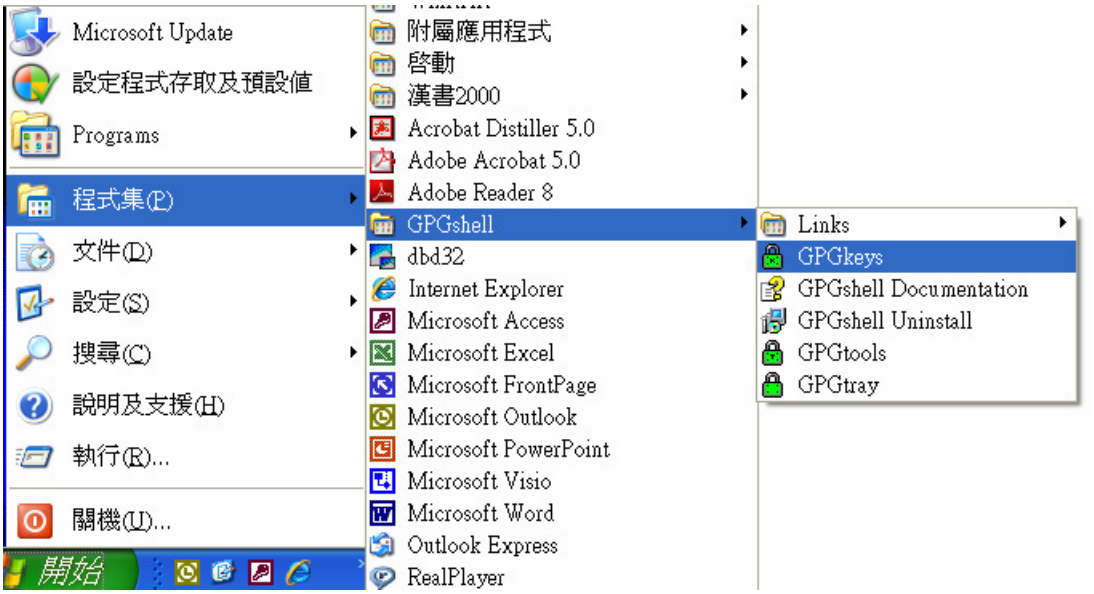
99.10

GPG（The GNU Privacy Guard）操作說明

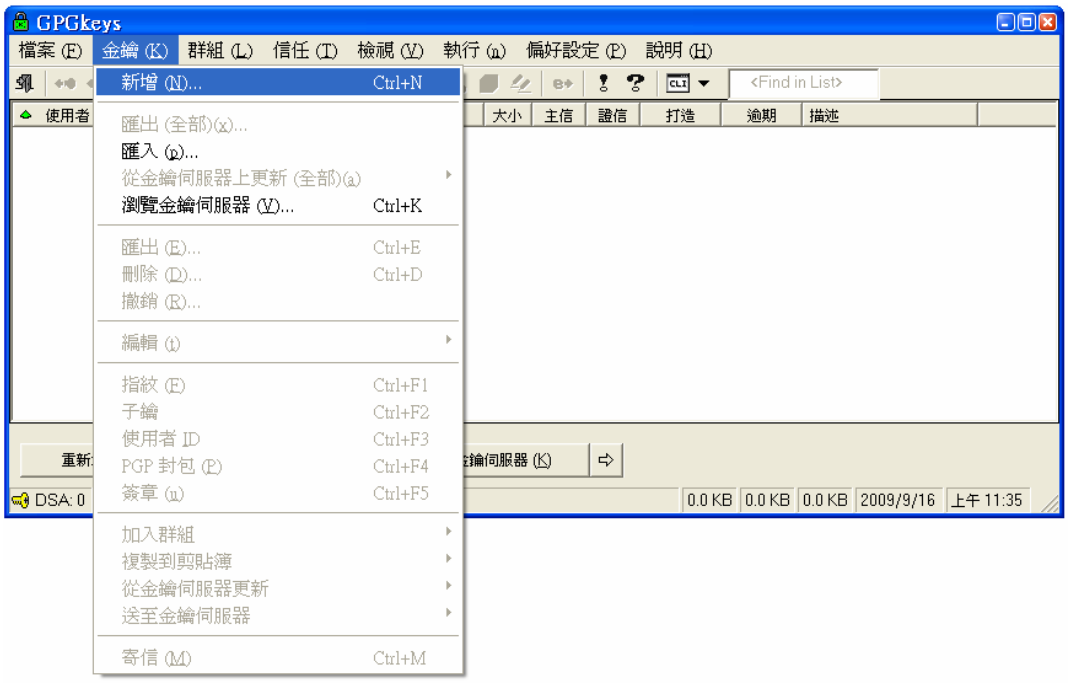
一、鑰匙對製作

(一)執行 GPG 製作鑰匙對

1.點選程式集之 GPGshell 下選擇 GPGkeys。

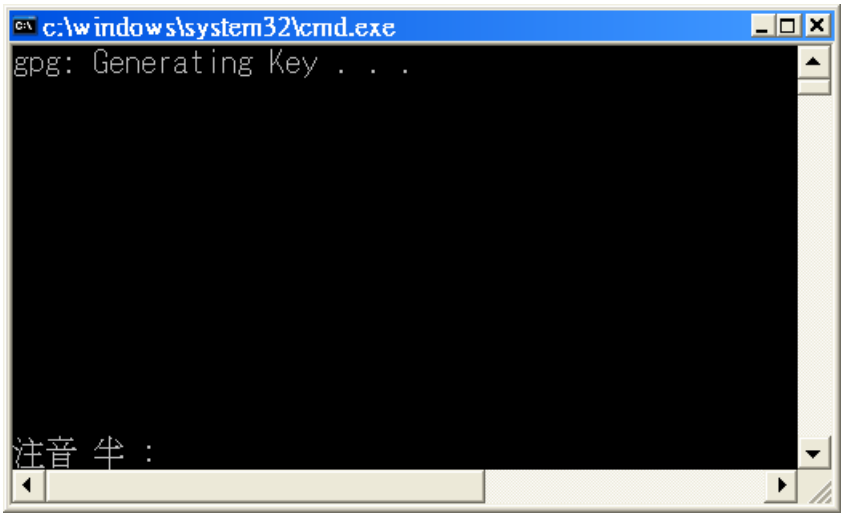


