**GNU PrivacyGuard**

**Sistema operativo: GNU/Linux**

* Para la instalación teclearemos:

**sudo apt-get install gnupg**

* Para chequear la versión de gnupg que tenemos instalada:

**gpg --version**

# Creación y subida de las claves

* A continuación, procederemos a crear nuestra clave:

**sudo gpg --gen-key**

* **sudo gpg --send-keys --keyserver pgp.rediris.es $GPGKEY** donde, en lugar de $GPGKEY, deberemos colocar la clave creada con anterioridad. Por ejemplo: si obtenemos una frase como “gpg: key **9E373CC3** marked as ultimately trusted”. 9E373CC3 será la clave que debemos añadir en el comando de arriba.

Si ese paso da error, haz lo siguiente:

* Exportar la clave utilizando este comando:

gpg --export -a "ID-Clave" > miclave.asc

* Copia el contenido del archivo miclave.asc.
* Abre pgp.rediris.es en el navegador.
* Pega el contenido copiado en el cuadro bajo el lema “Submit a key”
* Haz click en el botón “Submit this key”.
* Click Submit.
* En esta **página** web podremos confirmar que la clave ha sido enviada correctamente: <http://pgp.rediris.es>
* (Paso no necesario) Con el objetivo de probar el funcionamiento de la clave, crearemos un fichero de texto plano “prueba” y a continuación lo encriptaremos. El comando a teclear será el siguiente:

**sudo gpg -c prueba**. Creará un fichero prueba.pgp .

* (Paso no necesario) Para ver las claves privadas que tenemos usaremos el comando:

**gpg --list-secret-key**

* (Paso no necesario) Para ver las claves públicas usaremos:

**gpg --list-key**

# Cifrado con clave pública

* En otra máquina virtual con Ubuntu y “gpg” instalado recogeremos la clave pública creada anteriormente:

**gpg --keyserver pgp.rediris.es --recv-keys 9E373CC3**

Si ese paso da error, haz lo siguiente:

* Copia el contenido de la clave.
* Pega ese contenido en un archivo de nombre clave.asc y guárdalo.
* Importa la clave usando este comando:

gpg --import clave.asc

* (Paso no necesario) Las llaves tienen una huella que son una serie de números únicos que se usan para verificar que una llave pertenece realmente al propietario. Para ver dicha huella lo hacemos con el comando:

**gpg --fingerprint ID llave o correo que colocamos al crear el par de llaves**

* Creamos un fichero nuevo de nombre “texto” en esta máquina virtual y lo encriptaremos con la clave pública que hemos obtenido hace un momento:

**sudo gpg --armor --recipient 9E373CC3 --encrypt texto**

Vemos que este comando ha creado “texto.asc”. Enviamos   
 “texto.asc”a la máquina virtual donde tenemos la clave privada.

# Descifrado con clave privada

* En caso de querer descifrar el archivo con la clave privada ejecutamos - en la primera máquina virtual-:

**sudo gpg -d texto.asc ----->** *para ver el mensaje por pantalla.*

**sudo gpg --output texto –d texto.asc ----->** *para que se guarde en el fichero de nombre “texto”.*

Nos pedirá el passphrase para desbloquear la clave privada y descifraremos el fichero.