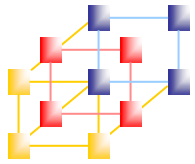


**PGP Lab**

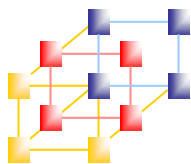
---



# 先看看金鑰對的產生

---

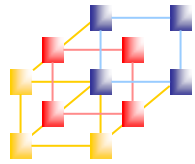
- Puttygen.exe



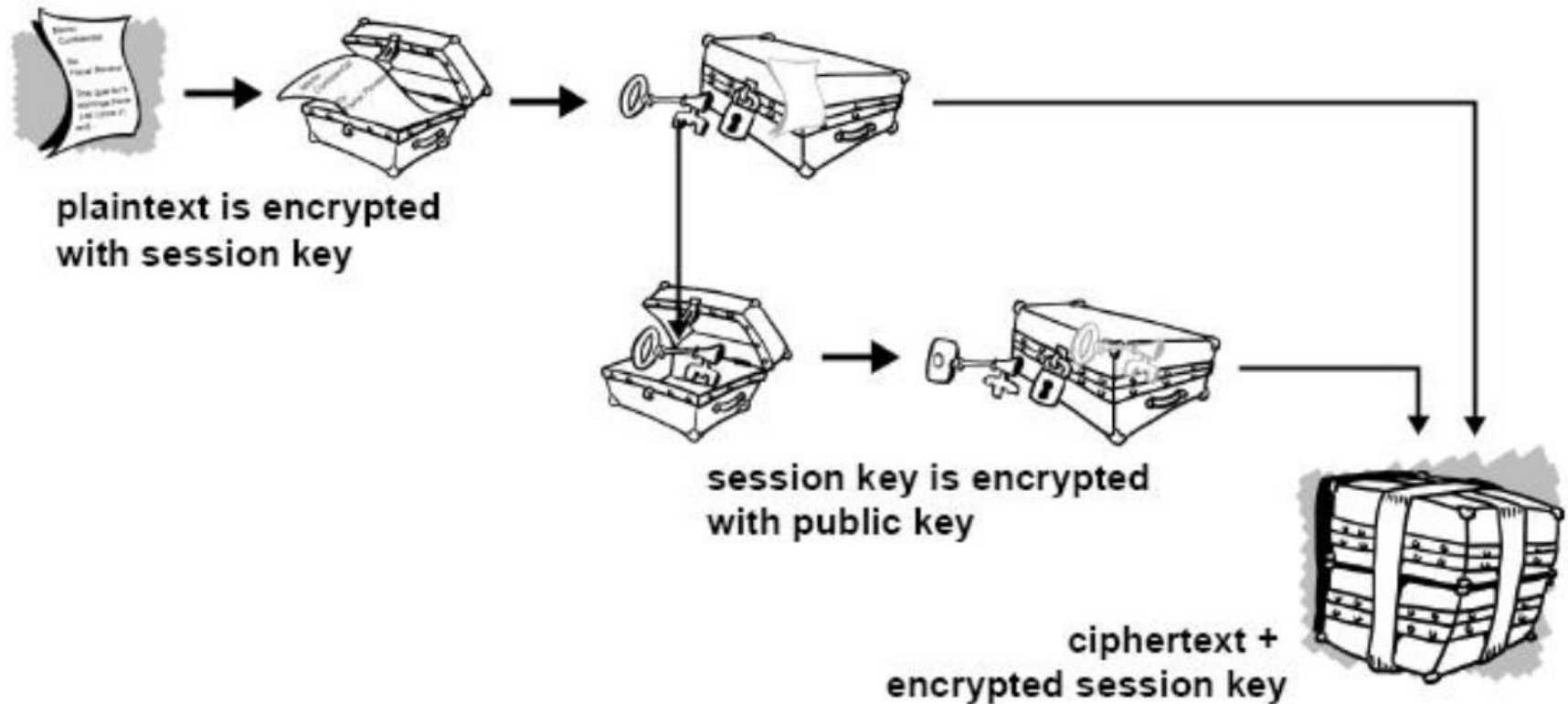
# GPG Full Demo

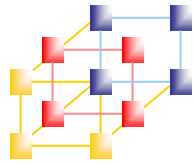


- <https://gnupg.org/index.html>
  - 加密
  - 解密
  - 簽章
  - 驗簽章
  - 加密+簽章
  - 解密+驗簽章

