

Práctica

Firma Digital con GnuPG

Franco Larrea

2º SMR-A
(Prof. Fernando Albert González)
Instituto IES SAN VICENTE

Índice

Teoría.....	Pag.
Tareas y cuestiones.....	Pag.
Problemas encontrados.....	Pag.
Fuentes.....	Pag.
Alumnos participantes.....	Pag.

Teoría

Para realizar esta practica es conveniente saber algunos conceptos:

Firma digital

¿Que es?

Una firma digital es un mecanismo criptográfico que permite al receptor de un mensaje firmado digitalmente identificar a la entidad originadora de dicho mensaje y confirmar que el mensaje no ha sido alterado desde que fue firmado por el originador (integridad).

GnuPG

¿Que es?

GNU Privacy Guard (GnuPG o GPG) es una herramienta de cifrado y firmas digitales desarrollado por Werner Koch. Es software libre licenciado bajo la GPL.

GPG utiliza el estándar del IETF denominado OpenPGP.

Vamos a intercambiar documentos firmados con las opciones:

- **--clearsign:** El documento a firmar se encuentra en claro y se añade la firma para verificar el origen.
 - `gpg --clearsign documento_secreto`
- **-s:** documento firmado. El resultado es un fichero comprimido (binario) ilegible.
 - `gpg -s documento_secreto`
- **-b:** se utiliza cuando se desea que la firma aparezca en un fichero separado; cuando se quiere firmar un archivo binario, como ficheros comprimidos, ejecutables...
 - `gpg -b documento_secreto`
- En todas estas opciones además de descifrar el mensaje en las dos últimas, se verificará la firma con la opción `--verify` en las tres opciones.

Esta práctica se ha realizado en un Ubuntu 18.04



Primero crearemos 3 ficheros diferentes, cada uno lo firmaremos con diferentes opciones.

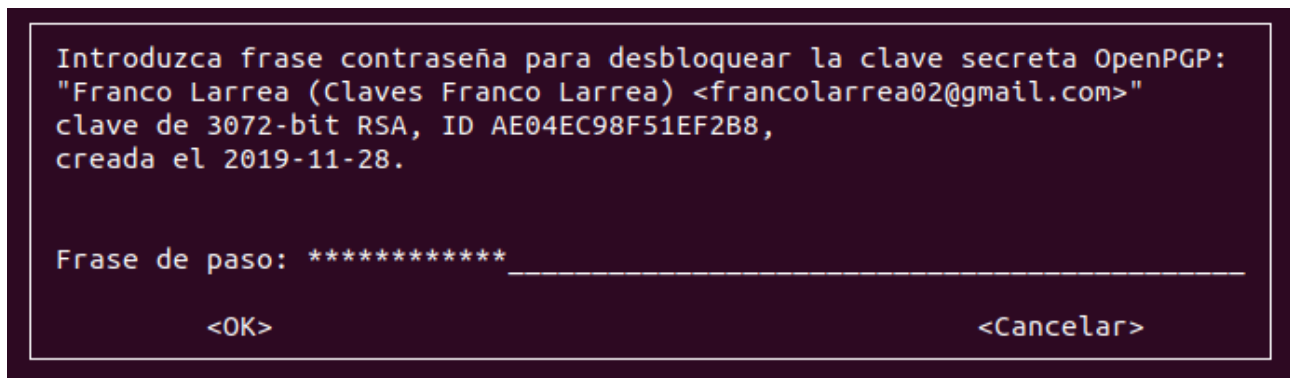
Vamos a empezar firmando el “texto1” con la opción:

- `gpg --clearsign texto1`

```
gpg --clearsign texto1
```

Firmando con esta opción el mensaje se mantiene en claro y se añade la firma al final del mismo mensaje.

Nos pedirá nuestra clave privada para firmar el mensaje, todos los mensajes los estamos firmando con nuestra clave privada. Cualquier persona que tenga nuestra clave pública puede verificar que el documento es de nuestra procedencia.



A continuación firmaremos el “texto2” con la opción:

- **gpg -s texto2**

```
gpg -s texto2
```

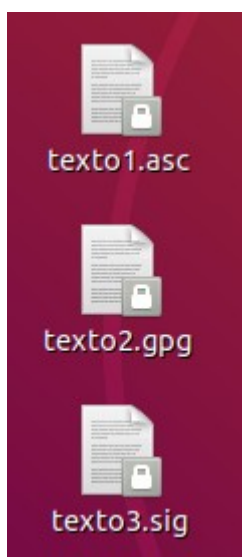
Firmando con esta opción el mensaje se firma y se cifra siendo ilegible.

