

# Pràctica 3: GnuPG\*

14 d'agost de 2006

## 1 Enunciat de la pràctica

La pràctica consisteix en enviar un missatge criptografiat (xifrat) i signat. Per poder realitzar-la, cal primer generar-se un parell de claus (privada i pública), configurar-se el gestor de correu. Per últim, cal enviar un correu al professor, però ha d'estar signat i xifrat. Per fer-ho us haureu de comprovar les vostres respectives claus públiques i identitats.

## 2 Generar la clau

Al servidor hi ha instal·lat el programa GnuPG. Des d'un terminal seguiu els següents passos:

```
leo@ranganathan:~$ gpg --gen-key
gpg (GnuPG) 1.4.3; Copyright (C) 2006 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.
```

Aleshores ens farà una sèrie de preguntes que haurem de respondre:

- Tipus de clau?. Trieu l'opció predeterminada: 1

Seleccioneu quin tipus de clau voleu:

- (1) DSA and Elgamal (default)
- (2) DSA (només signar)
- (5) RSA (només signar)

La vostra selecció?

- Mida de la clau? Accepteu el valor per defecte 2048.

---

\*Aquest document està basat ampliament en el document font original d'en René Mèrou

DSA keypair will have 1024 bits.  
ELG-E keys may be between 1024 and 4096 bits long.  
What keysize do you want? (2048)  
La grandària sol·licitada és 2048 bits

- Temps de validesa? Introduïu 1m, que vol dir un mes i ratifiqueu-lo.

Especifiqueu el temps de validesa de la clau.

0 = la clau no caduca  
<n> = la clau caduca als n dies  
<n>w = la clau caduca a les n setmanes  
<n>m = la clau caduca als n mesos  
<n>y = la clau caduca als n anys

Indiqueu la validesa de la clau (0) 1m  
Key expires at dl 19 jun 2006 12:26:54 CEST  
Is this correct? (y/N) y

- Nom i Cognoms? Posa les teves dades:

You need a user ID to identify your key; the software constructs the user ID from the Real Name, Comment and Email Address in this form:

"Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Nom i cognoms: Shiyali Ramamrita Ranganathan

- Adreça electrònica? Poseu la de ranganathan o qualsevol altre vostre.

Adreça electrònica: shiyalirr@ranganathan.ub.es

- Comentari? Poseu algun comentari que us identifiqui aquella adreça o el que creieu convenient.

Comentari: Adreça Documentació

- A partir d'allà només cal seguir la confirmació de tots els passos. Per sortir, premeu la tecla 'o'.

Esteu usant el joc de caràcters 'utf-8'.

Heu triat l'identificador d'usuari:

"Shiyali Ramamrita Ranganathan (Adreça Documentació) <shiyalirr@ranganathan.ub.es>"

Canvia (N)om, (C)omentari, (E)mail o (O) d'acord / (X) ixo

- Cal una contrasenya per a protegir la clau secreta. És important que pogueu recordar aquesta contrassenya, però no és recomanable escriure-la enlloc.

Introduïu la contrasenya:

Cal generar molts bits aleatòriament. És bona idea fer alguna altra cosa (teclejar, moure el ratolí, usar els discos) durant la generació de nombres primers; açò dona oportunitat al generador de nombres aleatoris d'aconseguir prou entropia.



Raó de la revocació: La clau ja no s'usa  
certificat per si perdem la clau o el password  
Is this okay? (y/N) y

You need a passphrase to unlock the secret key for  
user: "Shiyali Ramamrita Ranganathan (Adreça Documentació) <shiyalirr@ranganathan.ub.>  
1024-bit DSA key, ID 70EDBB59, created 2006-05-20

I ja veiem el resultat final.

S'ha creat un certificat de revocació.

Si us plau, mogueu-lo a un medi que pugueu amagar; si Mallory aconseguix accés a aquest certificat pot utilitzar-lo per a fer la vostra clau inservible. És intel·ligent imprimir aquest certificat i amagar-lo, per si el vostre medi es torna il·legible. Però aneu amb compte: el sistema d'impressió de la vostra màquina podria emmagatzemar les dades i fer-les disponibles a altres!

Si cal més endavant activar definitivament la revocació, només caldrà importar aquest (cert-revoc-arch.asc) i després enviar-lo al servidor.

```
$gpg --import cert-revoc-arch.asc  
$gpg --send-keys 70EDBB59
```

## 4 Enviar i rebre claus al servidor de claus

Si no tenim cap problema de configuració, només cal enviar la clau al servidor per defecte (en el nostre cas `hkp://subkeys.gpg.net`) fent servir la comanda:

```
gpg --send-keys 70EDBB59
```

on 70EDBB59 és el ID de la nostra clau. Per acabar, si volem mostrar l'empremta de la clau (fingerprint), només cal:

```
gpg --fingerprint 70EDBB59
```

## 5 I ara què?

Un cop tenim la nostra clau generada podem configurar el gestor de correu per signar i/o encriptar els nostres missatges. S'ha de tenir en compte que:

- Signar un correu és posar unes marques de forma que, qualsevol persona que tingui la part pública amb la que s'ha signat aquell missatge, pugui verificar-lo.
- Xifrar un missatge és un procés on l'emissor codifica el missatge mitjançant la clau pública del destinatari i només es pot desxifrar amb la clau privada del destinatari.

- Disposar de la clau pública d'una persona no vol dir res en especial. Per assegurar-nos que és aquella la persona que ha emès el missatge, hem de verificar amb un document d'identitat que aquella persona és qui diu qui és i que aquella és la seva clau pública.
- Un cop verificat l'autenticació de la persona, aleshores podem signar la clau d'aquella persona.

## 6 Fonts d'informació

Font original del document

<http://bulma.net/body.phtml?nIdNoticia=1684>