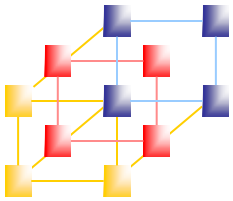
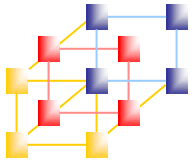


PGP Lab

先看看金鑰對的產生

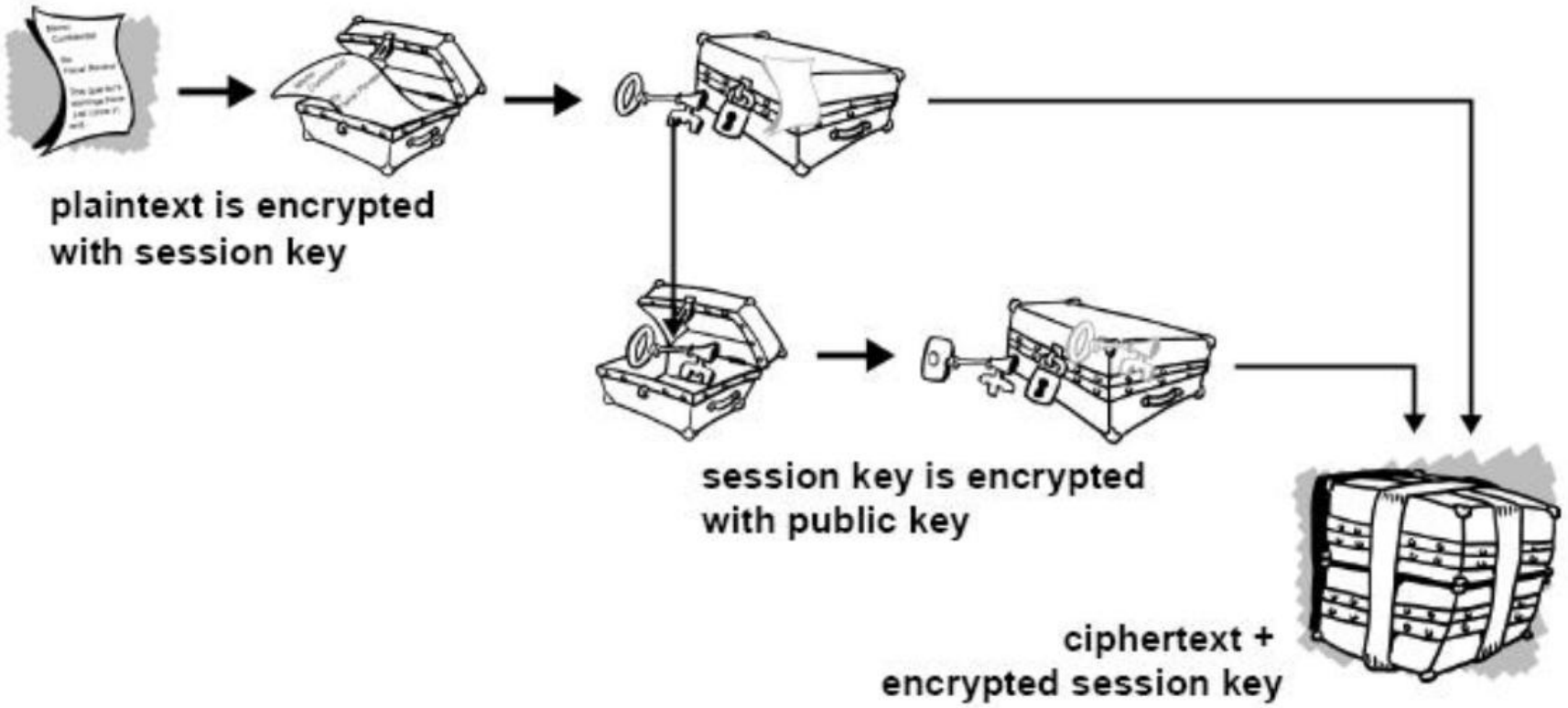
- Puttygen.exe



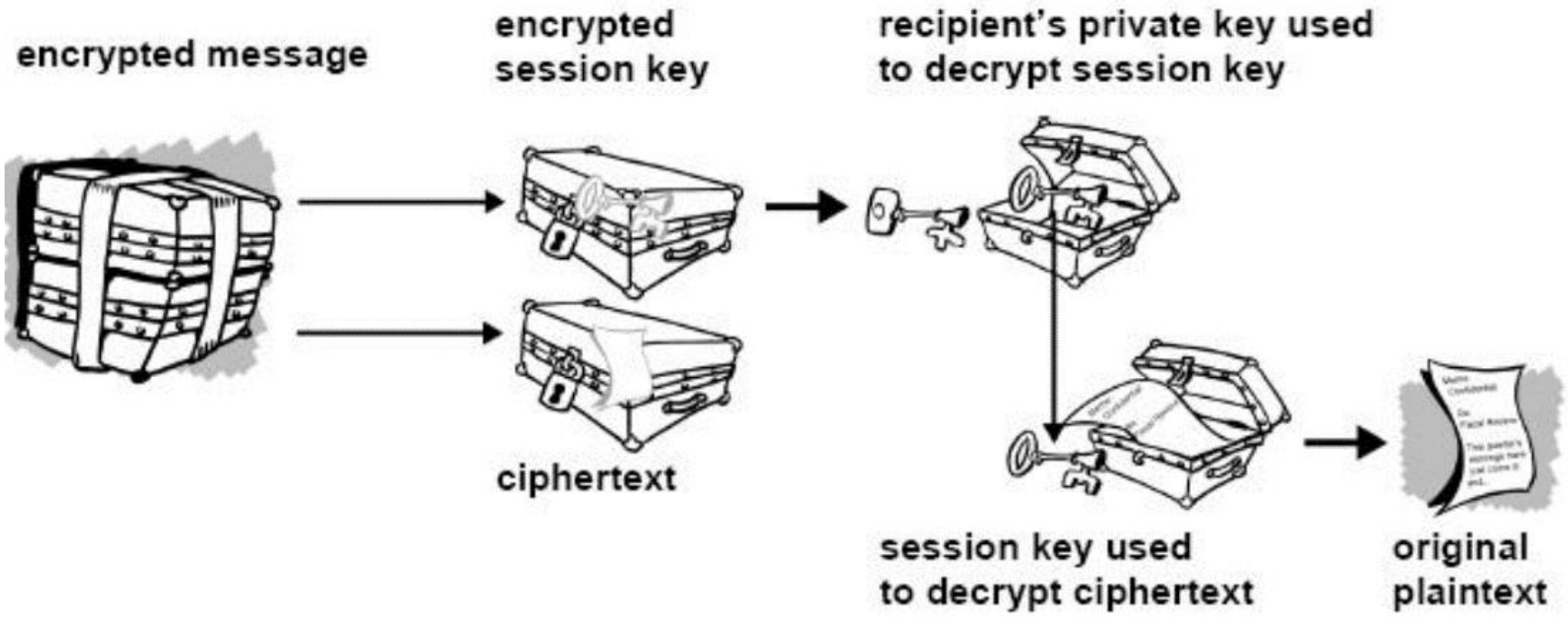
GPG Full Demo

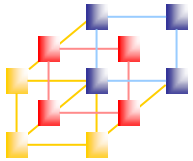
- https://gnupg.org/index.html
  - 加密
  - 解密
  - 簽章
  - 驗簽章
  - 加密+簽章
  - 解密+驗簽章

PGP Encrypt


plaintext is encrypted
with session key
session key is encrypted
with public key
ciphertext +
encrypted session key

PGP Decrypt


encrypted message
encrypted session key
recipient's private key used to decrypt session key
ciphertext
session key used to decrypt ciphertext
original plaintext

