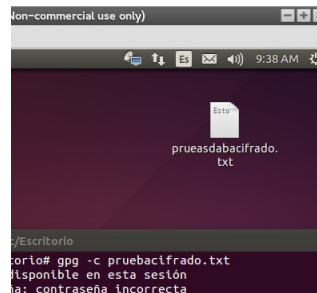
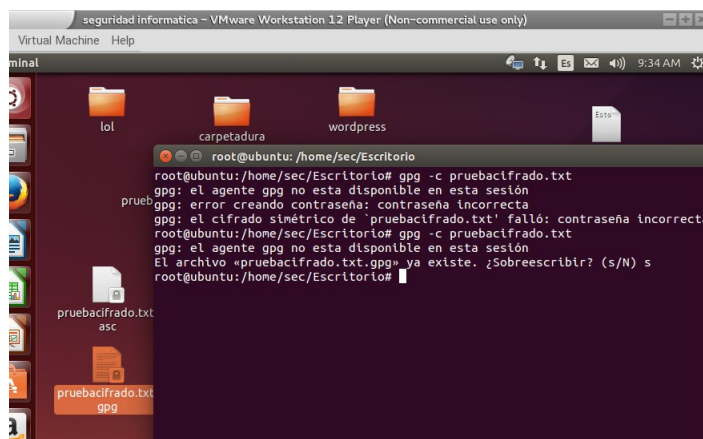


Cifrado simétrico de un documento

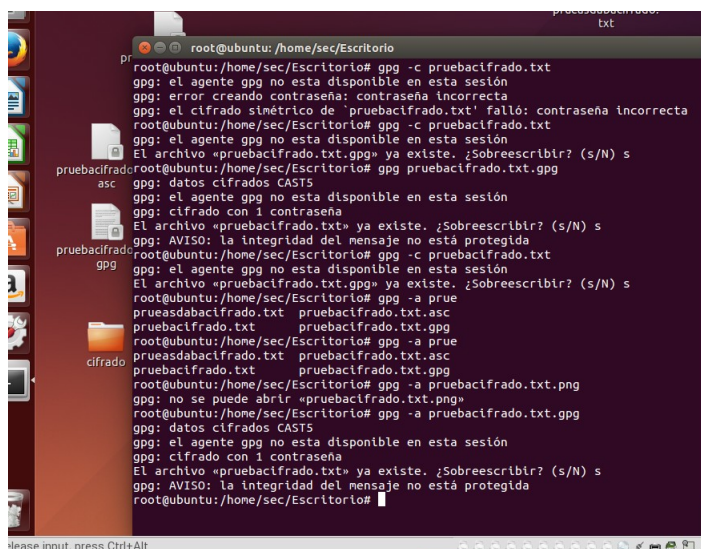
Primero tenemos que crear un documento de texto



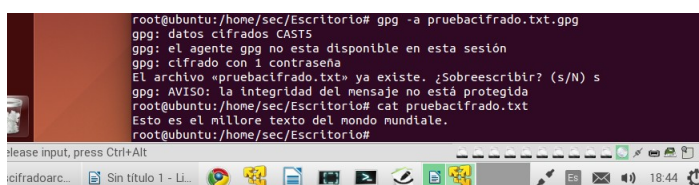
Después tenemos que cifrar el documento, para ello usamos el siguiente comando
gpg -c pruebasdabacifrado.txt



Para descifrarlo usamos el comando
gpg -a pruebasdabacifrado.txt.gpg



Para visualizarlo usamos el comando
cat pruebasdabacifrado.txt



Creación de clave publica y privada

Para generar la clave publica usamos el comando
gpg --gen-key

```
gpg: anillo «/root/.gnupg/secring.gpg» creado
root@ubuntu:/home/sec/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.

gpg: anillo «/root/.gnupg/secring.gpg» creado
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
```

El tipo de clave le ponemos 1

La longitud 2048

El periodo de validez de la clave le he puesto 5 meses (leí tarde lo de 1 mes)

```
Virtual Machine Help
Terminal
root@ubuntu:/home/sec/Escritorio
¿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)? <5>m
valor inválido
¿Validez de la clave (0)? <5>
valor inválido
¿Validez de la clave (0)? 5m
La clave caduca Thu 03 Aug 2017 11:34:15 AM PDT
¿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) <heinrich@duesseldorf.de>"

Nombre y apellidos: der dichter
asda.jpeg
```

Nos pedirá un identificador de usuario el cual rellenamos con los datos que nos pide

