Gnu Privacy Guard (GnuPG) Mini Howto (Català)

Michael Fischard v. Mollard <*fischer@math.uni-goettingen.de*> (versió original en alemany)
Brenno J.S.A.A.F. de Winter <*brenno@dewinter.com*> (versió en anglès)
Horacio <*homega@ciberia.es*> (versió en castellà)
Josep Monés i Teixidor <*jmones@puntbarra.com*> (versió en català)
Versió 0.1.3, 17 de maig de 2002

Aquest document mostra com emprar GNU Privacy Guard (GnuPG), un sistema de xifratge de codi obert (programari lliure) compatible amb OpenPGP. Per poder mantenir aquest programa totalment lliure s'ha evitat l'ús de l'algoritme RSA i d'altres algoritmes patentats. El document original el va escriure Michael Fischer v. Mollard en alemany. Va ser posteriorment traduït a l'anglès, i revisat, per Brenno J.S.A.A.F. de Winter. Finalment, va ser traduït al castellà i novament revisat a partir de la versió anglesa. El document en català es basa principalment en la darrera revisió de la versió anglesa però també inclou la traducció d'un capítol només present en la versió en castellà.

Contents

1 Conceptes bàsics **2**

1.1 Xifratge de clau pública . . . 2
1.2 Signatures digitals . . . 3
1.3 Anells de confiança . . . 3
1.4 Límits de seguretat . . . 4

2 Instal·lació **4**

2.1 Codi font de GnuPG . . . 4
2.2 Configuració . . . 4
2.3 Compilació . . . 5
2.4 Instal·lació . . . 5

3 Ús i gestió de les claus **6**

3.1 Generant una clau . . . 6
3.2 Exportant claus . . . 7
3.3 Important les claus . . . 7
3.4 Revocant una clau . . . 7
3.5 Administració de les claus . . . 8
3.6 Signant les claus . . . 8

4 Xifrant i desxifrant **9**

4.1 Xifrar . . . 9
4.2 Desxifrar . . . 10

5 Signant i verificant signatures 10
5.1 Signar . . . 10
5.2 Verificar . . . 11
6 GnuPG + PGP 11
6.1 Ús d'algoritmes *no lliures* . . . 11
6.2 Signatura digital amb GnuPG . . . 12
6.3 Importar anells de claus de PGP a GnuPG . . . 12
6.4 Emprar anells de claus de PGP amb GnuPG . . . 14
7 Interfícies gràfiques 15
7.1 Interfícies gràfiques . . . 16
7.1.1 GPA . . . 16
7.1.2 Seahorse . . . 16
7.1.3 Geheimnis . . . 16
7.2 Programes de correu electrònic . . . 16
7.2.1 Evolution . . . 17
7.2.2 Mozilla i Enigmail . . . 17
7.2.3 Kmail . . . 17
8 Fonts d'informació 17
8.1 GnuPG . . . 17
8.2 PGP . . . 18
8.3 Servidors de claus . . . 18
8.4 Llibres . . . 18
9 A propòsit d'aquest document 18
9.1 Versions . . . 19

1 Conceptes bàsics

Comentari per les versions destinades a impressió: *Degut a dificultats tècniques, el guió doble, que s'empra en les opcions llargues de GnuPG, el text contingut en paràgrafs es representa visualment com a guions simples. Per tant, interpreteu-los com a guions simples en els casos d'opcions llargues.*

1.1 Xifratge de clau pública

Per poder entendre millor el sistema de xifratge emprat pels sistemes de claus asimètriques (de claus públiques i privades), és necessari entendre la diferència amb els sistemes de claus simètriques (claus secretes).

Els sistemes de xifratge de *clau simètrica* són aquells en els que la clau que s'empra per xifrar les dades és la mateixa que s'utilitza per desxifrar-los. En el cas del correu electrònic, el remitent xifra el missatge amb una *clau secreta*, perquè el destinatari el pugui desxifrar, necessita obtenir prèviament aquesta mateixa clau de manera «segura», o sigui, de manera que terceres persones no tinguin l'oportunitat d'obtenir aquesta clau. Si no es té certesa que l'intercanvi de claus ha estat segur, la validesa del sistema és nul·la.

Els sistemes de xifratge amb *claus asimètriques*, en canvi, empren dues claus diferents per al xifratge i el desxifratge de les dades. El el cas anterior del correu electrònic, el remitent empraria la *clau pública* del destinatari per xifrar el missatge, i el destinatari desxifraria el missatge amb la seva pròpia *clau privada*. Així doncs, la *clau privada* no ha de ser accessible per a **ningú** que no en sigui el propietari, mentre que la *clau pública*, pot ser entregada a qualsevol persona. En un sistema de xifratge ben implementat, la *clau privada* no es pot obtenir a partir de la *clau pública*.

El punt crucial de tot aquest sistema és que la *clau privada* ha de mantenir-se en secret i només el seu propietari hi ha de tenir accés. NO ENVIEU AQUESTA CLAU A TRAVÉS D'INTERNET. De la mateixa manera és molt perillós utilitzar GnuPG a través de `telnet` (considereu la possibilitat de no emprar mai telnet degut als riscos de seguretat importants que presenta).

1.2 Signatures digitals

El concepte de **signatura digital** es basa en la verificació de l'autoria d'un missatge. Això vol dir que el destinatari d'un missatge pot comprovar que el «suposat» remitent és qui diu que és. Per fer-ho, el remitent, una vegada ha escrit el missatge, el signa emprant la seva pròpia clau privada. El destinatari, una vegada ha rebut el missatge, comprovarà l'autenticitat d'aquest, és a dir, el verificarà emprant la clau pública del remitent.

Aquest mètode és d'especial utilitat per a reduir els riscos de seguretat en els nostres sistemes (ens podrien enviar un suposat pegat per a un programa, i ser en realitat un virus o un troià); també podrien enviar-nos informació o dades, com provinents d'una font lícita o fiable. En ambdós casos, no seria gaire difícil falsificar la direcció i el nom del remitent, però sí impossible falsificar-ne la signatura digital.

