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.

debian

```
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?
```

debian

```
¿Cambia (N)ombre, (C)omentario, (D)irección o (V)ale/(S)alir? v
Necesita una frase contraseña para proteger su clave secreta.

Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/consola, 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.
+++++++++++++++...+++++.++++++++++..+++++++++++++++...++++++++++.++++++++++++++++++++++++++++++.++++++++++++++.+++++.+++++++
++++++++++++++++++>++++++++++.............+++++
Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/consola, 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: key ED884842 marked as ultimately trusted
claves pública y secreta creadas y firmadas.

gpg: comprobando base de datos de confianza
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
pub   1024D/ED884842 2006-09-07
      Key fingerprint = 96E1 839A F328 7E0B B2BC  205E 6B3F DF1A ED88 4842
uid                  Daniel Vazart <dvazart@gmail.com>
sub   1024g/6236943A 2006-09-07

ono:~#
```

debian

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 publica 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.

debian

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

mQGiBEUANw8RBADivcaqPZU3BWpJRtAMShBoe4qBw66/i+lGZC+sMJlYHP/8Gx90
wM5HFqfVpbDC5kcwk3KJiGlKaUKoDG6/RUu25vM/c9m0P+FOQf3AGyhaLFPHt9kH
PVZJ1sJXRebAmEFMYk45phePT5kUHsXyvSeHx3gbM8wN4iheqgcCUqQsHwCg6PhY
rH0l2pJHxJZn9Qv2W/opjyMEAMDxfhXl/sWYmSEKcpj0ZQEH7yduvTmdU/HhaScY
L0CxW6MhWFTrmd8a4gMmdQ9Z+U2MIY99qY7QO5vBME4QrYQ+ECFpzWrHvFFhUA+9
J7J8Wav+j8XB6PalpAuH0UfE1w5aaeh1RJZtkDL60RHVXnXHq5HJk0kRw0pyIPum
9DgwA/9jGTtnY/6rKd/bQ+YYk0cE0iv89ArDKJXIQKZDYeWmgA/2ebG08hsWXQ4U
GaQpttX5klJBRBx4xq2ezvs5qC5gIlC0DCKkGZ1FvxOoNDKtLIa4Q0KATHG/RUDj
nBjDZhzLRswdX34MF8uHuwkAcMijU+ZnwrQFnVG8vU2NoDgFjbQhRGFuaWVsIFZh
emFydCA8ZHZhemFydEBnbWFpbC5jb20+iF4EExECAB4FAkUANw8CGwMGCwkIBwMC
AxUCAwMWAgECHgECF4AACgkQaz/fGu2ISEKF/wCg3fI3gyMGjak27Zsv0iforq0g
FnkAn1iQ2XGuXlSmoczhMlmzeu8y6u34uQENBEUANxAQBADlwpsWMWMcYjWOfIK0
Ojkmf4+qdoxVe+0AuEhtV3YbEUNEeMnp0vWsXen6pcQuG+Hv/iC6B0nYaRmq6IOo
Ab67kL92eQLlaKw9yuwqZKci1WbE11PuLorbWDn+6VPggPO8bXypNP28E91I01NF
RqTjlUJXOSWhlwSDsevltn0U1wADBQQA1Np+X/iybgrzv9DCGy9vluYV540+ceDW
woNV/HQa8WmG9OPHZWU16RgJEYqjFFXEEA0j/x+kxEw+2/X2czMpAQ3eAzGV+Oe9
JB8eSE7Xoy0/t856KuKh1lKQbI3gdgIQGWXYKNKPdPymyJebotOL+1UWsAx5Y2d1
fJuSMz0MRbqISQQYEQIACQUCRQA3EAIbDAAKCRBrP98a7YhIQqZBAJ4zBjx0N7nK
is18fz8a71umeGba2ACeN+I4c+QAbW/oD0N4sq63kn0YYi4=
=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
ono:~#
```

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:~#
```

debian

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
```

debian

Resumiendo...

- También tenemos una sola clave privada que es con la que vamos a desencriptar 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
```

