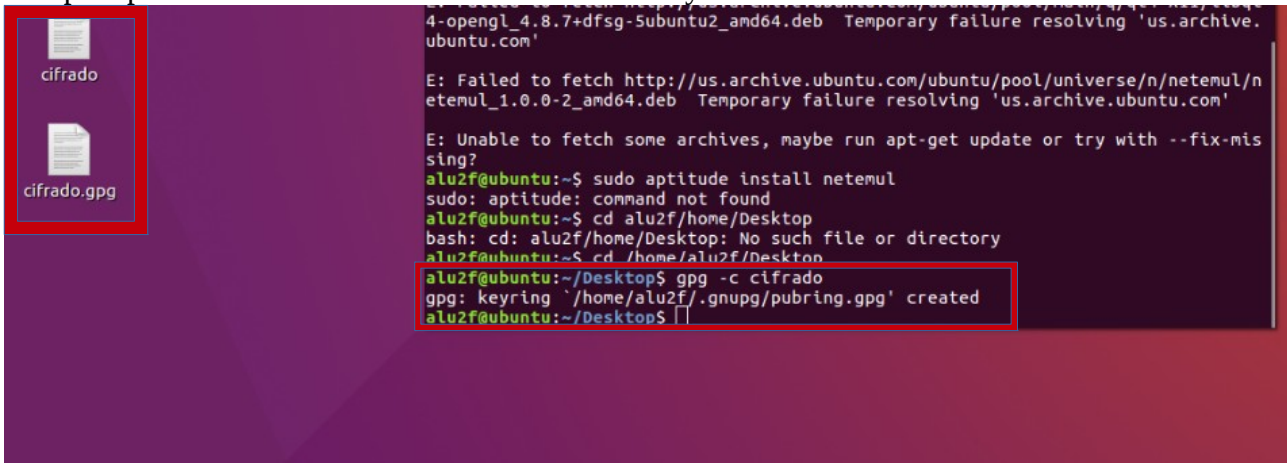


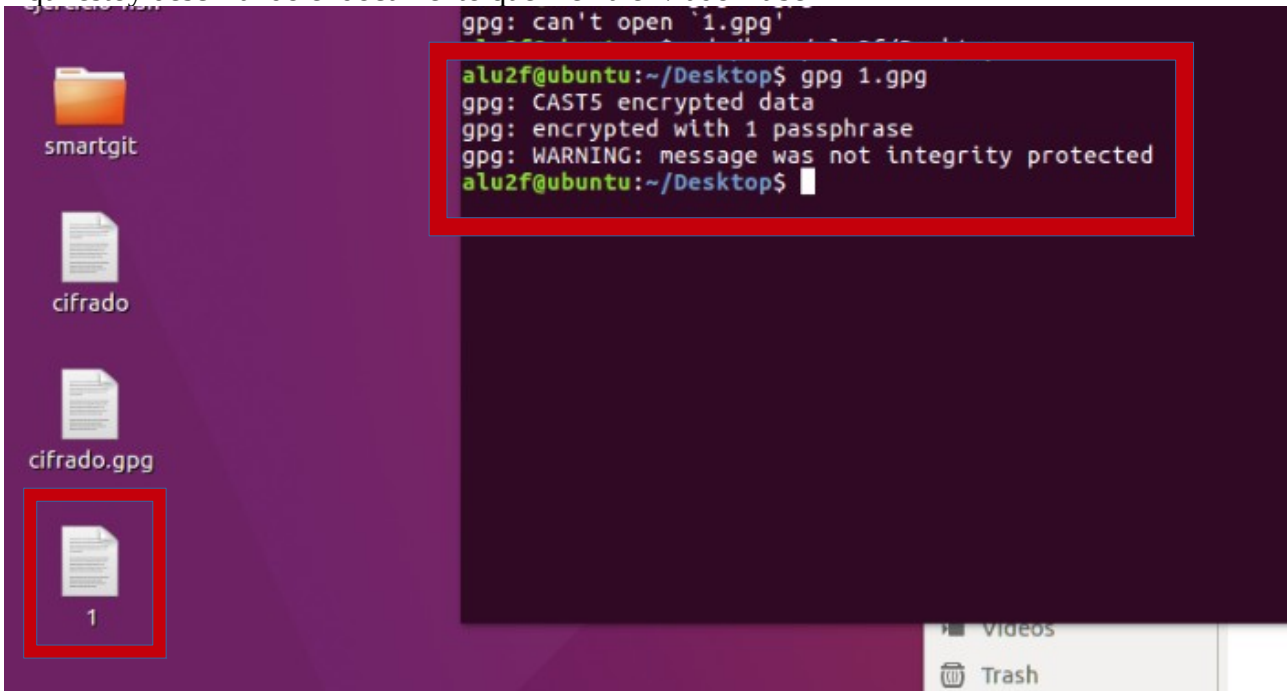
PRÁCTICA DE CRIPTOGRAFÍA

1) El ejercicio 1 lo realicé con mi compañero Rubén.

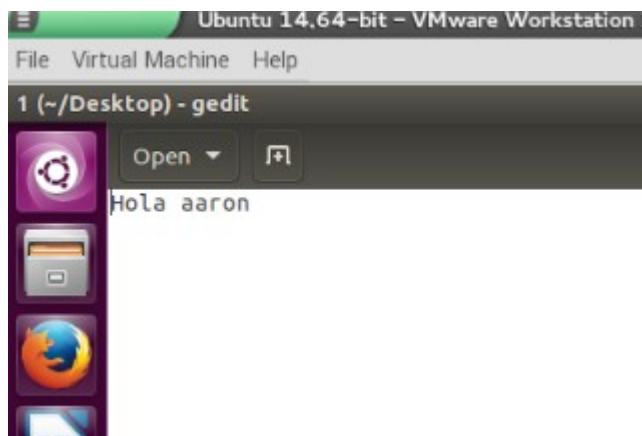
Nos pide primeramente crear un documento de texto y cifrarlo.



Aquí estoy descifrando el documento que me ha enviado Rubén



Al descifrarlo muestra el mensaje del documento de texto.



Despues tenemos que cifrarlo otra vez pero añadiendo la opción -a.

```
alu2f@ubuntu: ~/Desktop
alu2f@ubuntu:~$ gpg 1.gpg
gpg: can't open '1.gpg'
alu2f@ubuntu:~$ cd /home/alu2f/Desktop
alu2f@ubuntu:~/Desktop$ gpg 1.gpg
gpg: CAST5 encrypted data
gpg: encrypted with 1 passphrase
gpg: WARNING: message was not integrity protected
alu2f@ubuntu:~/Desktop$ gpg -ca cifrado
alu2f@ubuntu:~/Desktop$
```

Seguidamente mostramos el contenido con la opción cat y comprobamos que se ha cifrado correctamente

```
gpg: WARNING: Message was not integrity protected
alu2f@ubuntu:~/Desktop$ gpg -ca cifrado
alu2f@ubuntu:~/Desktop$ cat 1.asc
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.11 (GNU/Linux)

jA0EAWMCZWkInTAQfJFgySJg2ghFe49D/1HEFrZgqvP6qk32mw0AxGD6RlsxLMxC
SXXF
=5Tbt
-----END PGP MESSAGE-----
alu2f@ubuntu:~/Desktop$
```

2)El ejercicio 2 nos pide crear un par de claves pública y privada, y que tenga de validez 1 mes. Tenemos que usar el comando `gpg --gen-key`.

```
Virtual Machine Help
alu2f@ubuntu: ~/Desktop
alu2f@ubuntu:~/Desktop$ gpg --gen-key
gpg (GnuPG) 1.4.20; Copyright (C) 2015 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? 1
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 Thu 06 Apr 2017 12:34:20 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: Aaron
Email address: heyron53@gmail.com
Comment:
You selected this USER-ID:
    "Aaron <heyron53@gmail.com>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit?
Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? o
You need a Passphrase to protect your secret key.

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.
```

Aquí marcamos que queremos que la clave dure 1 mes.

