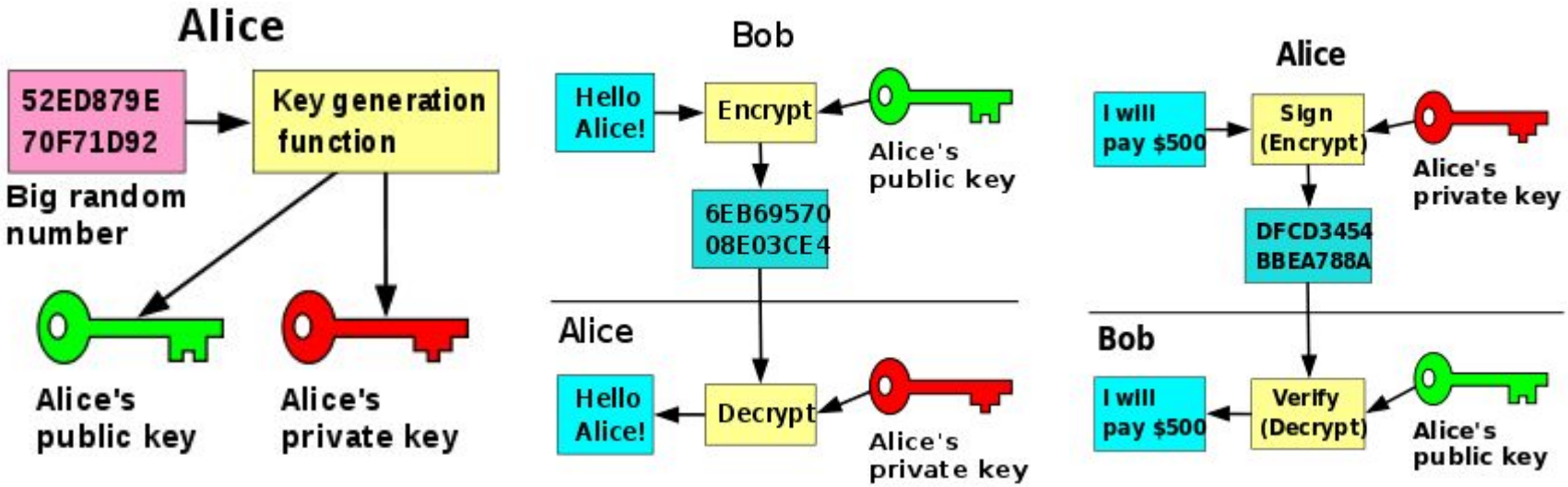
Taller de signatures GPG

Aniol Martí - David Pinilla

Criptografia de clau pública

- Dues claus:
  - Pública / Privada
  - Normalment s'utilitza l'algorisme RSA.



Generació Xifrat Signatura

Augmentar la seguretat

Editar el fitxer ~/.gnupg/gpg.conf i afegir al final:

```
# 32 bit IDs are too weak and have collisions

keyid-format long

# “Disable” SHA1

personal-digest-preferences SHA256

cert-digest-algo SHA256

default-preference-list SHA512 SHA384 SHA256 SHA224 AES256
AES192 AES CAST5 ZLIB BZIP2 ZIP Uncompressed
```

Creació del parell de claus

Atenció: es recomanen claus de mida 4096 bits i amb SHA-2 com a algorisme de hashing.

Creació del parell de claus:

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

o, si volem més detalls (molt recomanable):

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

Generació del certificat de revocació:

```
$ gpg --gen-revoke [KEY_ID] > ~/.gnupg/revok-[KEY_ID].crt
```

Publiquem la nostra clau pública:

```
$ gpg --send-key 1A2B3C4D5E6F7G8H
```

Signar i Xifrar

Per a signar text o fitxers

```
$ gpg -[a]s [ nom del fitxer ]
```

-a → Armor: Genera una sortida ASCII

-s → Signar: Signa el text introduït (s'acaba amb Ctrl-D)

o el fitxer passat com a paràmetre

Per a xifrar

```
$ gpg -[a]e -r ALTREID1 [ nom del fitxer ]
```

Introducció a les subclaus

- Et protegeix en certes ocasions.
- Fa el control de les claus més simple.
- Diferents subclaus per dispositiu.

Generar subclaus

Fer un backup del directori .gnupg:

```
$ umask 077 && tar -cvzf ~/gnupg-backup-pre.tgz ~/.gnupg
```

Editar la nostra clau:

```
$ gpg --edit-key NOSTREID
```

Afegir subclau:

```
gpg> addkey
```

```
gpg> save
```

Copiar subclaus

Fem una còpia de l'anell:

```
$ tar cvzf ~/gpg-backup-post.tgz ~/.gnupg
```

Copiem el fitxer .tgz a un llapis USB encriptat.

Eliminem els dos backups locals:

```
$ shred -u ~/gpg-backup-post.tgz ~/gpg-backup-pre.tgz
```

Eliminem la màster

Els propers passos es realitzen al portàtil

Copiem el .tgz del llapis al portàtil.

```
$ cp /media/usb-encriptat ~/gpg-backup-post.tgz
```

```
$ gpg --export-secret-subkeys NOSTREID >
/media/usb-encriptat/subkeys
```

```
$ gpg --delete-secret-key NOSTREID
```

```
$ gpg --import /media/usb-encriptat/subkeys
```

```
$ shred -u /media/usb-encriptat/subkeys
```

FESTA DE FIRMES

1- Baixar la clau.