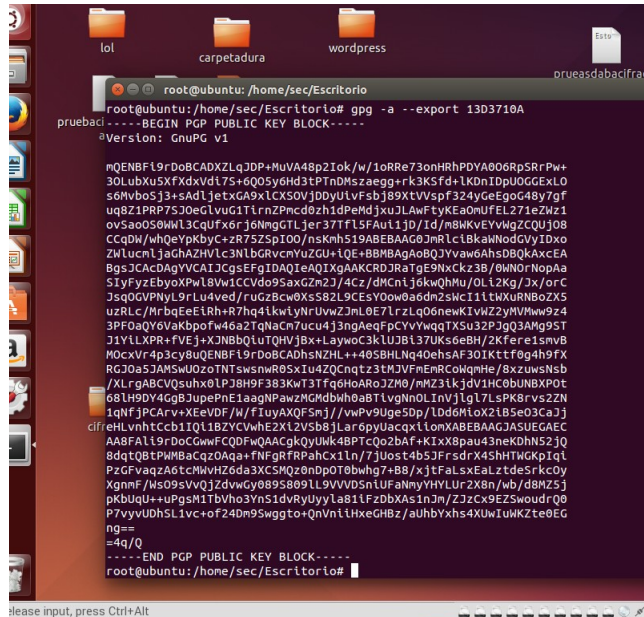
```
Virtual Machine Help
Terminal
root@ubuntu:/home/sec/Escritorio
.....
Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/console, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.
.....
gpg: /root/.gnupg/trustdb.gpg: se ha creado base de datos de confianza
gpg: clave 13D3710A marcada como de confianza absoluta
claves pública y secreta creadas y firmadas.

gpg: comprobando base de datos de confianza
gpg: 3 dudosa(s) necesaria(s), 1 completa(s) necesaria(s),
modelo de confianza PGP
gpg: nivel: 0 validez: 1 firmada: 0 confianza: 0-, 0q, 0n, 0m, 0f, 1u
gpg: siguiente comprobación de base de datos de confianza el: 2017-08-03
pub 2048R/13D3710A 2017-03-06 [[caduca: 2017-08-03]]
Huella de clave = C7D4 00E6 477F 68C2 F829 2F2D C945 A4E0 13D3 710A
uid der dichter <heinrich@duesseldorf.de>
sub 2048R/89D61DB1 2017-03-06 [[caduca: 2017-08-03]]

root@ubuntu:/home/sec/Escritorio#
```

Importar y exportar claves publicas

para visualizar nuestra clave publica usamos el comando
gpg -a --export 13D3710A (key id)

