

Seguridad Informática

## PRÁCTICA DE CRIPTOGRAFÍA

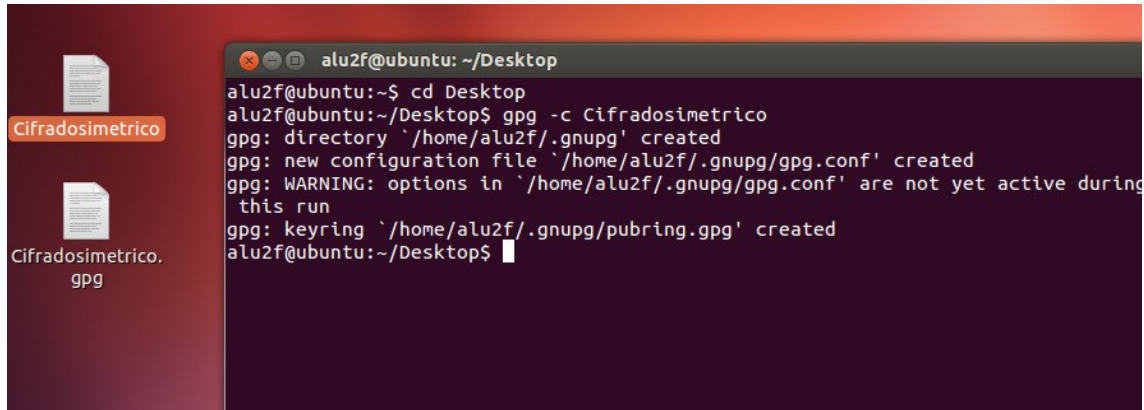
Daniel Cabrerizo San Miguel

## Cifrado simétrico

1º Creamos el documento que vamos a encriptar.

2º Ciframos el documento con alguna contraseña acordada con el compañero de al lado.

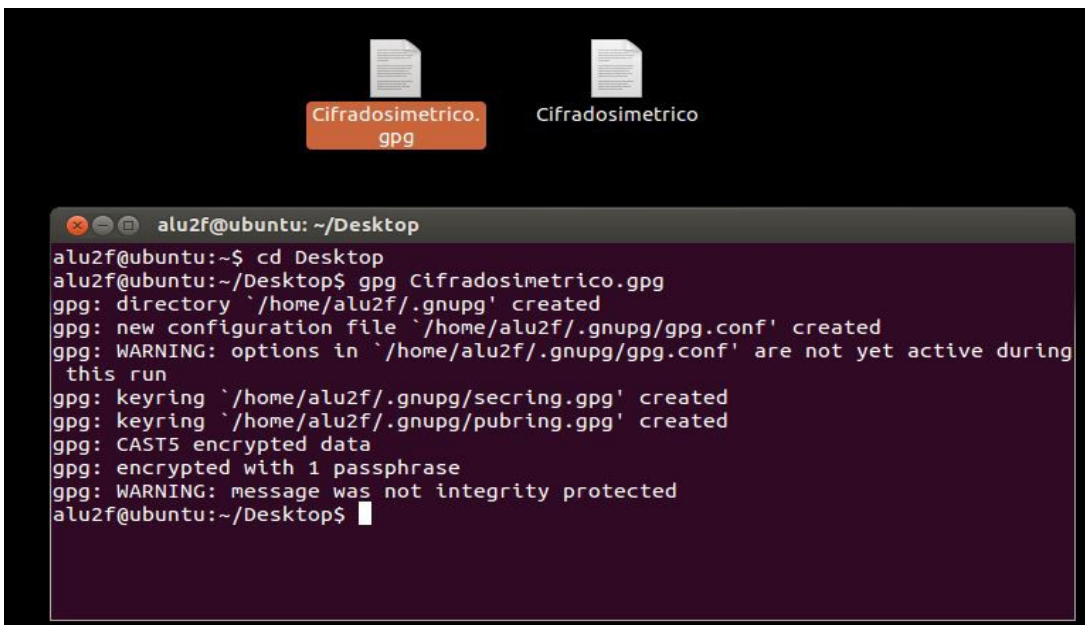
( **gpg -c Documentoacifrar** )



3º Haz llegar por algún medio al compañero de al lado el documento que acabas de cifrar.

