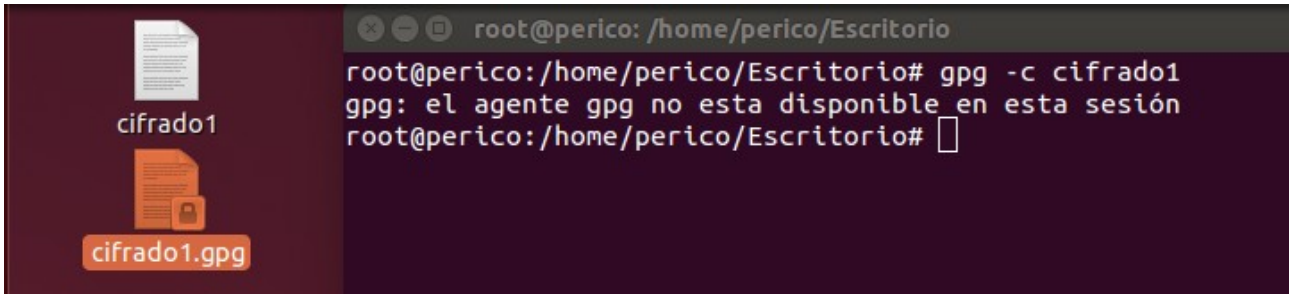
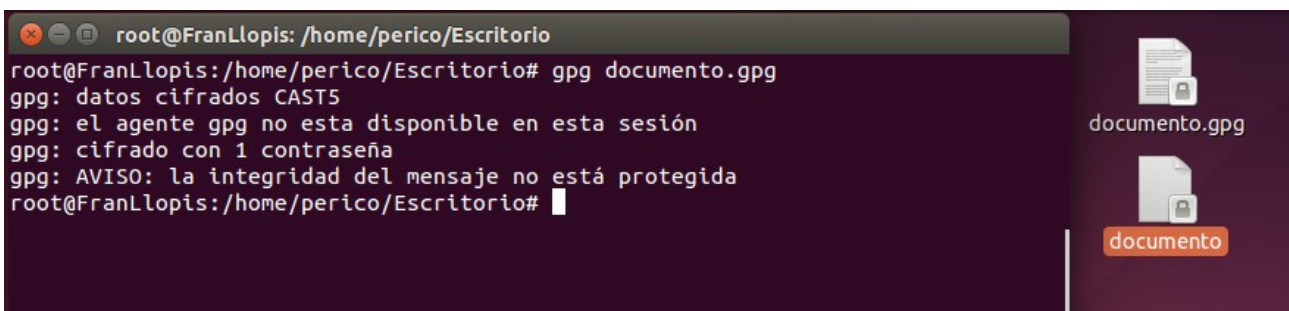


PRACTICA CRIPTOGRAFÍA

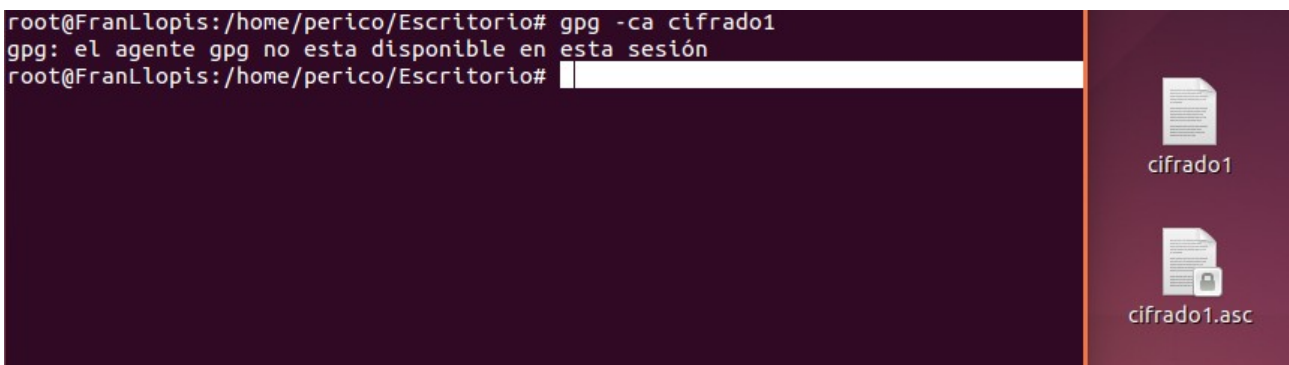
Para cifrar un documento debemos, tras crear el documento usar el comando `gpg -c documento`.