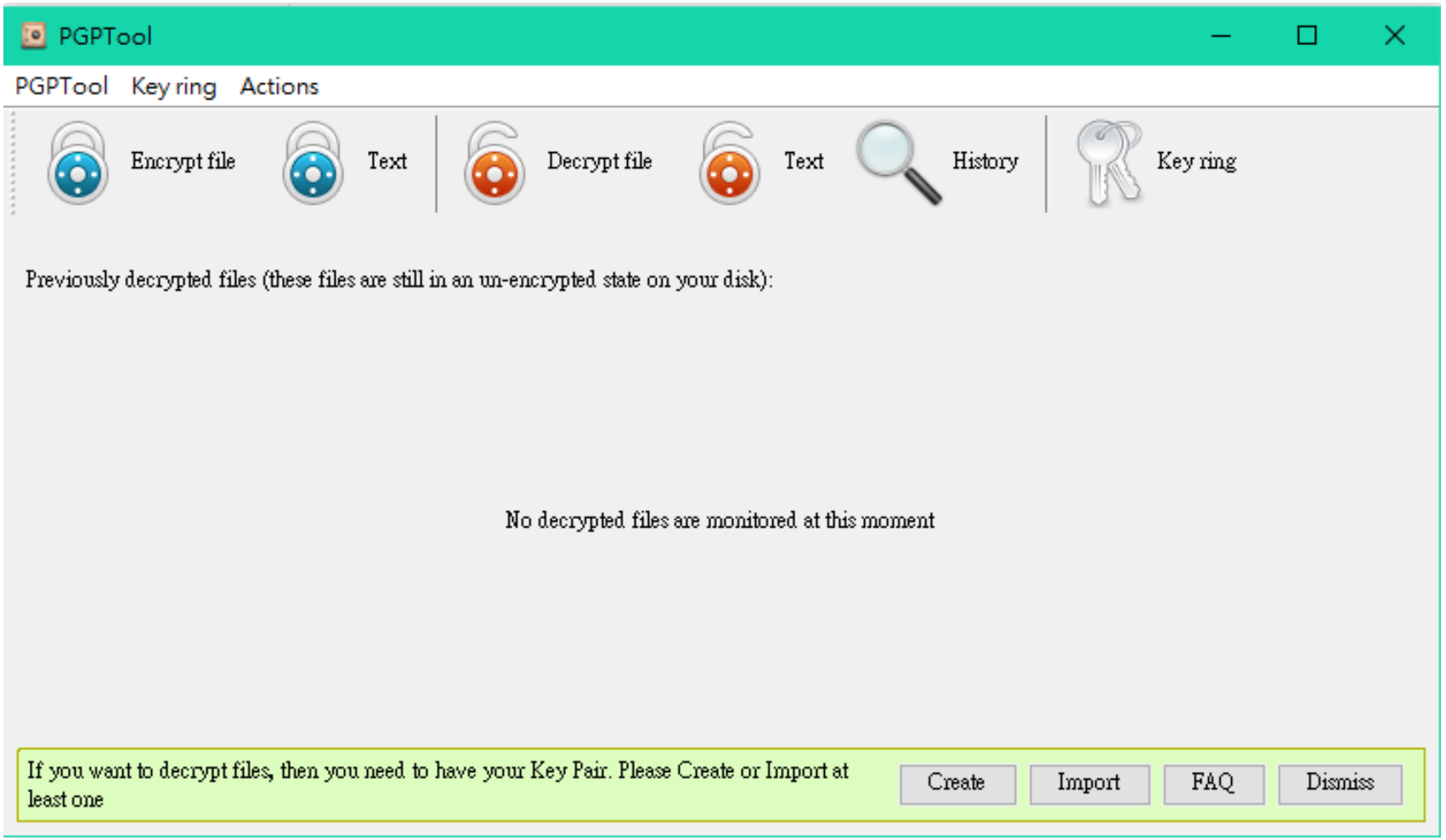


PGP Tool Download

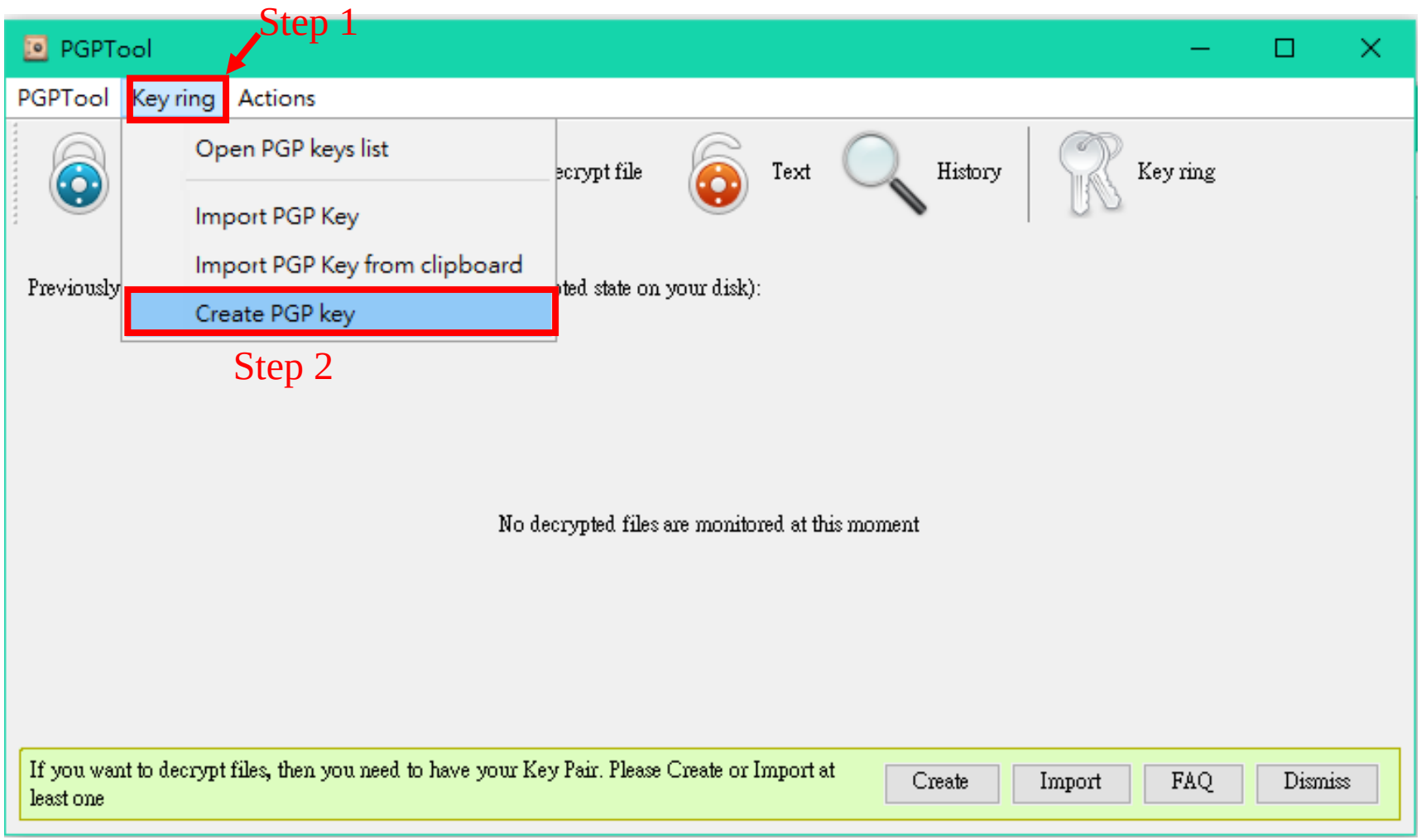
https://pgptool.github.io/

https://www.java.com/zh-TW/download/

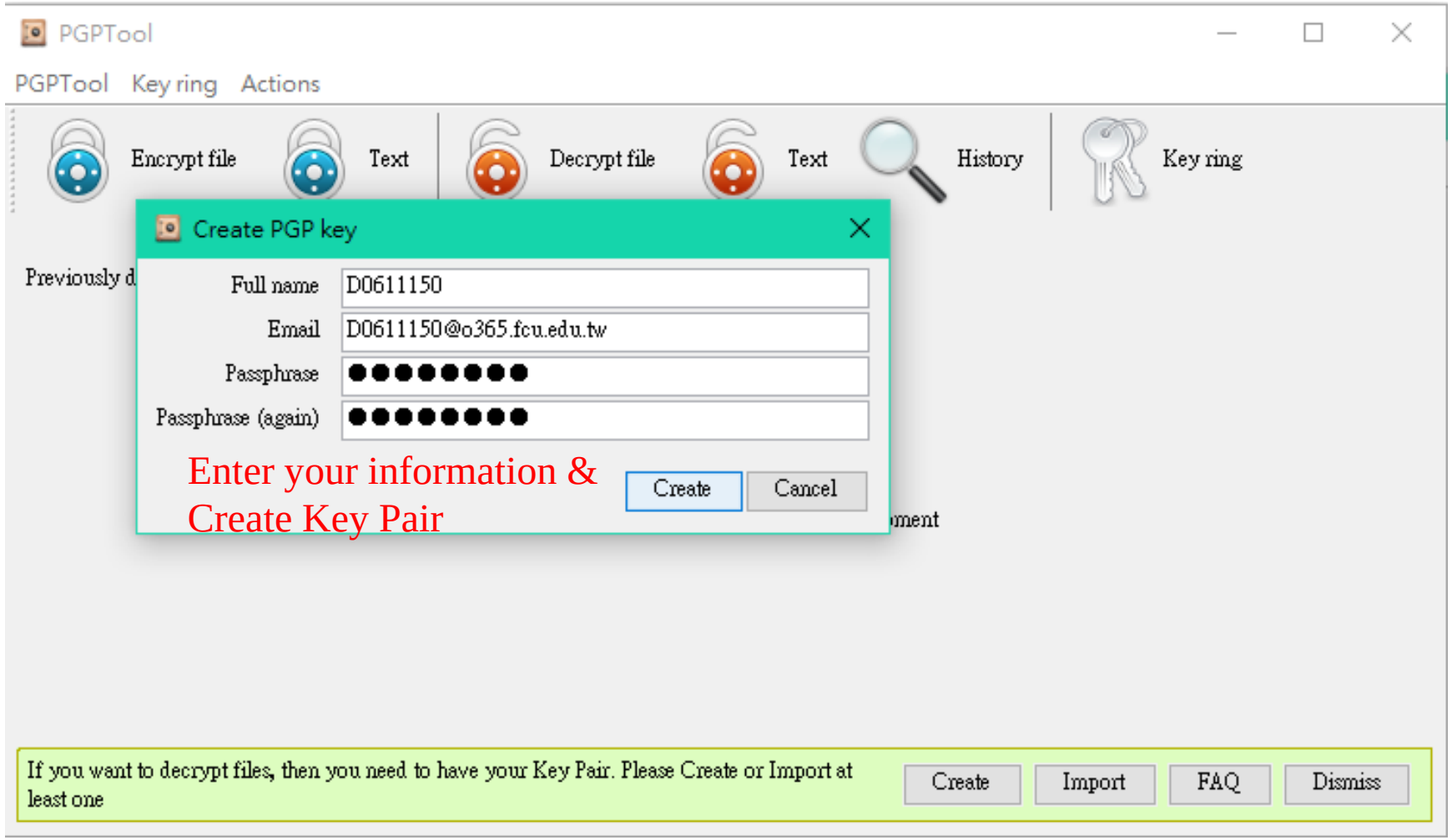