También tenemos que añadir un nombre y un gmail para la identificación.

```
Virtual Machine Help
2f@ubuntu: ~/Desktop
You selected this USER ID:
"Aaron <heyron53@gmail.com>"
Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit?
Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? o
You need a Passphrase to protect your secret key.

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.

Not enough random bytes available. Please do some other work to give
the OS a chance to collect more entropy! (Need 186 more bytes)

.+++++
.....+++++
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.

Not enough random bytes available. Please do some other work to give
the OS a chance to collect more entropy! (Need 82 more bytes)
...+++++

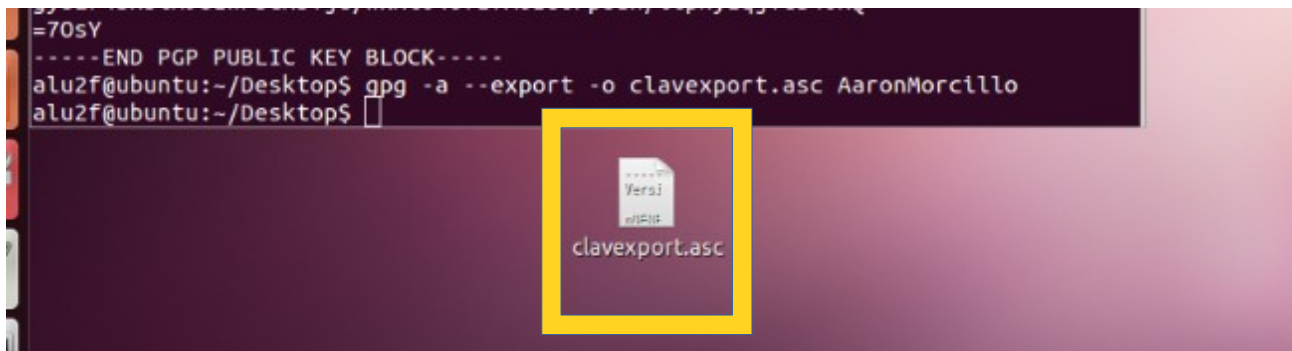
Not enough random bytes available. Please do some other work to give
the OS a chance to collect more entropy! (Need 55 more bytes)
....+++++
gpg: /home/alu2f/.gnupg/trustdb.gpg: trustdb created
gpg: key AB876D91 marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0 valid: 1 signed: 0 trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2017-04-06
pub 2048R/AB876D91 2017-03-07 [expires: 2017-04-06]
    Key fingerprint = 3C0D BD44 410A 0E35 ED67 A350 687F 95E7 AB87 6D91
uid                                Aaron <heyron53@gmail.com>
sub 2048R/103F04A5 2017-03-07 [expires: 2017-04-06]
```

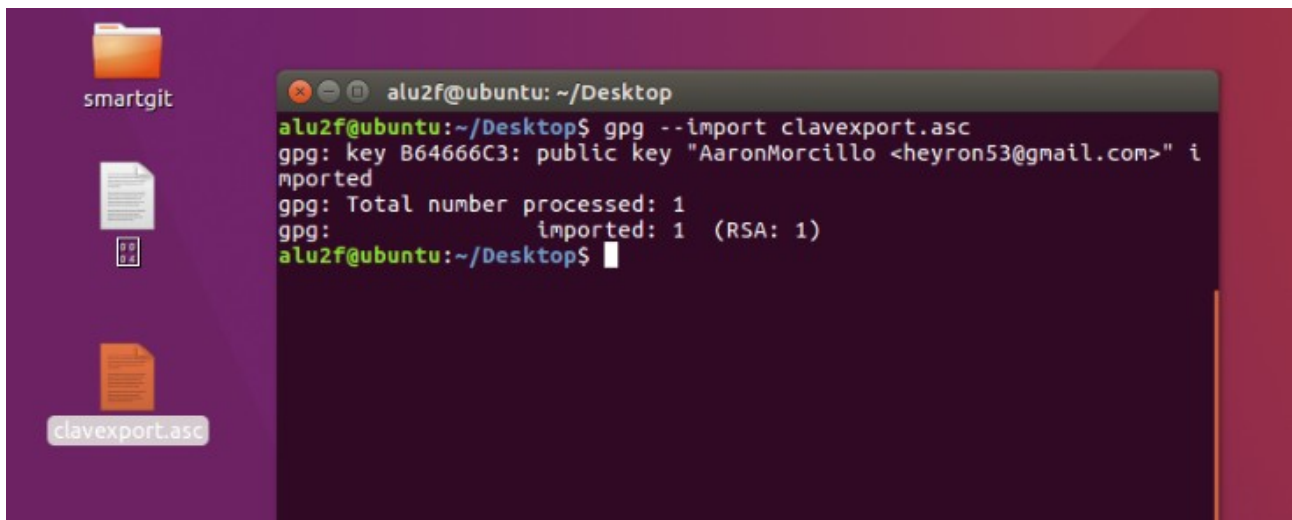
Tras completar la configuración las claves se habrán creado