Por ultimo firmaremos el “texto3” con la opción:

- **gpg -b texto3**

```
gpg -b texto3
```

Firmando con esta opción la firma se genera en un documento aparte, por lo que tendremos que mandar el documento 3 junto a la firma de este.



Aquí podemos ver los tres archivos firmados:

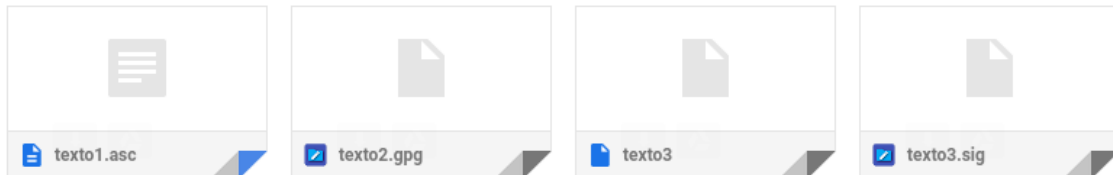
- El texto1.asc esta en claro.
- El texto2.gpg esta cifrado.
- El texto3.sig es solo la firma del “texto3”.

Mensajes firmados 1, 2 y 3 >



Franco Larrea <francolarrea02@gmail.com>
para frgb2000 ▾

4 archivos adjuntos



Enviaremos estos archivos a nuestro compañero Fran. (Además de la firma del texto3 tendremos que mandar el texto3).

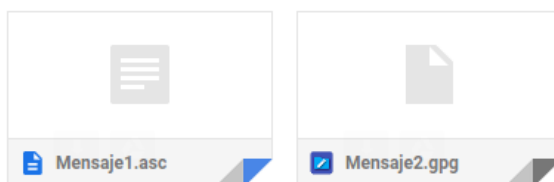
Fran también me ha mandado 4 archivos cifrados.

Mensaje 1 y 2 > Recibidos x



TheFunnyLows
para mí ▾

2 archivos adjuntos



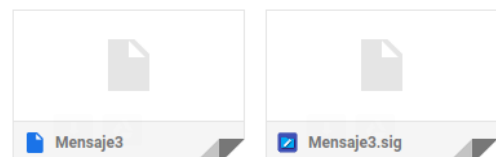
Mensaje3 > Recibidos x



TheFunnyLows
para mí ▾

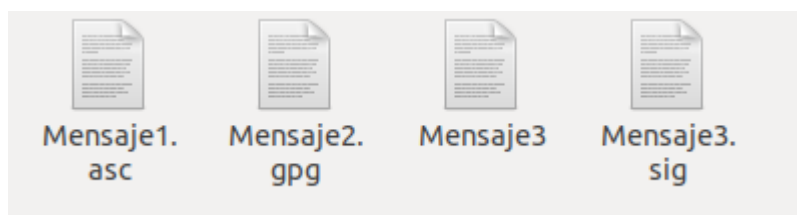
🌐 inglés ▾ > español ▾ [Traducir mensaje](#)

2 archivos adjuntos



Descargaremos los archivos.

Aquí podemos ver los archivos descargados.



```
root@machine103:/home/fmol107/Descargas# ls
Mensaje1.asc Mensaje2.gpg Mensaje3 Mensaje3.sig
```

En todas las comprobaciones de firma que vamos a realizar en esta práctica estamos usando la clave pública de nuestro compañero Fran. Esta la tenemos instalada en nuestro sistema desde la práctica anterior.