Com ja hem comentat, la verificació d'un missatge signat digitalment es duu a terme mitjançant l'ús de la *clau pública* del remitent **sobre el text** del propi missatge. D'aquesta manera no només podem verificat la identitat de l'autor, sinó que també podem comprovar la integritat del missatge, ja que la signatura digital ha estat generada amb el **text** i la **clau privada**. Així doncs, una alteració o modificació del text «a posteriori», o qualsevol manipulació del missatge (especialment si fem ús de les especificacions MIME/PGP), donaria com a resultat un error en la verificació.

1.3 Anells de confiança

Un punt feble dels algoritmes de clau asimètrica és la transmissió de les claus públiques. Un intrús podria posar en circulació una clau pública amb un identificador d'usuari fals. Si es xifren missatges amb aquesta clau, l'intrús podria desxifrar i llegir els missatges. Si llavors l'intrús el xifrés amb la clau pública autèntica de l'usuari i li passés, aquest atac no seria perceptible.

La solució de `PGP` (i per tant la solució de `GnuPG`) és la signatura de les claus. La clau pública d'un usuari pot estar **signada** per altres usuaris. L'objectiu d'aquestes signatures és que l'usuari que signa reconeix que l'UID (identificador d'usuari) de la clau signada pertany a l'usuari a qui diu que pertany. A partir d'aquí és responsabilitat de l'usuari de `GnuPG` decidir fins a quin punt es refia de la signatura. Una clau es pot consiferar fiable que es confia en el remitent i se sap amb seguretat que la clau signant pertany a aquella persona. Només quan es pot confiar plenament en la clau del signant, es pot confiar en la clau a la que signa (i en les signatures generades amb aquesta clau). Per tenir la seguretat que la clau és correcta, s'ha de comparar amb la seva **empremta digital** mitjançant un mitjà de canal fiable. Per exemple, podríem buscar el seu telèfon a la guia i trucar-lo, demanant-li que ens digues l'empremta digital a viva veu per tal de poder-li donar confiança absoluta.

1.4 Límits de seguretat

Si el que es vol és mantenir la confidencialitat de les dades que es posseixen, no n'hi ha prou amb determinar quin algoritme de xifratge cal emprar; és necessari també pensar amb la seguretat general del sistema. En principi, `PGP` està considerat com suficientment segur, i fins aquest moment, no se sap de cap cas en el que una clau PGP hagi estat trencada. Això no vol dir que tot el que s'ha xifrat sigui segur. Per exemple, si la NSA (l'Agència de Seguretat Nacional dels EUA) hagués aconseguit trencar una clau PGP d'alguna manera, probablement no ho farien públic. Però, encara que les claus de PGP fossin absolutament impossibles de trencar, hi ha d'altres tipus d'atacs que poden ser utilitzats per trencar-ne la seguretat. A principis de febrer de 1999, es va descobrir un troià que cercava claus privades de PGP en el disc dur i els transferia mitjançant FTP. Si s'hagués escollit una contrasenya feble, un atacant podria haver obtingut fàcilment les claus privades.

Una altra possibilitat tècnica (encara que més difícil) és la d'un troià que recollís tot el que s'escriu pel teclat i ho transmetés a l'atacant. També és possible, encara que difícil, passar el contingut d'una pantalla a una altra. En aquest cas, no caldria fer cap anàlisi de les dades xifrades, ja que es tindria accés a les dades abans de xifrar.

Per tot això, és necessari una planificació de la seguretat que estigui ben prevista i que en minimitzi els perills.

La idea no és crear una atmosfera de paranoia entre la gent, sinó deixar clar que per tenir un sistema segur no n'hi ha prou amb instal·lar un programa criptogràfic, ja que, si bé és un pas cap a un sistema més segur, no és la solució completa. Troians com els que aparegueren el març del 1999 amb el virus Melissa van demostrar que moltes empreses no estan preparades pel que fa a la seguretat.

2 Instal·lació

2.1 Codi font de GnuPG.

El web oficial per la descàrrega de `GnuPG` és *la pàgina oficial de GnuPG* . Allà també hi trobareu els enllaços a rèpliques oficials.

Degut a restriccions legals no es permet descarregat material criptogràfic des de servidors localitzats als EUA a les persones que no hi resideixen. Als EUA existeixen lleis que restringeixen l'exportació de codi criptogràfic així com dels programes que l'inclouen. Per aquesta raó PGP sempre es troba disponible en dues versions: una internacional i l'altra per als EUA.

El codi font de la versió internacional es va exportar en format de text ascii imprimit en un llibre. A continuació es va escanejar a Europa (Oslo). Se'n pot obtenir més informació a la *pàgina international de PGP* . La versió internacional de PGP pot ser importada lliurement als EUA sempre i que no es torni a reexporta-la.

Si ja teniu instal·lada una versió de `GnuPG` o `PGP`, hauríeu de comprovar la signatura del fitxer (vegeu 5 (Signatures)).

2.2 Configuració

Es pot obtenir GnuPG com a un paquet binari de *Debian*

(.deb), com a un paquet binari de *RedHat* (.rpm), o en codi font.

GnuPG s'inclou en la darreres distribucions de RedHat Linux. Si aquestes distribucions, per comprovar si teniu GnuPG instal·lat en el vostre sistema, empreu:

```
rpm -q gnupg
```

Els paquests esmentats són fitxers comprimits que es poden instal·lar amb les eines corresponents, segons la distribució. Si necessiteu instal·lar GnuPG en altres sistemes operatius, necessitareu compilar-lo a partir del codi font. S'agraïrà que qui compili un paquet d'instal·lació per altres sistemes o arquitectures, el faci de domini públic.

Com que la gran part del desenvolupament de GnuPG es fa en màquines x86 sota *Linux* , l'adaptació del programa a d'altres sistemes diferents no hauria de suposar cap problema. La llista de sistemes operatius suportats per GnuPG es pot trobar a les pàgines de *GnuPG* . El procediment que es descriu a continuació no és exclusiu de cap plataforma. Aquest procediment es pot utilitzar per instal·lar GnuPG a partir d'un fitxer comprimit de codi font (.tar.gz).