2.點選【金鑰】下拉選單，點選【新增】。

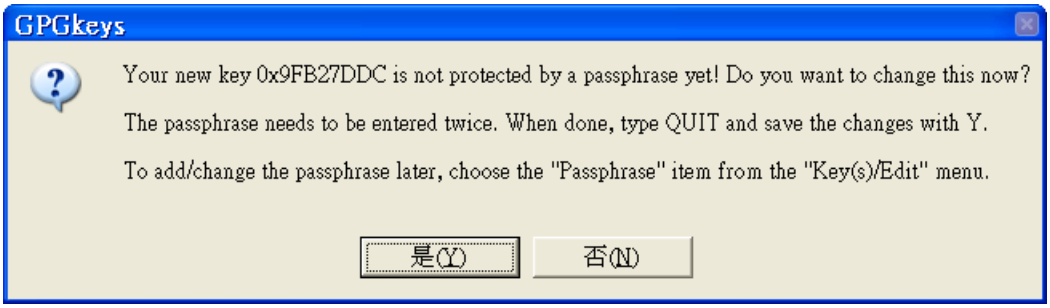


3.出現如下畫面，「姓名」欄輸入【key???】(???為單位代碼，本範例為 key979)；「電子郵件」欄輸入報名單位在大考中心登錄之聯絡信箱；「有效期限」設定鑰匙對的有效期限 (本範例為 2010 年 8 月 31 日)，亦可不設定期限(鑰匙對永遠有效)。完成後按【打造】鍵。