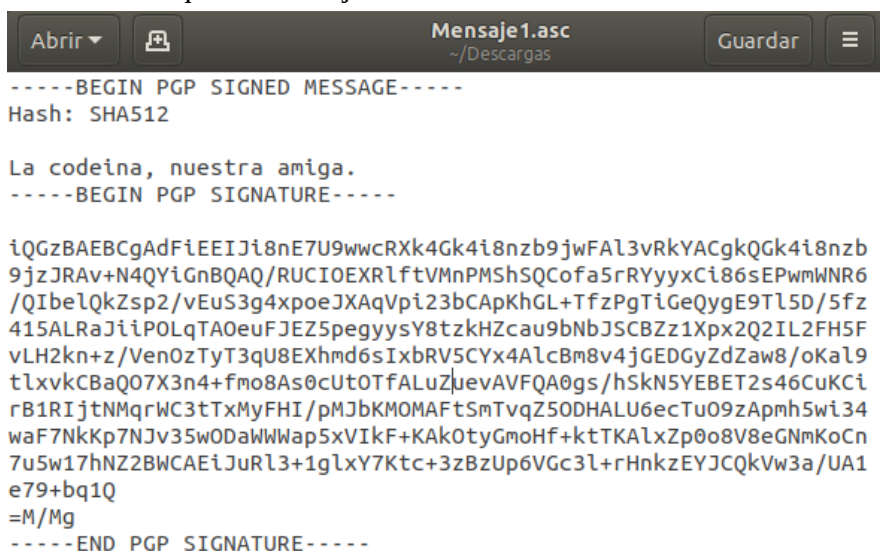
Podemos ver que claves tenemos instaladas con el comando **gpg -k**.

```
root@machine103:/home/fmol107/Descargas# gpg -k
/root/.gnupg/pubring.kbx
-----
pub   rsa3072 2019-11-28 [SC] [caduca: 2019-12-28]
      663E0D6C60F133DEC51C61B0AE04EC98F51EF2B8
uid   [ absoluta ] Franco Larrea (Claves Franco Larrea) <francolarrea02@gmail.com>
sub   rsa3072 2019-11-28 [E] [caduca: 2019-12-28]

pub   rsa3072 2019-12-02 [SC] [caduca: 2020-01-01]
      2098BC9C4ED4F70C1C4579381A4E22F27CDBF63C
uid   [ desconocida ] Francisco Gómez Benimeli (Práctica) <frgb2000@gmail.com>
sub   rsa3072 2019-12-02 [E] [caduca: 2020-01-01]
```

Primero voy a verificar el Mensaje1.asc.

Podemos ver que el mensaje esta en claro.



```
Mensaje1.asc
~/Descargas

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

La codeína, nuestra amiga.
-----BEGIN PGP SIGNATURE-----

iQGzBAEBCgAdFiEEIji8nE7U9wwcRXk4Gk4i8nzb9jwFAL3vRkYACgkQGk4i8nzb
9jzJRAv+N4QYiGnBQAQ/RUCIOEXRlftVMnPMShSQCoFa5rRYyyxCi86sEPwmWNR6
/QIbelQkZsp2/vEuS3g4xpoeJXAqVpi23bCApKhGL+TfzPgTiGeQygE9TL5D/5fz
415ALRaJiiPOLqTA0euFJEZ5pegyysY8tzkHZcau9bNbJSCBZz1Xpx2Q2IL2FH5F
vLH2kn+z/VenOzTyT3qU8EXhmd6sIxbrV5CYx4AlcBm8v4jGEDGyZdZaw8/oKa19
tlxvkCBAQ07X3n4+fmo8As0cUt0TfALuZJuevAVFQA0gs/hSkN5YEBET2s46CuKCi
rB1RIjtnMqrWC3tTxMyFHI/pMJbKMOMAFtSmTvqZ50DHALU6ecTu09zApmh5wi34
waf7NkKp7NJv35wODaWWwap5xVIkF+KAK0tyGmoHf+ktTKALxZp0o8V8eGNmKoCn
7u5w17hNZ2BWCAEiJuRl3+1glxY7Ktc+3zBzUp6VGc3l+rHnkzEYJCQkVw3a/UA1
e79+bbq1Q
=M/Mg
-----END PGP SIGNATURE-----
```

Para comprobar el mensaje simplemente usaremos el comando:

- **gpg --verify Mensaje1.asc**

```
root@machine103:/home/fmol107/Descargas# gpg --verify Mensaje1.asc
gpg: Firmado el mar 10 dic 2019 08:16:22 CET
gpg:      usando RSA clave 2098BC9C4ED4F70C1C4579381A4E22F27CDBF63C
gpg: Firma correcta de "Francisco Gómez Benimeli (Práctica) <frgb2000@gmail.com>" [d
esconocido]
gpg: ATENCIÓN: ¡Esta clave no está certificada por una firma de confianza!
gpg:      No hay indicios de que la firma pertenezca al propietario.
Huellas dactilares de la clave primaria: 2098 BC9C 4ED4 F70C 1C45  7938 1A4E 22F2 7C
DB F63C
```

La firma de este mensaje es correcta.

