# SEGURIDAD ENCRIPTADA

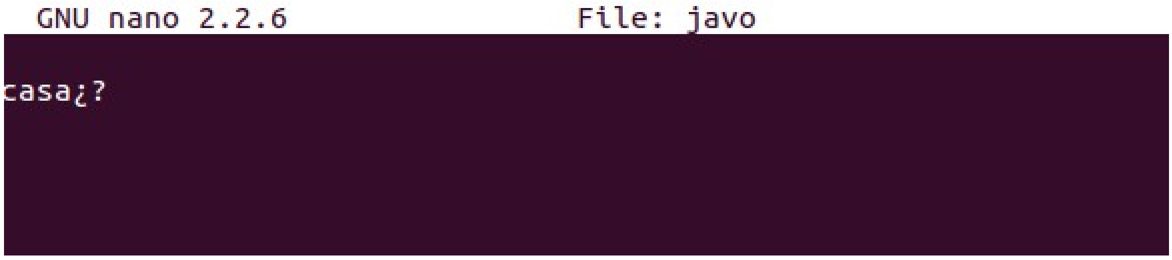
# GPG

JAVIER BORBOLLA UREÑA

# Ejercicio 1

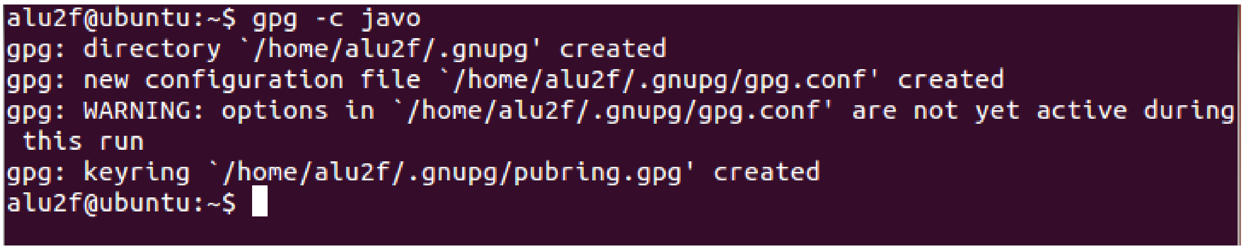
## *Cifrado simetrico*

1. Creo un documento con un texto



```
  GNU nano 2.2.6                 File: javo

casa¿?
```

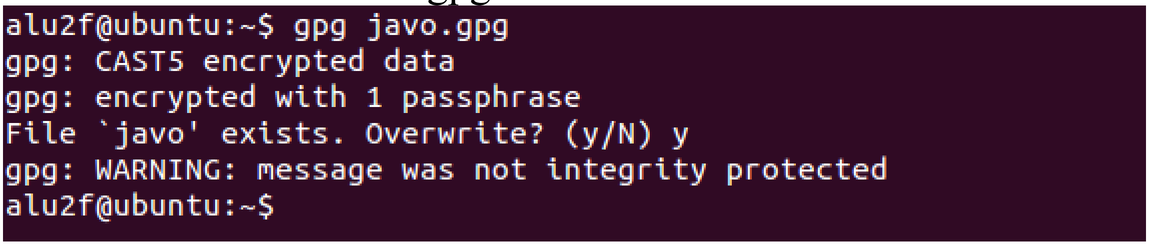
2. Lo cifro con una contraseña



```
alu2f@ubuntu:~$ gpg -c javo
gpg: directory `/home/alu2f/.gnupg' created
gpg: new configuration file `/home/alu2f/.gnupg/gpg.conf' created
gpg: WARNING: options in `/home/alu2f/.gnupg/gpg.conf' are not yet active during
 this run
gpg: keyring `/home/alu2f/.gnupg/pubring.gpg' created
alu2f@ubuntu:~$ 
```