Con esto nos crea un archivo cifrado, y para descifrar un documento que nos halla enviado un compañero ejecutaremos `gpg documento.gpg` y introducimos su contraseña.



Y si queremos cifrarlo con ASCII ejecutaremos `gpg -ca documento`.



Ahora crearemos una clave pública y una privada para ello ejecutamos `gpg --gen-key`, en tipo de clave ponemos 1, de longitud de las claves pondremos el por defecto 2048, de periodo de validez 1 mes, de identificador nuestro nombre, apellido, etc..., y la contraseña.

```
root@FranLlopis:/home/perico/Escritorio# gpg --gen-key
gpg (GnuPG) 1.4.16; Copyright (C) 2013 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.

Seleccione el tipo de clave deseado:
  (1) RSA y RSA (por defecto)
  (2) DSA y ElGamal (por defecto)
  (3) DSA (sólo firmar)
  (4) RSA (sólo firmar)
¿Su elección? 1
las claves RSA pueden tener entre 1024 y 4096 bits de longitud.
¿De qué tamaño quiere la clave? (2048) 2048
El tamaño requerido es de 2048 bits
Especifique el periodo de validez de la clave.
  0 = la clave nunca caduca
  <n> = la clave caduca en n días
  <n>w = la clave caduca en n semanas
  <n>m = la clave caduca en n meses
  <n>y = la clave caduca en n años
¿Validez de la clave (0)? 1m
La clave caduca mié 05 abr 2017 18:20:55 CEST
¿Es correcto? (s/n) s

Necesita un identificador de usuario para identificar su clave. El programa
construye el identificador a partir del Nombre Real, Comentario y Dirección
de Correo electrónico de esta forma:
  "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Nombre y apellidos: Fran Llopis
Dirección de correo electrónico: franllopis@correo.com
Comentario:
Ha seleccionado este ID de usuario:
  «Fran Llopis <franllopis@correo.com>»

¿Cambia (N)ombre, (C)omentario, (D)irección o (V)ale/(S)alir? █
```