Descomprimiu i desarxiveu el paquet amb el codi font amb l'ordre (suposant que teniu `Gnu tar` instal·lat):

```
$ tar xvzf gnupg-?.?.?.tar.gz
```

Després de desempaquetar-lo, canvieu al directori on heu descomprimit el codi font. Llavors executeu:

```
$ ./configure
```

Amb aquest pas no hauria de succeir res d'especial. Si executeu

```
$ ./configure --help
```

podeu veure les opcions de configuració disponibles per a la compilació. Si apareixen problemes referents a la internacionalització (GET text), podeu incloure una versió que està inclosa amb el codi font emprant la opció `-with-included-gettext`, o bé desactivar la internacionalització amb l'opció `-disable-NLT`.

2.3 Compilació

A continuació, compileu el codi font amb l'ordre:

```
$ make
```

La compilació hauria de transcórrer sense cap problema. Si passés quelcom anormal seguiu els passos següents (en el mateix ordre en què es descriuen aquí): Primer proveu de solucionar-ho vosaltres mateixos (fent ús de la documentació existent). Llavors assegureu-vos que el vostre problema no és un error conegut (comproveu el fitxer BUGS a *http://www.gnupg.org* . Si cap d'aquests passos no solucionen el vostre problema, envieu la vostra pregunta a la llista de correu de GnuPG (en anglès) (vegeu 8 (Fonts d'informació)). Si el vostre problema està relacionat amb la ruta d'accés, podeu provar `make clean`, executar `./configure` un altre cop i intentar una vegada més compilar (amb `make`).

2.4 Instal·lació

Llavors escriviu:

```
$ make install
```

que copiarà el programa i les pàgines del manual al directori d'instal·lació. Si no heu canviat el directori d'instal·lació en executar `./configure`, llavors el directori d'instal·lació serà `/usr/local/share/gnupg`. Podeu trobar aquest directori en el fitxer `options.skel`. Si canvieu `options.skel`, si es copia a `~/.gnupg/options` els ajustaments apropiats s'usaran de forma predeterminada. L'acció de copiar haria de realitzar-se automàticament en crear ~/.gnupg/. Totes les opcions possibles estan ben documentades i provar d'explicar-les aquí no seria de gaire utilitat.

Podeu executar GnuPG com a suid root. D'aquesta manera, el programa s'executa amb tots els drets que té el superusuari, i s'exclou la possibilitat que certes parts del sistema es desin externament i altres persones les puguin llegir. No m'és possible de valorar els riscos d'executar el programa com a superusuari. Però executant el programa com a suid root s'hauria d'estar alerta dels perills de cavalls de Troia, ja que un troià executant-se com a superusuari podria malmetre tit el sistema. Si per aquesta raó (o per qualsevol altra) escolliu de no executar GnuPG com a superusuari, podeu desactivar l'avís activant `no-secmem-warning` a `~/.gnupg/options`.

3 Ús i gestió de les claus

3.1 Generant una clau

Amb l'ordre

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

podeu general un nou parell de claus (el parell es composa de clau pública i clau privada). La primera pregunta és quin algoritme s'emprarà. Podeu llegir més a propòsit dels algoritmes a

PGP DH vs. RSA FAQ `http://www.hertreg.ac.uk/ss/pgpfaq.html`

o a 8.4 (Applied Cryptography). L'algoritme recomanat per GnuPG és DSA/ElGamal, ja que no està patentat.

La següent pregunta és la longitud de la clau. Aquesta decisió depèn molt de cada usuari. Heu d'escollir entre la seguretat i el temps de càlcul. Si una clau és més llarga, el risc de trencar el missatge si és interceptat decreix. Però amb claus més llarges el temps de càlcul també augmenta. Si el temps de càlcul és un problema, heu de tenir en compte que voleu emprar la clau durant algun temps. Tothom sap que el rendiment aritmètic augmenta molt ràpidament, ja que els nous processadors són cada vegada més ràpids. Tingueu això en compte. La llargada mínima requerida per GnuPG és de 768 bits, encara que molta gent opina que hauria de ser de 2048 (que és el màxim de GnuPG en aquest moment). Per a DSA, 1024 és una llargada fixa. Si la seguretat té prioritat envers el temps de càlcul, hauríeu d'escollir la mida de clau més llarga disponible.

El sistema demana a continuació que introduïu el nom, un comentari i l'adreça de correu electrònic. La clau es clacula en base a aquestes dades. Podeu canviar aquesta informació més tard (vegeu 3.5 (Administració de claus). La direcció de correu electrònic que escolliu hauria de ser vàlida, ja que serà emprada per signar l'identificador d'usuari. Si aquesta direcció es modifica d'alguna manera, la signatura no es correspondria.

Finalment heu d'introduir una contrasenya. Noteu la diferència entre els termes anglesos per la paraula «contrasenya»: el terme "password" denota una "paraula de pas", mentre que el terme "passphase" denota una "frase de pas". Per tant, aquesta contrasenya s'ha de composar de més d'una paraula. Per a que una contrasenya sigui efectiva (segura), haurà de contenir els elements següents:

- ha de ser llarga;
- ha de combinar majúscules, minúscules i nombres;
- ha de contenir caràcters especials (no alfanumèrics);
- ha de ser difícil d'endevinar (no ha de ser, doncs, noms, dates de naixement, números de telèfon, de targeta de crèdit o de compte corrent, noms i nombre de fills, ...).

En general, per tal d'aconseguir una contrasenya forta és aconsellable intercal·lar maJúsCUlEs amb mInÚS-cuLEs, nombres, i d'altres caràcters no alfanumèrics. En escollir les paraules i les frases s'han d'evitar les paraules massa òbvies, dates significatives, i no heu d'emprar mai cites de llibres o frases cèlebres. Dit això, heu d'assegurar-vos que la contrasenya que escolliu sigui suficientment difícil perquè no pugui ser vulnerada amb un «atac de força bruta», ni tan sols per un «atac de diccionari», però suficientment fàcil perquè NO LA OBLIDEU. Si oblidéssiu la vostra contrasenya, la clau quedaria totalment inutilitzada, i tota la informació que s'hagi xifrat amb aquesta clau no podria ser desxifrada. Per tal d'evitar aquesta possibilitat es recomana crear certificats de revocació junt amb les claus (vegeu 3.4 (Revocació)).