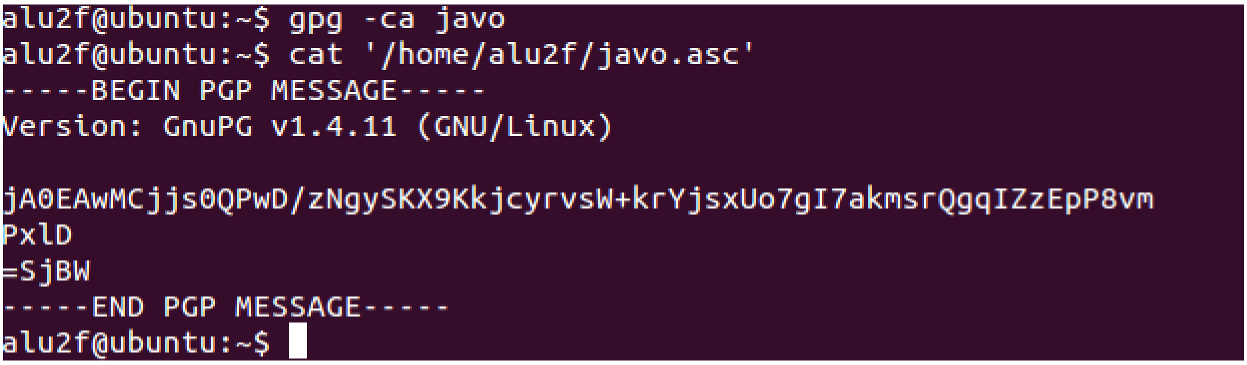
3. No tengo compañero porque estoy en mi casa. (Sad-time)

4. Descifro el documento gpg



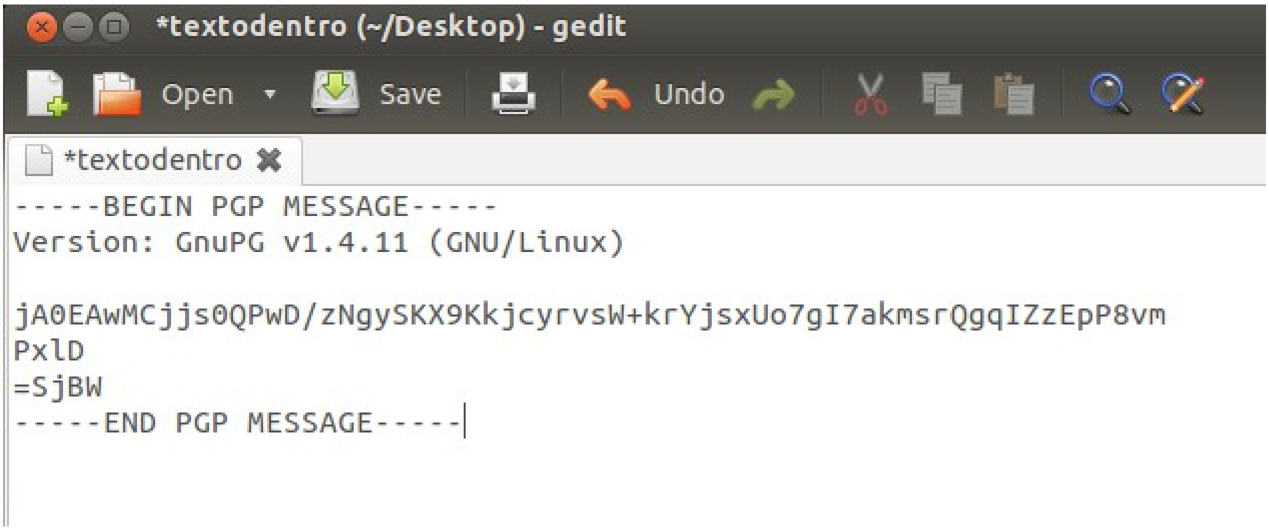
```
alu2f@ubuntu:~$ gpg javo.gpg
gpg: CAST5 encrypted data
gpg: encrypted with 1 passphrase
File `javo' exists. Overwrite? (y/N) y
gpg: WARNING: message was not integrity protected
alu2f@ubuntu:~$
```