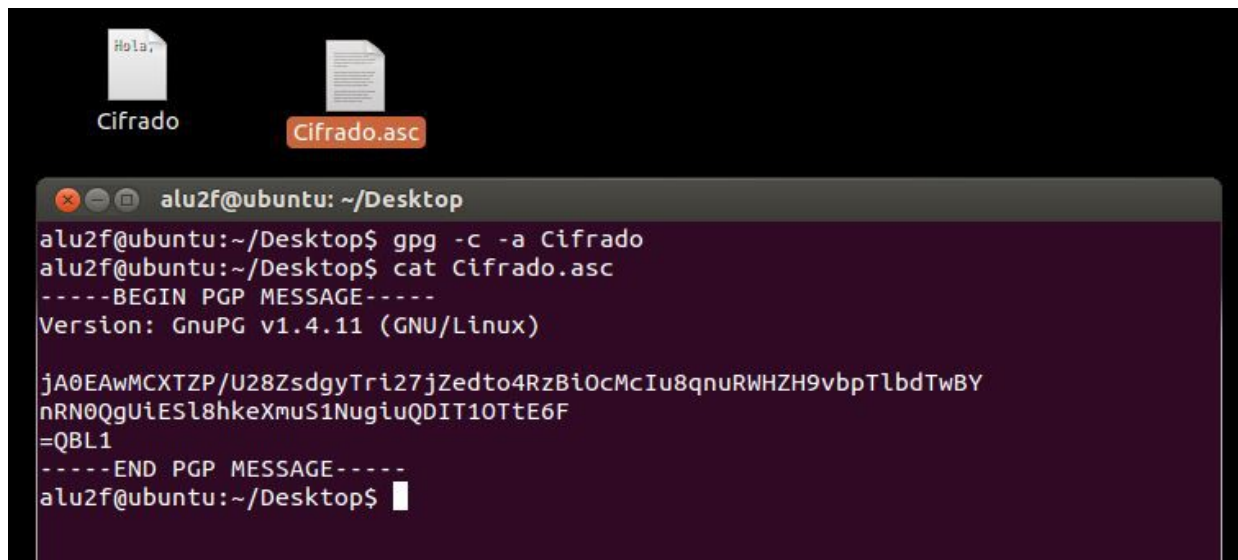
4º Descifra el documento que te ha hecho llegar tu compañero de al lado.

( **gpg Archivadescifrar.gpg** )



5º Repite el proceso anterior, pero añadiendo la opción -a. Observa el contenido del archivo generado con un editor de textos o con la orden cat.

Tenemos que usar el comando **gpg -c -a Documentoacifrar**

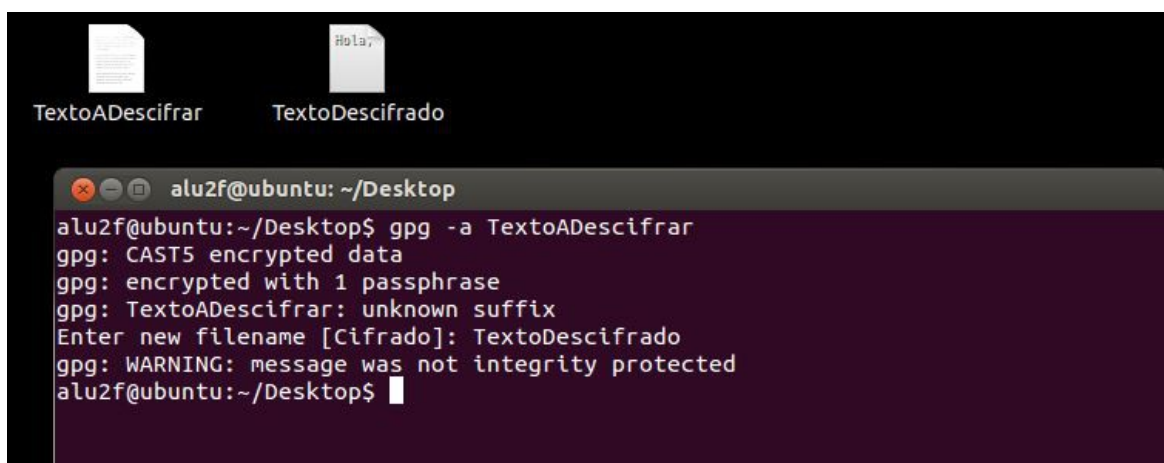


```
alu2f@ubuntu: ~/Desktop
alu2f@ubuntu:~/Desktop$ gpg -c -a Cifrado
alu2f@ubuntu:~/Desktop$ cat Cifrado.asc
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.11 (GNU/Linux)

jA0EAWMCXTZP/U28ZsdgyTri27jZedto4RzBi0cMcIu8qnuRWHZH9vbpTlbdTwBY
nRN0QgUiESl8hkeXmuS1NugiuQDIT10TtE6F
=QBL1
-----END PGP MESSAGE-----
alu2f@ubuntu:~/Desktop$
```

6º Copia y pega el contenido del archivo cifrado anteriormente y envíalo por mail a tu compañero para que lo descifre.