Una vegada que s'han introduït totes les dades necessàries, el sistema comença a generar les claus. Aquest procés triga un temps que depèn de la llargada de les claus. Durant aquest procés, el programa recull dades aleatòries que emprarà per generar les claus; una manera d'ajudar a fer més aleatori aquest procés és cambiar a una consola virtual diferent i emprar el teclat mentre el procés està en marxa. La clau que genereu sempre serà diferent. Si genereu una clau ara i una altra d'aquí 5 minuts amb exactament la mateixa informació, obtindreu dues claus diferents. Aquesta és la raó per la qual no heu d'oblidar mai la vostra contrasenya.

3.2 Exportant claus

L'ordre per exportar una clau d'un usuari és la següent:

```
$ gpg --export [UID]
```

Si no es designa cap identificador d'usuari (UID) s'exportaran totes les claus presents. El resultat s'envia per defecta a `stdout`, però amb l'opció `-o` podem especificar que s'envïi a un fitxer. Es recomana emprar l'opció `-a` per tal de que el resultat sigui un fitxer de ASCII de 7 bits en comptes d'un fitxer binari.

Si exporteu les vostra clau pública, la podeu facilitar a les persones amb les que voleu comunicar-vos de forma segura. La clau es pot exportar publicant-la a la vostra plana *web*, emprant *finger*, *ftp*, enviant-la a un servidor de claus públiques com per exemple http://www.pca.dfn.de/dfnpca/pgpkserv/, o qualsevol altre mètode.

3.3 Important les claus

En rebre la clau pública d'algú (o vàries claus públiques), les heu d'afegir a la vostra base de dades de claus per tal de poder-les utilitzar. Per importar-les a la base de dades, heu d'executar l'ordre següent:

```
$ gpg --import [nom del fitxer]
```

Si s'omet el nom del fitxer, les dades es llegiran de `stdin`. El fitxer pot contenir una sola clau o més d'una, que pertanyin a una o més persones.

3.4 Revocant una clau

Hi ha diverses raons per les quals podeu voler revocar una clau existent. Per exemple, que la clau privada hagi estat robada, hagi canviat el UID (identificador d'usuari), que ja no sigui prou llarga, etc. En tots aquests casos, el comandament per revocar la clau és:

```
$ gpg --gen-revoke
```

Això crea un **certificat de revocació**. Per poder-ho fer, necessiteu la clau privada, sinó qualsevol podria crear un certificat i revocar una clau que no fos seva. Això té un desavantatge, si hem oblidat la contrasenya, la clau no serveix de res, i tampoc es pot generar un certificat de revocació. Per aquesta raó, és aconsellable generar un certificat de revocació en crear el parell de claus. Si ho feu, però, guardeu-lo en un lloc segur perquè ningú no pugui emprar-lo i revocar la clau.

3.5 Administració de les claus

En el sistema GnuPG hi ha un fitxer que actua com una mena de base de dades. En aquest fitxer es desen totes les dades relacionades amb les claus, inclosos els valors que fan referència al grau de confiança (*Ownertrust*); per a més informació sobre el grau de confiança llegiu 3.6 (Signant les claus)).

Amb l'ordre

```
$ gpg --list-keys
```

es mostraran totes les claus presents. Per veure també totes les signatures escriviu:

```
$ gpg --list-sigs
```

(vegeu 3.6 (Signant les claus) per a més informació).

Per veure les empremtes digitals (*fingerprints*) escriviu:

```
$ gpg --fingerprint
```

Les "empremtes digitals" serveixen per confirmar la identitat d'una persona. Aquesta ordre ens mostra una llista alfanumèrica (relacionada amb la clau) que podem compravar, per exemple, per telèfon.

Per veure el llistat de claus privades escriviu:

```
$ gpg --list-secret-keys
```

Nota: el llistat d'empremtes digitals i de signatures de les claus privades no té cap utilitat directa més de la de donar-nos aquesta informació.

Per tal d'esborrar una clau pública executeu l'ordre:

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

Per eliminar una clau privada escriviu:

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

Hi ha encara un altre comandament important que té relació amb la gestió de les claus:

```
$ gpg --edit-key UID
```

Emprant aquesta ordre podeu editar (entre d'altres coses) la data d'expiració, afegir una empremta digital i signar la vostra clau. Per realitzar aquestes operacions necessiteu la contrasenya. En executar aquesta ordre veureu una linia de comandaments.

3.6 Signant les claus

Com s'ha comentat anteriorment, hi ha un taló d'Aquil·les al sistema: l'autentificació de les claus públiques. Si teniu una clau pública errònia, ja us podeu oblidar dels valor del xifratge. Per tal d'evitar aquests riscos existeix la possibilitat de signar les claus. Quan tenim la certesa que una clau és vàlida i que pertany a qui diu que pertany, podem signar-la digitalment, de manera que la nostra signatura donarà fe (als que confien en la nostra signatura) que aquella clau pública correspon a aquell ID d'usuari.

Si executeu l'ordre:

```
$ gpg --edit-key UID
```

per la clau que voleu signar, podreu signar-la amb la subordre:

```
Command> sign
```

Només heu de signar una clau quan estigueu ABSOLUTAMENT SEGURS que la clau és autèntica!!! En realitat, només es pot estar segur quan la clau ha estat rebuda en mà, o, per exemple, si s'ha rebut per correu i a continuació s'ha comprovar l'empremta digital de la clau per algun altre mitjà (per exemple, per telèfon). No heu de signar mai cap clau basant-vos en una suposició.

Basant-se en les signatures disponibles en una clau i en el «grau de confiança», `GnuPG` determina la validesa de les claus. El grau de confiança (*Ownertrust*) és un valor que el propietari d'una clau empra per determinar el nivell de confiança per una clau concreta. Aquests valors són:

- 1 = Don't know (No ho sé)
- 2 = I do NOT trust (No hi confio)
- 3 = I trust marginally (Hi confio poc)
- 4 = I trust fully (Hi confio plenament)

Si l'usuari no es refia d'una signatura, ho pot indicar i refusar la confiança en la mateixa. La informació sobre la confiança no es desa en el mateix fitxer que el de les claus, sinó que en un altre diferent.