5. Ahora vuelvo a cifrarlo con el parametro "a"



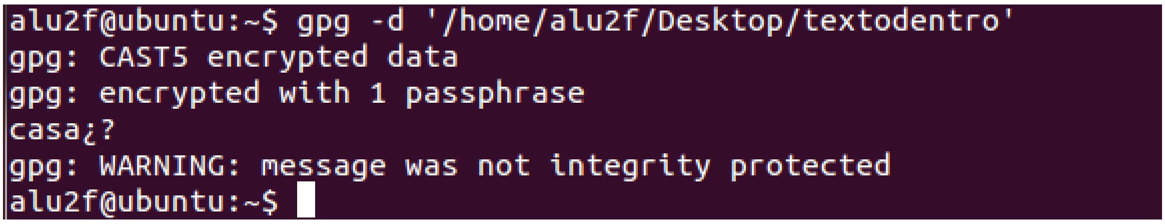
```
alu2f@ubuntu:~$ gpg -ca javo
alu2f@ubuntu:~$ cat '/home/alu2f/javo.asc'
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.11 (GNU/Linux)

jA0EAwMCjjs0QPwD/zNgySKX9KkjcyrvsW+krYjsxUo7gI7akmsrQgqIZzEpP8vm
PxlD
=SjBW
-----END PGP MESSAGE-----
alu2f@ubuntu:~$
```

6.Escribo el contenido en un texto



```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.11 (GNU/Linux)

jA0EAwMCjjs0QPwD/zNgySKX9KkjcyrvsW+krYjsxUo7gI7akmsrQgqIZzEpP8vm
PxlD
=SjBW
-----END PGP MESSAGE-----
```