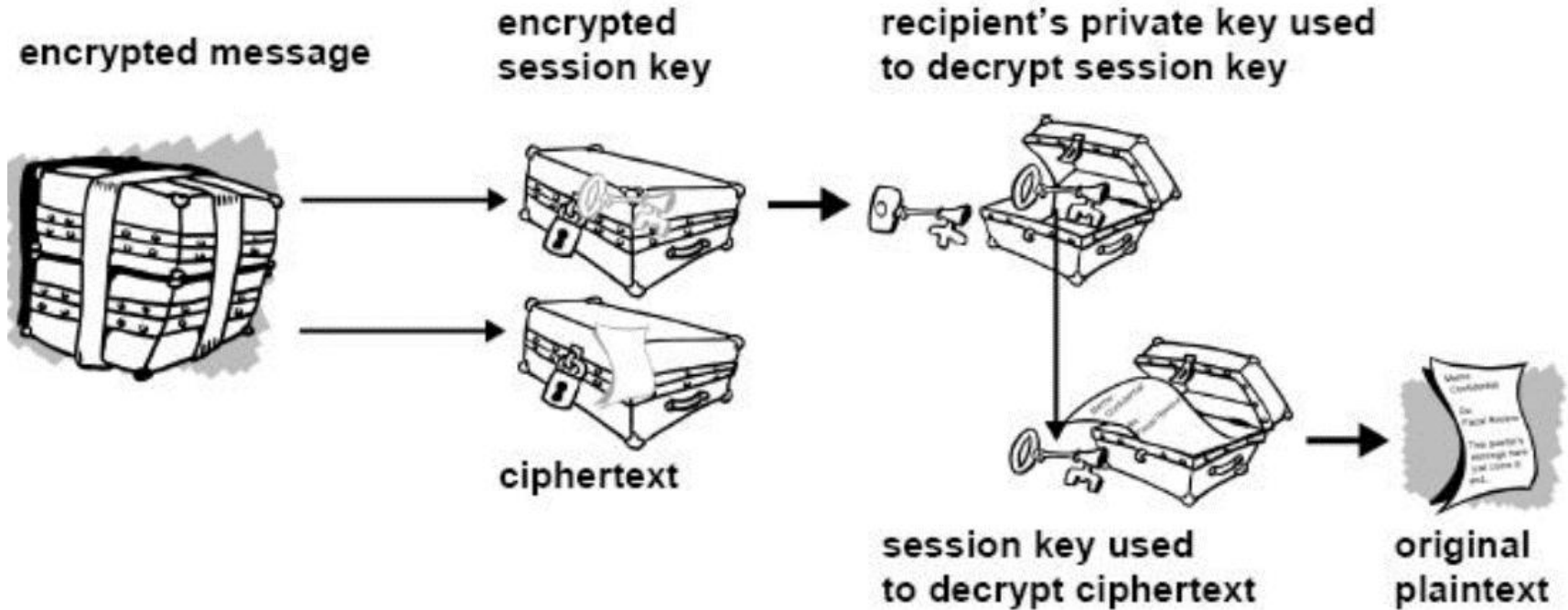


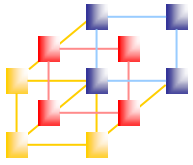
# PGP Encrypt





# PGP Decrypt



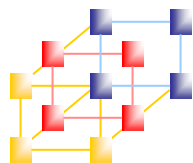


# PGP Tool Download

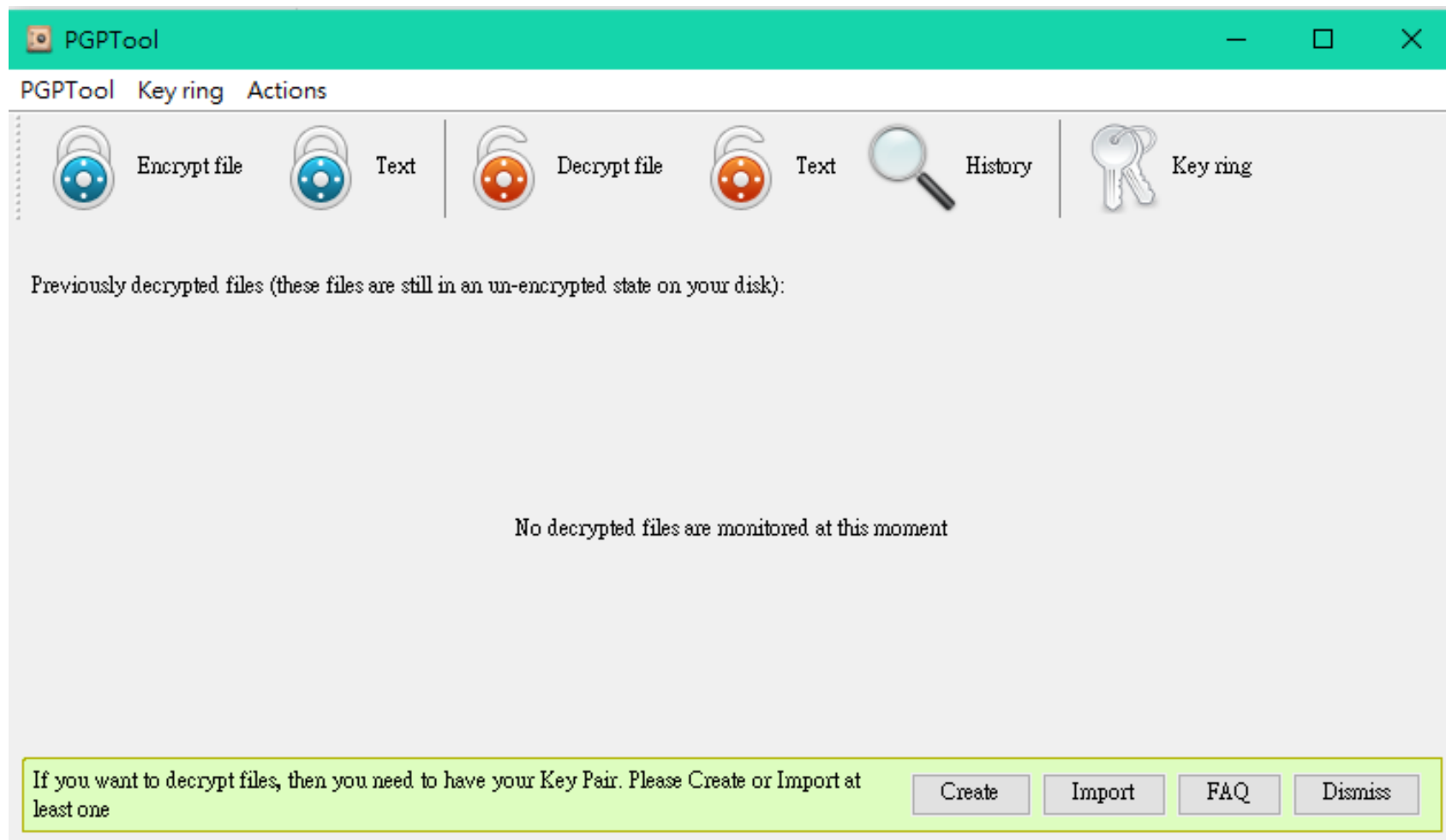
---

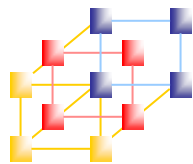
<https://pgptool.github.io/>