4 Xifrant i desxifrant

Després d'haver-ho instal·lat i configurat tot tal com voleu, podeu començar a xifrar i desxifrar.

És possible que quan vulguem xifrar o desxifrar quelcom, tingueu més d'una clau privada en el nostre anell de claus. Si això passa, és necessari seleccionar-ne una com activa. Per fer-ho, es pot emprar l'opció

```
-u UID
```

o bé l'opció

```
--local-user UID
```

També podeu afegir la línia següent al fitxer de configuració `$HOME/.gnupg/options`:

```
default-key UID
```

Si desitgeu indicar l'UID d'un destinatari per xifrar un fitxer amb la seva clau, ho podeu fer amb l'opció

```
-r
```

o bé l'opció

```
--recipient
```

4.1 Xifrar

L'ordre per xifrar és la següent:

```
$ gpg -e [fitxer]
```

o bé:

```
$ gpg --encrypt [fitxer]
```

El programa demanarà el UID del destinatari (o dels destinataris, és possible posar-ne més d'un). Es pot evitar que el programa ho pregunti emprant l'ordre:

```
$gpg -er [UID del destinatari] [fitxer]
```

`GnuPG` generarà un fitxer xifrat amb el nom `[fitxer].gpg`. També podem emprar l'opció:

```
--armor
```

o bé

```
-a
```

perquè el fitxer generat sigui del tipus ASCII de 7 bits. L'ordre seria doncs:

```
$ gpg -a -er [UID del destinatari] [fitxer]
```

Aquesta ordre generarà un fitxer codificat de nom `[fitxer].asc` amb el format ASCII de 7 bits.

Heu de tenir en compte que el fet de xifrar un fitxer (o un missatge) l'únic que fa és protegir les dades amb un xifratge que només pot desfer el destinatari; no protegeix del risc que algú intenti suplantar la nostra identitat. Per tal d'evitar-ho, només cal signar digitalment tot allò que es xifri (vegeu 5 (Signatures)).

4.2 Desxifrar

L'ordre per desxifrar és:

```
$ gpg [-d] [fitxer]
```

o bé:

```
$ gpg [--decrypt] [fitxer]
```

En aquest cas no és necessària l'opció, és opcional, ja que `gpg` utilitza per defecte:

```
--decrypt
```

En els casos anteriors, el resultat es mostra a `stdout` (habitualment la sortida de l'intèrpret d'ordres), però el podeu redireccionar amb l'opció:

```
-o [fitxer]
```

, on [fitxer] és el nom del fitxer on vulgueu el resultat.

5 Signant i verificant signatures

Signar i verificar signatures és una part molt important dels sistemes de criptografia de clau pública. L'usuari pot signar una sèrie de dades o un document, per la qual cosa utilitza la seva clau privada. Per verificar les signatures d'altres usuaris, és necessari obtenir prèviament les seves claus públiques.

5.1 Signar

Per signar un fitxer amb la vostra clau, utilitzeu l'ordre:

```
$ gpg -s [fitxer]
```

o bé

```
$ gpg --sign [fitxer]
```

Aquesta ordre, a més de produir una signatura digital, també comprimeix el fitxer, per la qual cosa el resultat és un fitxer binari il·legible. Per produir un fitxer signat legible (en format ASCII), s'empra l'ordre:

```
$ gpg --clearsign [fitxer]
```

D'aquesta manera, tant la signatura com les dades signades, són legibles en un editor.

La signatura també es pot generar en un fitxer separat (de les dades). Aquesta opció és molt recomanable especialment quan es signen fitxers binaris (per exemple, fitxers comprimits). Per realitzar-ho s'ha d'utilitzar l'ordre:

```
$ gpg -b [fitxer]
```

o bé

```
$ gpg --detach-sign [fitxer]
```

Aquest és el mode que MIME/PGP empra per signar els missatges de correu electrònic. Aquest mode és molt útil quan s'ha de signar un binari, per exemple, per distribuir-lo, ja que la signatura es basa en el binari però va en un fitxer apart. L'opció `-armor` també pot ésser d'utilitat en aquests casos.

Sovint haureu de signar i xifrar un fitxer alhora. L'ordre que permet fer això és:

```
$ gpg [-u Remitent] [-r Destinatari] [--armor] --sign --encrypt
[fixer]
```

La funcionalitat de les opcions `-u` (`-local-user`) i `-r` (`-recipient`) és la que s'ha descrit anteriorment.

5.2 Verificar

En desxifrar un fitxer xifrat que també hagi estat signat digitalment, la signatura es verifica automàticament. En tot cas, és possible verificar la signatura simplament amb l'ordre:

```
$ gpg [--verify] [fitxer]
```

Aquesta ordre només funcionarà (és clar) quan tingueu la clau pública del remitent.

6 GnuPG + PGP

En ser `PGP` un programa més antic que `GnuPG`, és normal que un usuari nou de `GnuPG` tingui ja instal·lada alguna versió de `PGP` al seu sistema, i que desitgi mantenir les seves claus velles després d'actualitzar-se a `GnuPG`. Doncs bé, no només és possible importar el contingut dels anells de claus, sinó que, alternativament, és possible que `GnuPG` gestioni els anells de claus de `PGP 2.6.3` i `PGP 5.0`.

Hi ha altres «problemes» de compatibilitat que també tractarem en aquest capítol, com són les signatures de tipus **V4** generades per `GnuPG`, o de l'ús per part de `PGP` dels algoritmes propietaris `RSA` o `IDEA`. Començarem per aquesta darrera qüestió.

6.1 Ús d'algoritmes *no lliures*

L'ús d'algoritmes amb patents restrictives per part de `PGP` representa un problema donat que la filosofia al voltant de `GnuPG` és la d'implementar un sistema criptogràfic lliure. Així doncs, les patents sobre aquests algoritmes n'impossibiliten una implementació total. Però `GnuPG` també pretén cumplir amb les normes dels «estàndards» d' *OpenPGP* .