PGP Tool


PGPTool
PGPTool
Key ring
Actions
Encrypt file
Text
Decrypt file
Text
History
Key ring
Previously decrypted files (these files are still in an un-encrypted state on your disk):
No decrypted files are monitored at this moment
If you want to decrypt files, then you need to have your Key Pair. Please Create or Import at least one
Create
Import
FAQ
Dismiss

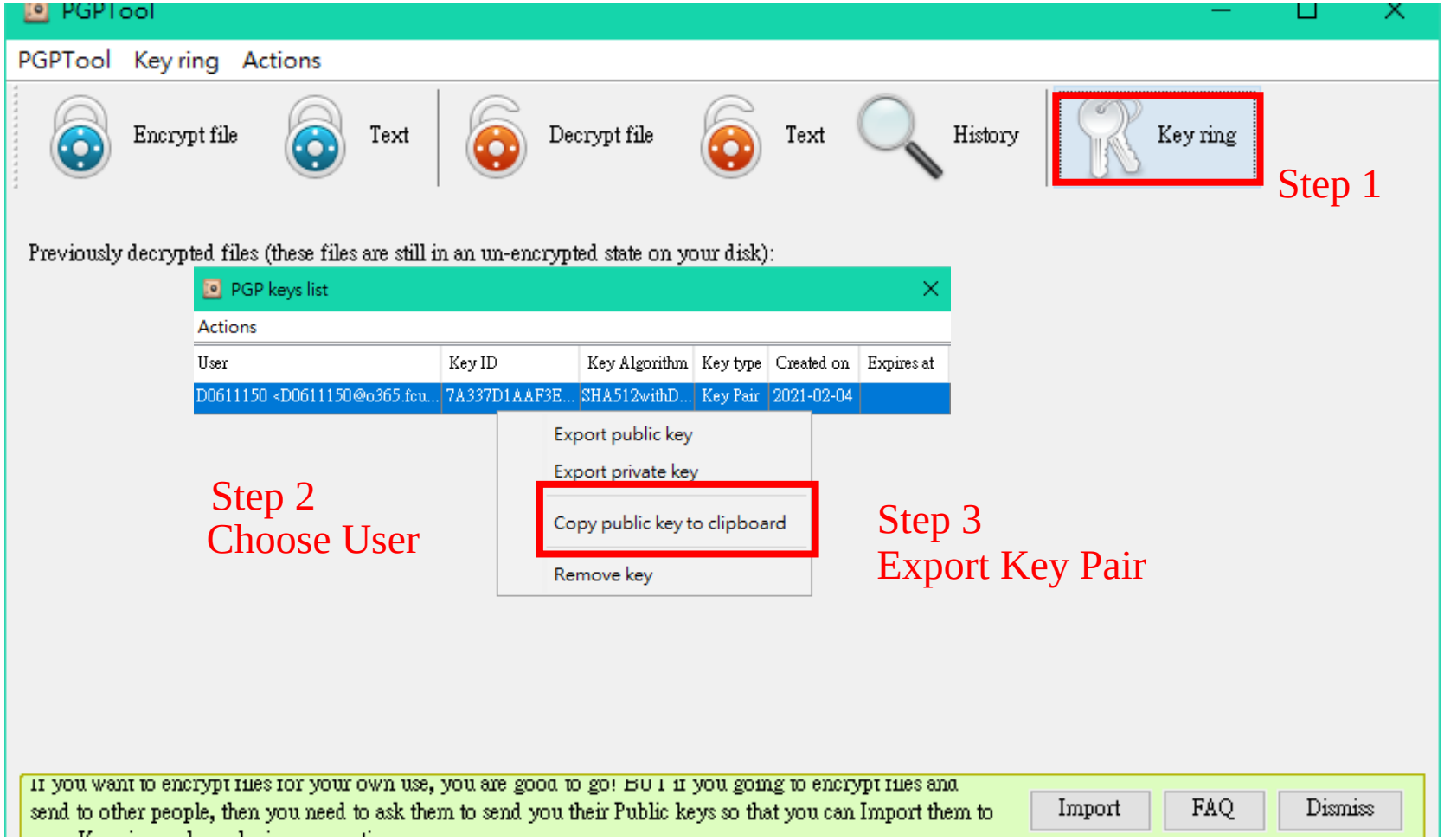
Create Key Pair (1/2)