3) En este ejercicio he utilizado 2 máquinas virtuales.

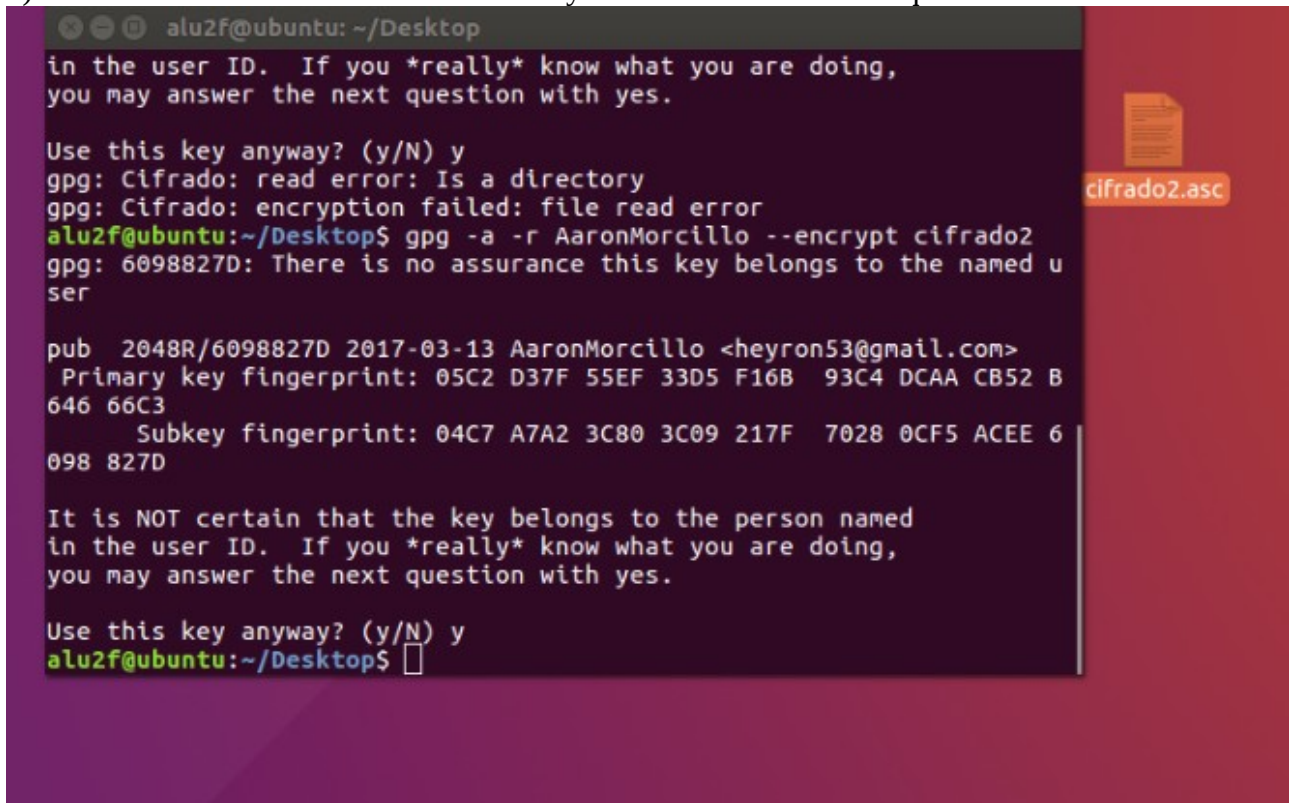
Primero tenemos que exportar las claves públicas, ese archivo lo tenemos que enviar a la otra máquina.



