

Usando GnuPG

Por. Daniel Vazart.

debian

Generar un par de Claves

- La primera pregunta es qué algoritmo se va a usar. El algoritmo recomendado por GnuPG es DSA/ElGamal, ya que éste no está patentado.
- La siguiente pregunta es la longitud de la clave.
- El sistema nos pedirá a continuación que se introduzca el nombre, comentario y dirección de correo electrónico.

```
ono:~# gpg --gen-key
gpg (GnuPG) 1.4.1; Copyright (C) 2005 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.

Por favor seleccione tipo de clave deseado:
  (1) DSA and Elgamal (default)
  (2) DSA (sólo firmar)
  (5) RSA (sólo firmar)
Su elección: 1
DSA keypair will have 1024 bits.
ELG-E keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 1024
El tamaño requerido es de 1024 bits
Por favor, especifique el período 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)? 0
Key does not expire at all
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>"

Nombre y apellidos: Daniel Vazart
Dirección de correo electrónico: dvazart@gmail.com
Comentario:
Ha seleccionado este ID de usuario:
  "Daniel Vazart <dvazart@gmail.com>"

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

The Debian logo, consisting of the word "debian" in a white, lowercase, sans-serif font, positioned in the bottom right corner of a dark blue background.

Exportar la Clave

- Al exportar la clave pública se amplía el abanico de personas con las que se podrá comunicar de modo seguro.
- Con la opción `-a` se exportará la clave pública en formato de texto plano y no en binario.
- Una vez tenemos la clave, podemos publicarla en nuestra pagina WEB, nuestros correos electrónicos o en servidores de claves PGP.

```
ono:~# gpg --export -a Daniel
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.1 (GNU/Linux)

mQGIBEUANw8RBADi vcaqPZU3BwpJRtAMShBoe4qBw66/i+lGZC+sMJLYHP/8Gx9O
wM5HFqfVpbDC5kcwk3KJiGlKaUKoDG6/RUu25vM/c9m0P+F0Qf3AGyhaLFPHT9kH
PVZJ1sJXRebAmEFMYk45phePT5kUHsXyvSeHx3gbM8wN4iheqgcCUqQsHwCg6PhY
rH0l2pJHxJZn9Qv2W/opjyMEAMDxfhXl/swYmSEKcpj0ZQEH7yduvTmdU/HhaScY
L0Cxw6MhwFT rmd8a4gMmdQ9Z+U2MIY99qY7Q05vBME4QrYQ+ECFpzWrHvFFhUA+9
J7J8Wav+j8XB6Pa1pAuH0UfE1w5aaeh1RJZtkDL60RHVXnXHq5HJk0kRwOpyIPum
9DgwA/9jGTtnY/6rKd/bQ+YYk0cE0i v89ArDKJXIQKZDYewmgA/2ebG08hswXQ4U
GaQpttX5klJBRBx4xq2ezvs5qC5gILCODCKkGZ1Fvx0oNDKtLIa4Q0KATHG/RUDj
nBjDZhzLRswdX34MF8uHuwkAcMi jU+ZnwrQFnVG8vU2NoDgFj bQhRGFuaWVsIFZh
emFydCA8ZHZhEmFydEBnbWFpbC5jb20+iF4EEExECAB4FAkUANw8CGwMGCwkIBwMC
AxUCAwMwAgECHgECF4AACgkQaz/fGu2ISEKF/wCg3fI3gyMGjak27Zsv0i forq0g
FnkAnliQ2XGuXlSmoczHmlmzeu8y6u34uQENBEUANxAQBADlwpsWMwMcYjw0fIK0
Ojkmf4+qdoxVe+0AuEhtV3YbEUNEeMnp0vwsXen6pcQuG+Hv/iC6B0nY aRmq6IOo
Ab67kL92eQLlaKw9yuwqZKci1wbE11PuLorbWdn+6VPggP08bXypNP28E91I01NF
RqTj lUJX0SwhlwSDsevltn0U1wADBQQA1Np+X/iybgrzv9DCGy9vluYV540+ceDw
woNV/HQa8WmG90PHZWU16RgJEYqjFFXEEA0j/x+kxEw+2/X2czMpAQ3eAzGV+0e9
JB8eSE7Xoy0/t856KuKh1lKQbI3gdgIQGWXYKNKpDPymyJebot0L+1UwsAx5Y2d1
fJuSMz0MRbqISQQYEQIACQUCRQA3EAIbDAAKCRBrP98a7YhIQqZBAJ4zBjx0N7nK
is18fz8a7lumeGba2ACeN+I4c+QAbw/oDON4sq63kn0YYi4=
=Gz2I
-----END PGP PUBLIC KEY BLOCK-----
ono:~# █
```

debian

Exportar la Clave

- Con la opción `-o` se puede exportar la clave a un archivo para enviarla en forma de archivo adjunto (muy útil para correos electrónicos).