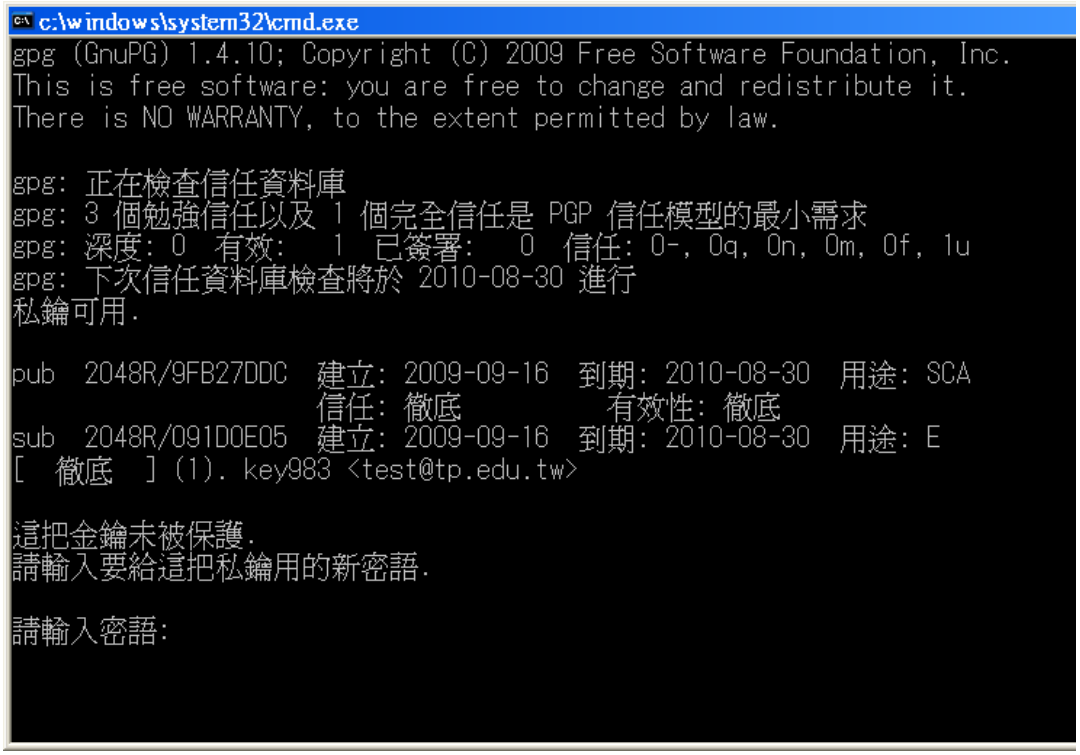
4.出現如下畫面開始製作鑰匙對，完成後會自動關閉。



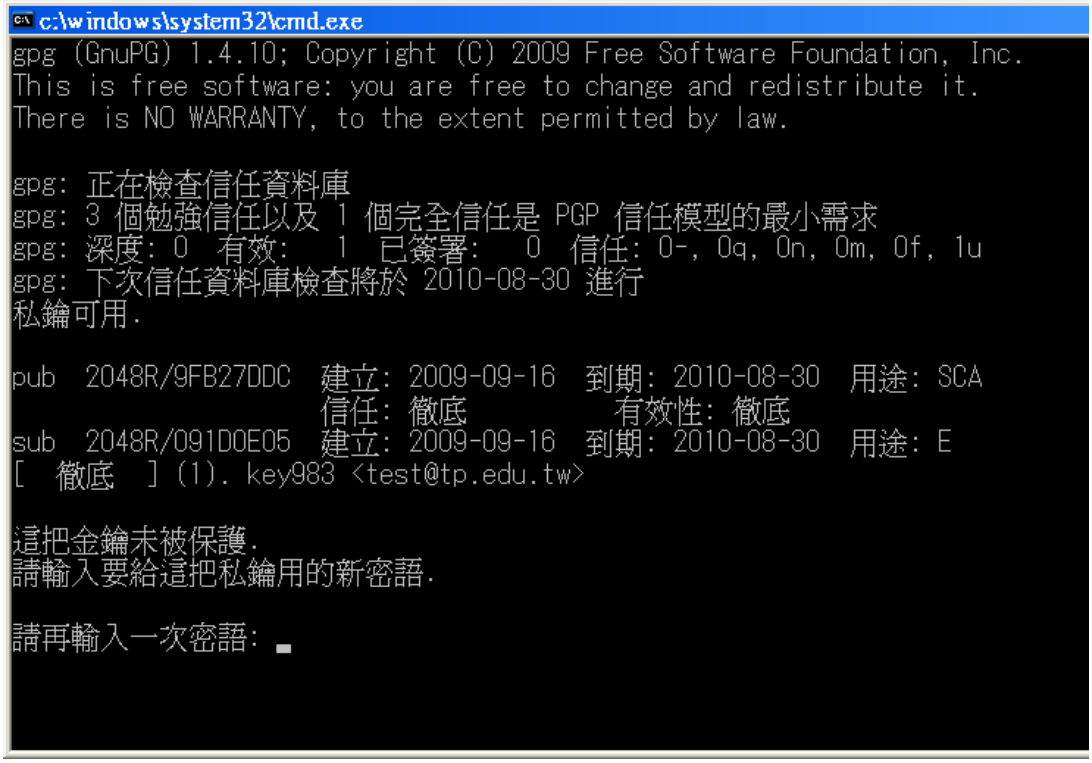
5.出現如下畫面，按【是】鍵。



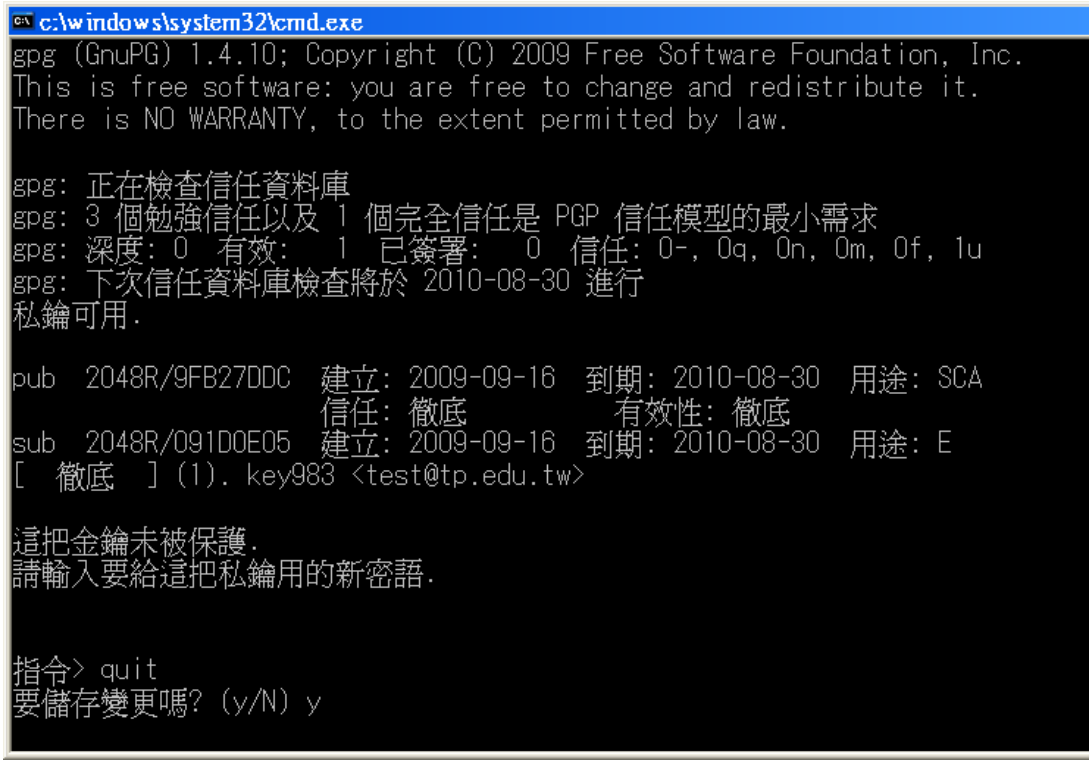