En la otra máquina importamos las claves con el siguiente comando, de esta forma las máquinas podrán enviarse archivos cifrados sin problemas.



4) Ahora vamos a cifrar un archivo de texto y lo enviamos a la otra máquina.

A terminal window on an Ubuntu desktop. The user is in the directory ~/Desktop. The terminal shows the execution of 'gpg -a -r AaronMorcillo --encrypt cifrado2'. It displays the key fingerprint for AaronMorcillo and asks for confirmation to use the key. The user responds 'y'. The output is a file named 'cifrado2.asc' on the desktop.

```
alu2f@ubuntu: ~/Desktop
in the user ID. If you *really* know what you are doing,
you may answer the next question with yes.

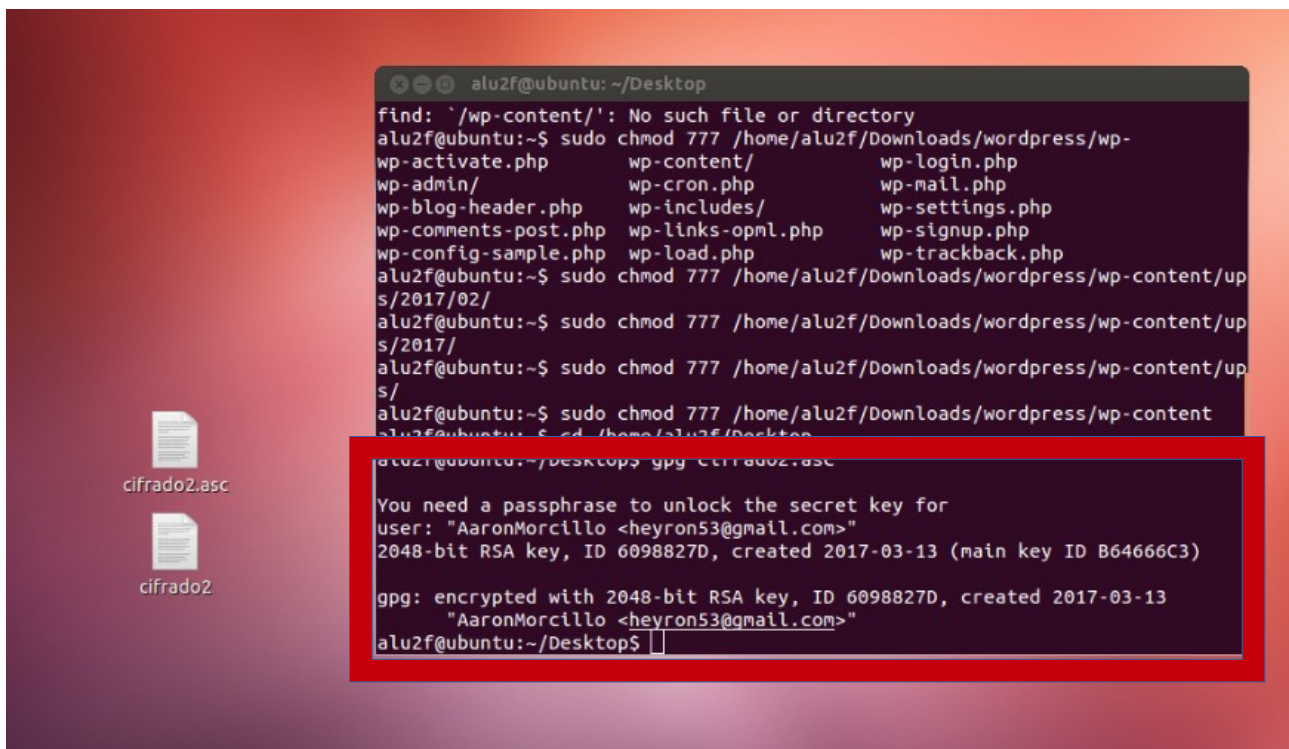
Use this key anyway? (y/N) y
gpg: Cifrado: read error: Is a directory
gpg: Cifrado: encryption failed: file read error
alu2f@ubuntu:~/Desktop$ gpg -a -r AaronMorcillo --encrypt cifrado2
gpg: 6098827D: There is no assurance this key belongs to the named u
ser

pub 2048R/6098827D 2017-03-13 AaronMorcillo <heyron53@gmail.com>
  Primary key fingerprint: 05C2 D37F 55EF 33D5 F16B 93C4 DCAA CB52 B
646 66C3
    Subkey fingerprint: 04C7 A7A2 3C80 3C09 217F 7028 0CF5 ACEE 6
098 827D

It is NOT certain that the key belongs to the person named
in the user ID. If you *really* know what you are doing,
you may answer the next question with yes.

Use this key anyway? (y/N) y
alu2f@ubuntu:~/Desktop$
```

