GPG

manejo llaves

generar contraseña (se recomienda el máximo disponible, 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
```

<WRAP round tip 60%> esto parece no funcionar </WRAP> generar clave pública a partir de la clave privada:

```
$ ssh-keygen -yf ejemplo.rsa
```

firma/encriptado/desencriptado

firmar la PUB key de alguien:

```
$ gpg --sign-key UID
```

forzar encriptado desde CLI:

```
$ gpg --trust-model always -r "Miguel Angel Torres" --encrypt ~/$FICHERO.tar.gz
```

descifra fichero.gpg en ficher_salida usando la clave del usuario «Miguel Angel Torres»:

```
$ gpg -u "Miguel Angel Torres" --output "fichero_salida" "fichero.gpg"
```

automatizar desencriptado:

```
$ echo "password" | gpg -u "Miguel Angel Torres Egea" --output "fichero_salida" --passphrase-fd 0 "fichero.gpg"
```

```
$ cat /path/to/file | gpg -u "Miguel Angel Torres Egea" --output "fichero_salida" --passphrase-fd 0 "fichero.gpg"
```

documentación

- https://www.gnupg.org/gph/es/manual.html
- http://www.gnupg.org/gph/en/manual/book1.html

From:
https://matebcn.eu/ - **miguel angel torres egea**

Permanent link:
https://matebcn.eu/criptografia:gpg:start

Last update: **11/11/2016 20:55**