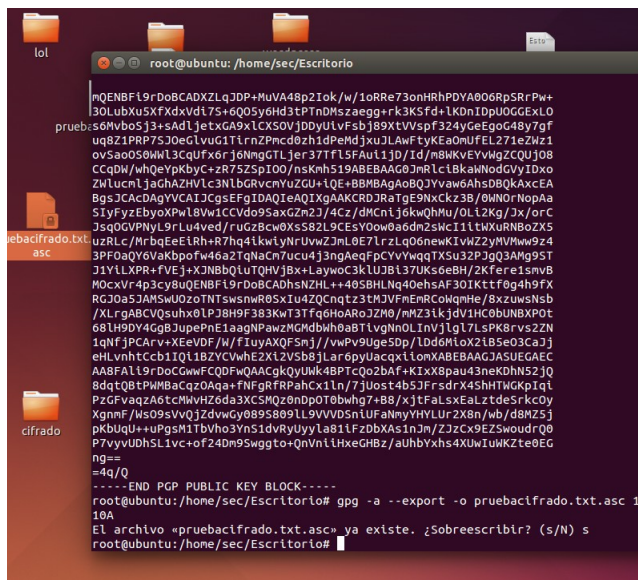


A terminal window on an Ubuntu system. The prompt is root@ubuntu: /home/sec/Escritorio. The command executed is gpg -a --export 13D3710A. The output shows a long block of ASCII text representing the public key, starting with -----BEGIN PGP PUBLIC KEY BLOCK----- and ending with -----END PGP PUBLIC KEY BLOCK-----.

```
root@ubuntu: /home/sec/Escritorio# gpg -a --export 13D3710A
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1

mQENBF19rDoBCADKXZLqJDP+MuVA48p2Iok/W/1oRRe73onHRHPDYA006RpSRrPw+
30LubXu5XfXdxVd17S+6Q05y6Hd3tPTnDMsZaegg+rk3K5fd+LKDnIDpU0GGExL0
s6Mvbo5j3+sadLjetxGA9xLCXSOVjDDyULvFsbj89XtVVspF324yGeEgoG48y7gf
uq8Z1PRP75J0eGLvug1TlRnZPncd0zh1dPeMdjxuJLAWfTyKEaOmUFEL271eZWz1
ov5a0S0WnL3CqUfX6rj6NmgGTLjer37TfLSFAu1jD/Id/m8WKvEYVwqZCQUj08
CcQdW/whQeYpkybc+zR75ZSp100/nSkh519ABEBAAGJmRlclBkaWNoZGVyIDxo
ZWlucnljaGhaZHVlc3NlbGRvcnVpZGU+IQE+BBMBAgAoBQJYvaw6AhsDBQKAcCEA
BgsJCAcDAGVYVCA1JCgsEFQIDAQIeAQIAXgAAKCRDJaTgE9NxCkz3B/0WNO/NopAa
SIyFyzEbyoXPwL8Vw1CCVdo9SaxGZm2J/4Cz/dMcn1j6kwQhMu/OLl2Kg/Jx/orC
JsqOGVPnyL9rLu4ved/rugZBcw0Xs582L9CEsY0ow0a6dm2sWc11tWxURNBoZX5
uzRLc/MrbqEeE1Rh+R7hq4ikwYnRuvwZJnL0E7LrzLq06newKIVWZ2yVMWmw9z4
3PFOaQY6VakbpoFw46a2TqNaCn7uc4j3ngAeqFpCYVvWqTXSu32PjgQ3AMg9ST
J1YlLXPR+FVEj+XJNBbQlUTQHVjBx+Laywoc3kLUJB137UKs6eBH/2Kfere1smvB
MocxVr4p3cy8uQENBF19rDoBCADhsNZHL++40SBHLNq40ehsAF30IKttf0g4h9FX
RGJ0a5JAM5WU0z0TNTswsNwR0SxiU4ZQCNqtz3tMjVfEmRC0wqHmE/8xzuwsNsb
/XLrgABCVQsuhx0LPJ8H9F383kWT3TfGqHoAoR0JZM0/mMZ3ikjdVlHC0bUNBXPot
68LH9DY4GgBJupePnE1aagNPawzMGmdbwh0aBtlvgNnOLInVjlgL7LSPK8rvs2ZN
1qNfjPCArv+XEeVDF/W/fIuyAQFSnj/vwPv9Uge50p/Ldd6MioX2lB5e03CaJj
cfreHLvnhtccb1I1BZYCVWhe2Xl2VSB8jLar6pyUacqx1onXABEBAAGJA5UEGAEC
AABFAl9rDoCgWwFCQDFwQAACgkQyUmk4BPTCQo2bAF+KIX8pau43neKdHN52jQ
8dqtQBtPwMbaCqz0Aqa+fNgrFRpAhCxl1n/7J0ust4b5JFrdrX4SHHTWGKpIqL
PzGFvaqA6tcMwVhZ6da3XCSMQz0ndPOT0bwhg7+BB/xjTfLsXeaLztdesRkc0y
XgnnF/Ws09sVvQjZdvwGy089S809LL9VVVD5nIUfANmyYHVLUR2X8n/wb/dmZ5j
pKBUQu++uPgsm1Tbvho3YnS1dvRyUyylab1fZDbXAs1nJm/ZJzCk9EZSoudrQ0
P7vyvUDhSL1vc+of24Dm9Swggt+QnVnltHxeGHBz/aUhbYxhs4XUuIWkZte0EG
ng==
-----END PGP PUBLIC KEY BLOCK-----
root@ubuntu: /home/sec/Escritorio#
```

Para exportar la clave usamos el comando
gpg -a --export -o pruebacifrado.txt.asc