Para ver tu clave publica ejecutamos `gpg --gen` (Nombre y apellido que pusiste)

```

root@FranLlopis:/home/perico# gpg -a --export Fran Llopis
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1

mQENBFi9jccBCACucmrCu5dZjGQVgmDkYVqLgHfw+U/klfxVNBK1Ae/OthYpJWdV
bcLzmRq4ln5uWTb018Fj1jyuvbcbto8wrJtSdRkGY4V9M9/59PC7kqFwzQySq1mm
RBvWwewza4PLtyfIV/0d8k0Ejt2hS0zLyzGVzKAucI3bb2ZWBG1Xw2OD7tPUpzLT
QZnjzasdC02wi/d0fgztq1vzCF/lQri9/9D2/AnmmS/u0WUUVH3fpBwPme9mUaX+n
dTeCKvRV/5aNTTrtPSeWp7AW6H94bybi8K3VPyQEHCrk+n1ape2pXcd9Pkve13iY4
Jc/tXfXRrSgzd2YsIygniEswChHj60RiEd15ABEBAAG0I0ZyYW4gTGxvcGJlZlDxm
cmFubGxvcGJlZlDmVncnJlby5jb20+iQE+BBMBAGAOBQJYvY3HAhsDBQKAJ40ABgsJ
CmCDagYVCAIJGSEFgIDAQIEAQIAAAKCRBBOKOGKTXnmhDmB/0exsMfBoIDMMaa
wR8b1AJenFGx/+s6MHoSYcLUlP001zE+ZuKjx8GVgbydQUzLKy4lF8pCgoDF/quo
dW9pbmWwMjw+m3uWpCyauki0msQ/5VjaZvhls5AEgcAko3V3eRxEoDMzd/CoibwO
Es39Knm26ILhuxaGB46uL1mGvJYlBtMQftG5iDwXXku/iU1tfZyKnjqKAcfG6c6
1MtPrPCH0526f1avgL8qJnfYKY/X0SceKSVJXE2+cUzzE9y/4LtfYtoxsN7WMUaO
OhYPJr9S8g7g0B1MMJYyTQLXfTTbm5WX5QJrmI2IoCgTmxihwHaUv/pCCULpnqBF
2FJ6MbQQuQENBFi9jccBCACvjxR3N0TSKXRfN4w1E72rsUB1CEPbdjLXXDqhj1r5
B7iiJzVNH6e6bQnR9WxRUINVXnDoqZTNl2+n3muxvJgON2zZeZAe02Eqv6Za4uAr
Bmjfbv1vT8bcaiwm7+Bak0oUVwbZQQ4+VknZR6UrPvIi/gmdgkxQi/ocuvnP+8KK
Em11hrxmbhlHOQViEakr2Ed0TrskJgXJG/doewhThej9B0EfHwoAFxwr1kYnHAcv
vJf4AjQhWFREV4EOCD/e/L5RY6TvRL998Sh4wgJ0pNgY37iDhIj4rEvUb3w9AAJf
PLWan9Z1c7/1eNn4tb/rwW0VaDV+usABcfEzE3cH2Sa1ABEBAAGJASUEGAECBA85
A1i9jccCGwWFCQANtjQAACgkQKQAcjh155r7bgf/U4aq10pZLL+3JEQalBb217r
GoaSPG3lctl7AWy7puIEctZOXuYXdoX00r35SPxR7sBVSVXHaN8vXvnru+kTj42
RL5EEQXewJn2kuqGhnYoVzE46BClaeic1nq8HRKGWxuWDTl1+EkFe1vM/sDGqNbb
ZhYGMvy27e+tMWKJLVQ4qI0cqgaBRDSVu0BeizjBDowTAoAGQpbfD0mLjkgkKH9g
PjQ50JCJUG0iLDrvxLpRWyGs+O6H3p/KC58RHqj3X6Tx7fcy1BXsjHmsREMzN3JU
iNmh02AE2ULDMasjXoUiHV3+gc3HYm3TG80w8HKDuQRLsvyDVHRBw2qL0OpZtZkB
DQRYvteBAQgAwXECAVLjweHbCWpm+7PdBC1cmnBb924mGb0W1+/cYEzpbLVIsmA
6aDR1AWL+YTqno50okZ8ia2pY/gm7acFJ2J/VU8MMYgXQLVrTE9RxQknL8YPQJXp
yOHhCFLpzqawMWj/YmmvvzHdz9HWpKv0/Axi85LPCW2vvGWFXyUqGiZ0Jk4vHpq2
LTk3MSEiCD2WT7GwWimZuno5YUMZ7c+k5/U9P/b1b5eaFGky9HumWr9Y087qsIAW
xZX01ib/Ohln1M8hYIslBhqmnakdnME3qZhqZXBkji1b6wgnewC0C3K0AuYL3Fgd6
g2TCNFnfj0Awva0vGZLCr6U7+QokZ0lsmwARAQABTCJGcmFmIE9xsb3BpcyA8ZnJh
bm9sbnB3b3Bjb3J3Y2W8uZXMX+iQE+BBMBAGAOBQJYvteBAhsDBQKAJ40ABgsJCAcD
AgVCAIJCgSEFgIDAQIEAQIAAAKCRBK3Pz0/IEM8+/HCACINo3SNLjAxiImymppe
32rQmuM1CH10qNPGkYdAncruiGhHaI5Yb3rCJvLH0Gc7rxPFQ9gC33gSfqkdK6DW
lPtDhnZn2musJzDkJ65A47GzaY0+AK8tLVjn4pF00PBq7h0Ssbm66y5/ZUPnFRhy

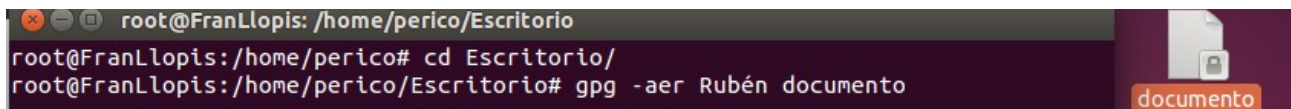
```

Y si queremos exportarla a un archivo que podremos enviar ejecutamos `gpg -a --export (Nombre y apellido utilizados) > (Nombre que tendra el archivo)`.



```
root@FranLlopis:/home/perico# gpg -a --export Fran Llopis > miclave.asc
root@FranLlopis:/home/perico#
```

Para enviar un mensaje cifrado ejecutaríamos `gpg -aer (ID:Nombre y apellido de la otra persona) (documento a enviar)`.

