enchive

- pequeña utilidad de encriptación basada en clave pública/privada con encriptación basada en salsa20 (curva elíptica)
- a destacar:
  - ligero y rápido
  - multiplataforma
  - regeneración private key a partir de una frase
- más información:
  - https://nullprogram.com/blog/2017/03/12/
  - https://github.com/skeeto/enchive

compilar

- descargar el repositorio: `git clone https://github.com/skeeto/enchive.git`
- compilar con `make PREFIX=~/bin/enchive install`
  - después podemos enlazarlo con **/usr/local/bin** → `ln -s ~/bin/enchive/bin/enchive /usr/local/bin/enchive`
  - en MAC me ha pedido que instale `xcode-select install`

uso

- podemos proteger la clave privada (para desencriptar) con una contraseña
- las claves se guardan en **~/.config/enchive**
- genera un par de claves a partir de una frase, lo que nos permite regenerar las keys en caso de necesidad:

```
enchive keygen --derive
```

  - **secret key passphrase** es la frase que genera la clave privada
  - **protection passphrase** es la contraseña que protege la clave privada
- genera un **<file>.enchive**, fichero encriptado del original (sin pedir contraseñas):

```
enchive [--pubkey=<enchive_pub_key>] archive <file>
```

- solicita, si la tuviese, la contraseña de la clave privada para extraer la información:

```
enchive [--seckey=<enchive_sec_key>] extract <file>.enchive
```

  - `--agent[=seconds]` permite retener en memoria la contraseña por si hemos de hacer varias operaciones (durante 15 minutos por defecto, o especificar los segundos)
- muestra la huella de la clave (para verificar con otra persona):

```
enchive fingerprint
```

- otros parámetros:
  - `--pubkey <file>.pub` : especifica el fichero de clave pública a usar
  - `--seckey <file>.sec` : especifica el fichero de clave privada a usar

ejemplos

- cadena de texto, encriptada y envíada a través de transfer.sh:

```
echo "mi mama me mima mucho" | enchive archive | transfer <IDENTIFICADOR>
```

  - pruebas con base64 no han funcionado:

```
base64 --output mate2.b64.enchive --input -<<< $(echo "mi mama me mima mucho" | enchive archive)
base64 --decode --output mate2.enchive --input mate2.b64.enchive
#enchive: checksum mismatch!
```

- desencriptar:

```
curl https://transfer.sh/2bxTD6/mate.test | enchive extract > mate.txt # transfer.sh URL is a example
```

alternativas & colaboraciones

- https://keybase.io/
- https://transfer.sh
  - `transfer.sh/<FILE_DESCRIPTOR>/scan <FILE>`
  - `transfer.sh/<FILE_DESCRIPTOR>/virustotal <FILE>`

claves públicas

- mtorrese: mtorrese.pub
- mate: mate.pub