Después tenemos que descifrar el archivo que hemos recibido.

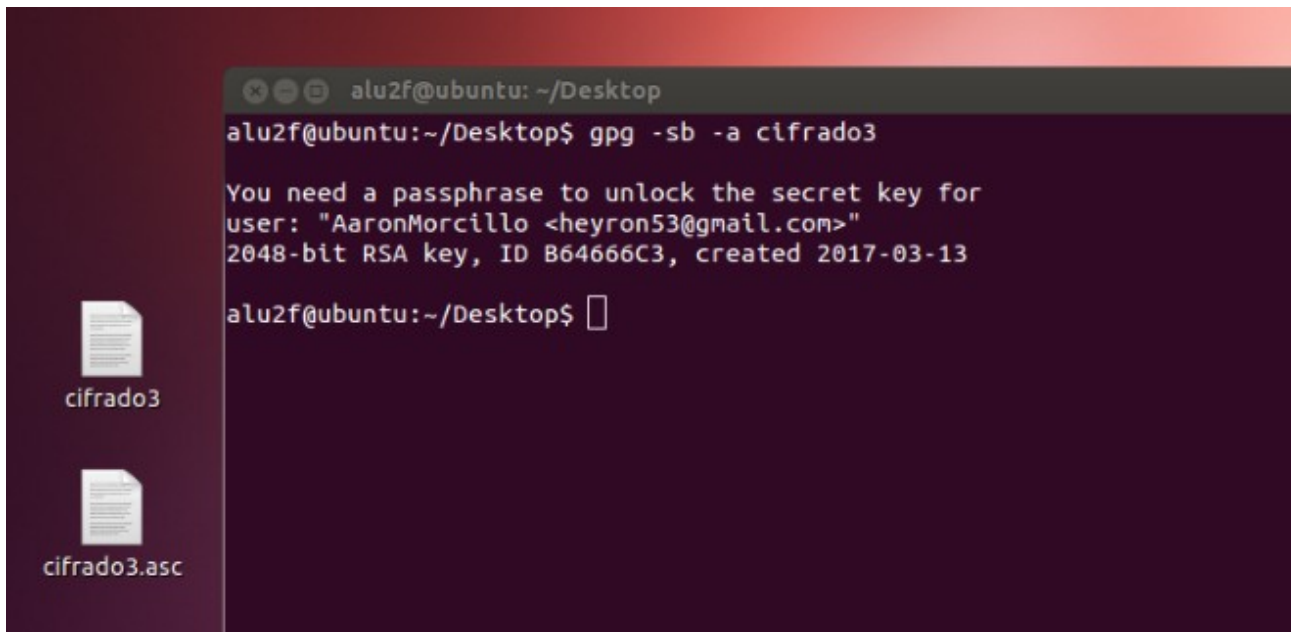
A terminal window on an Ubuntu desktop. The user is in the directory ~/Desktop. The terminal shows the execution of 'gpg -d cifrado2.asc'. It prompts for a passphrase to unlock the secret key for AaronMorcillo. The user enters the passphrase. The output is a file named 'cifrado2' on the desktop.

```
alu2f@ubuntu: ~/Desktop
find: '/wp-content/': No such file or directory
alu2f@ubuntu:~$ sudo chmod 777 /home/alu2f/Downloads/wordpress/wp-
wp-activate.php wp-content/ wp-login.php
wp-admin/ wp-cron.php wp-mail.php
wp-blog-header.php wp-includes/ wp-settings.php
wp-comments-post.php wp-links-opml.php wp-signup.php
wp-config-sample.php wp-load.php wp-trackback.php
alu2f@ubuntu:~$ sudo chmod 777 /home/alu2f/Downloads/wordpress/wp-content/up
s/2017/02/
alu2f@ubuntu:~$ sudo chmod 777 /home/alu2f/Downloads/wordpress/wp-content/up
s/2017/
alu2f@ubuntu:~$ sudo chmod 777 /home/alu2f/Downloads/wordpress/wp-content/up
s/
alu2f@ubuntu:~$ sudo chmod 777 /home/alu2f/Downloads/wordpress/wp-content
alu2f@ubuntu:~$ cd /home/alu2f/Desktop
alu2f@ubuntu:~/Desktop$ gpg -d cifrado2.asc

You need a passphrase to unlock the secret key for
user: "AaronMorcillo <heyron53@gmail.com>"
2048-bit RSA key, ID 6098827D, created 2017-03-13 (main key ID B64666C3)

gpg: encrypted with 2048-bit RSA key, ID 6098827D, created 2017-03-13
      "AaronMorcillo <heyron53@gmail.com>"
alu2f@ubuntu:~/Desktop$
```