6.自行設定「密碼(密語)」，至少 6 個字元，輸入後按【Enter】鍵。



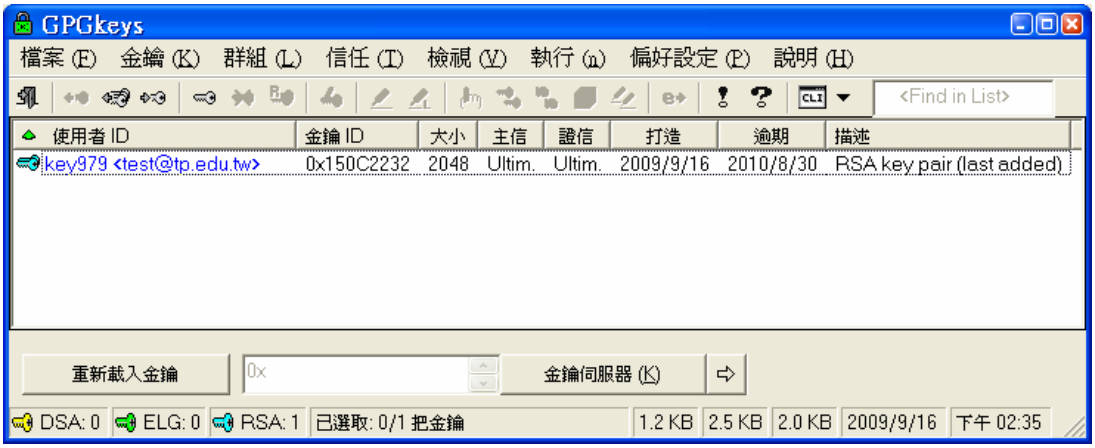
7. 再次輸入「密碼(密語)」後按【Enter】鍵。



8.先出現「指令>」輸入「quit」後，按【Enter】鍵。接著出現「要儲存變更嗎?」輸入「y」後，按【Enter】鍵。

