PASOS PARA ENCRIPTAR

(1) Generar un nuevo par de claves

La opción de la línea de órdenes -gen-key se usa para generar un nuevo par de claves primario.

javier:~$ gpg -gen-key

(2) Generar un certificado de revocación

javier:~$ gpg -output D58711B7.asc -gen-revoke 0xD58711B7
sec 1024D/D58711B7 1999-09-24 Javier (Paramo S.L.) javier@casa.es

(3) Intercambiar claves

Para poder comunicarse con otros, el usuario debe intercambiar las claves públicas. Para obtener una lista de las claves en el fichero («anillo») de claves públicas, se puede usar la opción de la línea de órdenes -list-keys.

javier:~$ gpg -list-keys
/home/javier/.gnupg/pubring.gpg
---
pub 1024D/D58711B7 1999-09-24 Javier (Paramo S.L.) <javier@casa.es>
sub 1024g/92F6C9E3 1999-09-24

(4) Exportar una clave pública

Para poder enviar una clave pública a un interlocutor, antes hay que exportarla. Para ello se usará la opción de la línea de órdenes -export. Es necesario un argumento adicional para poder identificar la clave pública que se va a exportar. Como en la opción anterior -gen-revoke, hay que usar el identificador de clave o cualquier parte del identificador de usuario para identificar la clave que se desea exportar.

javier:~$ gpg -output javi.gpg -export javier@casa.es

La clave se exporta en formato binario, y esto puede no ser conveniente cuando se envía la clave por correo electrónico o se publica en una página web. Por tanto, GnuPG ofrece una opción de la línea de órdenes -armor5
que fuerza que la salida de la orden sea generada en formato armadura-ASCII, parecido a los documentos codificados con uuencode. Por regla general, cualquier salida de una orden de GnuPG, v.g.. claves, documentos cifrados y firmas, pueden ir en formato armadura-ASCII añadiendo a la orden la opción -armor.

javier:~$ gpg -armor -output javi.asc -export javier@casa.es
---BEGIN PGP PUBLIC KEY BLOCK---
Version: GnuPG v0.9.8 (GNU/Linux)
Comment: For info see http://www.gnupg.org

(5) Importar una clave pública

Se puede añadir una clave pública al anillo de claves públicas mediante la opción -import.

```
javier:~$ gpg -import arancha.gpg
gpg: key B63E132C: public key imported
gpg: Total number processed: 1
gpg: imported: 1
javier:~$ gpg -list-keys
/home/javier/.gnupg/pubring.gpg
---------------------
pub 1024D/D58711B7 1999-09-24 Javier (Paramo S.L.) <javier@casa.es>
sub 1024g/92F6C9E3 1999-09-24
pub 1024D/B63E132C 1999-09-24 Aranzazu (A.G.deZ.) <arancha@nav.es>
sub 1024g/581A915F 1999-09-24
```

Una vez que la clave haya sido importada, es necesario validarla. GnuPG usa un potente y flexible modelo de confianza que no requiere que el usuario dé validez personalmente a cada clave que importe. Sin embargo, algunas claves pueden necesitar que el usuario les dé validez de forma personal. Una clave se valida verificando la huella digital de la clave, y firmando dicha clave para certificar su validez. La huella digital se puede ver con la opción de la línea de órdenes -fingerprint, pero para certificar la clave hay que editarla.

```
javier:~$ gpg -edit-key arancha@nav.es
pub 1024D/B63E132C created: 1999-09-24 expires: never trust: -/q
sub 1024g/581A915F created: 1999-09-24 expires: never
    (1)         Aranzazu (A.G.deZ.) arancha@nav.es

pub 1024D/B63E132C 1999-09-24 Aranzazu (A.G.deZ.) <arancha@nav.es>
Fingerprint: 4203 82E2 448C BD30 A36A 9644 0612 8A0F B63E 132C
```