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

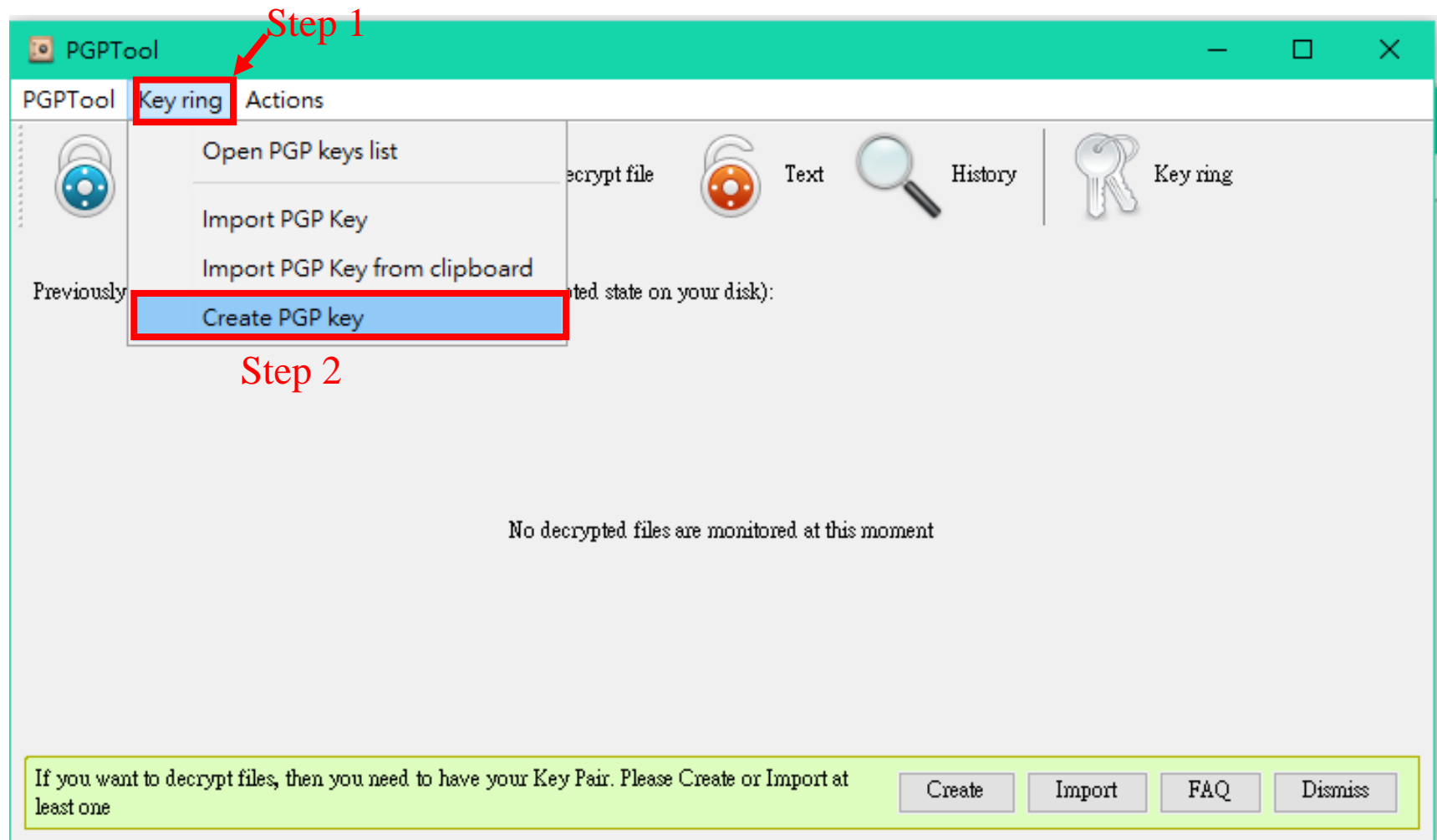


# PGP Tool

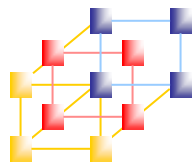




# Create Key Pair (1/2)







# Create Key Pair (2/2)

PGPTool

PGPTool Keyring Actions

Encrypt file Text Decrypt file Text History Key ring

Previously d

**Create PGP key**

Full name D0611150

Email D0611150@o365.fcu.edu.tw

Passphrase ●●●●●●●●

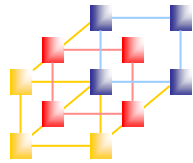
Passphrase (again) ●●●●●●●●

**Enter your information & Create Key Pair**

Create Cancel

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



# Export Key Pair

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):

