

# Cifrado asimétrico

GPG es un proyecto libre parte de GNU que implementa el estándar PGP de cifrado. [Esta](#) es su página de proyecto. Viene instalado o es instalable en cualquier distribución Linux, pero también está disponible para otros sistemas.

1. Emplearemos gpg para la generación de un par de claves para cifrado asimétrico mediante: `gpg --gen-key` Durante el proceso de generación se nos irán haciendo diversas preguntas, como el tipo de cifrado que queremos utilizar, la intensidad de cifrado, la fecha de expiración de la clave en cuestión y nuestro nombre y apellidos así como una dirección de correo, que es lo que va a constituir el USERID.

Nos va a bastar con aceptar las opciones que ya vienen por defecto, ya que en la mayoría de los casos éstas son apropiadas:

- Tipo de claves, la primera opción (DSA and ElGamal) que nos permite encriptar y firmar.
- Tamaño de las claves que se puede elegir entre 1024 y 4096 bits. Por defecto se recomienda 2048, a mayor tamaño más segura es la clave y mayor el tiempo de cómputo al encriptar y desencriptar.
- Tiempo de validez queremos que tenga la clave. Por defecto viene la opción 0 que es que no caduque nunca. En el caso de poner que caduque al cabo de cierto tiempo habrá que volver a generar las claves y volver a mandar la nueva clave pública a aquellos que usaban la que ha caducado.
- Último paso, generar la clave, se nos va a preguntar por una frase de paso o passphrase, es decir, una contraseña. Esta contraseña nos va a asegurar que nadie más que nosotros mismos va a poder usar esta clave GPG, por lo que es importante elegir una contraseña fuerte y difícil de adivinar, pero que sea lo suficientemente clara para nosotros como para no olvidarla, puesto que si esto sucede no podremos volver a utilizar más la clave gpg relacionada.

```
[marta@parsek ~]$ gpg --gen-key
gpg (GnuPG) 2.2.17; Copyright (C) 2019 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Nota: Usa "gpg --full-generate-key" para el diálogo completo de generación de clave.
GnuPG debe construir un ID de usuario para identificar su clave.

Nombre y apellidos: Marta Sanchez Gazquez
Dirección de correo electrónico: marta.sanchez@iescamp.es
Ha seleccionado este ID de usuario:
  "Marta Sanchez Gazquez <marta.sanchez@iescamp.es>"
```

**Es muy importante no usar acentos en el nombre en esta práctica, ya que el servidor de claves que vamos a utilizar no sabe realizar búsquedas con acentos.** En otras circunstancias no debería haber problemas por su uso.

Cuando se produce el proceso de generación de las claves es buena idea reproducir mp3, mover el ratón... , para que se generen números aleatorios y se creen antes las claves.


Si es la primera vez que se ejecuta nos crea un directorio en el que guardará el fichero de configuración así como los archivos `secring.gpg` y `pubring.gpg`. En el primero se almacenarán las claves privadas y en el segundo las claves públicas.

Para ver las claves públicas que tenemos disponibles hay que hacerlo con el comando `gpg --list-keys` o `gpg -k`. Esto lo que haces listar las claves que hay disponibles dentro del fichero `pubring.gpg`.

Para ver las claves privadas que tenemos disponibles hay que hacerlo con el comando `gpg --list-secret-keys`. Esto lo que haces listar las claves que hay disponibles dentro del fichero `secring.gpg`.

Se llama anillos a los archivos en los que se guardan las claves públicas y las privadas. Si se quiere borrar alguna clave primero hay que borrar la clave privada y después la pública. Para borrar claves privadas se hace con el comando `gpg --delete-secret-key ClaveID`. Para las claves públicas se hace con el comando `gpg --delete-key ClaveID`.

```
pub  rsa2048 2019-10-21 [SC] [caduca: 2021-10-20]
      0D6079C788646F93B75C36CB0BF8D9496FF062F6
uid   [ absoluta ] Marta Sanchez Gazquez <marta.sanchez@iescamp.es>
sub   rsa2048 2019-10-21 [E] [caduca: 2021-10-20]
```



## Copia y distribución de claves

Una vez generadas las claves, para que el resto de personas y entidades puedan comprobar nuestros mensajes firmados, tenemos que darles nuestra clave pública. Esto se puede hacer de varias maneras:

1. Subiéndola a un servidor de claves públicas. Los servidores de claves suelen estar interconectados, es decir, que subiendo la clave a un servidor, el resto ya tiene conocimiento de la existencia de nuestra nueva clave. El servidor `pgp` de `rediris` puede ser usado para este propósito. La orden a teclear para remitir nuestra clave es:

`gpg --send-keys --keyserver pgp.rediris.es ClaveID`

```
[marta@parsek ~]$ gpg --keyserver pgp.rediris.es --send-keys 0D6079C788646F93B75C36CB0BF8D9496FF062F6
gpg: enviando clave 0BF8D9496FF062F6 a hkp://pgp.rediris.es
```

Para hacer una búsqueda de claves públicas, de entidades o usuarios con los que queramos comunicarnos o verificar un mensaje recibido de éstos: `gpg --keyserver NombreDelServidor --search-keys ClaveID`

Para bajarnos dicha clave pública: `gpg --keyserver NombreDelServidor --recv-keys ClaveID`

2. Enviándola por correo o dándola en un soporte portable (USB, CD/DVD, etc.), mediante un fichero. Si tan solo queremos que no sea de dominio tan público sino que solo unos pocos tengan conocimiento de nuestra clave pública, para ello deberemos volcar esta clave a un fichero de texto. El comando para ello podría realizarse de 2 formas:

`gpg - -armor - - output ficheroedecave - - export ClaveID`

Es importante **tener una copia aparte de nuestra clave privada**, para que en caso de desastre informático o pérdida de datos podamos **recuperarla**. Para exportar la clave privada a un fichero y poder tener una copia de seguridad: `gpg --armor --output fichoedecave --export-secret-key ClaveID`

Después de emplear el método de distribución deseado, el comando a ejecutar en la máquina destinataria para importar una clave volcada en un fichero, es: `gpg - - import ficheroedecaves`