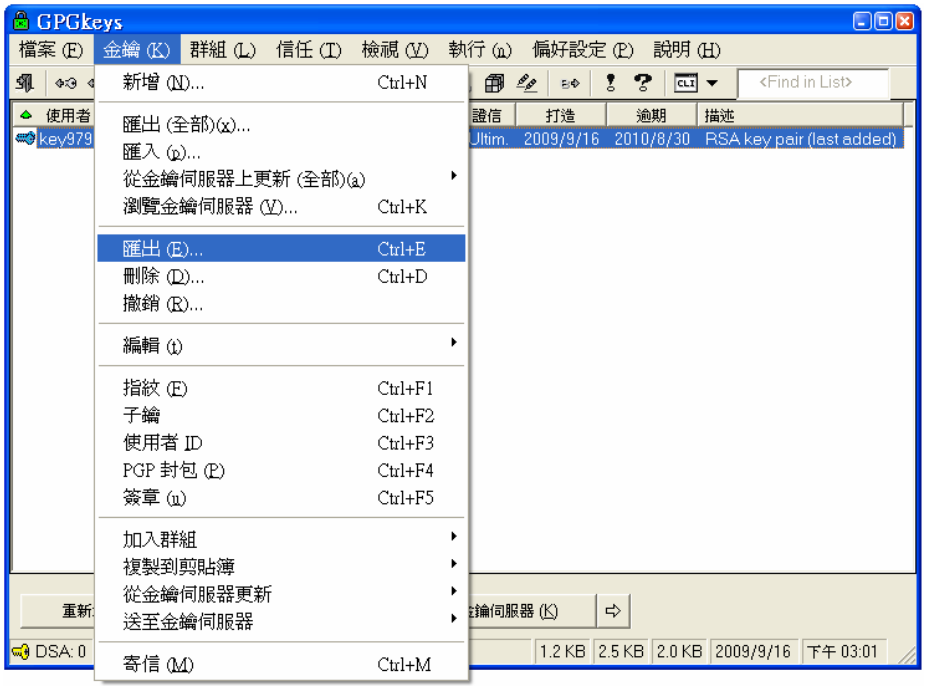


9.出現如下畫面，表示鑰匙對已產生。

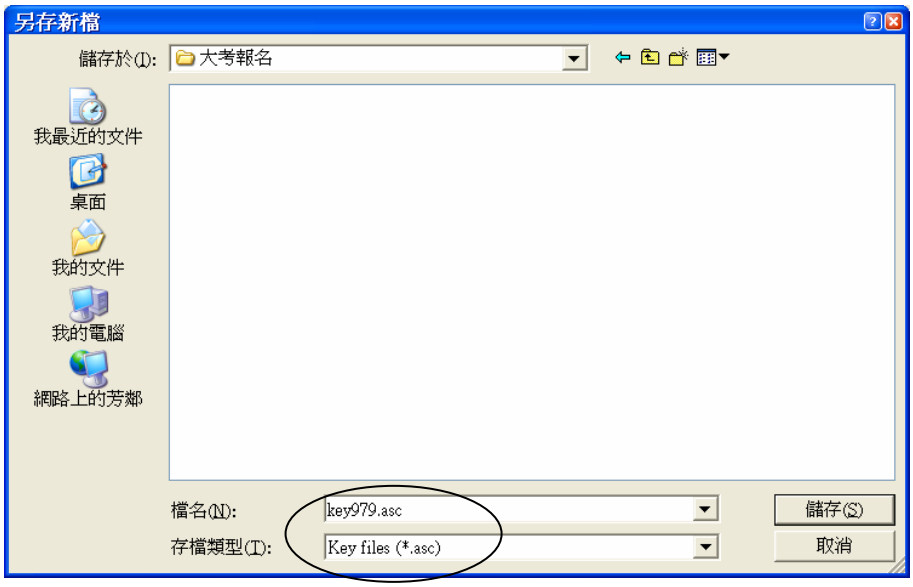


(二)匯出公鑰及私鑰

1.選取欲匯出之鑰匙對(如本範例 key979)，點選【金鑰】下拉選單，點選【匯出】。