Existeixen unes extensions per a *RSA* i *IDEA* que poden ser instal·lades i permeten un cert ús d'aquests algoritmes. Les claus generades per `PGP 2.6.x` són del tipus `RSA`, i l'algoritme de xifratge emprat és `IDEA` (també pot ser emprat per `PGP 5.x`). És possible conseguir el codi font d'aquests algoritmes als fitxers *rsa.c* i *idea.c* .

També existeixen els binaris instal·lables d'aquestes extensions per algunes distribucions de *Linux*

, com per exemple *Debian* (comproveu-ho per a d'altres distribucions).

6.2 Signatura digital amb GnuPG

`GnuPG` és l'únic sistema capaç d'implementar signatures digitals **V4** (segons *OpenPGP*) i aquesta n'és l'opció per defecte, però en aquest cas `PGP` no és capaç de verificar-les. És possible obligar a `GnuPG` a emprar **V3**, de dues maneres:

- Indicant-ho en el fitxer de configuració `$HOME/.gnupg/options` afegint la línia:

```
force-v3-sigs
```

- Indicant aquesta opció cada vegada que es desitgi signar un missatge en **V3**:

```
$ gpg <opció> --force-v3-sigs [fitxer]
```

6.3 Importar anells de claus de PGP a GnuPG

Intentarem explicar com exportar les claus públiques i privades des dels nostres anells de claus `PGP` als anells de claus `GnuPG`.

NOTA: aquest mètode s'ha extret del *PGP2GnuPG*

Howto de Caskey L. Dickson i no l'he provat personalment. L'última actualització del «PGP2GnuPG Howto» data del desembre de 1998. Per aquesta raó, i per poder integrar `PGP` amb `GnuPG`, recomano l'ús del mètode que s'explica a la 6.4 (secció següent), ja que és més senzill i fiable.

Suposant que tingueu instal·lades dues versions de `PGP` per a `Unix/Linux`, tenim els seus respectius anells de claus públiques i privades a `$HOME/.pgp/`:

- pubring.pgp -> fitxer de claus públiques de `PGP 2.6.x`
- secring.pgp -> fitxer de claus privades de `PGP 2.6.x`
- pubring.pkr -> fitxer de claus públiques de `PGP 5.x`
- secring.skr -> fitxer de claus privades de `PGP 5.x`

A continuació utilitzaríem les ordres que corresponguin a cada verió per tal d'extreure les claus que desitgem.

Així, per extreure una clau de `PGP 2.6.x`:

```
$ pgp -kx UID fitxer anell
```

per exemple:

```
$ pgp -kx Pepe clavepepe2 ~/.pgp/pubring.pgp
```

Aquesta operació ens donaria el fitxer clavepepe2.pgp. Per extreure'n la nostra clau privada, no hauríem de fer cap altra cosa que indicar el nostre UID i el fitxer de les claus privades `~/.pgp/secring.pgp`. No em consta que hi hagi cap manera d'indicar més d'un UID amb `PGP 2.6.3`, si en sabeu alguna, si us plau envieu-me un *mensaje* (NT: adreça de correu de l'autor d'aquesta secció i de la traducció a la versió castellana del document).

Una vegada s'ha extret la clau només s'ha d'importar al fitxer de `GnuPG`:

```
$ gpg --import clavepepe2
```

Per extreure una clau de `PGP 5.0`:

```
$ pgpk -x UID -o fitxer
```

per exemple:

```
$ pgpk -x Pepe -o clavepepe5
```

En aquest cas, el fitxer per defecte és el de claus públiques, i obtindríem el fitxer clavepepe5 tal i com hem indicat.

Una vegada més, només ens queda importar la clau:

```
$ gpg --import clavepepe5
```

Ja que `PGP 5.0` no ens permet indicar el fitxer sobre el que volem operar, la extracció de la clau privada es complica una miqueta. La solució ve donada per un sistema superior com el de GnuPG:

Aquest procediment posa en risc la clau privada durant un breu període de temps, així que no hauria de ser emprat en un sistema multiusuari o públic. Els passos a seguir són:

- Extreure la clau pública corresponent a la clau provada que volem exportar, i importar-la a `GnuPG`.
- Esborrar la contrasenya de la clau privada!! (es recomana fer una còpia de seguretat del fitxer secring.skr):

```
$ pgpk -e UID
```

per exemple:

```
$ pgpk -e 0x614DB9FA

sec  1024 0x614DB9FA 1998-03-22 ---------- DSS        Sign & Encrypt

sub  1024 0x2B9E0571 1998-03-22 ---------- Diffie-Hellman

uid  Horacio <homega@vlc.servicom.es>

uid  Horacio <homega@correo.com>


1024 bits, Key ID 0x614DB9FA, created 1998-03-22

"Horacio <homega@vlc.servicom.es>"

"Horacio <homega@correo.com>"
```

```
Do you want to unset this key as axiomatic [y/N]? N

Do you want to unset this key as axiomatic [y/N]? N

Do you want to add a new user ID [y/N]? N

Do you want to change your pass phrase (y/N)? Y
Need old passphrase. Enter pass phrase: <introduïu la contrasenya>
Need new passphrase. Enter pass phrase: <deixeu-ho buit>
Enter it a second time. Enter pass phrase: <deixeu-ho buit>
Changing master key passphrase...

Changing subkey passphrase...

Do want to set this as your default key [y/N]? N

Keyrings updated.
```

- El pas següent és exportar la clau privada. Com ja hem pogut veure, `PGP 5.0` és incapaç de fer-ho, així que emprarem `GnuPG`:

```
$ gpg --export-secret-keys --secret-key-ring ~/.pgp/secring.skr 0x614DB9FA > lamevaclau
```

Tot això en una sola línia, i es crearà el fitxer `lamevaclau`.

- Ara ja podem importar la clau privada a GnuPG:

```
$ gpg --import < lamevaclau
```

Swguidament torneu a introduir una contrasenya a la clau des de `GnuPG`.

6.4 Emprar anells de claus de PGP amb GnuPG

És possible evitar tota aquesta operació anterior, mantenint instal·lades les diferents versions de `PGP` al mateix temps que la de `GnuPG`. Essent `GnuPG` un sistema superior i més nou, pot reconéixer els anells de claus de `PGP` com a propis.