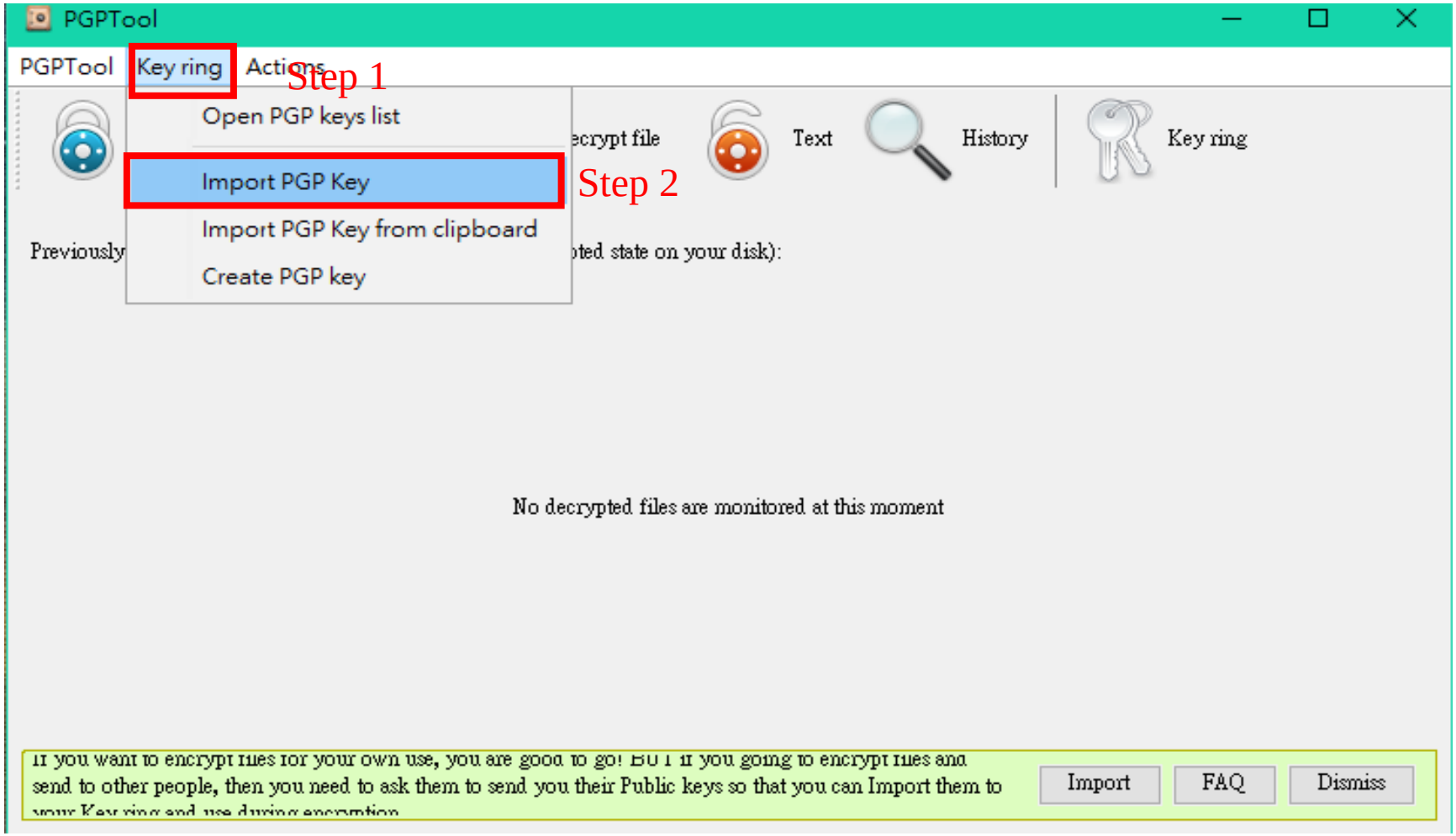
Create Key Pair (2/2)