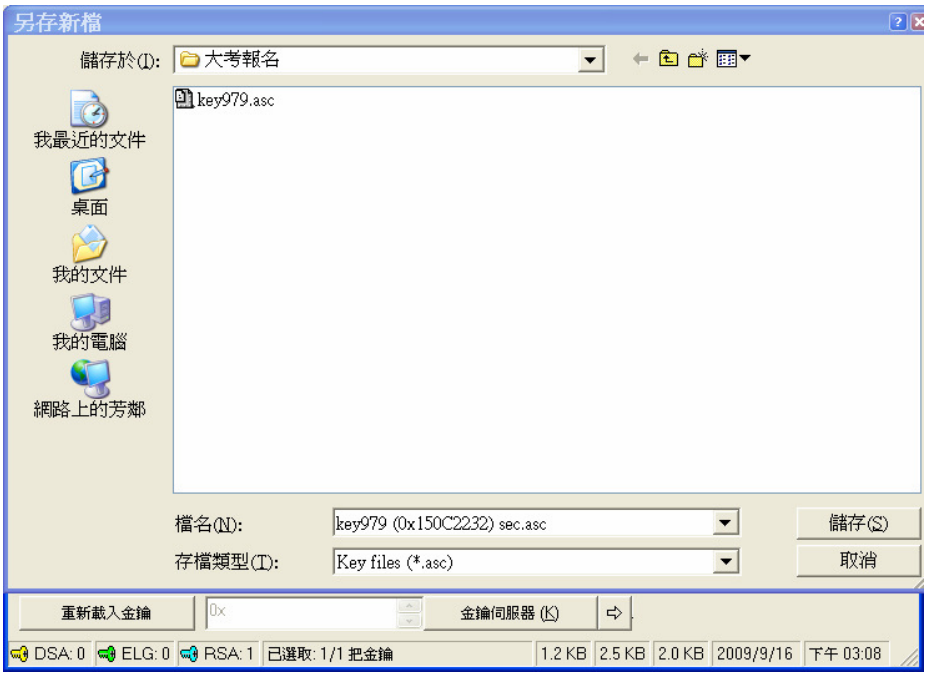
2.選擇儲存公鑰檔的目錄(資料夾)（如本範例之公鑰檔【key979.asc】儲存於 [大考報名] 資料夾中），將原預設之檔名 key979 (0x150C2232) pub.asc 改為 key???.asc（???為單位代碼，如本範例 key979），再按【儲存】鍵。