En el cas de `PGP 5.0`, n'hi ha prou amb afegir la ruta d'accés completa als fitxers de claus de `PGP 5.0`, precedit per `keyring` o `secret-keyring`, al final del fitxer `~/.gnupg/options` segons correspongui:

```
keyring ~/.pgp/pubring.pkr
secret-keyring ~/.pgp/secring.skr
```

Els fitxers de claus de `PGP 2.6.3` són reconeguts per `GnuPG` per defecto. Si això no fos així, només caldria repetir la mateixa operació anterior adaptant-la a les circumstàncies:

```
keyring ~/.pgp/pubring.pgp
secret-keyring ~/.pgp/secring.pgp
```

Si a continuació feu un llistat de les claus públiques amb `GnuPG`, observareu que llegeix els tres fitxers, `~/.gnupg/pubring.gpg`, `~/.pgp/pubring.pkr`, y `~/pubring.pgp`:

```
$ gpg --list-keys

    /home/usuario/.gnupg/pubring.gpg
```

```
    --------------------------------
    pub 1024D/57548DCD 1998-07-07 Werner Koch (gnupg sig)
    <dd9jn@gnu.org>
    pub 1024D/A95AF46C 1998-11-29 Brenno J.S.A.A.F. de Winter
    <brenno@dewinter.com>
    sub 3072g/A3CA62A0 1998-11-29

  (... y demás claves públicas DSA/ElGamal...)

    /home/usuario/.pgp/pubring.pkr
    ------------------------------
    pub 1024D/FAEBD5FC 1997-04-07 Philip R. Zimmermann <prz@pgp.com>
    sub 2048g/42F0A0A0 1997-04-07

  (... etc DSS/Diffie-Helman...)

    /home/usuario/.pgp/pubring.pgp
    ------------------------------
    pub 1024R/88A17FF5 1995-09-11 IRIS-CERT, Spain

  (... etc RSA...)
```

El mateix succeïria amb les claus privades:

```
$ gpg --list-secret-keys

    /home/horacio/.gnupg/secring.gpg
    --------------------------------
    sec 1024D/42337AE6 1999-03-14 Horacio (comentari)
    <homega@vlc.servicom.es>
    ssb 2048g/1F177864 1999-03-14

    /home/horacio/.pgp/secring.skr
    ------------------------------
    sec 1024D/7992AB40 1998-05-04 Horacio <homega@vlc.servicom.es>
    uid Horacio <homega@correo.com>
    ssb 2048g/917366AE 1998-05-04

    /home/horacio/.pgp/secring.pgp
    ------------------------------
    sec 1024R/32D4A925 1997-09-23 Horacio <homega@vlc.servicom.es>
```

7 Interfícies gràfiques

Per fer més fàcil l'ús de GnuPG, teniu una àmplia varietat de programes que empren o són compatibles amb el xifratge de GnuPG. Hi ha interfícies gràfiques que permeten administrar les claus amb el ratolí i també hi ha molts MUA (Mail User Agents) que permeten xifrar i signar missatges de correu electrònic de forma molt senzilla. Hi ha una llista quasi bé completa de front ends a la pàgina *GnuPG Frontends* . En destacarem alguns d'ells a continuació.

7.1 Interfícies gràfiques

7.1.1 GPA

GPA , *GNU Privacy Assistant* és una interfície d'usuari gràfica per Gnu Privacy Guard (GnuPG). Aquest és el front end gràfic estàndard que ofereix el projecte GnuPG. Amb GPA, podeu veure el vostre anell de claus, importar i exportar claus, generar claus, editar-ne les propietats i xifrar, signar o desxifrar documents.

Instal·lar GPA és senzill. Descarregueu-ne el codi font comprimit, descomprimiu-lo i llavors executeu l'ordre:

```
$ ./configure; make
# make install
```

Executeu el programa escrivint:

```
$ gpa
```

7.1.2 Seahorse

Seahorse

és una interfície gràfica de GnuPG per a GNOME. Es pot emprar per signar, xifrar, verificar i desxifrar text i fitxers. El text es pot obtenir del porta-retalls, o el podeu escriure directament en el petit editor que porta. Seahorse és també un gestor de claus que es pot utilitzar per editar quasi bé totes les propietats de les claus que emmagatzemeu en el vostre anell de claus.

Podeu instal·lar Seahorse mitjançant un paquet per a la vostra distribució, o bé descarregant-vos un fitxer comprimit amb el codi font. Instal·lar l'aplicació des del codi font es fa com amb qualsevol altre paquet. Descarregeu-lo, descomprimiu-lo, executeu `configure` i feu `make install`. La instal·lació es fa sota el directori `/usr/local` i inserta un element de menú al menú d'aplicacions de GNOME.

7.1.3 Geheimnis

Geheimnis

és un front-end per GNUPG que està basat en KDE. Se suposa que té totes les funcions de GPA i Seahorse. Lamentablement, quan vaig provar de compilar el programa em vaig quedar encallat perquè em mancava una lliberia (/usr/lib/libfam.la).

7.2 Programes de correu electrònic

Els programes de correu electrònic (o MUAs) més populars permeten l'ús de GnuPG. Entre aquests, hi ha almenys els següents:

- Evolution
- Balsa
- Mozilla
- Pine
- Kmail
- Eudora
- Mutt

- exmh

Amb tota certesa n'hi ha molts més, però és quasi bé impossible provar-los tots.

Emprant GnuPG des del vostre programa de correu us permet desxifrar missatges de correu electrònic que us enviïn xifrats amb la vostra clau pública, signar els vostres missatges per tal que el destinatari pugui estar segur que en sou l'autor i xifrar el vostre correu electrònic amb les claus públiques dels destinataris.

7.2.1 Evolution

Evolution, el programa més corrent per GNOME, conté integrada la possibilitat d'emprar el xifratge de GnuPG i de PGP. Per poder-lo configurar per tal de poder signar i desxifrar missatges, heu d'introduir el vostre ID d'usuari a la pestanya 'Seguretat' de les propietats del compte de correu.

Quan envieu un nou missatge no l'estareu signant o xifrant per defecte. Per fer-ho, heu de seleccionar 'Signa amb PGP' i 'Xifra amb PGP' del menú 'Seguretat'.