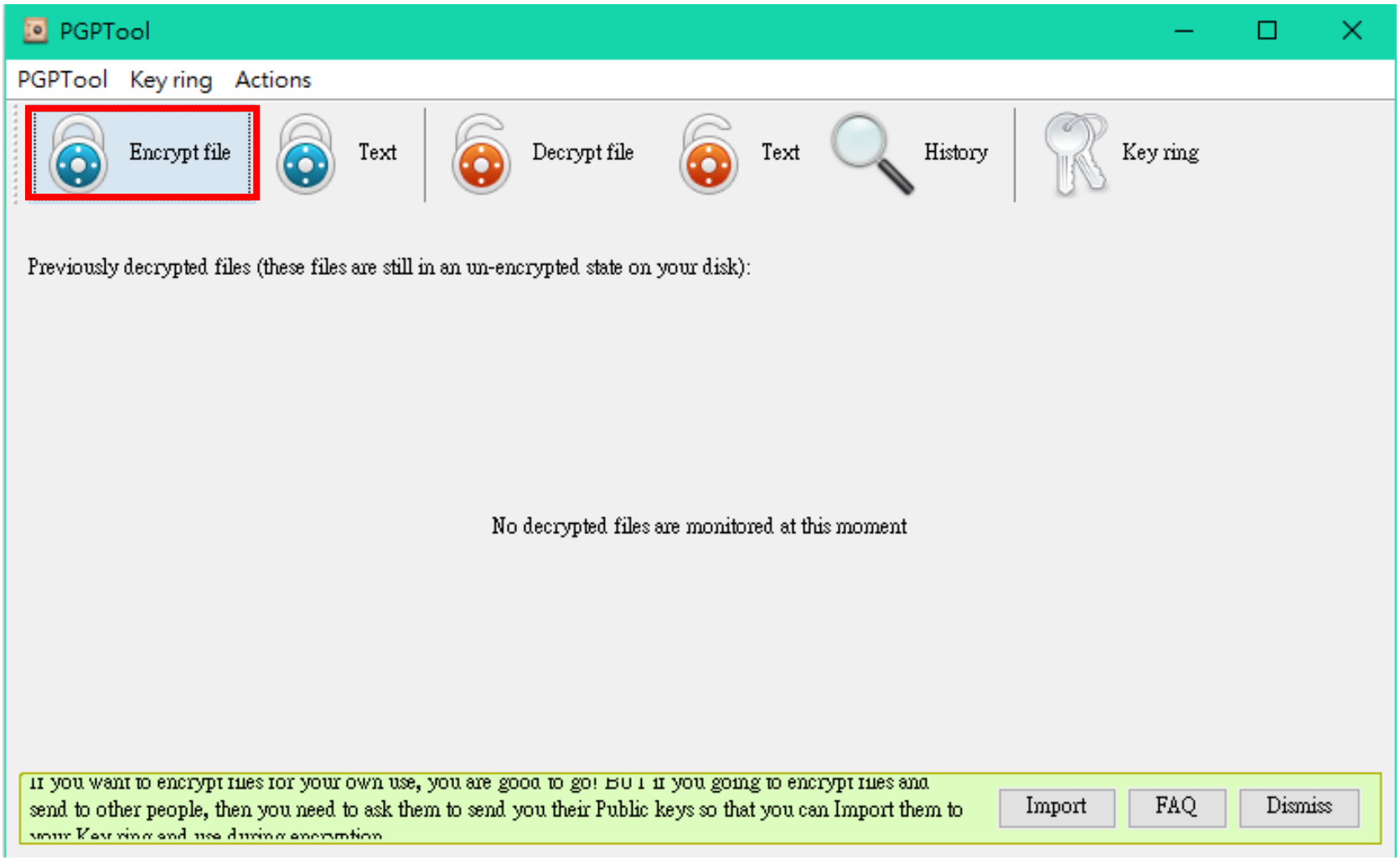
Export Key Pair



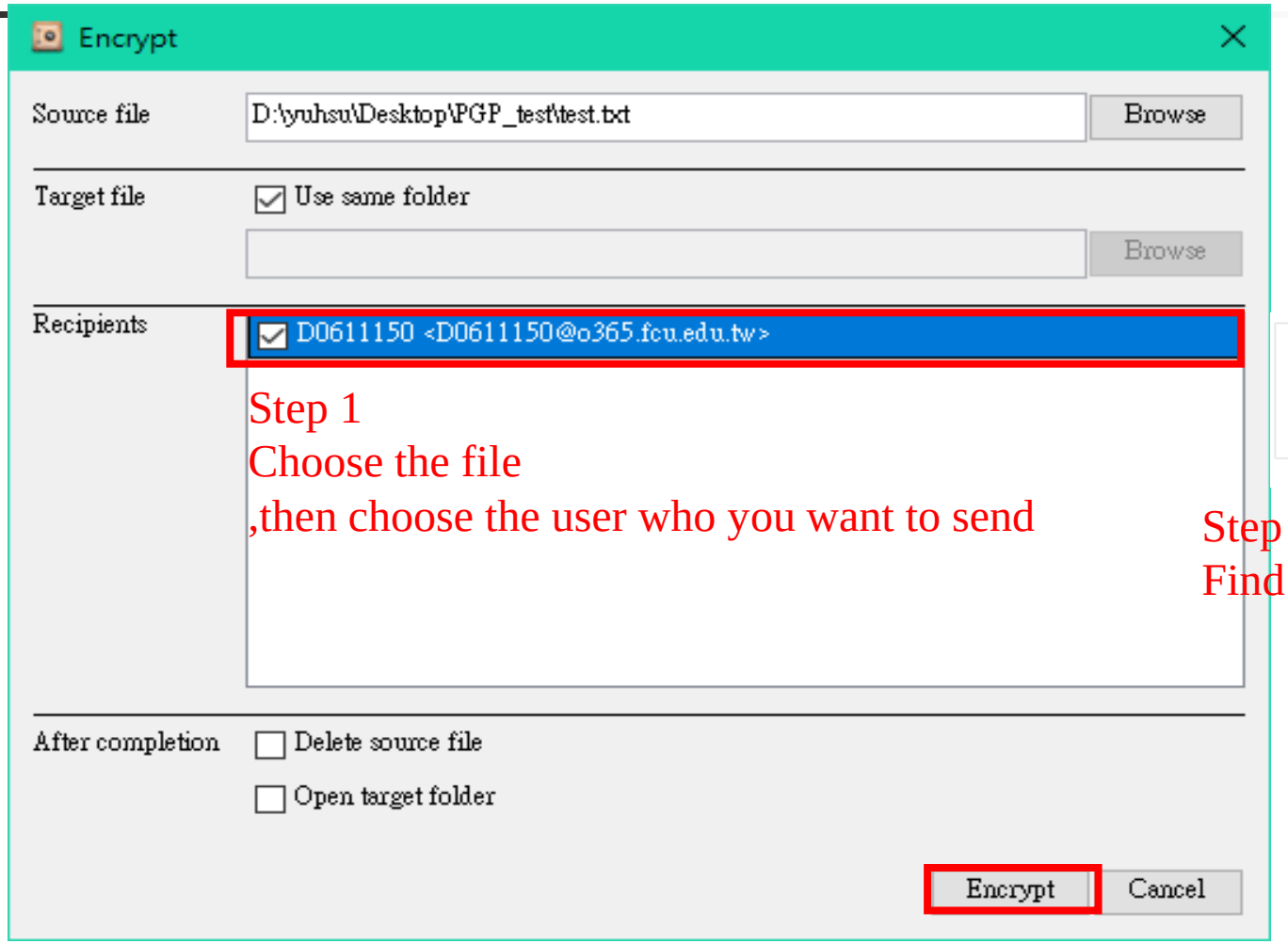
Import Public Key