2- Comprovar el fingerprint.

3- Signar la clau.

4- Exportar i enviar la clau.

5- Assignar la confiança.

Baixar la clau

```
$ gpg --keyserver subkeys.pgp.net --recv-keys ALTREID1
```

Comprovar el Fingerprint

```
$ gpg --fingerprint ALTREID1
```

Signar la clau

```
$ gpg --sign-key ALTREID1
```

exportar la clau signada

```
gpg --armor --export 00AA11BB22CC33DD | gpg --encrypt -r
00AA11BB22CC33DD --armor --output
00AA11BB22CC33DD-signedBy-1A2B3C4D5E6F7G8H.asc
```

Assignar la confiança

```
$ gpg --edit-key ALTREID1

gpg> trust

  1 = I don't know or won't say

  2 = I do NOT trust

  3 = I trust marginally

  4 = I trust fully

  5 = I trust ultimately

  m = back to the main menu
```

Importar i pujar la clau signada

Importar la clau signada (rebuda, per exemple, per correu electrònic):

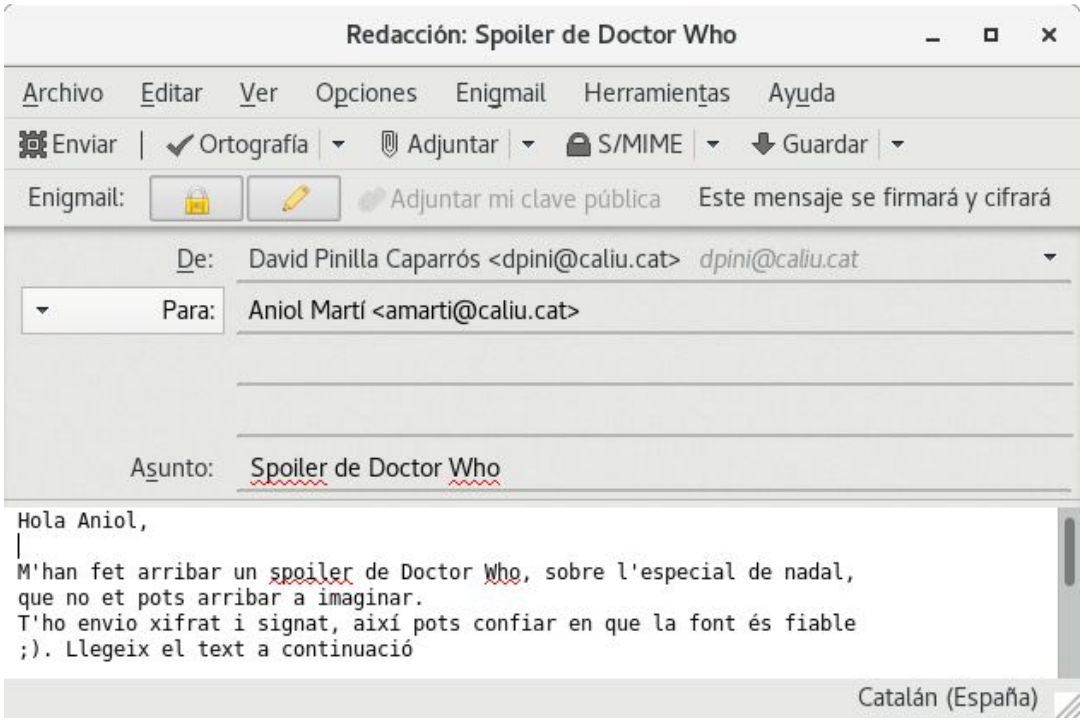
```
gpg --import 1A2B3C4D5E6F7G8H-signedBy-00AA11BB22CC33DD.asc
```

Pujar la clau pública actualitzada a un servidor de claus:

```
gpg --send-key 1A2B3C4D5E6F7G8H
```

Eines de gestió de GPG gràfiques

- Extensió per al client de correu Thunderbird: Enigmail
- Utilitat de gestió amb interfície GTK: Seahorse
- Utilitat de gestió amb interfície QT: KGPG



Més coses interessants!

Un gestor de passwords, basat en GPG:

https://www.passwordstore.org/

Un servei online (SaaS **PRIVATIU**) on publicar la teva identitat, juntament amb la teva clau pública. Permet enviar missatges xifrats, xat amb altres usuaris, i compartir fitxers xifrats. Client i kbfs **lliures**.

https://keybase.io i https://github.com/keybase

Referències

- https://wiki.debian.org/Keysigning
- https://wiki.ubuntu.com/CatalanTeam/FestaDeFirmes/2012-05-12
- https://www.void.gr/kargig/blog/2013/12/02/creating-a-new-gpg-key-with-subkeys/
- https://keyring.debian.org/creating-key.html
- http://llistes.cpl.upc.edu/listinfo/caliu-info