```
ono:~# gpg --export -a -o clave.txt Otro
ono:~# ls
amsn_received      cursos2006-08-03.txt  imagenes           pruebas
asimetricas.ppt   cursos2006-ago-10.txt jabber             RadioComunicaciones_y_Antenas.pps
awstats_stallman.txt cursos2006II.txt     lista_de_correos_FIUC.csv Redirect.html
awstats.txt       dbootstrap_settings lista_de_correos_FIUC.csv~ reportes
celulares-cesde.odt Desktop             logs              sc_trans_040
CESDE              documentos          M3.ppt            seguridad.ppt
clave.txt          Elalbumdelabuelo.ppt moodle_upuser     servicios.corriendo.stallman.txt
cripto-cesde.ppt  export.png          myBusinessLetterTemplate.ott shoutcast-1-9-5-linux-glibc6
criptografia.ppt  gen-key2.png       paquetes_stallman.txt shoutcast-playlist.pls
Criptografia.ppt  gen-key.png        playlists         usando-gnupg.ppt
criptografia.rtf  Grupo empresarial~ programas
```

Importar una Clave

- Cuando se recibe la clave pública de otra persona hay que añadirla a la base de datos para poder hacer uso de ella.

```
ono:~# gpg --import clave.txt
gpg: key F8025D16: public key "Otro Usuario <compras.wiplash@gmail.com>" imported
gpg: Cantidad total procesada: 1
gpg:             importadas: 1
ono:~# █
```

Resumiendo...

- En este punto, tenemos 2 claves publicas: La primera de ellas es mi clave publica y la otra es la que se importo desde el archivo enviado por el usuario "Otro".

```
ono:~# gpg --list-keys
/root/.gnupg/pubring.gpg
-----
pub   1024D/ED884842 2006-09-07
uid           Daniel Vazart <dvazart@gmail.com>
sub   1024g/6236943A 2006-09-07