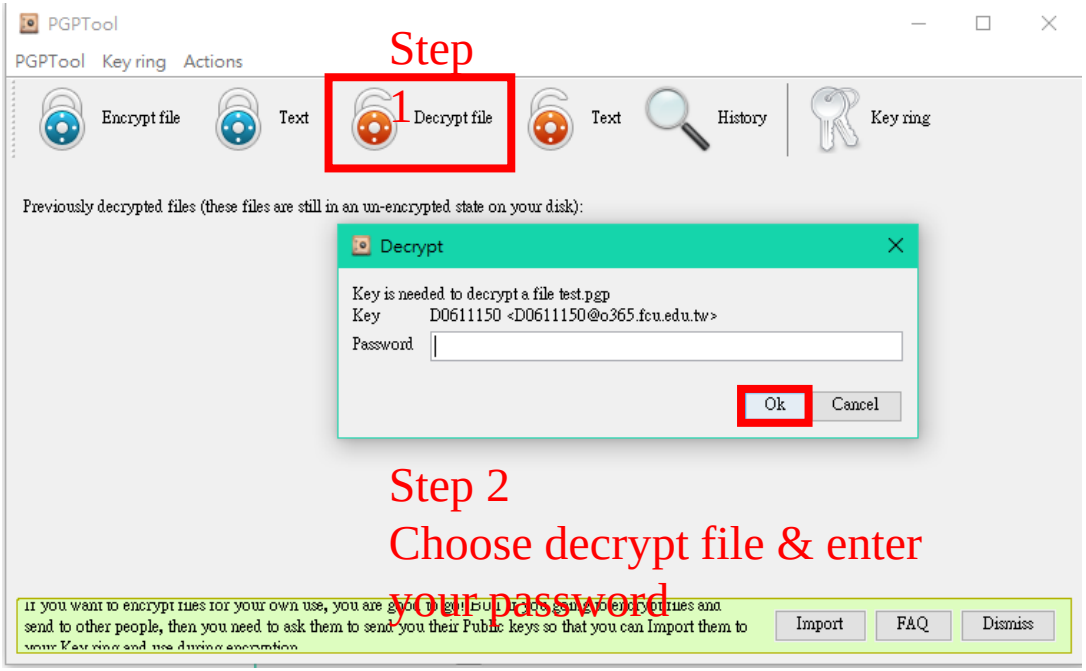
Encrypt File (1/2)



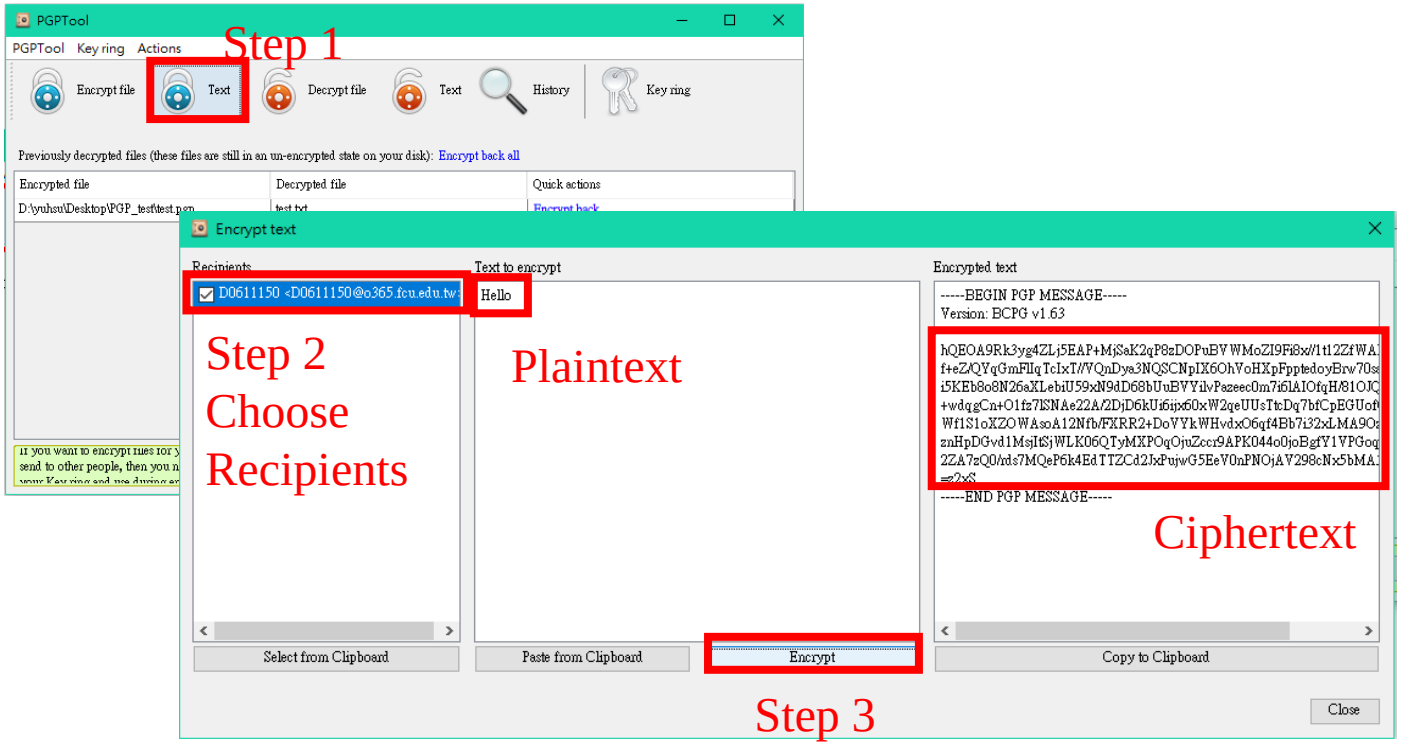
Encrypt File (2/2)