La huella digital de una clave se verifica con el propietario de la clave. Esto puede hacerse en persona o por teléfono, o por medio de otras maneras, siempre y cuando el usuario pueda garantizar que la persona con la que se está comunicando sea el auténtico propietario de la clave. Si la huella digital que se obtiene por medio del propietario es la misma que la que se obtiene de la clave, entonces se puede estar seguro de que se está en posesión de una copia correcta de la clave.
Después de comprobar la huella digital ya se puede firmar la clave con el fin de validarla. Debido a que la verificación es un punto débil en criptografía de clave pública, es aconsejable ser cuidadoso en extremo y *siempre* comprobar la huella digital de una clave con la que nos dé el propietario antes de firmar dicha clave.

```
Command> sign
pub 1024D/B63E132C created: 1999-09-24 expires: never trust: -/q
Fingerprint: 4203 82E2 448C BD30 A36A 9644 0612 8A0F B63E 132C
Aranzazu (A.G.deZ.) <arancha@nav.es>
Are you really sure that you want to sign this key
with your key: "Javier (Paramo S.L.) <javier@casa.es>"
```

```
Really sign? y
You need a passphrase to unlock the secret key for
user: "Javier (Paramo S.L.) <javier@casa.es>"
1024-bit DSA key, ID D58711B7, created 1999-09-24
Enter passphrase:
```

Una vez firmada, el usuario puede comprobar la clave para obtener un listado de las firmas que lleva y para ver la firma que le acaba de añadir. Cada identificador de usuario tendrá una o más auto firmas, así como una firma por cada usuario que haya validado la clave en cuestión.

```
Command> check
uid Aranzazu (A.G.deZ.) <arancha@nav.es>
sig! B63E132C 1999-09-24 [self-signature]
sig! D58711B7 1999-09-24 Javier (Paramo S.L.) <javier@casa.es>
Command> quit
```

(6) Cifrar y descifrar documentos

Cada clave pública y privada tiene un papel específico en el cifrado y descifrado de documentos. Se puede pensar en una clave pública como en una caja fuerte de seguridad. Cuando un remitente cifra un documento usando

una clave pública, ese documento se pone en la caja fuerte, la caja se cierra, y el bloqueo de la combinación de ésta se gira varias veces. La parte correspondiente a la clave privada, esto es, el destinatario, es la combinación que puede volver a abrir la caja y retirar el documento. Dicho de otro modo, sólo la persona que posee la clave privada puede recuperar un documento cifrado usando la clave pública asociada al cifrado.

Con este modelo mental se ha mostrado el procedimiento de cifrar y descifrar documentos de un modo muy simple. Si el usuario quisiera cifrar un mensaje para Javier, lo haría usando la clave pública de Javier, y él lo descifraría con su propia clave privada. Si Javier quisiera enviar un mensaje al usuario, lo haría con la clave pública del usuario, y éste lo descifraría con su propia clave privada.

Para cifrar un documento se usa la opción -encrypt. El usuario debe tener las claves públicas de los pretendidos destinatarios. El programa espera recibir como entrada el nombre del documento que se desea cifrar o, si éste se omite, una entrada típica. El resultado cifrado se coloca en la salida típica o donde se haya especificado mediante la opción -output. El documento se comprime como medida adicional de seguridad, aparte de cifrarlo.

```
javier:~$ gpg -output doc.gpg -encrypt -recipient arancha@nav.es doc
```

La opción -recipient se usa una vez para cada destinatario, y lleva un argumento extra que especifica la clave pública con la que será cifrado el documento. El documento cifrado sólo puede ser descifrado por alguien con una clave privada que complemente uno de las claves públicas de los destinatarios. El usuario, en

este caso el remitente, no podrá descifrar un documento cifrado por sí mismo a menos que haya incluido su propia clave pública en la lista de destinatarios.
Para descifrar un mensaje se usa la opción -decrypt. Para ello es necesario poseer la clave privada para la que el mensaje ha sido cifrado. De igual modo que en el proceso de cifrado, el documento a descifrar es la entrada, y el Resultado descifrado la salida.

```
arancha% gpg -output doc -decrypt doc.gpg
You need a passphrase to unlock the secret key for
user: "Aranzazu (A.G.deZ.) <arancha@nav.es>"
1024-bit ELG-E key, ID 581A915F, created 1999-09-24 (main key ID
B63E132C)
Enter passphrase:
```