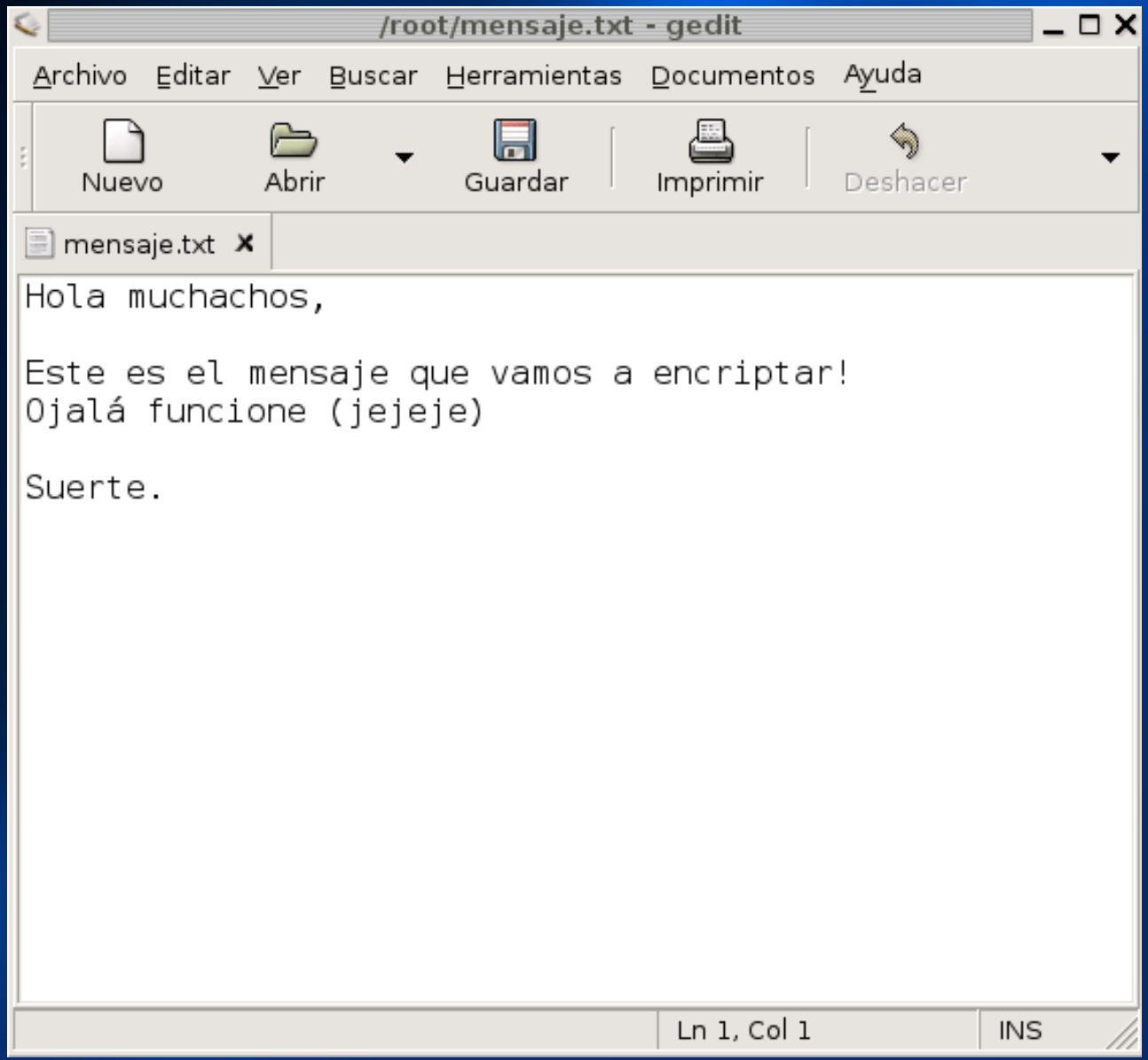
debian

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 encripción en modo texto y no en binario.
- El resultado será un archivo con la extensión .asc

debian

Mensaje a encriptar:



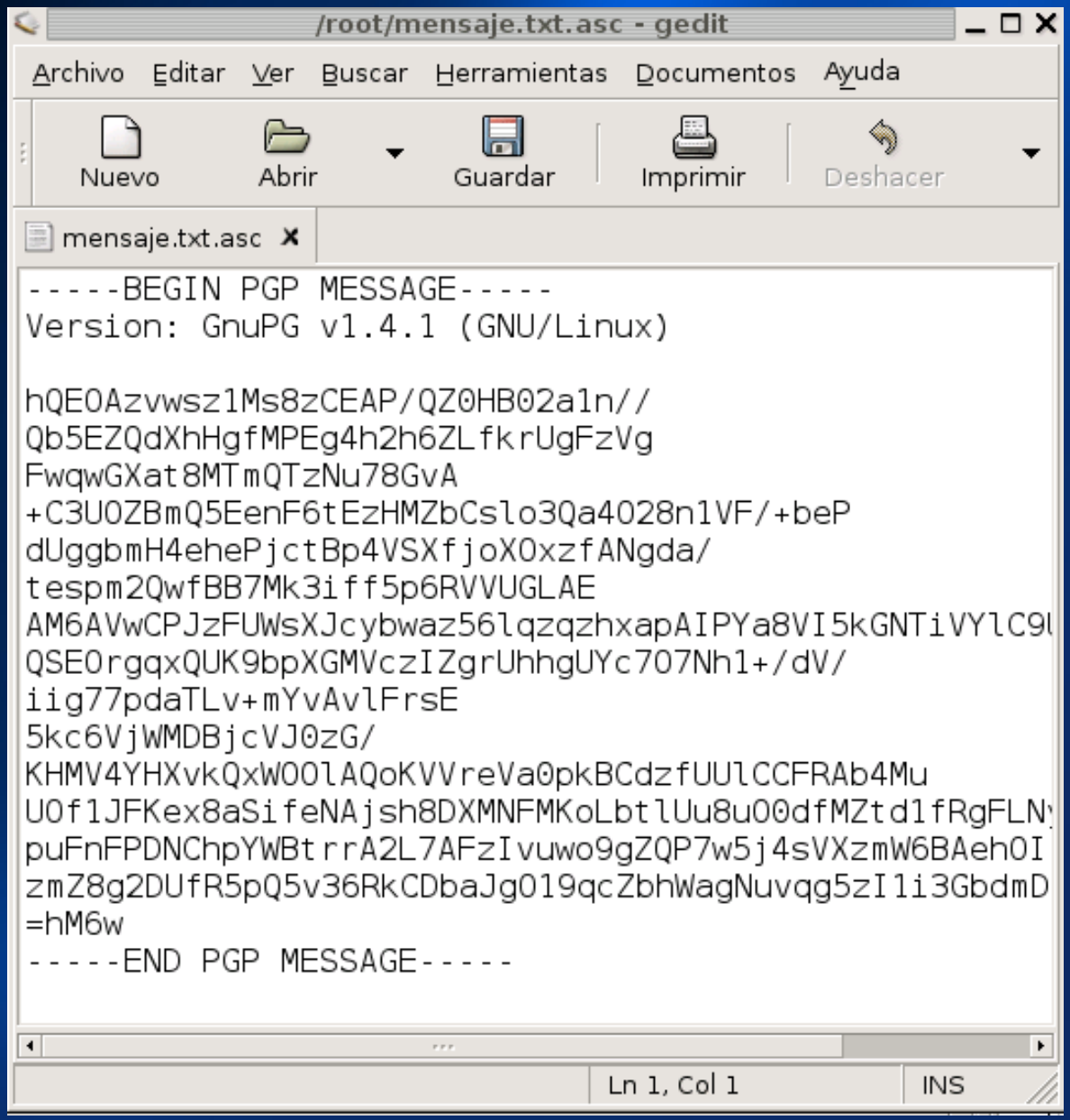
debian

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           mensajetxt.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:~#
```

debian

Mensaje Encriptado:



debian

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.

debian

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:~#
```

debian