PGP keys list

| User                          | Key ID          | Key Algorithm  | Key type | Created on | Expires at |
|-------------------------------|-----------------|----------------|----------|------------|------------|
| D0611150 <D0611150@o365.fc... | 7A337D1AAF3E... | SHA512withD... | Key Pair | 2021-02-04 |            |

Export public key  
Export private key  
Copy public key to clipboard  
Remove key

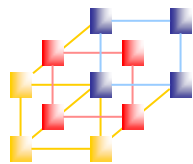
Step 1

Step 2  
Choose User

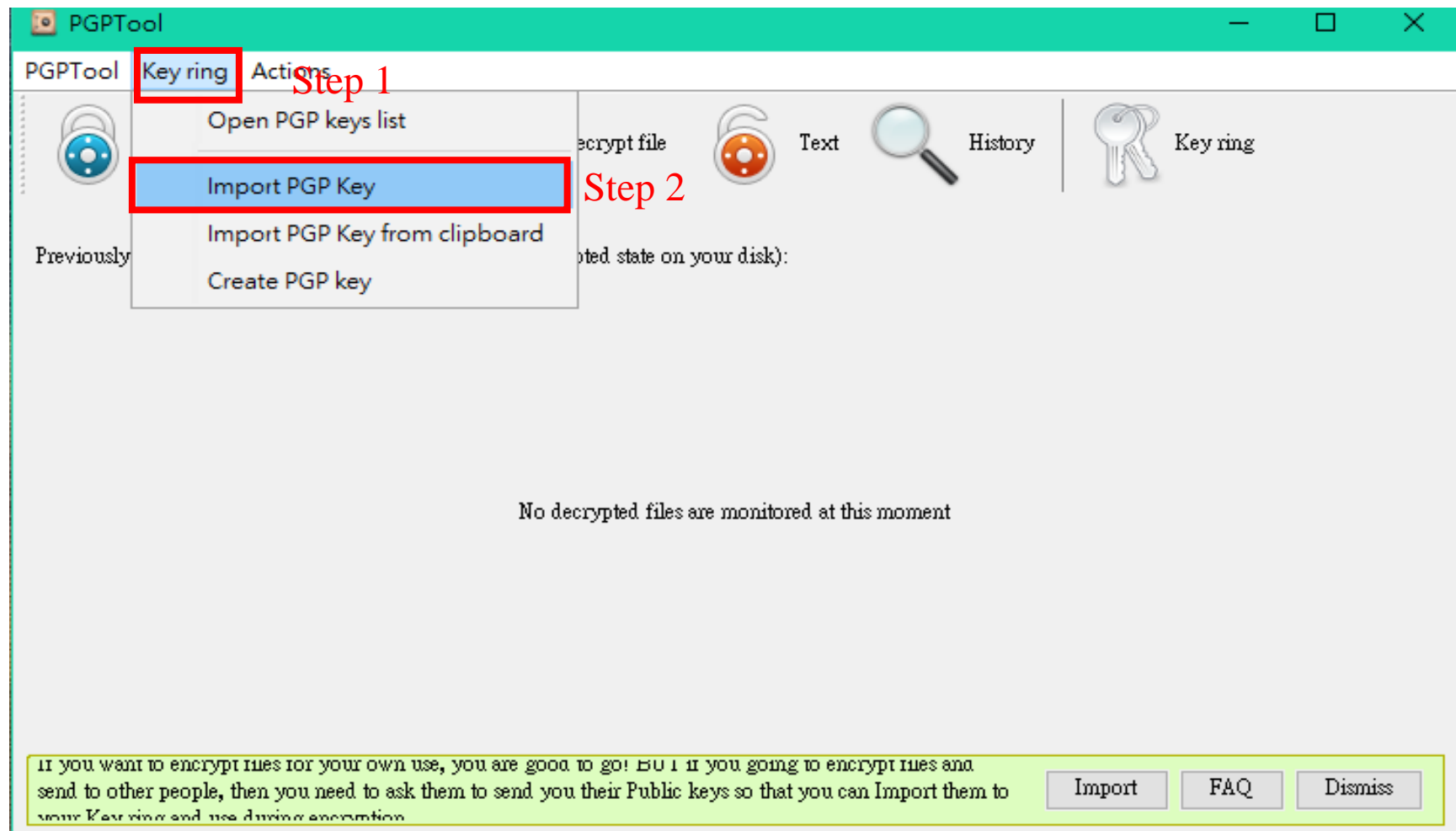
Step 3  
Export Key Pair

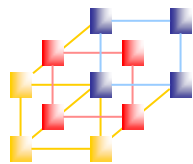
If you want to encrypt files for your own use, you are good to go! But if you going to encrypt files and send to other people, then you need to ask them to send you their Public keys so that you can Import them to