También es posible cifrar documentos sin usar criptografía de clave pública. En su lugar, se puede usar sólo una clave de cifrado simétrico para cifrar el documento. La clave que se usa para la cifrada simétrica deriva de la contraseña dada en el momento de cifrar el documento, y por razones de seguridad, no debe ser la misma contraseña que se esté usando para proteger la clave privada. El cifrado simétrico es útil para asegurar documentos cuando no sea necesario dar la contraseña a otros. Un documento puede ser cifrado con una clave simétrica usando la opción -symmetric.

```
javier:~$ gpg -output doc.gpg -symmetric doc
```

(7) Firmar y verificar firmas

Capítulo 1. Primeros Pasos
Una firma digital certifica un documento y le añade una marca de tiempo. Si posteriormente el documento fuera modificado en cualquier modo, el intento de verificar la firma fallaría. La utilidad de una firma digital es la misma que la de una firma escrita a mano, sólo que la digital tiene una resistencia a la falsificación. Por ejemplo, la distribución del código fuente de GnuPG viene firmada con el fin de que los usuarios puedan verificar que no ha habido ninguna manipulación o modificación al código fuente desde que fue archivado.
Para la creación y verificación de firmas, se utiliza el par público y privado de claves en una operación que es diferente a la de cifrado y descifrado. Se genera una firma con la clave privada del firmante. La firma se verifica por medio de la clave pública correspondiente. Por ejemplo, Javier haría uso de su propia clave privada para firmar digitalmente la entrega de su última ponencia a la Revista de Química Inorgánica. El editor asociado que la recibiera, usaría la clave pública de Javier para comprobar la firma, verificando de este modo que el envío proviene realmente de Javier, y que no ha sido modificado desde el momento en que Javier lo firmó. Una consecuencia directa del uso de firmas digitales es la dificultad en negar que fue el propio usuario quien puso la
Firma digital, ya que ello implicaría que su clave privada ha sido puesta en peligro.
La opción de línea de órdenes -sign se usa para generar una firma digital. El documento que se desea firmar es la entrada, y la salida es el documento firmado.

```
javier:~$ gpg -output doc.sig -sign doc
You need a passphrase to unlock the private key for
user: "Javier (Paramo S.L.) <javier@casa.es>"
1024-bit DSA key, ID D58711B7, created 1999-09-24
Enter passphrase:
```

El documento se comprime antes de ser firmado, y la salida es en formato binario. Con un documento con firma digital el usuario puede llevar a cabo dos acciones: comprobar sólo la firma o comprobar la firma y recuperar el documento original al mismo tiempo. Para comprobar la firma se usa la
Opción -verify. Para verificar la firma y extraer el documento se usa la opción -decrypt. El documento con la firma es la entrada, y el documento original recuperado es la salida.

```
arancha% gpg -output doc -decrypt doc.sig
gpg: Signature made Fri Sep 24 12:02:38 1999 CDT using DSA key ID
D58711B7
gpg: Good signature from "Javier (Paramo S.L.) <javier@casa.es>"
```

(8) Documentos con firmas ASCII

Las firmas digitales suelen usarse a menudo para firmar mensajes de correo electrónicos o en los grupos de noticias. En estas situaciones no se debe comprimir el documento al firmarlo, ya que para aquellos que no dispongan de un sistema para procesarlo sería ininteligible.

```
javier:~$ gpg -clearsign doc
You need a passphrase to unlock the secret key for
user: "Javier (Paramo S.L.) <javier@casa.es>"
1024-bit DSA key, ID D58711B7, created 1999-09-24
```