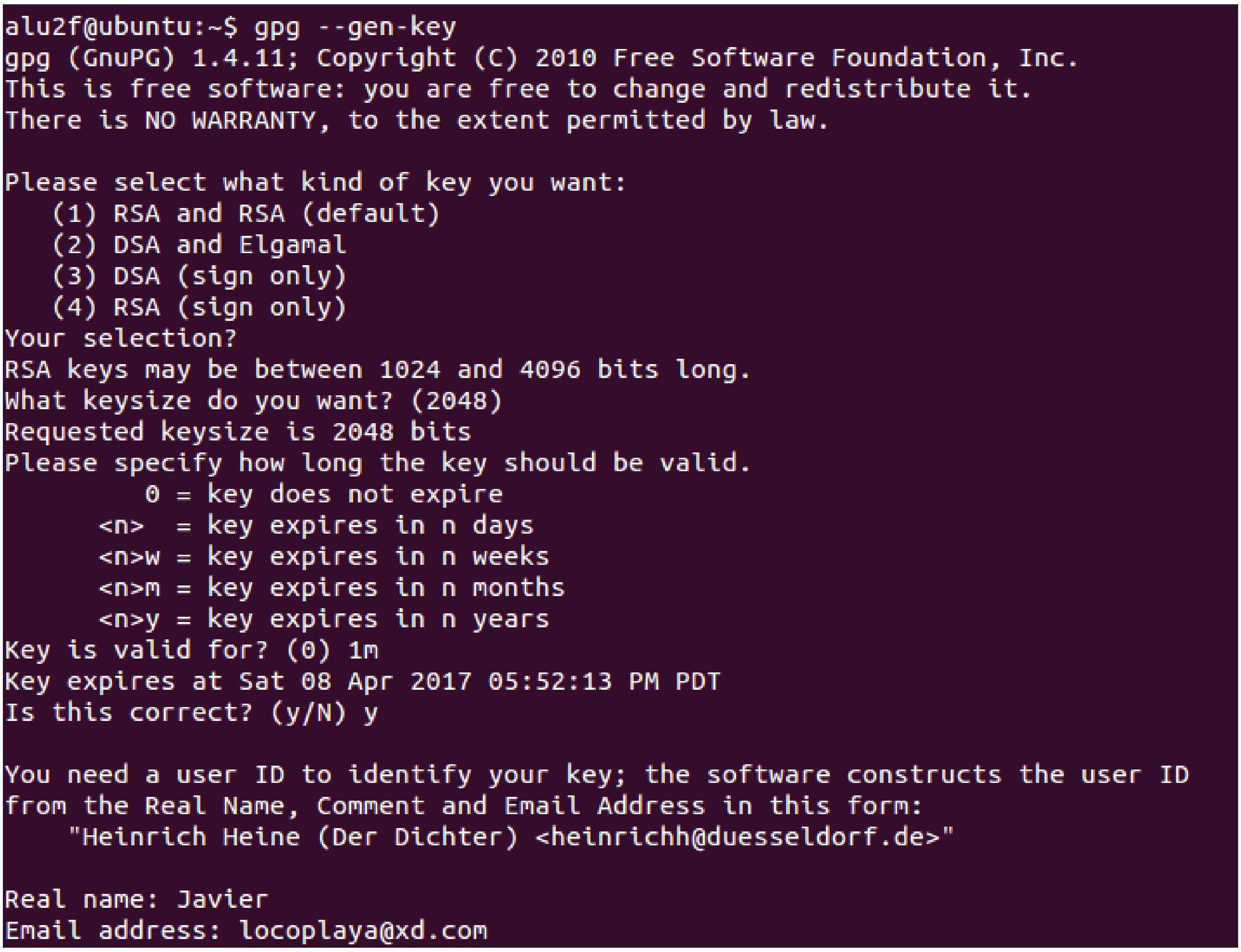
7.Y ahora lo descifro



```
alu2f@ubuntu:~$ gpg -d '/home/alu2f/Desktop/textodentro'
gpg: CAST5 encrypted data
gpg: encrypted with 1 passphrase
casa¿?
gpg: WARNING: message was not integrity protected
alu2f@ubuntu:~$
```

# Ejercicio 2
# *Claves publicas y privadas*

1.La clave durará 1 mes

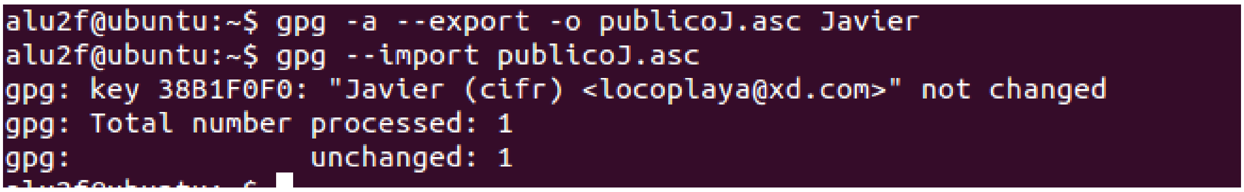


```
alu2f@ubuntu:~$ gpg --gen-key
gpg (GnuPG) 1.4.11; Copyright (C) 2010 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

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)
Your selection?
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048)
Requested keysize is 2048 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) 1m
Key expires at Sat 08 Apr 2017 05:52:13 PM PDT
Is this correct? (y/N) y

You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: Javier
Email address: locoplaya@xd.com
```