Import FAQ Dismiss

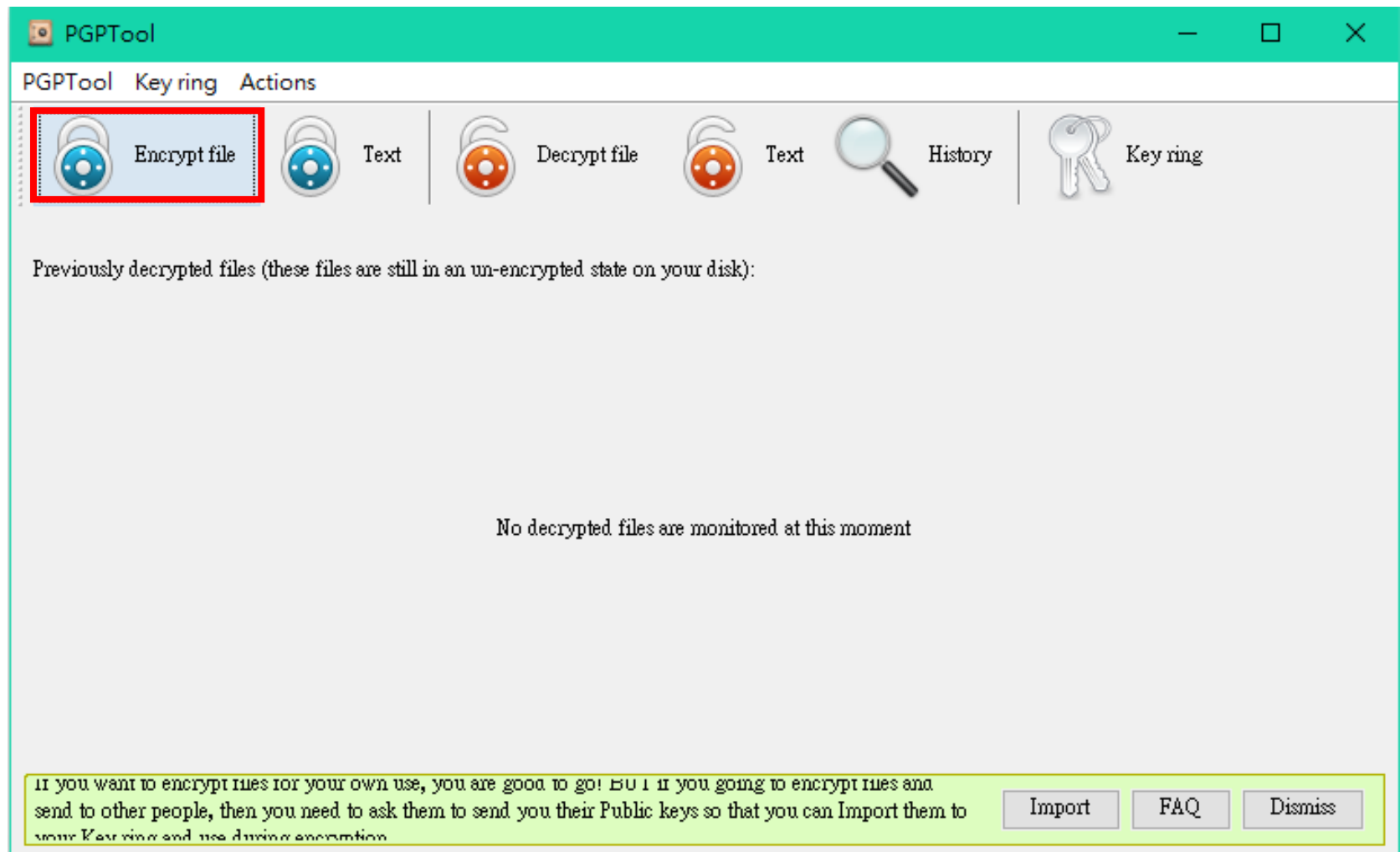


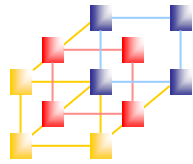
# Import Public Key





# Encrypt File (1/2)





# Encrypt File (2/2)

**Encrypt**

Source file:

Target file: ☒ Use same folder

Recipients: ☒ D0611150 <D0611150@o365.fcu.edu.tw>

After completion: ☐ Delete source file  
☐ Open target folder

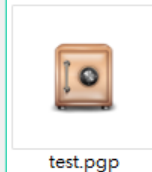
Step 1

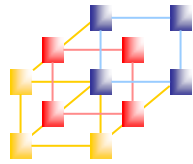
Choose the file

,then choose the user who you want to send