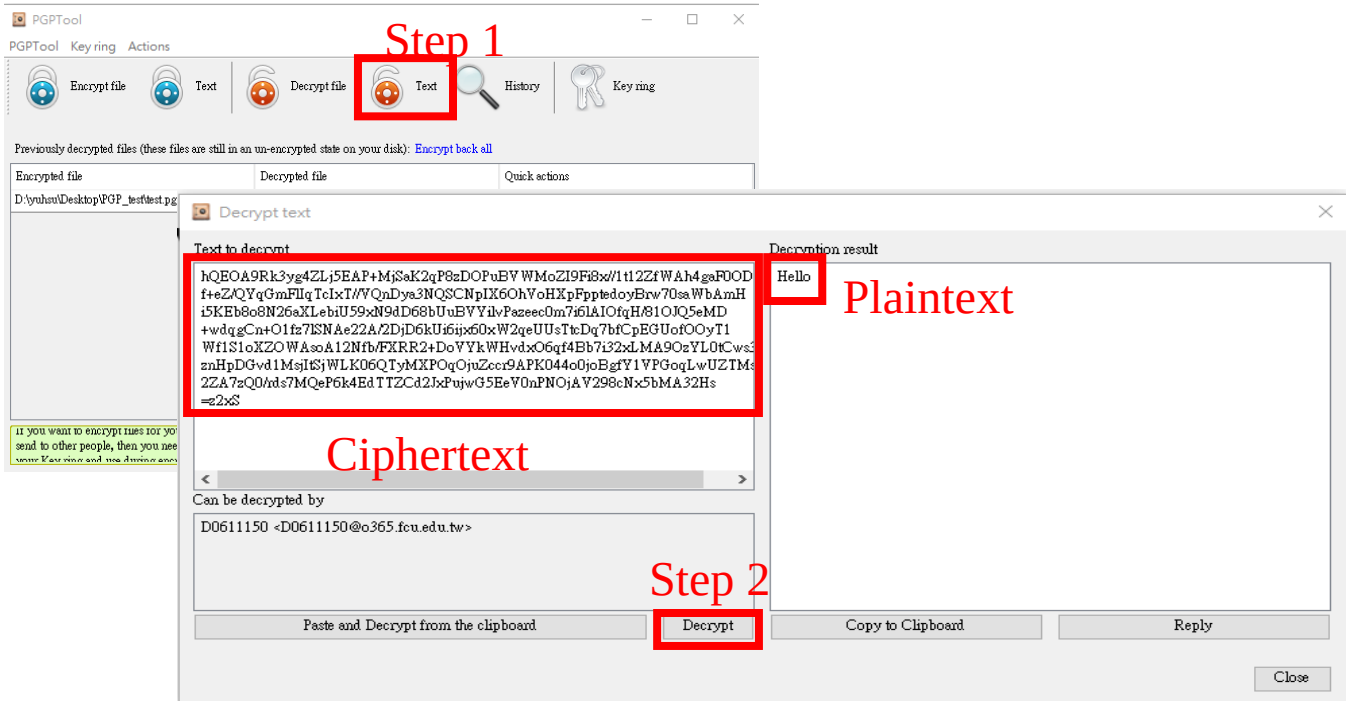
Decrypt File



Encrypt Text

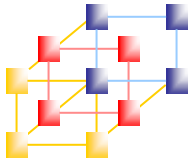


Decrypt Text



Quiz 8

- 有電腦的
  - 上iLearn把以下檔案抓下來：
    - STUDENT_TEST - Keypair.asc
    - STUDENT_TEST.txt
      - → 匯入金鑰串並解開，將那首歌的名字寫在白紙上 (可Google、可寫中文)
- 沒有電腦的
  - 就…寫今天晚餐吃什麼好了 → 參考一下 XDa
- 請將答案寫在紙條上，下課收來講桌。
- ((請記得寫上班級姓名學號



Quiz 9

- 有電腦的
  - 上iLearn把以下檔案抓下來：
    - IECS - Publickey.asc
      - → 匯入公鑰，把班級姓名學號加密後將密文回覆在討論串下
- 沒有電腦的
  - 回家上iLearn把以下檔案抓下來：
    - IECS - Publickey.asc
      - → 匯入公鑰，把班級姓名學號加密後將密文回覆在討論串下