# Ejercicio 3

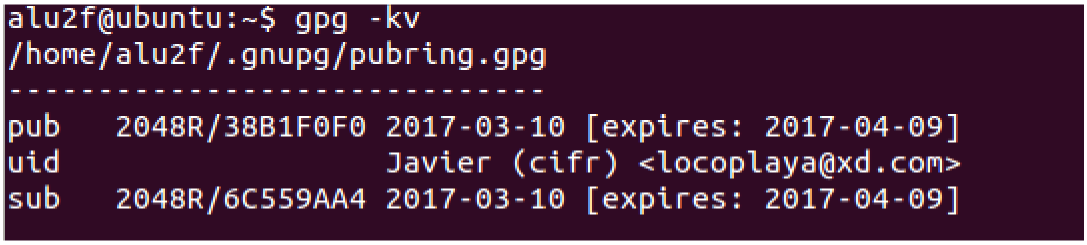
## *Exportar/Importar clave pública*

1. Exporto mi clave publica y luego la exporto



```
alu2f@ubuntu:~$ gpg -a --export -o publicoJ.asc Javier
alu2f@ubuntu:~$ gpg --import publicoJ.asc
gpg: key 38B1F0F0: "Javier (cifr) <locoplaya@xd.com>" not changed
gpg: Total number processed: 1
gpg:               unchanged: 1
alu2f@ubuntu:~$ 
```

2. Aqui también deberia de salir el de mi compañero peero bueno :/

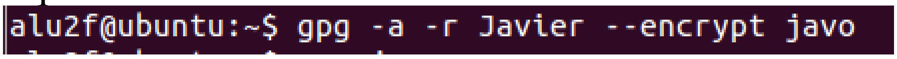


```
alu2f@ubuntu:~$ gpg -kv
/home/alu2f/.gnupg/pubring.gpg
------------------------------
pub   2048R/38B1F0F0 2017-03-10 [expires: 2017-04-09]
uid                  Javier (cifr) <locoplaya@xd.com>
sub   2048R/6C559AA4 2017-03-10 [expires: 2017-04-09]
```

# Ejercicio 4

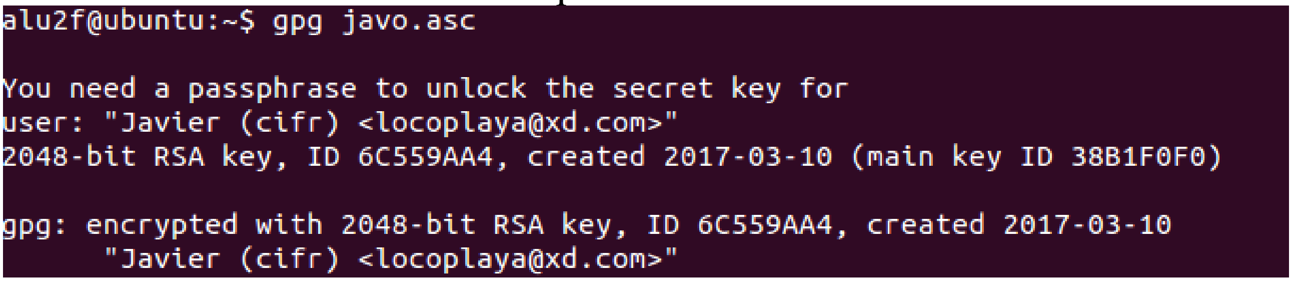
## *Cifrado/Descifrado de un documento*

1. Comprendo que si tuviese guardada la clave publica de un compañero tendría que poner donde pone "Javier" la ID de la clave del compañero.



```
alu2f@ubuntu:~$ gpg -a -r Javier --encrypt javo
```

