

GPG

manejo llaves

generar contraseña (4096bits):

```
$ gpg --gen-key
```

entra en modo comando gpg, múltiples acciones disponibles:

```
$ gpg --edit-key <UID>
```

exporta clave pública, para repartir, formato binario:

```
$ gpg --export UID
```

exporta clave pública, para repartir, formato texto:

```
$ gpg --armor --export UID
```

exporta clave secreta

```
$ gpg --export-secret-keys UID
```

importar clave pública:

```
$ gpg --import <pubkey>
```

```
$ gpg --allow-secret-key-import --import <seckey>
```

borrar llave pública:

```
$ gpg --delete-key UID
```

borrar llave privada:

```
$ gpg --delete-secret-key UID
```

borrar llave pública y privada:

```
$ gpg --delete-secret-and-public-key UID
```

listado/exportación

- \$ gpg --list-keys
- \$ gpg --list-public-keys
- \$ gpg --list-secret-keys
- \$ gpg --fingerprint
- \$ ssh-keygen -yf ejemplo.rsa → generar clave pública a partir de la clave privada

firma/encryptado/desencryptado

- `$ gpg --sign-key UID`
- `$ gpg --trust-model always -r «Miguel Angel Torres» --encrypt ~/FICHERO.tar.gz`
- `$ gpg -u «Miguel Angel Torres» --output «fichero_salida» «fichero.pgg»`
- `$echo «password» | gpg -u «Miguel Angel Torres Egea» --output «fichero_salida» --passphrase-fd 0 «fichero.pgg»` → automatizar desencryptado

documentación

- <http://www.gnupg.org/gph/en/manual/book1.html>

From:

<https://miguelangel.torresegea.es/wiki/> - miguel angel torres egea

Permanent link:

<https://miguelangel.torresegea.es/wiki/criptografia:pgg:start?rev=1478893030>

Last update: **11/11/2016 11:37**