pub   1024D/F8025D16 2006-09-07
uid           Otro Usuario <compras.wiplash@gmail.com>
sub   1024g/4CB3CCC2 2006-09-07
```

Resumiendo...

- También tenemos una sola clave privada que es con la que vamos a desenscriptar los mensajes que nos envían.

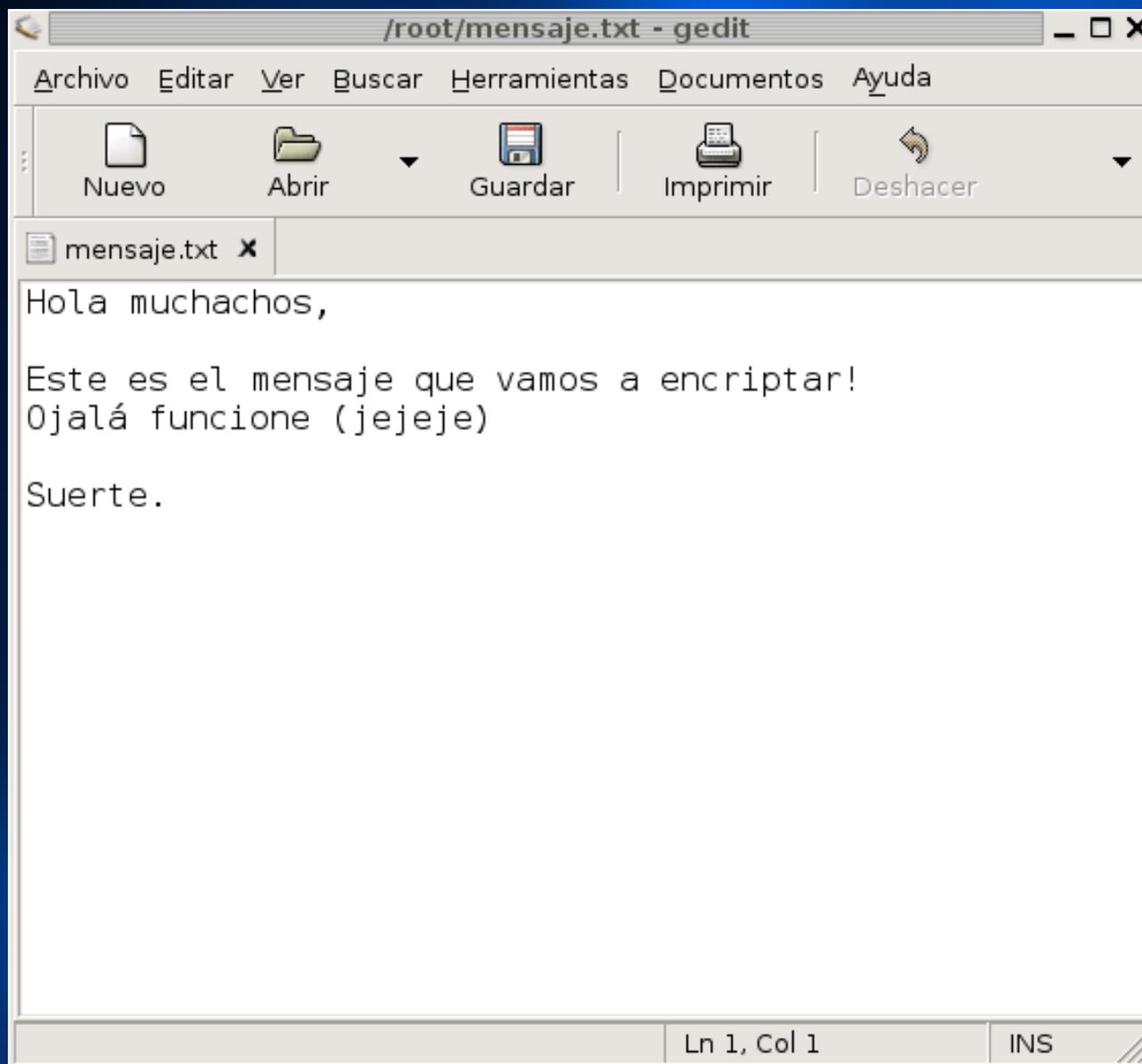
```
ono:~# gpg --list-secret-keys
/root/.gnupg/secring.gpg
-----
sec   1024D/ED884842 2006-09-07
uid           Daniel Vazart <dvazart@gmail.com>
ssb   1024g/6236943A 2006-09-07
```

Encriptar...

- Para encriptar un archivo, debemos utilizar la opción -e (encriptar) seguida de la opción -r (recipiente) para especificar el usuario (clave publica) a quien se enviará el mensaje.
- también es posible utilizar la opción -a para que se genere una encriptación en modo texto y no en binario.
- El resultado será un archivo con la extensión .asc

debian

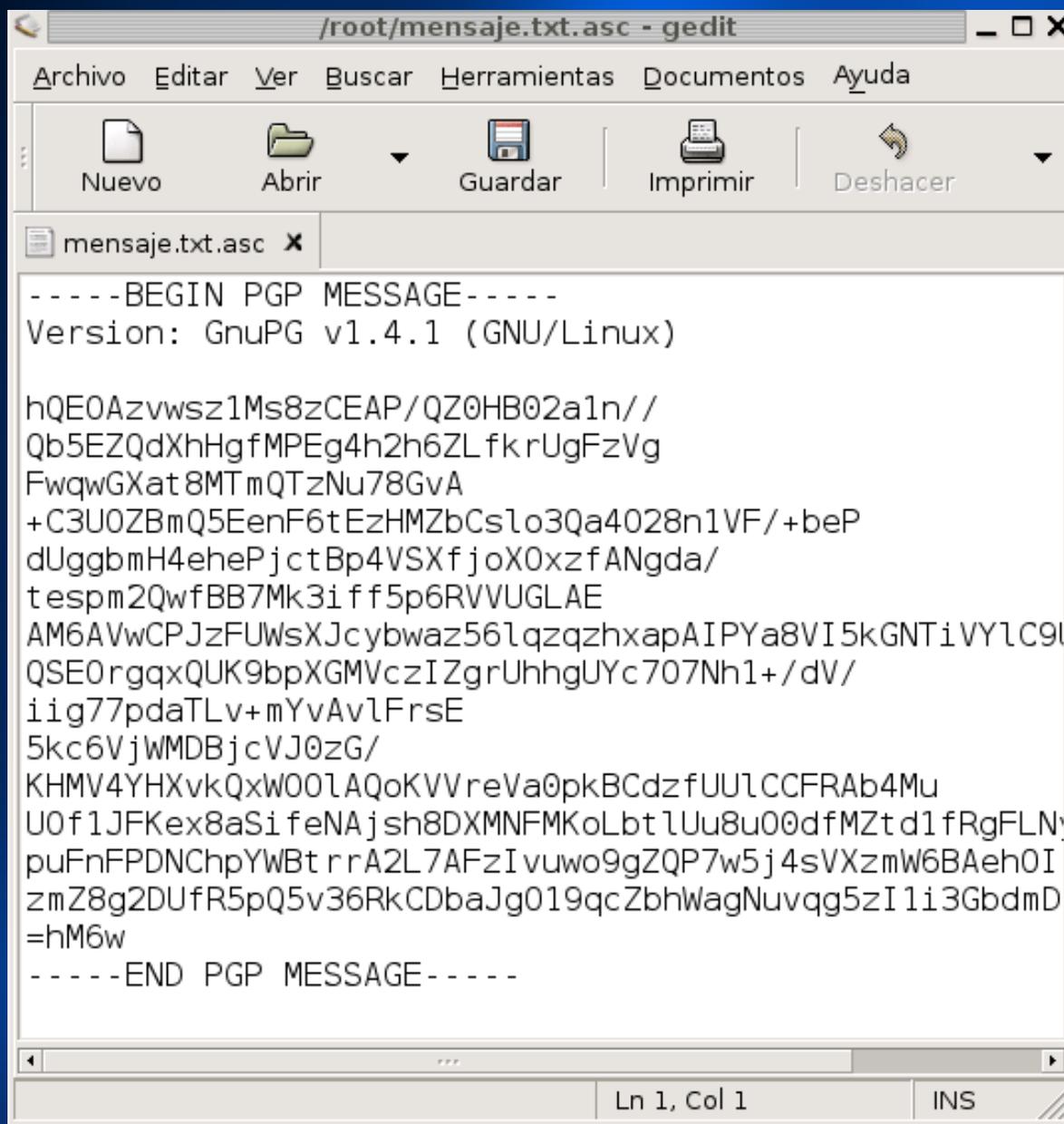
Mensaje a encriptar:



Encriptando...