2. Ahora descifro el archivo que he cifrado antes.



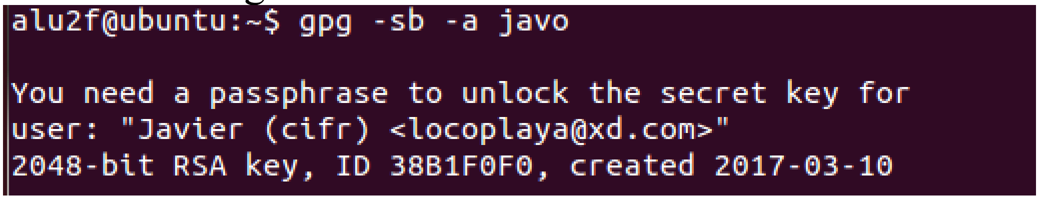
```
alu2f@ubuntu:~$ gpg javo.asc

You need a passphrase to unlock the secret key for
user: "Javier (cifr) <locoplaya@xd.com>"
2048-bit RSA key, ID 6C559AA4, created 2017-03-10 (main key ID 38B1F0F0)

gpg: encrypted with 2048-bit RSA key, ID 6C559AA4, created 2017-03-10
      "Javier (cifr) <locoplaya@xd.com>"
```

3.

# Ejercicio 5

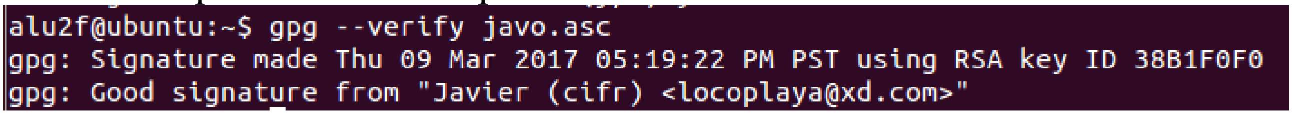
## *Firma digital*

1. Creo la firma digital



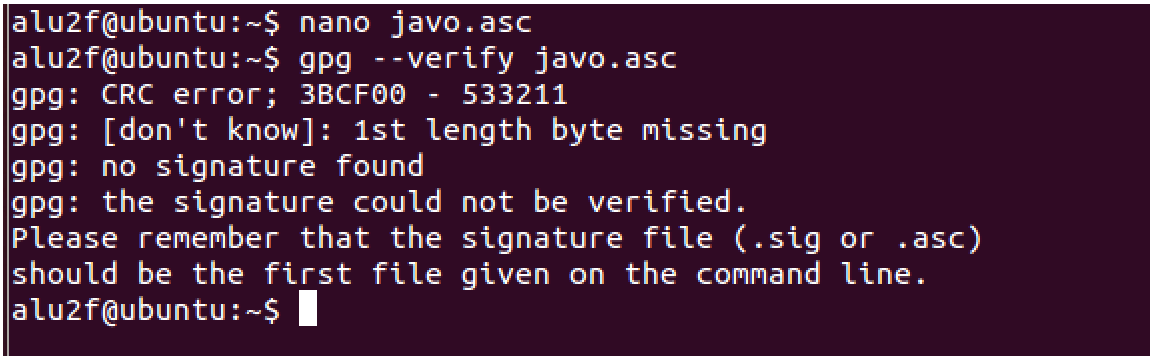
```
alu2f@ubuntu:~$ gpg -sb -a javo

You need a passphrase to unlock the secret key for
user: "Javier (cifr) <locoplaya@xd.com>"
2048-bit RSA key, ID 38B1F0F0, created 2017-03-10
```

2.Verifico que está firmado por mi



```
alu2f@ubuntu:~$ gpg --verify javo.asc
gpg: Signature made Thu 09 Mar 2017 05:19:22 PM PST using RSA key ID 38B1F0F0
gpg: Good signature from "Javier (cifr) <locoplaya@xd.com>"
```

3.Por ultimo modifico el archivo y lo verifico otra vez



```
alu2f@ubuntu:~$ nano javo.asc
alu2f@ubuntu:~$ gpg --verify javo.asc
gpg: CRC error; 3BCF00 - 533211
gpg: [don't know]: 1st length byte missing
gpg: no signature found
gpg: the signature could not be verified.
Please remember that the signature file (.sig or .asc)
should be the first file given on the command line.
alu2f@ubuntu:~$ █
```

Efectivamente, como lo he cambiado, no encuentra mi firma