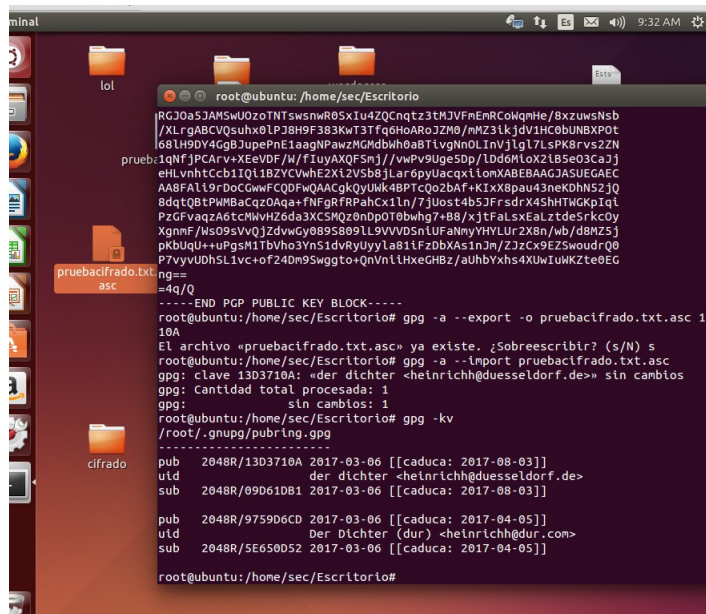


A terminal window on an Ubuntu system. The prompt is root@ubuntu: /home/sec/Escritorio. The command executed is gpg -a --export -o pruebacifrado.txt.asc 13D3710A. The output shows the same long block of ASCII text as the previous screenshot, but it is being written to a file named pruebacifrado.txt.asc. The prompt returns to root@ubuntu: /home/sec/Escritorio#.

```
root@ubuntu: /home/sec/Escritorio# gpg -a --export -o pruebacifrado.txt.asc 13D3710A
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1

mQENBF19rDoBCADKXZLqJDP+MuVA48p2Iok/W/1oRRe73onHRHPDYA006RpSRrPw+
30LubXu5XfXdxVd17S+6Q05y6Hd3tPTnDMsZaegg+rk3K5fd+LKDnIDpU0GGExL0
s6Mvbo5j3+sadLjetxGA9xLCXSOVjDDyULvFsbj89XtVVspF324yGeEgoG48y7gf
uq8Z1PRP75J0eGLvug1TlRnZPncd0zh1dPeMdjxuJLAWfTyKEaOmUFEL271eZWz1
ov5a0S0WnL3CqUfX6rj6NmgGTLjer37TfLSFAu1jD/Id/m8WKvEYVwqZCQUj08
CcQdW/whQeYpkybc+zR75ZSp100/nSkh519ABEBAAGJmRlclBkaWNoZGVyIDxo
ZWlucnljaGhaZHVlc3NlbGRvcnVpZGU+IQE+BBMBAgAoBQJYvaw6AhsDBQKAcCEA
BgsJCAcDAGVYVCA1JCgsEFQIDAQIeAQIAXgAAKCRDJaTgE9NxCkz3B/0WNO/NopAa
SIyFyzEbyoXPwL8Vw1CCVdo9SaxGZm2J/4Cz/dMcn1j6kwQhMu/OLl2Kg/Jx/orC
JsqOGVPnyL9rLu4ved/rugZBcw0Xs582L9CEsY0ow0a6dm2sWc11tWxURNBoZX5
uzRLc/MrbqEeE1Rh+R7hq4ikwYnRuvwZJnL0E7LrzLq06newKIVWZ2yVMWmw9z4
3PFOaQY6VakbpoFw46a2TqNaCn7uc4j3ngAeqFpCYVvWqTXSu32PjgQ3AMg9ST
J1YlLXPR+FVEj+XJNBbQlUTQHVjBx+Laywoc3kLUJB137UKs6eBH/2Kfere1smvB
MocxVr4p3cy8uQENBF19rDoBCADhsNZHL++40SBHLNq40ehsAF30IKttf0g4h9FX
RGJ0a5JAM5WU0z0TNTswsNwR0SxiU4ZQCNqtz3tMjVfEmRC0wqHmE/8xzuwsNsb
/XLrgABCVQsuhx0LPJ8H9F383kWT3TfGqHoAoR0JZM0/mMZ3ikjdVlHC0bUNBXPot
68LH9DY4GgBJupePnE1aagNPawzMGmdbwh0aBtlvgNnOLInVjlgL7LSPK8rvs2ZN
1qNfjPCArv+XEeVDF/W/fIuyAQFSnj/vwPv9Uge50p/Ldd6MioX2lB5e03CaJj
cfreHLvnhtccb1I1BZYCVWhe2Xl2VSB8jLar6pyUacqx1onXABEBAAGJA5UEGAEC
AABFAl9rDoCgWwFCQDFwQAACgkQyUmk4BPTCQo2bAF+KIX8pau43neKdHN52jQ
8dqtQBtPwMbaCqz0Aqa+fNgrFRpAhCxl1n/7J0ust4b5JFrdrX4SHHTWGKpIqL
PzGFvaqA6tcMwVhZ6da3XCSMQz0ndPOT0bwhg7+BB/xjTfLsXeaLztdesRkc0y
XgnnF/Ws09sVvQjZdvwGy089S809LL9VVVD5nIUfANmyYHVLUR2X8n/wb/dmZ5j
pKBUQu++uPgsm1Tbvho3YnS1dvRyUyylab1fZDbXAs1nJm/ZJzCk9EZSoudrQ0
P7vyvUDhSL1vc+of24Dm9Swggt+QnVnltHxeGHBz/aUhbYxhs4XUuIWkZte0EG
ng==
-----END PGP PUBLIC KEY BLOCK-----
root@ubuntu: /home/sec/Escritorio# gpg -a --export -o pruebacifrado.txt.asc 13D3710A
El archivo 'pruebacifrado.txt.asc' ya existe. ¿Sobreescribir? (s/N) s
root@ubuntu: /home/sec/Escritorio#
```

