利用GPG 加密工具來加密檔案 (For 非對稱式加密)

目錄表

GPG 是實現公鑰及私鑰加密的方式,即爲非對稱式加密。通常加密 方式:公鑰加密檔案,私鑰解密;假若相反地是數位簽章 :私鑰簽屬,公鑰檢驗來達到數位簽章的不可否認性。

GPG 加密步驟

1. 首先A電腦會產生公私鑰

```
$gpg --list-keys -->看看A電腦是否已有金鑰對
```

```
$gpg --gen-key -->開始產生金鑰對
請選擇你要使用的金鑰種類:
   (1) RSA 和 RSA (預設)
   (2) DSA 和 Elgamal
   (3) DSA (僅能用於簽署)
```

```
   (4) RSA (僅能用於簽署)
你要選哪一個? enter
RSA 金鑰的長度可能介於 1024 位元和 4096 位元之間.
你想要用多大的金鑰尺寸? (2048) enter

你所要求的金鑰尺寸是 2048 位元
請指定這把金鑰的有效期限是多久.
         0 = 金鑰不會過期
      <n>  = 金鑰在 n 天後會到期
      <n>w = 金鑰在 n 週後會到期
      <n>m = 金鑰在 n 月後會到期
      <n>y = 金鑰在 n 年後會到期
金鑰的有效期限是多久? (0) 1 enter

金鑰將會在 西元2012年03月14日 (週三) 10時20分23秒 到期
以上正確嗎? (y/N)y enter

GnuPG 需要建構使用者 ID 以識別你的金鑰.

眞實姓名:Acomputerkey  enter      -->重要,指定一個user id
電子郵件地址: andy@utshop.tw  enter
註釋: test  enter

你選擇了這個使用者 ID:
    "Acomputerkey (test) <andy@utshop.tw>"
變更姓名(N), 註釋(C), 電子郵件地址(E)或確定(O)/退出(Q)? O enter
再來,就會有提示視窗要你輸入兩次密碼  (加密你的私鑰)

我們需要產生大量的隨機位元組. 這個時候你可以多做一些事情
(像是敲打鍵盤, 移動滑鼠, 讀寫硬碟之類的)
```

```
這會讓隨機數字產生器有更多的機會獲得夠多的亂數
(就到自己的電腦 亂打字來產生更多亂數)

gpg: 金鑰 A994E5B6 已標記成徹底信任了
公鑰和私鑰已建立及簽署.

gpg: 正在檢查信任資料庫
gpg: 3 個勉強信任以及 1 個完全信任是 PGP 信任模型的最小需求
gpg: 深度: 0  有效:   2  已簽署:   0  信任: 0-, 0q, 0n, 0m, 0f, 2u
gpg: 下次信任資料庫檢查將於 2012-03-14 進行
pub   2048R/A994E5B6 2012-03-13 [到期: 2012-03-14]
      金鑰指紋 = BC27 35B7 A1FD 62B4 67BB  D6C5 72B0 A3A0 A994 E5B6 (金鑰指紋後
uid                  Acomputerkey (test) <andy@utshop.tw>
sub   2048R/8E439DBA 2012-03-13 [到期: 2012-03-14]
```

2. A匯出自己的A公鑰,再傳給B電腦

```
$gpg  --list-keys
/home/andy/.gnupg/pubring.gpg
------------------------------
pub   2048R/A994E5B6 2012-03-13 [到期: 2012-03-14]
uid                  Acomputerkey (test) <andy@utshop.tw>
sub   2048R/8E439DBA 2012-03-13 [到期: 2012-03-14]
```

```
$gpg --armor (以ASSAIC碼輸出) --output file --export keyid
```

```
$gpg --armor --output Akey --export A994E5B6
```

```
scp Akey B位址:.
```

3. B再把A傳來的A公鑰匯入自己的電腦中

```
$gpg --import Akey
```

4. B就可用A公鑰加密B檔案,加密後的B檔案再回傳A電腦

```
$gpg --encrypt (加密) --armor -r keyid  想加密的檔案
```

```
echo "My name is B file" >Bfile
```

```
$gpg --encrypt --armor -r A994E5B6 Bfile
```

```
$ls -l Bfile.asc (即是已加密的檔案)
```

```
再把Bfile.asc傳給A
```

5. A電腦就用A私鑰解開加密B檔案

```
$gpg --decrypt Bfile.asc > Bfile
```

```
會彈出要你輸入密碼
```

```
$cat Bfile
My name is B file
```

文件簽名與驗證

承上一個項目的環境,A電腦先產生金鑰對,A電腦匯出公鑰傳給B電腦。

```
A$gpg --sign install.log.syslog
Enter passphrase:

install.log.syslog.gpg #再將install.log.syslog.gpg傳給B電腦
```

```
B$gpg --verify install.log.syslog.gpg

gpg: Signature made Fri 20 Jul 2012 03:34:37 PM CST using DSA key ID FE4B6BCF
gpg: Good signature from "andyTest <ali88.cha@hotmail.com>"
```

參考資料

- GnuPG Gentoo 使用者指南
- (GnuPG) 袖珍 HOWTO (中文版)
- 網路安全與實務理論-PGP/GnuPG-楊中皇