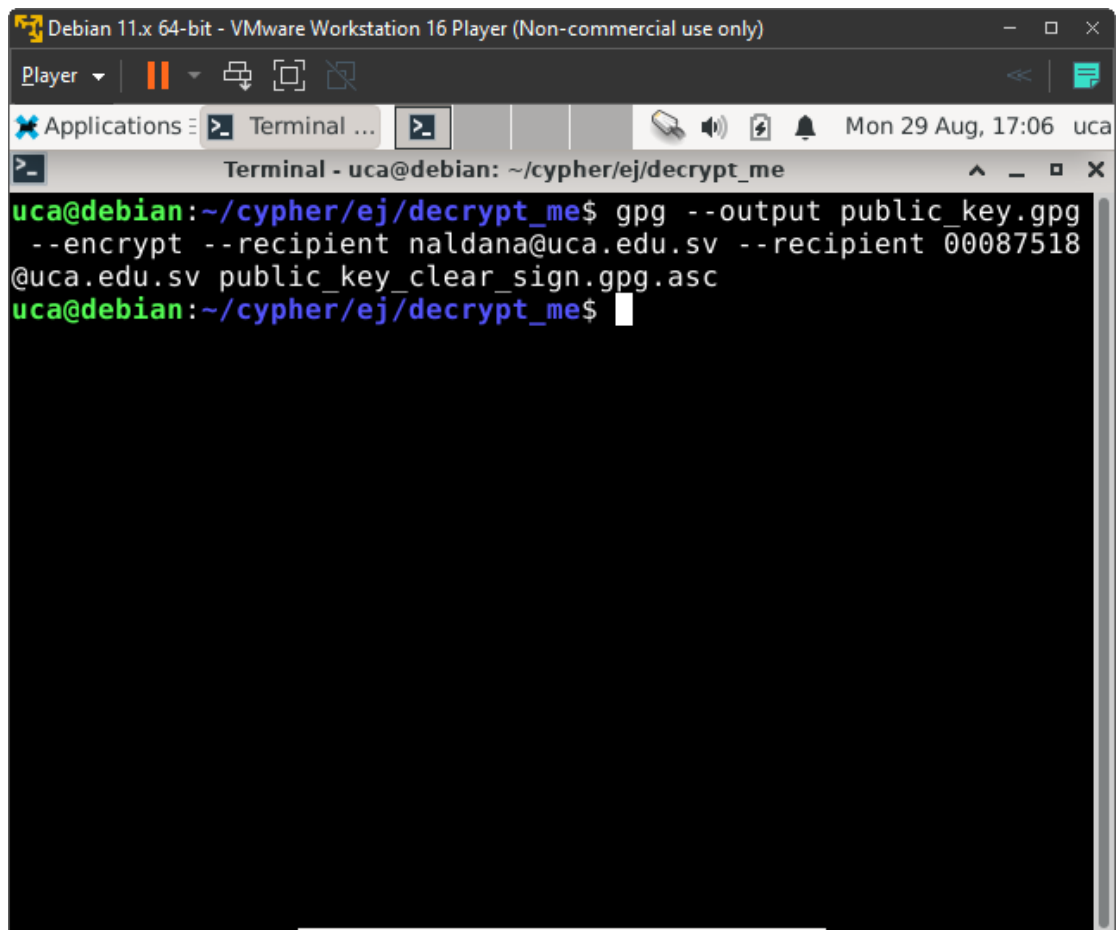
Verificando firmas desacopladas



```
Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications Terminal ...
Terminal - uca@debian: ~/cypher
y.txt
54 gpg --output history.txt.gpg --armor --symmetric histo
ry.txt
55 nano history.txt.gpg
56 clear
57 history > historyPublicKey.txt
58 cat historyPublicKey.txt
59 clear
60 gpg --list-key
61 clear
62 mkdir cypher
63 clear
64 cd cypher/
65 clear
66 history > history.txt
uca@debian:~/cypher$ gpg --verify doc.sig doc
gpg: Signature made Mon 29 Aug 2022 04:35:19 PM CST
gpg: using RSA key 2C70F14013CB31BD2E209FF8E1A8
89FD80865AF3
gpg: Good signature from "Oscar Juarez (juarezgonzalez) <00126
320@uca.edu.sv>" [ultimate]
uca@debian:~/cypher$
```