5) En el último ejercicio hemos creado una firma digital con el siguiente comando, después enviamos el archivo a la otra máquina.



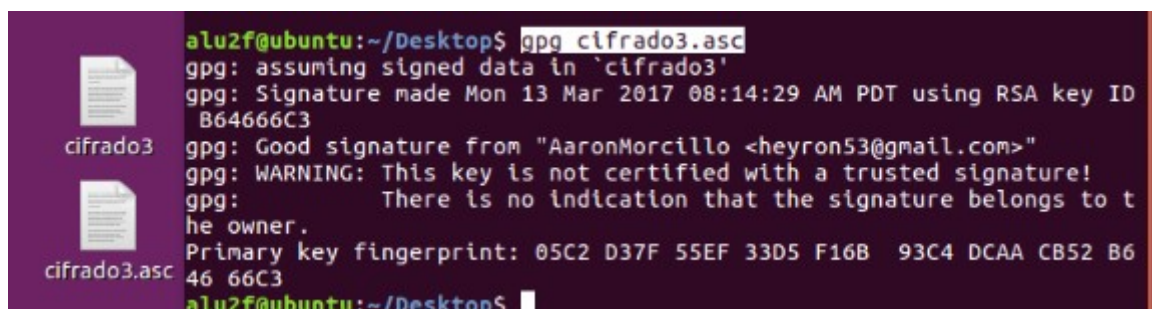
A terminal window on an Ubuntu desktop. The desktop background is dark purple. On the left, there are two file icons: 'cifrado3' and 'cifrado3.asc'. The terminal window has a title bar with window controls and the text 'alu2f@ubuntu: ~/Desktop'. The command 'gpg -sb -a cifrado3' has been entered. The output shows a prompt for a passphrase to unlock a secret key for user 'AaronMorcillo <heyron53@gmail.com>', a 2048-bit RSA key with ID B64666C3, created on 2017-03-13. The prompt is currently empty.

```
alu2f@ubuntu: ~/Desktop
alu2f@ubuntu:~/Desktop$ gpg -sb -a cifrado3

You need a passphrase to unlock the secret key for
user: "AaronMorcillo <heyron53@gmail.com>"
2048-bit RSA key, ID B64666C3, created 2017-03-13

alu2f@ubuntu:~/Desktop$
```