Para importar la clave usamos el comando
gpg --import pruebacifrado.txt.asc



```
root@ubuntu: /home/sec/Escritorio
RGCJ0a5JAMSU0zoTNTswnR05xiu4ZQcngtz3tMJVFmEnRCoWqmHe/8xzuwsNsb
/XLrgABCVQsuhx0LPJ8H9F383KwT3Tf6HoARoJZM0/mMZ3lkjdV1HC0bUNBXp0t
68LH9DY4GgBJupePnE1aagNPawzMGmDbwH0aBTivgNnOLInVjlgL7LSPK8rvs2ZN
prueb: iQNTjPCArv+XEEVDF/W/fIuyAQFSnj//vwPv9UgeSdp/Ldd6HtoX2l8Se03caJj
eHLvnhTccbiTq1BZVCVwhE2XZvSb8Lar6pyUeqxionXABEBACJASUEGAE
AABFAl9rDcGwwFCQDFwQAACgkoyUWk4BPTC0o2bAF+KIX8pau43nekDhNS2jQ
8dqtQBtPwMBacQz0Aqa+fNfgrFRPahCx1ln/7JUost4b5JFrSdrX4SHHTGKpIql
PzCFvaqzA6tcMkvHZ6da3XCSWQz0ndp0T0bwhg7+B8/xjtfALsxEalZtdeSrkc0y
XqnmF/Ws09svvQjZdvGy0895809LL9VVVDsnlUFAmnyVHVLur2X8n/wb/d8MZ5j
pkBuQu++uPgsm1Tbvho3Yn51dvRyUyylab1fZDbXAsin3m/ZJzCx9EZSwoudrQ0
P7vyvUDhSL1vc+of24Dm9Swggt0+QnVnliHxeGHBz/aUhbYxhs4XUwIUWKzte0EG
gpg==
-----BEGIN PGP PUBLIC KEY BLOCK-----
root@ubuntu: /home/sec/Escritorio# gpg -a --export -o pruebacifrado.txt.asc 13
10A
El archivo «pruebacifrado.txt.asc» ya existe. ¿Sobreescribir? (s/N) s
root@ubuntu: /home/sec/Escritorio# gpg -a --import pruebacifrado.txt.asc
gpg: clave 13D3710A: «der dichter <heinrichh@duesseldorf.de>» sin cambios
gpg: Cantidad total procesada: 1
gpg:      sin cambios: 1
root@ubuntu: /home/sec/Escritorio# gpg -kv
/root/.gnupg/pubring.gpg
-----
pub  2048R/13D3710A 2017-03-06 [[caduca: 2017-08-03]]
uid  der dichter <heinrichh@duesseldorf.de>
sub  2048R/09D61DB1 2017-03-06 [[caduca: 2017-08-03]]

pub  2048R/9759D6CD 2017-03-06 [[caduca: 2017-04-05]]
uid  Der Dichter (dur) <heinrichh@dur.com>
sub  2048R/5E650D52 2017-03-06 [[caduca: 2017-04-05]]
root@ubuntu: /home/sec/Escritorio#
```