EJERCICIO

2. Encriptando con recipientes Miguel Y Nestor.

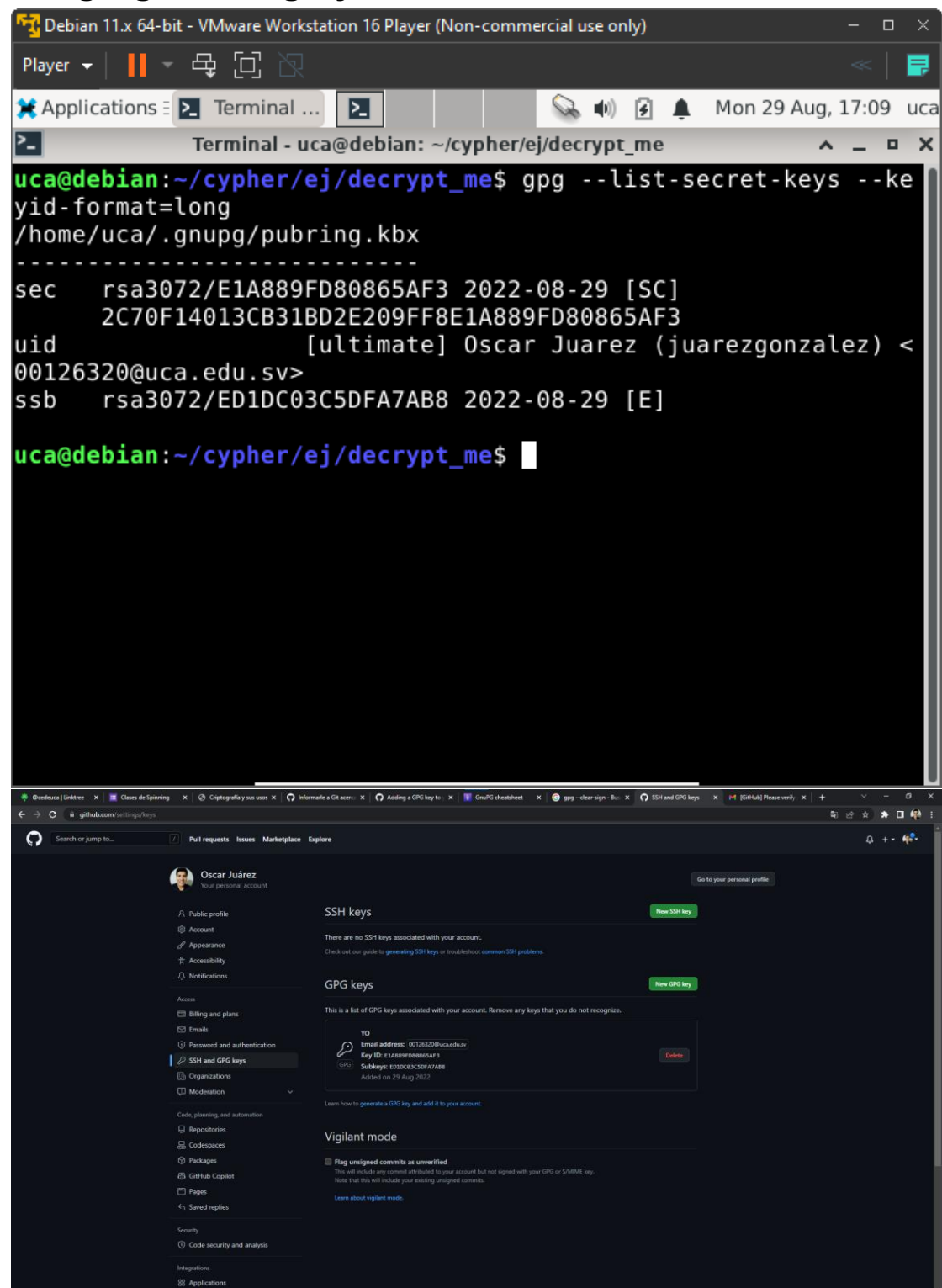


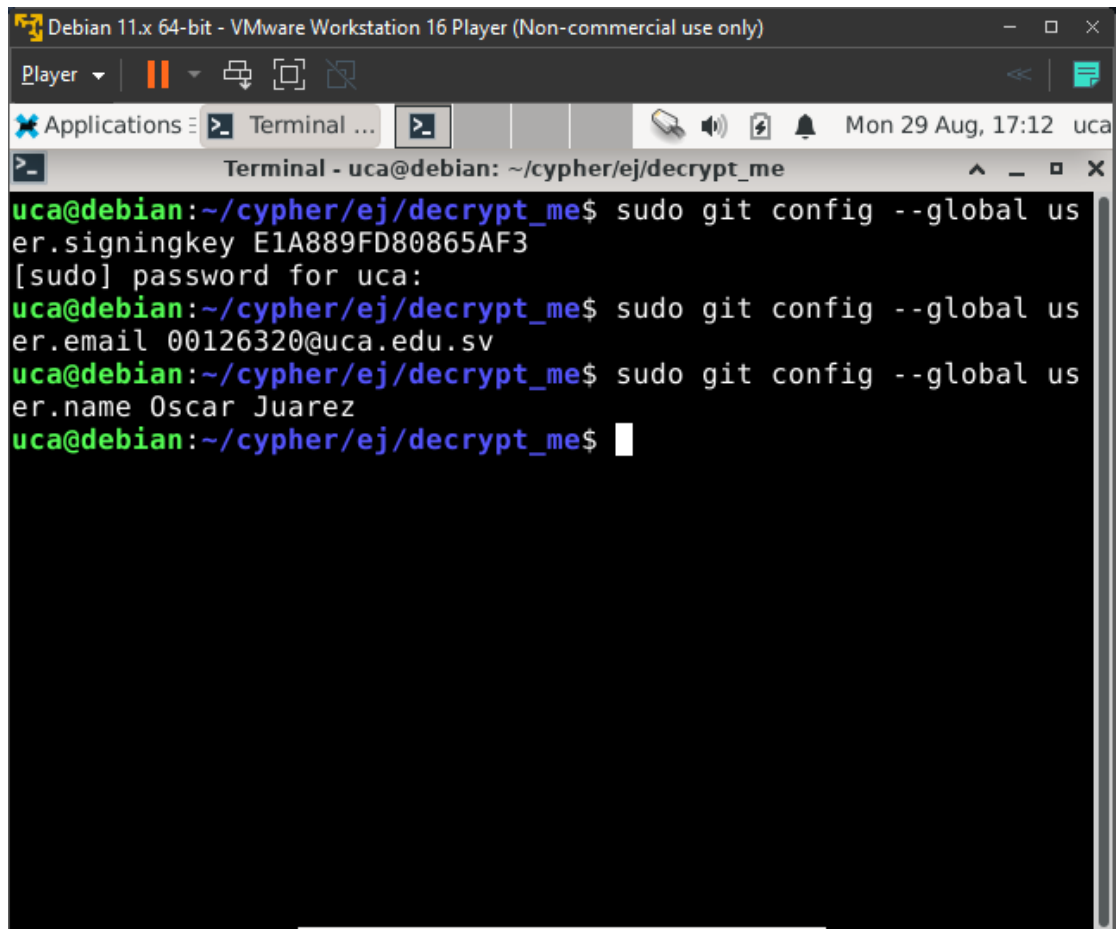
The screenshot shows a terminal window titled "Terminal - uca@debian: ~/cypher/ej/decrypt_me" within a "Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)" environment. The terminal displays the following command and output:

```
uca@debian:~/cypher/ej/decrypt_me$ gpg --output public_key.gpg  
--encrypt --recipient naldana@uca.edu.sv --recipient 00087518  
@uca.edu.sv public_key_clear_sign.gpg.asc  
uca@debian:~/cypher/ej/decrypt_me$
```

```
Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications
Terminal ...
Terminal - uca@debian: ~/cypher/ej/decrypt_me
uca@debian:~/cypher/ej/decrypt_me$ gpg --output public_key.gpg
--encrypt --recipient naldana@uca.edu.sv --recipient 00087518
@uca.edu.sv public_key_clear_sign.gpg.asc
uca@debian:~/cypher/ej/decrypt_me$ cat public_key
cat: public_key: No such file or directory
uca@debian:~/cypher/ej/decrypt_me$ cat public_key.gpg