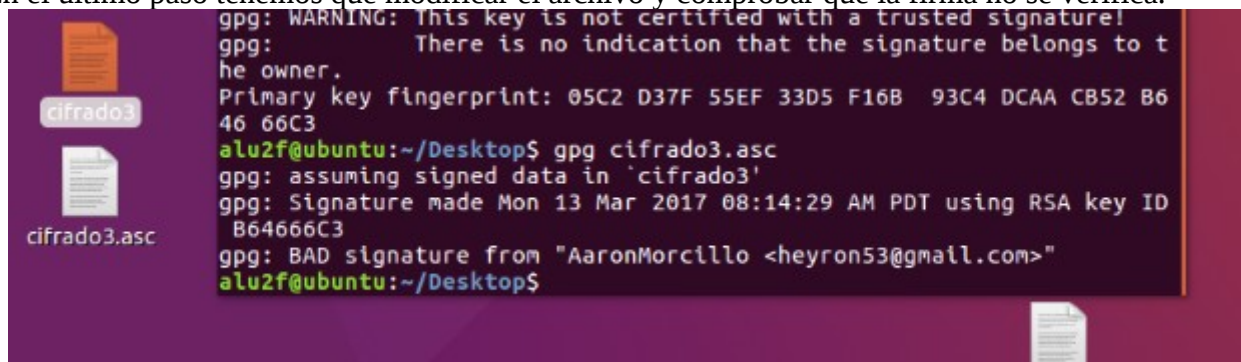
Después verificamos que la firma es correcta.



A terminal window on an Ubuntu desktop. The desktop background is dark purple. On the left, there are two file icons: 'cifrado3' and 'cifrado3.asc'. The terminal window has a title bar with window controls and the text 'alu2f@ubuntu: ~/Desktop'. The command 'gpg cifrado3.asc' has been entered. The output shows 'gpg: assuming signed data in `cifrado3`', 'gpg: Signature made Mon 13 Mar 2017 08:14:29 AM PDT using RSA key ID B64666C3', 'gpg: Good signature from "AaronMorcillo <heyron53@gmail.com>"', 'gpg: WARNING: This key is not certified with a trusted signature!', 'gpg: There is no indication that the signature belongs to the owner.', and 'Primary key fingerprint: 05C2 D37F 55EF 33D5 F16B 93C4 DCAA CB52 B646 66C3'. The prompt is currently empty.

```
alu2f@ubuntu:~/Desktop$ gpg cifrado3.asc
gpg: assuming signed data in `cifrado3`
gpg: Signature made Mon 13 Mar 2017 08:14:29 AM PDT using RSA key ID
B64666C3
gpg: Good signature from "AaronMorcillo <heyron53@gmail.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.
Primary key fingerprint: 05C2 D37F 55EF 33D5 F16B 93C4 DCAA CB52 B6
46 66C3
alu2f@ubuntu:~/Desktop$
```

En el último paso tenemos que modificar el archivo y comprobar que la firma no se verifica.



A terminal window on an Ubuntu desktop. The desktop background is dark purple. On the left, there are two file icons: 'cifrado3' and 'cifrado3.asc'. The terminal window has a title bar with window controls and the text 'alu2f@ubuntu: ~/Desktop'. The command 'gpg cifrado3.asc' has been entered. The output shows 'gpg: WARNING: This key is not certified with a trusted signature!', 'gpg: There is no indication that the signature belongs to the owner.', 'Primary key fingerprint: 05C2 D37F 55EF 33D5 F16B 93C4 DCAA CB52 B646 66C3', 'gpg: assuming signed data in `cifrado3`', 'gpg: Signature made Mon 13 Mar 2017 08:14:29 AM PDT using RSA key ID B64666C3', and 'gpg: BAD signature from "AaronMorcillo <heyron53@gmail.com>"'. The prompt is currently empty.

```
alu2f@ubuntu:~/Desktop$ gpg cifrado3.asc
gpg: assuming signed data in `cifrado3`
gpg: Signature made Mon 13 Mar 2017 08:14:29 AM PDT using RSA key ID
B64666C3
gpg: BAD signature from "AaronMorcillo <heyron53@gmail.com>"
alu2f@ubuntu:~/Desktop$
```