Ahora voy a verificar el Mensaje2.gpg.

Podemos ver que el mensaje esta cifrado.

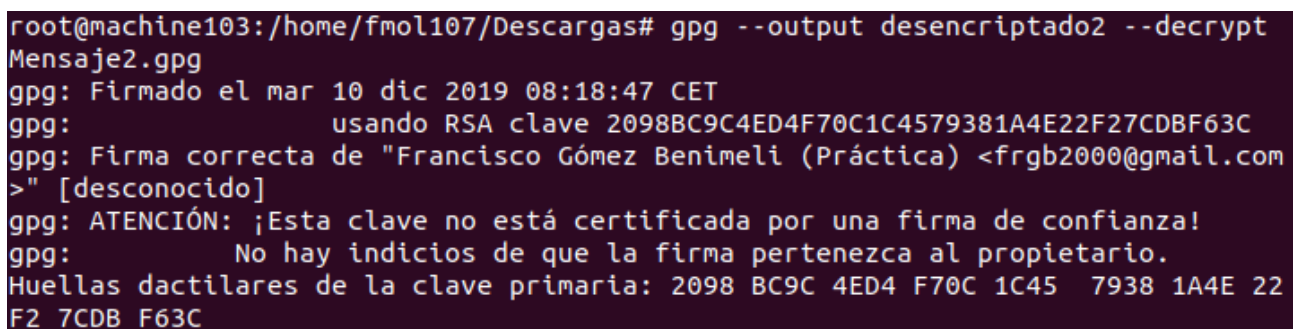


Podríamos verificarlo con la opción **--verify** para comprobar la firma pero no podríamos entender el mensaje.

Así que simplemente vamos a descifrarlo. En el proceso de descifrado también nos verifica la firma.

Desciframos el mensaje con la opción:

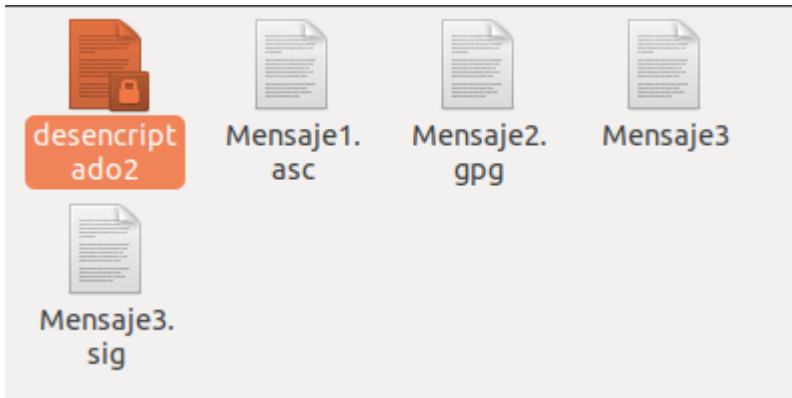
- **gpg --output descriptado2 --decrypt Mensaje2.gpg**



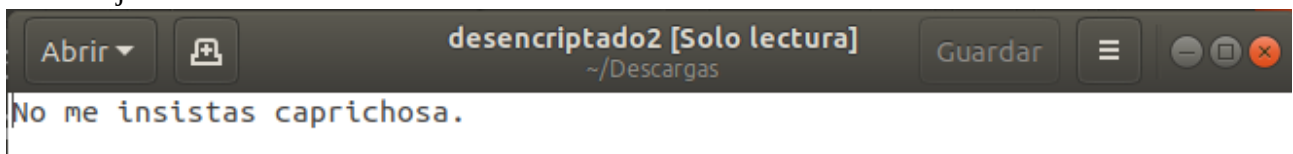
Podemos ver que la firma de este mensaje es correcta.

También nos ha generado un archivo con el mensaje descifrado.

Aquí podemos ver el archivo generado.



El mensaje ahora esta en claro.



También podemos verificar el archivo sin descifrar el mensaje. Para ello ejecutamos el comando:

- **gpg --verify Mensaje2.gpg**

```
root@machine103:/home/fmol107/Descargas# gpg --verify Mensaje2.gpg
gpg: Firmado el mar 10 dic 2019 08:18:47 CET
gpg: usando RSA clave 2098BC9C4ED4F70C1C4579381A4E22F27CDBF63C
gpg: Firma correcta de "Francisco Gómez Benimeli (Práctica) <frgb2000@gmail.com>" [desconocido]
gpg: ATENCIÓN: ¡Esta clave no está certificada por una firma de confianza!
gpg: No hay indicios de que la firma pertenezca al propietario.
Huellas dactilares de la clave primaria: 2098 BC9C 4ED4 F70C 1C45 7938 1A4E 22F2 7C DB F63C
root@machine103:/home/fmol107/Descargas#
```

Podemos ver que la firma sigue siendo correcta, ya que el archivo es el mismo.

