Pretty Good Privacy (PGP)

About PGP

- 1991年由Phil Zimmermann 所發表
- 近代密碼學相關產品中，最被廣泛採用的套裝軟體
- 採用被全世界密碼學專家公認最安全而且最可信賴的幾種基本密碼演算法
- 程式碼公開
- 免費軟體

下載及安裝

- 連結至http://www.pgpi.org/
- 依照作業系統抓取最新版本
- 解壓縮後執行安裝檔PGPDesktop32-983.exe
- License not require
- Key-pair 生成（內定2048bits RSA）
- 設定Passphrase

Key Generation Wizard

Your private key will be protected by a passphrase. It is important that you do not write this passphrase down.

Your passphrase should be at least 8 characters long and should contain non-alphabetic characters.

Passphrase: Hide Typing

Passphrase Quality :

Confirmation:

< 上一步(B) | 下一步(N) > | 取消 | 說明

Homework

- Install PGP
- Generate your key-pair
- Publish your public key to the PGP key-server
- Find my public key from the key-server
  - Using the name tsoraylin or
  - Using the mail address tsoraylin@gmail.com
- Encrypt (by my key) and sign (by your key) a message including
  - Your name
  - Student ID number
  - Mail address related to your public key
- Due date: 6/11