En rebre un missatge signat o xifrat, es desxifrarà automàticament i apareixerà un candau al final del text. Si premeu el candau, es verificarà la signatura i us mostrarà si és correcta o no.

7.2.2 Mozilla i Enigmail

Mozilla no inclou la possibilitat d'emprar GnuPG per ell mateix. Per emprar el xifrat GnuPG amb Mozilla, heu d'instal·lar un connector, com *EnigMail* . Enigmail és un connector per Mozilla/Netscape Mail que permet als usuaris accedir a les característiques d'autentificació i xifrat que facilita el programari GPG i PGP. Enigmail és capaç de xifrar i signar correu electrònic en enviar-lo, i també de desxifrar i verificar el correu rebut. També és capaç d'importar i exportar claus privades.

Instal·lar EnigMail en un sistema RedHat Linux és especialment senzill, ja que hi ha RPM disponibles per les darreres versions de Mozilla. S'han d'instal·lar dos paquets: `mozilla-enigmail-0.39-3.i386.rpm` i `mozilla-ipc-0.99-0_rh7x.rpm`. Després d'instal·lar aquests RPM, reinicieu Mozilla (o Netscape 6.x) i hauríeu de ser capaços d'emprar GnuPG en el vostre correu electrònic. Tingueu en compte, però, que EnigMail només xifra el text del vostre missatge. No xifra els afegits; haureu de xifrar qualsevol fitxer que vulgueu afegir separadament. En altres sistemes, probablement haureu d'instal·lar EnigMail a partir del codi font.

7.2.3 Kmail

Kmail, el programa de correu electrònic més corrent per KDE conté integrada la possibilitat d'emprar el xifratge de GnuPG i PGP. Per poder-lo configurar per tal de poder signar i desxifrar missatges, heu d'introduir el vostre ID d'usuari a la secció 'Identitat' de la configuració de Kmail. Quan envieu un nou missatge no l'estareu signant o xifrant per defecte. Per fer-ho, heu de seleccionar els butons 'Signa el missatge' i 'Xifra el missatge' de la barra d'eines.

8 Fonts d'informació

8.1 GnuPG

- La *pàgina web de GnuPG* `http://www.gnupg.org`
- La llista de correu electrònic de GnuPG, incloent la possibilitat de consultar els missatges antics i les descripcions a *la pàgina web de GnuPG* .

- La informació del project GnuPG (actualitzada fins la versió 0.9.2), tot i que encara no està prou acabada. I no s'ha d'oblidar:

  ```
  gpg --help
  ```

  . Aquesta és una font de molt de valor.

8.2 PGP

PGP és el programa de criptografia més antic que (encara) està àmpliament extès. Durant aquest temps s'han publicat nombrosos documents. Aquesta informació és molt útil. Molta d'aquesta informació és tan general que la podeu aplicar a GnuPG també. Mireu-vos les adreces següents per obtenir aquests documents:

- La *pàgina web internacional de PGP* `http://www.pgpi.com`
- La pàgina de *preguntes més freqüents de PGP DH vs. RSA* `http://www.hertreg.ac.uk/ss/pgpfaq.html`

  conté informació de les diferències entre aquests dos algoritmes. Aquests són els dos algoritmes que utilitza GnuPG.

8.3 Servidors de claus

- *Keyserver.net* `http://www.keyserver.net`
- `http://wwwkeys.eu.pgp.net`

8.4 Llibres

- B. Schneier, "Applied Cryptography, Second Edition", Wiley, 1996 Deutsche Ausgabe unter dem Titel "Angewandte Kryptographie", Addison-Wesley, 1996

9 A propòsit d'aquest document

```
Free Software Foundation, Inc.
59 Temple Place - Suite 330
Boston, MA 02111-1307
USA
```

9.1 Versions

Versió original en alemany: la **versió 0.1** va ser la primer versió en alemany.

Tots els canvis per la versió original, en alemany, estan documentats en un fitxer diff: *dieses Dokument*

- **Anglès versió 0.1.0**, del 30 d'abril del 1999. Aquesta versió és una traducció de la versió alemanya a l'anglès, amb alguns canvis.
- **Alemany versió 0.1.1**
  - Nova secció «Límits de seguretat»
  - Explicació de les signatures millorada
  - Alguns canvis suggerits per Werner Koch (gràcies!)
- **Castellà versió 0.1.2**, del 29 de maig del 1999.
  - Aquesta versió en castellà és la traducció de la versió anglesa, i s'han fet alguns canvis.
  - S'ha afegit el capítol sobre comptabilitat i interoperabilitat de `GnuPG` amb `PGP`.
- **Castellà versió 0.1.3**, del 28 de setembre de 1999.
  - S'ha reescrit a codi SGML (LinuxDoc) des del codi HTML.
  - Correcció d'alguns errors en castellà.
- **Anglès versió 0.1.2**, del 3 d'abril del 2002.
  - S'han corregit algunes faltes.
  - Nova secció sobre interfícies d'usuari.
- **Holandès versió 0.1.3**, del 17 de maig del 2002.
  - Traducció de la versió anglesa a l'holandès.
- **Català versió 0.1.3**, del 10 de desembre del 2002.
  - Traducció de la versió anglesa al català (amb molta influència de les modificacions realitzades en la versió castellana).

Notes per a la versió catalana: Podeu enviar qualsevol suggeriment o comentari sobre aquest document a Josep Monés i Teixidor ( ). Qualsevol comentari o correció és benvingut.

Notes per a la versió castellana: Cualquier comentario o corrección al documento que ayude a mejorarlo es bienvenido. Por favor, enviad cualquier sugerencia a <*homega@ciberia.es*> .

Notes per a la versió anglesa i neerlandesa: All remarks for this document can be sent to Brenno J.S.A.A.F. de Winter (*brenno@dewinter.com*). or Arjen Baart (*arjen@andromeda.nl*). Comments help us make a better document and are greatly appreciated.

Notes per a la versió alemanya: Anregungen, Kritik, Verbesserungen und Erweiterungen einfach an Michael Fischer v. Mollard <*fischer@math.uni-goettingen.de*> senden, damit dieses Dokument weiter verbessert werden kann.