7º Una vez has recibido el mensaje de tu compañero en tu mail, copialo en un archivo de texto para obtener el mensaje original.



```
alu2f@ubuntu: ~/Desktop
alu2f@ubuntu:~/Desktop$ gpg -a TextoADescifrar
gpg: CAST5 encrypted data
gpg: encrypted with 1 passphrase
gpg: TextoADescifrar: unknown suffix
Enter new filename [Cifrado]: TextoDescifrado
gpg: WARNING: message was not integrity protected
alu2f@ubuntu:~/Desktop$
```

## Creación de nuestro par de claves pública y privada

1º: Escribimos el comando **gpg --gen-key**

2º: Elegimos el tipo de clave que vamos a crear. ( Yo he elegido el predeterminado, el 1.)

3º: Elegimos la longitud de la clave, cuantos mas bits, mas segura será la clave.

4º: Tenemos que especificar cuánto tiempo de validez tendrá la clave. Como en el ejercicio nos pide 1 mes, ponemos 32.

5º: Nos pedirá que escribamos nuestro ID: Nombre, correo electrónico.

6º: Siguiendo estos pasos ya habríamos creado las claves pública y privada.

```
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? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 2014
Requested keysize is 2014 bits
rounded up to 2016 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) 32
Key expires at Thu 13 Apr 2017 04:49:09 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: Daniel
Email address: 13pcpa.danicabrerizo@gmail.com
Comment: Criptografia
You selected this USER-ID:
    "Daniel (Criptografia) <13pcpa.danicabrerizo@gmail.com>"
```

```

gpg: /home/alu2f/.gnupg/trustdb.gpg: trustdb created
gpg: key E37E97FD 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 2017-04-13
pub 2016R/E37E97FD 2017-03-12 [expires: 2017-04-13]
    Key fingerprint = F39F C407 6318 F2CF 7398 DF63 FDB1 82E4 E37E 97FD
uid          Daniel (Criptografia) <13pcpa.danicabrerizo@gmail.com>
sub 2016R/3ACC1C58 2017-03-12 [expires: 2017-04-13]

alu2f@ubuntu:~$ █

```

### Exportar e importar claves públicas

1. Exporta tu clave pública en formato ASCII y guárdalo en un archivo nombre\_apellido.asc y luego envíalo a un compañero/a.
2. Importa las claves públicas recibidas de vuestros/as compañeros/as.
3. Comprueba que las claves se han incluido correctamente en vuestro keyring.

1º El comando para exportar nuestra clave pública en formato ASCII y guardarlo en un archivo sería este: **"gpg -a --export NuestroID > nombreyapellido.asc"**.

2º Para importar una clave pública recibida usaremos este comando:  
**"gpg --import clavepublica.asc"**

3º Para comprobar que hemos importado la clave a nuestro keyring usaremos este comando **"gpg -kv"**.

```

alu2f@ubuntu: ~/Desktop
alu2f@ubuntu:~$ cd Desktop
alu2f@ubuntu:~/Desktop$ gpg --import DanielCabrerizo.asc
gpg: key E37E97FD: "Daniel (Criptografia) <13pcpa.danicabrerizo@gmail.com>" not
changed
gpg: Total number processed: 1
gpg:             unchanged: 1
alu2f@ubuntu:~/Desktop$ gpg -kv
/home/alu2f/.gnupg/pubring.gpg
-----
pub 2016R/E37E97FD 2017-03-12 [expires: 2017-04-13]
uid          Daniel (Criptografia) <13pcpa.danicabrerizo@gmail.com>
sub 2016R/3ACC1C58 2017-03-12 [expires: 2017-04-13]

alu2f@ubuntu:~/Desktop$