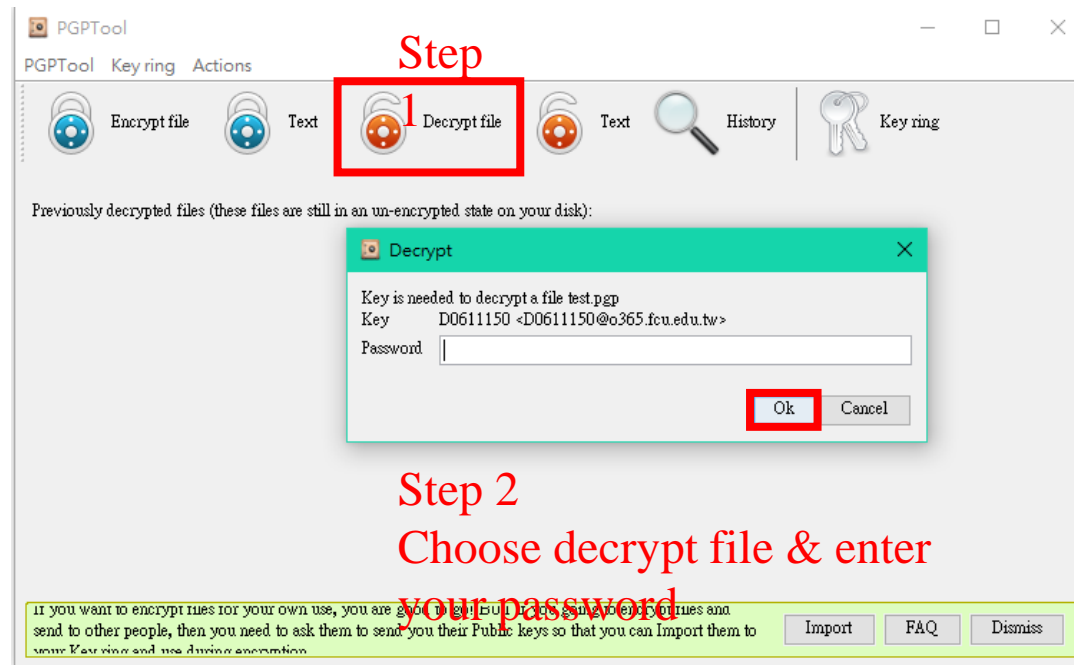
Step 2

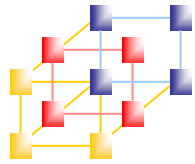
Find encrypted file





# Decrypt File





# Encrypt Text

**Step 1**

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): [Encrypt back all](#)

| Encrypted file                     | Decrypted file | Quick actions                |
|------------------------------------|----------------|------------------------------|
| D:\yuhua\Desktop\PGP_test\test.pgp | test.txt       | <a href="#">Encrypt back</a> |

