GNU Privacy Guard (GPG)

Jose Almirón Lopez

7 de septiembre del 2023

Índice

¿Qué es gpg? **2**
Generar unas claves para nuestro equipo mediante gpg **2**
Exportar nuestra clave pública **4**
Importar la clave pública anteriormente exportada de gpg **4**
Cifrar un archivo de texto con un mensaje con la clave pública anterior **4**
Descifrar un archivo recibido con nuestra clave privada **4**
Listar todas las claves privadas almacenadas en nuestro equipo **6**
Listar todas las claves públicas almacenadas en nuestro equipo **6**

¿Qué es gpg?

GPG es una herramienta de cifrado y firma digital ampliamente utilizada para garantizar la privacidad y la autenticidad de los datos.

En este ejercicio vamos a usar gpg para el envío de mensajes cifrados. De esta manera pondremos en práctica el principio de la confidencialidad.

Generar unas claves para nuestro equipo mediante gpg.

Para generar unas claves usamos el comando “gpg —gen-key”, y nos aparecerá un asistente interactivo que nos guiará a través del proceso de creación de claves

Esto nos creara las claves con los valores por defecto:

- Tipo de clave: RSA
- Tamaño de clave: 3072
- Fecha de expiración: 3 años
- Nombre y dirección de correo electrónico: estos valores si tenemos que indicarlos
- Passphrase: este valor es la contraseña, también debemos indicarlo

Si necesitamos generar un par de claves de forma más customizada, cambiando el tipo el tamaño o la fecha de expiración usaremos “gen —full-generate-key”

Exportar nuestra clave pública.

con el parámetro -a estamos indicando que queremos que se exporte en formato ASCII

```
~ gpg --export -a "Jose Almiron" > joseAlmiron.key
```

Importar la clave pública anteriormente exportada de gpg.

```
~ gpg --import joseAlmiron.key
gpg: clave EBF91262971D0E08: clave pública "Jose Almiron <jose_016al@outlook.com>" importada
gpg: Cantidad total procesada: 1
gpg:               importadas: 1
```

Cifrar un archivo de texto con un mensaje con la clave pública anterior.

```
~ took 7s gpg --encrypt --recipient "Jose Almiron" -o texto_cifrado.gpg texto.txt
```

Descifrar un archivo recibido con nuestra clave privada.

Para descifrar el fichero, nos pedirá tener la clave pública y la privada, y nos pedirá la contraseña que hayamos establecido a la hora de crear el par de claves, es decir si queremos enviar el fichero encriptado a otro usuario, este deberá importar la clave pública y la privada, así como saber la contraseña.

En el apartado anterior habiamos importado la clave publica, con esa clave solo podemos encriptar, pero a la hora de desencriptar nos falla por no tener la clave privada

```
~ gpg --output texto_descifrado.text --decrypt texto_cifrado.gpg
gpg: cifrado con clave de 3072 bits RSA, ID 145E20E41C629BC5, creada el 2023-10-07
      "Jose Almiron <jose_016al@outlook.com>"
gpg: descifrado fallido: No tenemos la clave secreta
```

Vamos entonces a exportar la clave privada, e importar desde el otro ordenador, para exportar la clave privada nos pedirá que introduzcamos la contraseña

```
~ gpg --export-secret-key -a "Jose Almiron" > private.key
```

Una vez hecho esto, ya podemos importarla desde nuestro otro ordenador y desencriptar el fichero

```
~ gpg --import private.key
gpg: clave EBF91262971D0E08: "Jose Almiron <jose_016al@outlook.com>" sin cambios
gpg: clave EBF91262971D0E08: clave secreta importada
gpg: Cantidad total procesada: 1
gpg:              sin cambios: 1
gpg:       claves secretas leídas: 1
gpg:   claves secretas importadas: 1

~ took 7s gpg --output texto_descifrado.text --decrypt texto_cifrado.gpg
gpg: cifrado con clave de 3072 bits RSA, ID 145E20E41C629BC5, creada el 2023-10-07
      "Jose Almiron <jose_016al@outlook.com>"

~ took 5s cat texto_descifrado.text
       File: texto_descifrado.text
   1   hola mundo
```

Si lo hacemos con el ordenador con el que hemos generado las claves no tendremos que hacer nada más, ya que ya contienen las claves privadas y publicas

```
~ gpg --output texto_descrifrado.txt --decrypt texto_cifrado.gpg
gpg: cifrado con clave de 3072 bits RSA, ID 145E20E41C629BC5, creada el 2023-10-07
      "Jose Almiron <jose_016al@outlook.com>"
```

Listar todas las claves privadas almacenadas en nuestro equipo.

```
~ gpg --list-secret-keys
/home/jose/.gnupg/pubring.kbx
------------------------------
sec   rsa3072 2023-10-07 [SC] [caduca: 2025-10-06]
      53C241A418522D79BE6F405CEBF91262971D0E08
uid           [  absoluta ] Jose Almiron <jose_016al@outlook.com>
ssb   rsa3072 2023-10-07 [E] [caduca: 2025-10-06]

sec   rsa2048 2023-10-07 [SC]
      DCAB1F74DEC43F9219818F474EA2C07ED17491C9
uid           [  absoluta ] claveSegura <jose_016al@outlook.com>
ssb   rsa2048 2023-10-07 [E]
```

Listar todas las claves públicas almacenadas en nuestro equipo

```
~ gpg --list-keys
/home/jose/.gnupg/pubring.kbx
------------------------------
pub   rsa3072 2023-10-07 [SC] [caduca: 2025-10-06]
      53C241A418522D79BE6F405CEBF91262971D0E08
uid           [  absoluta ] Jose Almiron <jose_016al@outlook.com>
sub   rsa3072 2023-10-07 [E] [caduca: 2025-10-06]

pub   rsa2048 2023-10-07 [SC]
      DCAB1F74DEC43F9219818F474EA2C07ED17491C9
uid           [  absoluta ] claveSegura <jose_016al@outlook.com>
sub   rsa2048 2023-10-07 [E]
```