000G00r00
00c00f]s00
l0Mw[0 .o00000Q00000-[@0000b000l00^F004y00<0J00000000fy0z00(0
^002H0E00:000000ggoZp0[0Z05!Uc
000V0000600pR,0000`G}00
00D0$00b0[# 0w0;000
0!0Z0!0N0(007z0H00p0U<0
0}0000 J00Si0
0E0T0002R000P?wz0000J0`t00B00Y0M0"00me?UmbY000,e0
00r|ly000xJ:00o"v0000 X0Re0@000i0*700#d500000!006 '0F00I30!0
00K000YlG0e!0wp0{00L_00E50000000090
0w0 '/i00100E?T0WY700C>0瀟0
N 000x"00Uq9000x00o]W00Y90r00000=0000j:00000@00ry00j0.0 i0vM00
s0N:0u00-H00Mo0^0000 0
0Y^V0:7,0k"000A0000L70o00)0#y100q00?0=0Ks0/0#.w:e'C00{30
```

3. Agregando a git y haciendo commit





```
Debian 11.x 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications
Terminal ...
Terminal - uca@debian: ~/cypher/ej/decrypt_me
uca@debian:~/cypher/ej/decrypt_me$ sudo git config --global user.signingkey E1A889FD80865AF3
[sudo] password for uca:
uca@debian:~/cypher/ej/decrypt_me$ sudo git config --global user.email 00126320@uca.edu.sv
uca@debian:~/cypher/ej/decrypt_me$ sudo git config --global user.name Oscar Juarez
uca@debian:~/cypher/ej/decrypt_me$
```