Encriptación asimétrica con GPG en Ubuntu

GPG o GNU Privacy Guard es una herramienta de cifrado asimétrico y firmas digitales, reemplazo del PGP (Pretty Good Privacy), aunque a diferencia de este, GPG está licenciado bajo la licencia de software libre GPL.

Esta herramienta está implementada normalmente en sistemas operativos GNU y se administra a través de comandos mediante el propio terminal. No obstante existen varias herramientas gráficas como la integrada en Ubuntu (*Contraseñas y claves)* que facilitan la administración a través de una sencilla interfaz gráfica.

¿Cómo generar claves?

Bastaría con **ejecutar en un terminal** el comando *gpg - -gen-key* y seguir las instrucciones que se mostrarán a continuación:

1. En primer lugar seleccionaremos el **tipo de clave** que queremos generar, en nuestro caso seleccionamos la primera y por defecto (*RSA y RSA*)

2. Más tarde será necesario decidir **el tamaño de la clave**, cuanto mayor sea el tamaño, mayor será la seguridad. El tamaño varía entre 512 y 2048, en nuestro caso optaremos por *2048*.

3. Después especificaremos la **validez de contraseña**, en nuestro caso, elegiremos la opción adecuada para que la contraseña nunca caduque.

4. Hecho esto**, especificaremos el nombre de usuario** con el que registraremos la clave, un **comentario** para esta y un **correo electrónico** para hacer referencia a ella en el servidor gpg.

5. **Establecemos una contraseña** de seguridad para la propia clave.

6. Antes de generar las contraseñas será necesario **generar bits aleatorios** para que la operación surta efecto, para ello podemos ejecutar aplicaciones o mover mismamente el propio ratón.

Una vez finalizado el proceso se nos facilitará el identificador de la clave o huella y esta será considerada como de confianza absoluta.

Consultar o salvar nuestras claves

Para consultar nuestras claves privadas o públicas a través del terminal, **nos ayudaremos de los modificadores: -** -export y - -armor.

Podemos utilizar redirecciones para almacenar las claves en el fichero que queramos.
No obstante si no las añadimos, las claves únicamente se mostrarán por pantalla pero no serán almacenadas en ningún fichero.

Clave pública:
gpg - -export [IDClave] - -armor [> fichero]

Clave privada:
gpg - -export-secret-key [IDClave] - -armor [> fichero]

Según manuales de GPG es conveniente guardar estas claves en ficheros .asc
El identificador de la clave únicamente será necesario si disponemos de varias claves generadas en nuestro equipo.

Almacenar la clave pública en un servidor GPG

Los servidores de claves GPG están relacionados entre sí, de manera que únicamente necesitaremos subir la clave pública a un único servidor para que cualquier usuario pueda obtenerla.

gpg [- - key-server Servidor] - -send-key IDClave

Al ejecutar este comando, nuestra clave será almacenada en pocos segundos en el servidor por defecto de GPG, no obstante podemos almacenarla en un determinado servidor gracias al modificador - - key-server.

Para consultar el identificador de una clave, podemos utilizar la aplicación **Contraseñas y claves** que incluye Ubuntu, o ejecutar el comando gpg - - list-keys

Descargar una clave pública GPG

De la misma manera que podemos almacenar nuestras claves públicas, podemos proceder a descargarlas a partir de su identificador o correo electrónico de referencia, para ello ejecutaremos el siguiente comando:

gpg [- - key-server Servidor] - -search-key IDClave|Email

De la misma manera que en el paso anterior, también podemos especificar de forma concreta el servidor en el que se encuentra almacenada dicha clave, para así acelerar aún más el proceso de búsqueda.

Firmando digitalmente ficheros

Para **verificar la identidad de un fichero**, podemos recurrir al firmado digital, para firmar digitalmente cualquier fichero, utilizaremos el siguiente comando

```
gpg - -clearsign Fichero
```

Este comando generará un fichero con igual nombre que el que hemos firmado, solo que con extensión .asc. Si procedemos a abrirlo, podremos observar cierta información que hace referencia a la clave con la que se ha firmado, además del propio mensaje.

Verificando la firma de un fichero

Para comprobar la procedencia de un fichero firmado, podemos proceder a **la comprobación de la firma digital y a la extracción del documento** mediante el comando:

```
gpg  - - output nombreficheronuevo   - -decrypt fichero.asc
```

El resultado de este comando sería un nuevo fichero con el mensaje original, además del resultado de la verificación de la firma digital.

De no tener la clave pública del emisor almacenada en su equipo, **debemos** proceder a **descargarla** de los servidores como se mencionó anteriormente.

Una vez la tengamos descargada debemos proceder a **considerarla como clave de confianza** mediante el comando para poder verificar su identidad…

```
gpg - -sign-key IDClave
```

Hecho esto, podremos **verificar la firma** sin problemas mediante el comando:

```
gpg - -output documento.asc
```

De esta forma la firma del documento .asc será comprobada.