SKS key server - Chromium

SKS key server x +

← → ↻ No es seguro | pgp.rediris.es ☆ ⋮

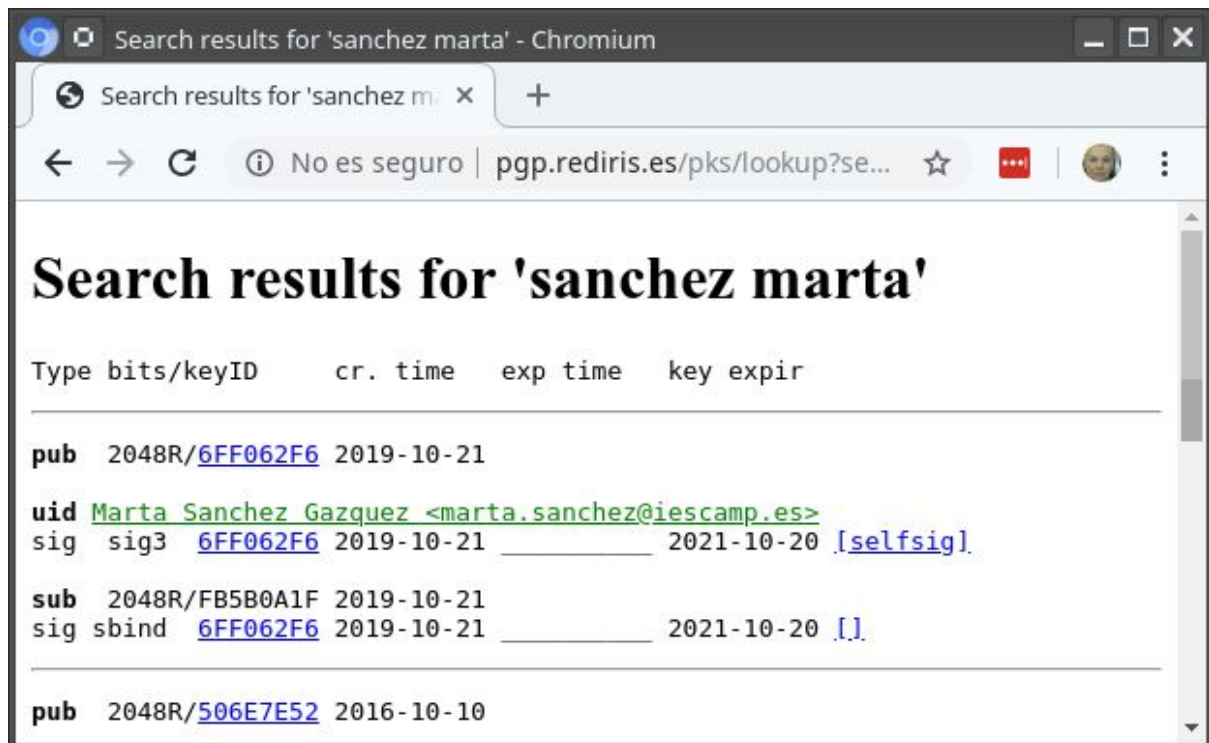
## RedIRIS SKS OpenPGP Key server

### Extract a key

You can find a key by typing in some words that appear in the userid (name, email, etc.) of the key you're looking for, or by typing in the keyid in hex format ("0x...")

Search for a public key

String	<input type="text" value="marta sanchez"/>
Show PGP Fingerprints	<input type="checkbox"/>
Show SKS full-key hashes	<input type="checkbox"/>
Get regular index of matching keys	<input type="radio"/>
Get verbose index of matching keys	<input checked="" type="radio"/>
Retrieve ascii-armored keys	<input type="radio"/>
Retrieve keys by full-key hash	<input type="radio"/>



## Eliminar claves distribuidas en servidores

Si se ha olvidado la contraseña o hemos perdido la clave privada, o consideramos que se encuentra en estado comprometida, podemos usar el **certificado de revocación** y subirlo a un servidor de claves. Esta clave ha de guardarse en un lugar seguro ya que si alguien la obtuviese podría revocar nuestras claves y dejarlas inutilizadas. La orden para generar este certificado es: `gpg -o revocacion.asc --gen-revoke ClaveID`

```
[marta@parsek ~]$ gpg -o revocacion.asc --gen-revoke 0D6079C788646F93B75C36CB0BF8D9496FF062F6
sec rsa2048/0BF8D9496FF062F6 2019-10-21 Marta Sanchez Gazquez <marta.sanchez@iescamp.es>
¿Crear un certificado de revocación para esta clave? (s/N) s
Por favor elija una razón para la revocación:
  0 = No se dio ninguna razón
  1 = La clave ha sido comprometida
  2 = La clave ha sido reemplazada
  3 = La clave ya no está en uso
  Q = Cancelar
(Probablemente quería seleccionar 1 aquí)
¿Su decisión? 0
Introduzca una descripción opcional; acábela con una línea vacía:
>
Razón para la revocación: No se dio ninguna razón
(No se dio descripción)
¿Es correcto? (s/N) s
se fuerza salida con armadura ASCII.
El fichero 'revocacion.asc' ya existe. ¿Sobreescribir? (s/N) s
Certificado de revocación creado.
```

Sí queremos revocar una clave hay que importar el fichero que tiene el certificado de revocación, una vez revocada la clave ya no podemos cifrar mensajes aunque sí se pueden descifrar.

Para importarla a nuestra relación de claves: `gpg --import revocacion.asc`

```
[marta@parsek ~]$ gpg --import revocacion.asc
gpg: clave 0BF8D9496FF062F6: "Marta Sanchez Gazquez <marta.sanchez@iescamp.es>" certificado de revocación importado
gpg: Cantidad total procesada: 1
gpg: nuevas revocaciones de claves: 1
gpg: marginals needed: 3 completes needed: 1 trust model: pgp
gpg: nivel: 0 validez: 3 firmada: 0 confianza: 0-, 0q, 0n, 0m, 0f, 3u
gpg: siguiente comprobación de base de datos de confianza el: 2021-10-20
```

El último paso es comunicar a los servidores de claves que nuestra clave ya no es válida, con la orden: `gpg --keyserver NombreDelServidor --send-keys ClaveID`. Tras realizar dicha operación podemos buscar y ver el estado del certificado en el servidor público de certificados.

```
[marta@parsek ~]$ gpg --keyserver pgp.rediris.es --send-keys 0D6079C788646F93B75C36CB0BF8D9496FF062F6
gpg: enviando clave 0BF8D9496FF062F6 a hkp://pgp.rediris.es
```



Como véis, el certificado está pero ha sido revocado.

**Haced una memoria con capturas de pantalla y las explicaciones pertinentes y subidla a Classroom**