**Step 2**  
Choose Recipients

Recipients: ☒ D0611150 <D0611150@e365.fcu.edu.tw>

Text to encrypt: Hello

**Plaintext**

**Step 3**

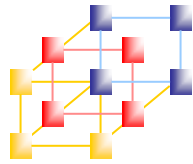
Encrypted text

-----BEGIN PGP MESSAGE-----  
Version: BCPG v1.63  
hQE0A9Rk3yg4ZLj5EAP+Mj8ak2qP8aDOPuBVWMoZl9F8x/1t12ZfWA  
f+eZQ/YqGmFlqTclxI/VQnDya3NQSCNpLX6OhVoHXpFpntedoyBrw70s  
i5KEb8o8N26aXLbU59xN9dD68bUuBVYulvPazee0m7u6lA1OfqH81OIQ  
+wdqgCn+O1fz7ISNAe22A/2DjD6kUj6ijx60xW2qeUUstDq7btCpEGUof  
Wt1S1oXZO WAsoA12Nfb/FXRR2+DoVYkWHvdxO6qf4Bb7i32xLMA9Oz  
znHpDGvd1Msl6;WLK06QTyMXPOqOjuZcc9APK044o0joBgtY1VPGoq  
2ZA7sQ0hds7MQeP6k4EdTTZCd2JkFujwG5EeV0nFNOjAV298cNx5bMA  
-----END PGP MESSAGE-----

**Ciphertext**

Select from Clipboard Paste from Clipboard **Encrypt** Copy to Clipboard

Close



# Decrypt Text

**Step 1**

PGPTool Key ring Actions

Encrypt file Decrypt file Text History Key ring

Previously decrypted files (these files are still in an un-encrypted state on your disk): [Encrypt back all](#)

| Encrypted file                     | Decrypted file | Quick actions |
|------------------------------------|----------------|---------------|
| D:\yuhua\Desktop\PGP_test\test.pgp |                |               |

**Decrypt text**

Text to decrypt

hQEOA9Rk3yg4ZLj5EAP+MjSsK2qP8zDOPuBV WMoZI9Fi8x//1t12ZfWAh4gaFOOD  
f+eZQYqGmFlq ToIxT//VQnDya3NQSCNpIX6OhVoHXpFppteoyBrw70saWbAmH  
i5KEb8o8N26aXLebiU59xN9dD68bUuBYVilvPazeec0m7i6lAIOfqH/81OIQ5eMD  
+wdqgCn+O1fs7ENAE22A/2DjD6kUi6ijx60xW2qeUUstDq7bfcPEGUofOOyT1  
Wf1S1oXZO WAsaA12Nfb/FKRR2+DoVYkWHvdXO6qf4Bb7i32xLMA90aYL0tCws3  
znHpDGvd1MsiI6jWlK06QTyMXPOqOjuZccr9APK044o0joEgfY1VPGoqLwUZTMt  
2ZA7zQO/nds7MQeP6k4EdTTZCd2JxPujwG5EeV0nPN0jAY298cNxs5bMA32Hs  
=e2xS

**Ciphertext**

Decryption result

Hello

**Plaintext**

Can be decrypted by

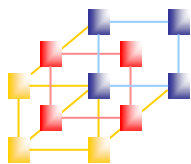
D0611150 <D0611150@o365.fcu.edu.tw>

Paste and Decrypt from the clipboard Decrypt Copy to Clipboard Reply

**Step 2**

Close

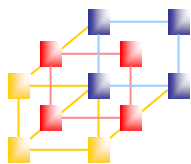




## Quiz 8



- 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