Para asegurarnos que se han incluido en el keyring usamos el comando
gpg -kv

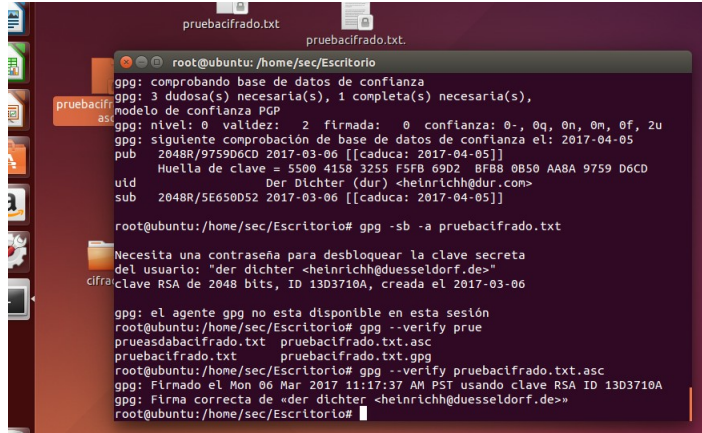
Firma digital de un documento

Para firmar un documento usamos el comando

gpg -sb -a pruebacifrado.txt

Para verificar la firma del documento usamos el comando

gpg --verify pruebacifrado.txt.asc



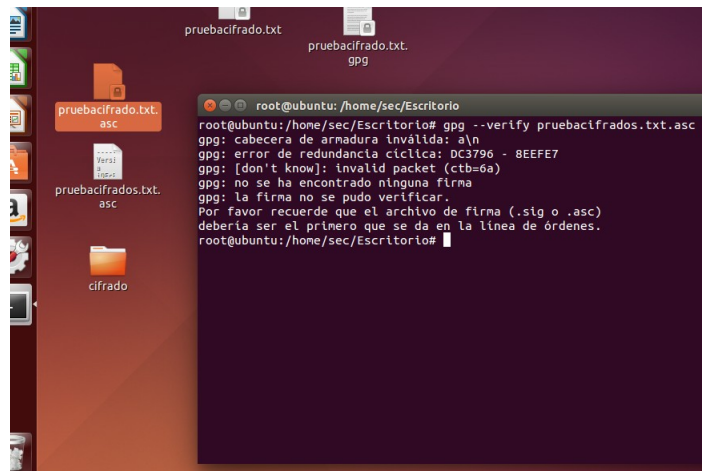
```
pruebacifrado.txt
pruebacifrado.txt.
root@ubuntu: /home/sec/Escritorio
gpg: comprobando base de datos de confianza
gpg: 3 dudosa(s) necesaria(s), 1 completa(s) necesaria(s),
modelo de confianza PGP
gpg: nivel: 0 validez: 2 firmada: 0 confianza: 0-, 0q, 0n, 0m, 0f, 2u
gpg: siguiente comprobación de base de datos de confianza el: 2017-04-05
pub 2048R/9759D6CD 2017-03-06 [[caduca: 2017-04-05]]
HueLLa de clave = 5500 4150 3255 F5F0 69D2 BF80 0B50 AA8A 9759 D6CD
uid Der Dichter (dur) <heinrichh@dur.com>
sub 2048R/5E650D52 2017-03-06 [[caduca: 2017-04-05]]

root@ubuntu: /home/sec/Escritorio# gpg -sb -a pruebacifrado.txt

Necesita una contraseña para desbloquear la clave secreta
del usuario: "der dichter <heinrichh@duesseldorf.de>"
clave RSA de 2048 bits, ID 13D3710A, creada el 2017-03-06

gpg: el agente gpg no esta disponible en esta sesión
root@ubuntu: /home/sec/Escritorio# gpg --verify prue
prueasdabacifrado.txt pruebacifrado.txt.asc
pruebacifrado.txt pruebacifrado.txt.gpg
root@ubuntu: /home/sec/Escritorio# gpg --verify pruebacifrado.txt.asc
gpg: Firmado el Mon 06 Mar 2017 11:17:37 AM PST usando clave RSA ID 13D3710A
gpg: Firma correcta de «der dichter <heinrichh@duesseldorf.de>»
root@ubuntu: /home/sec/Escritorio#
```

Si se modifica algo en el archivo nos dará un error como este



```
pruebacifrado.txt
pruebacifrado.txt.
gpg
root@ubuntu: /home/sec/Escritorio
root@ubuntu: /home/sec/Escritorio# gpg --verify pruebacifrados.txt.asc
gpg: cabecera de armadura inválida: a\n
gpg: error de redundancia ciclica: DC3796 - 8EEFE7
gpg: [don't know]: invalid packet (ctb=6a)
gpg: no se ha encontrado ninguna firma
gpg: la firma no se pudo verificar.
Por favor recuerde que el archivo de firma (.sig o .asc)
deberia ser el primero que se da en la linea de órdenes.
root@ubuntu: /home/sec/Escritorio#
```