Ahora vamos a verificar el ultimo mensaje, tendremos que tener en cuenta que la firma del mensaje 3 y el propio mensaje 3 tienen que estar en el mismo directorio.

Tendremos que verificar la firma del mensaje.

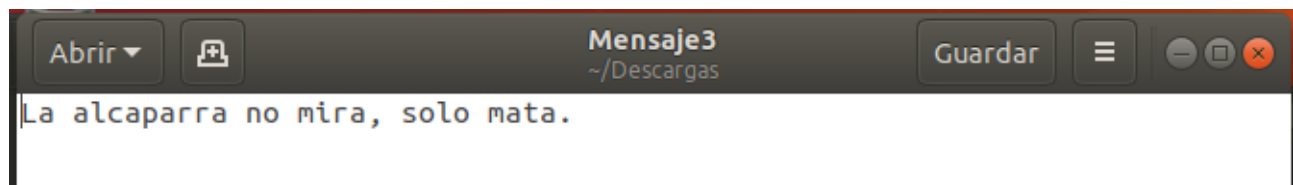
Para verificarla ejecutamos el comando:

- **gpg --verify Mensaje3.sig**

```
root@machine103:/home/fmol107/Descargas# gpg --verify Mensaje3.sig
gpg: asumiendo que los datos firmados están en 'Mensaje3'
gpg: Firmado el mar 10 dic 2019 08:19:32 CET
gpg: usando RSA clave 2098BC9C4ED4F70C1C4579381A4E22F27CDBF63C
gpg: Firma correcta de "Francisco Gómez Benimeli (Práctica) <frgb2000@gmail.com>" [desconocido]
gpg: ATENCIÓN: ¡Esta clave no está certificada por una firma de confianza!
gpg: No hay indicios de que la firma pertenezca al propietario.
Huellas dactilares de la clave primaria: 2098 BC9C 4ED4 F70C 1C45 7938 1A4E 22 F2 7CDB F63C
```

La firma de este archivo es correcta.

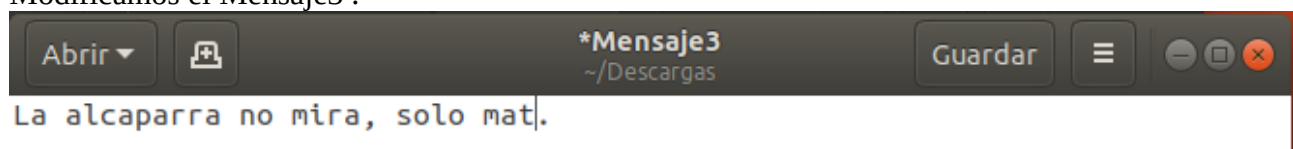
Aquí podemos ver el Mensaje3 de Fran:



En caso de que modifiquemos el mensaje3 y volviéramos a comprobar la firma, esta sería incorrecta.

Vamos a comprobarlo.

Modificamos el Mensaje3 .



Y volvemos a comprobar la firma.

```
root@machine103:/home/fmol107/Descargas# gpg --verify Mensaje3.sig
gpg: asumiendo que los datos firmados están en 'Mensaje3'
gpg: Firmado el mar 10 dic 2019 08:19:32 CET
gpg: usando RSA clave 2098BC9C4ED4F70C1C4579381A4E22F27CDBF63C
gpg: Firma INCORRECTA de "Francisco Gómez Benimeli (Práctica) <frgb2000@gmail.com>" [desconocido]
```

Después de modificar el Mensaje3 la comprobación es incorrecta.

Esto es debido a que Fran generó la firma en base al Mensaje3, si modificamos este mensaje se genera una firma diferente.

Problemas encontrados:

- Esta práctica se ha realizado sin dificultades.

Fuentes:

- https://es.wikipedia.org/wiki/GNU_Privacy_Guard
- https://es.wikipedia.org/wiki/Firma_digital

Alumnos participantes:

- Franco Matias Oscar Larrea
- Francisco Gomez Benimeli