```
ono:~# gpg -a -er Daniel mensaje.txt
ono:~# ls
amsn_received      cursos2006II.txt      jabber              playlists
asimetricas.ppt    dbootstrap_settings  lista_de_correos_FIUC.csv  programas
awstats_stallman.txt Desktop              lista_de_correos_FIUC.csv~  pruebas
awstats.txt        documentos           list-keys.png        RadioComunicaciones_y_Antenas.pps
celulares-cesde.odt Elalbumdelabuelo.ppt logs                 Redirect.html
CESDE              encriptando.png      M3.ppt              reportes
clave.txt          export.png           mensajeasc.png       sc_trans_040
cripto-cesde.ppt   export-txt.png       mensaje.txt          secret-keys.png
criptografia.ppt   gen-key2.png         mensaje.txt.asc      seguridad.ppt
Criptografia.ppt   gen-key.png          mensajes.txt.png     servicios.corriendo.stallman.txt
criptografia.rtf   Grupo empresarial~   moodle_upuser       shoutcast-1-9-5-linux-glibc6
cursos2006-08-03.txt imagenes             myBusinessLetterTemplate.ott  shoutcast-playlist.pls
cursos2006-ago-10.txt import.png           paquetes_stallman.txt  usando-gnupg.ppt
ono:~#
```

Mensaje Encriptado:



The image shows a screenshot of a gedit text editor window. The title bar reads "/root/mensaje.txt.asc - gedit". The menu bar includes "Archivo", "Editar", "Ver", "Buscar", "Herramientas", "Documentos", and "Ayuda". The toolbar contains icons for "Nuevo", "Abrir", "Guardar", "Imprimir", and "Deshacer". The main text area contains a PGP message:

```
-----BEGIN PGP MESSAGE-----  
Version: GnuPG v1.4.1 (GNU/Linux)  
  
hQE0Azvwsz1Ms8zCEAP/QZ0HB02a1n//  
Qb5EZQdXhHgfMPEg4h2h6ZLfk rUgFzVg  
FwqwGXat 8MTmQTzNu78GvA  
+C3U0ZBmQ5EenF6tEzHMZbCslo3Qa4028n1VF/+beP  
dUggbmH4ehePjctBp4VSXfjoX0xzfANgda/  
tespm2QwfBB7Mk3iff5p6RVVUGLAE  
AM6AVwCPJzFUWsXJcymbwaz56lqzqzhxapAIPYa8VI5kGNTiVYlC9l  
QSE0rgqxQUK9bpXGMVczIZgrUhhgUYc707Nh1+/dV/  
iig77pdaTLv+mYvAvlFrSE  
5kc6VjWMDBjcVJ0zG/  
KHMV4YHXvkQxw00lAQoKVVreVa0pkBCdzfUULCCFRAb4Mu  
U0f1JFKex8aSi feNAjsh8DXMNFMKoLbt lUu8u00dfMZtd1fRgFLN  
puFnFPDNChpYWBt rra2L7AFzIvuwo9gZQP7w5j4sVXzmW6BAehOI  
zmZ8g2DUfR5pQ5v36RkCDbaJg019qcZbhWagNuvqg5zI1i3GbdmD  
=hM6w  
-----END PGP MESSAGE-----
```

The status bar at the bottom indicates "Ln 1, Col 1" and "INS".

Desencriptar

- Para desencriptar se debe utilizar la opción -d seguida del nombre del archivo con extensión .asc
- Tambien se puede utilizar la opción -o para especificar el archivo de destino.

Desencriptar

```
ono:~# gpg -d mensaje.txt.asc
```

```
You need a passphrase to unlock the secret key for
```

```
user: "Daniel Vazart <dvazart@gmail.com>"
```

```
1024-bit ELG-E key, ID 6236943A, created 2006-09-07 (main key ID ED884842)
```

```
Introduzca frase contraseña: 
```

```
gpg: encrypted with 1024-bit ELG-E key, ID 6236943A, created 2006-09-07
```

```
    "Daniel Vazart <dvazart@gmail.com>"
```

```
Hola muchachos,
```

```
Este es el mensaje que vamos a encriptar!
```

```
Ojalá funcione (jejeje)
```

```
Suerte.
```

```
ono:~# 
```