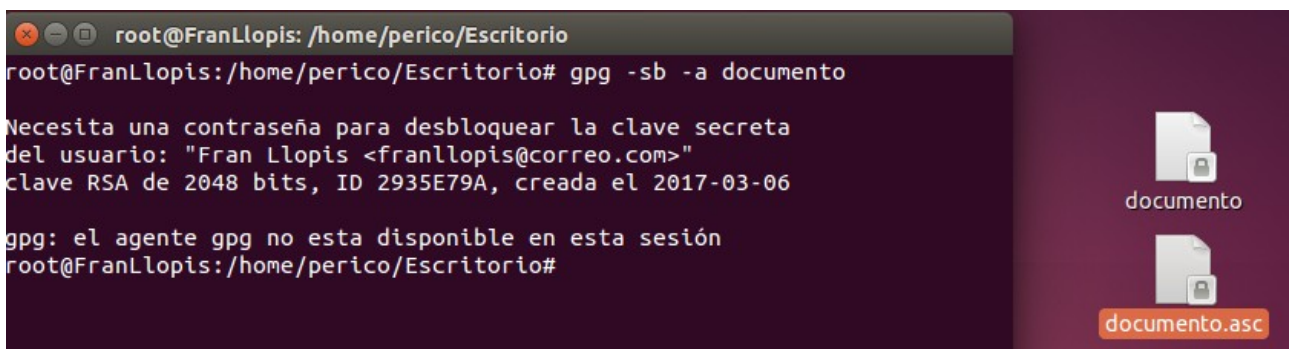


```
root@FranLlopis: /home/perico/Escritorio
root@FranLlopis:/home/perico# cd Escritorio/
root@FranLlopis:/home/perico/Escritorio# gpg -aer Rubén documento
```

documento

Y si nos envían un documento cifrado podremos descifrarlo con `gpg documento.asc` y contraseña nuestra clave privada.

Para crear una firma digital ejecutaremos `gpg -sb -a documento`



```
root@FranLlopis: /home/perico/Escritorio
root@FranLlopis:/home/perico/Escritorio# gpg -sb -a documento

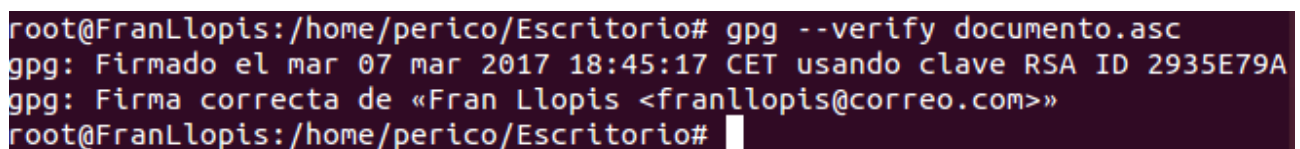
Necesita una contraseña para desbloquear la clave secreta
del usuario: "Fran Llopis <franllopis@correo.com>"
clave RSA de 2048 bits, ID 2935E79A, creada el 2017-03-06

gpg: el agente gpg no esta disponible en esta sesión
root@FranLlopis:/home/perico/Escritorio#
```

documento

documento.asc

Y para verificar ejecutaríamos `gpg --verify documento.asc`



```
root@FranLlopis:/home/perico/Escritorio# gpg --verify documento.asc
gpg: Firmado el mar 07 mar 2017 18:45:17 CET usando clave RSA ID 2935E79A
gpg: Firma correcta de «Fran Llopis <franllopis@correo.com>»
root@FranLlopis:/home/perico/Escritorio#
```