```

## Cifrado y descifrado de un documento

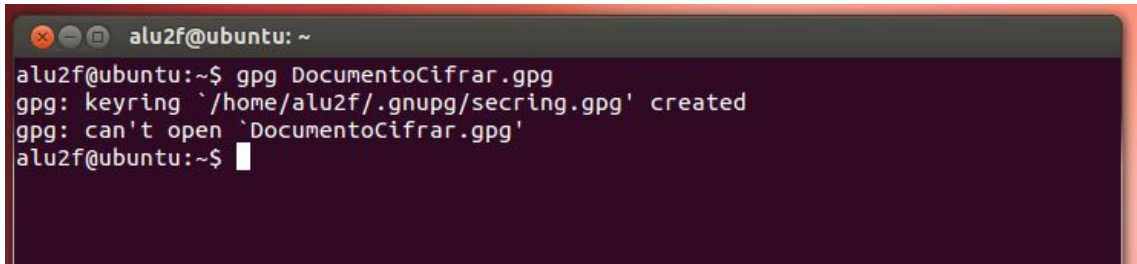
1. Cifraremos un archivo cualquiera y lo remitiremos por email a uno de nuestros compañeros que nos proporcionó su clave pública.
2. Nuestro compañero, a su vez, nos remitirá un archivo cifrado para que nosotros lo descifremos.
3. Tanto nosotros como nuestro compañero comprobaremos que hemos podido descifrar los mensajes recibidos respectivamente.
4. Por último, enviaremos el documento cifrado a alguien que no estaba en la lista de destinatarios y comprobaremos que este usuario no podrá descifrar este archivo.

1º Ciframos un documento cualquiera, con el comando “ **gpg -c Documento**”

3º Comprobamos que hemos importado la clave pública de nuestro compañero a nuestro keyrings con el comando “**gpg -kv**” y descriptamos el documento de nuestro compañero con el comando “ **gpg Documentocifrado.gpg** ”



4º Esto es lo que pasaría si intentamos descriptar el documento que nos ha pasado alguien sin haber importado su clave pública.

A terminal window titled 'alu2f@ubuntu: ~' with a dark purple background. The text inside shows the command 'gpg DocumentoCifrar.gpg' being entered. The output consists of three lines: 'gpg: keyring `/home/alu2f/.gnupg/secring.gpg' created', 'gpg: can't open `DocumentoCifrar.gpg'', and the prompt 'alu2f@ubuntu:~\$' followed by a cursor.

```
alu2f@ubuntu:~$ gpg DocumentoCifrar.gpg
gpg: keyring `/home/alu2f/.gnupg/secring.gpg' created
gpg: can't open `DocumentoCifrar.gpg'
alu2f@ubuntu:~$
```

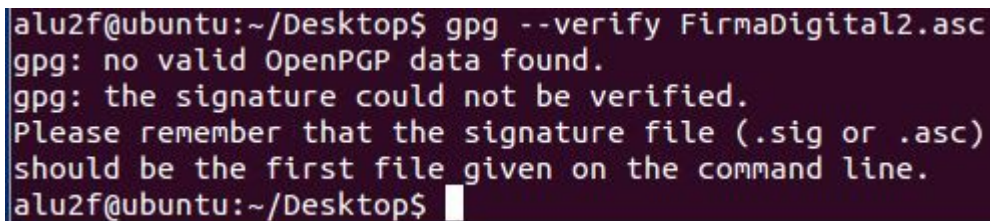
### Firma digital de un documento

1. Crea la firma digital de un archivo de texto cualquiera y envíale éste junto al documento con la firma a un compañero.
2. Verifica que la firma recibida del documento es correcta.
3. Modifica el archivo ligeramente, insertando un carácter o un espacio en blanco, y vuelve a comprobar si la firma se verifica.

1º Creamos un documento cualquiera y escribimos algo dentro de el, y con el comando “ **gpg -sb -a Documentoafirmar** ” lo firmamos.

2º Para verificar que la firma es correcta tenemos que usar el comando “**gpg –verify documentoafirmar.asc** ”

3º Esto es lo que pasa si modificamos el archivo firmado y despues lo verificamos.

A terminal window titled 'alu2f@ubuntu:~/Desktop\$' with a dark purple background. The text inside shows the command 'gpg --verify FirmaDigital2.asc' being entered. The output consists of three lines: 'gpg: no valid OpenPGP data found.', 'gpg: the signature could not be verified.', and 'Please remember that the signature file (.sig or .asc) should be the first file given on the command line.' followed by the prompt 'alu2f@ubuntu:~/Desktop\$' and a cursor.

```
alu2f@ubuntu:~/Desktop$ gpg --verify FirmaDigital2.asc
gpg: no valid OpenPGP data 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:~/Desktop$
```