3.按【確定】鍵，即完成匯出公鑰，請將該檔案於報名期間內傳送至本中心。

4.出現如下之畫面後，請按【是(Y)】匯出私鑰。

5.出現如下畫面，選擇匯出目錄(資料夾)後按【儲存】鍵。



6.按【確定】鍵，即完成匯出私鑰。

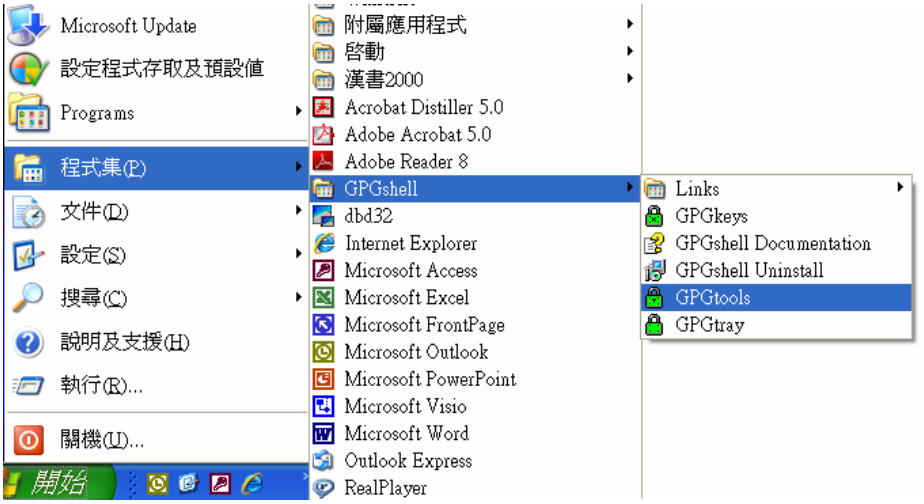
7.匯出之公鑰、私鑰檔名如下圖，請將該檔案備份並儲存安全之處備用。

※請妥善保存備份的公鑰檔及私鑰檔，若原有的鑰匙對不慎遺失或更換電腦，可將備份檔案匯入使用。

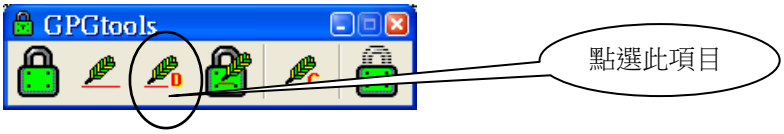
二、資料簽章

須簽章之資料為報名資料檔：學科能力測驗為 AO???.txt、術科考試為 DO???.txt、指定科目考試為 BO???.txt (???為單位代碼)。使用本中心集體報名作業軟體者，執行轉出後，檔案存在指定目錄下《如學測及術科為 C:**Sat\data、指考為 C:**Drse\data (**為學年度)》。

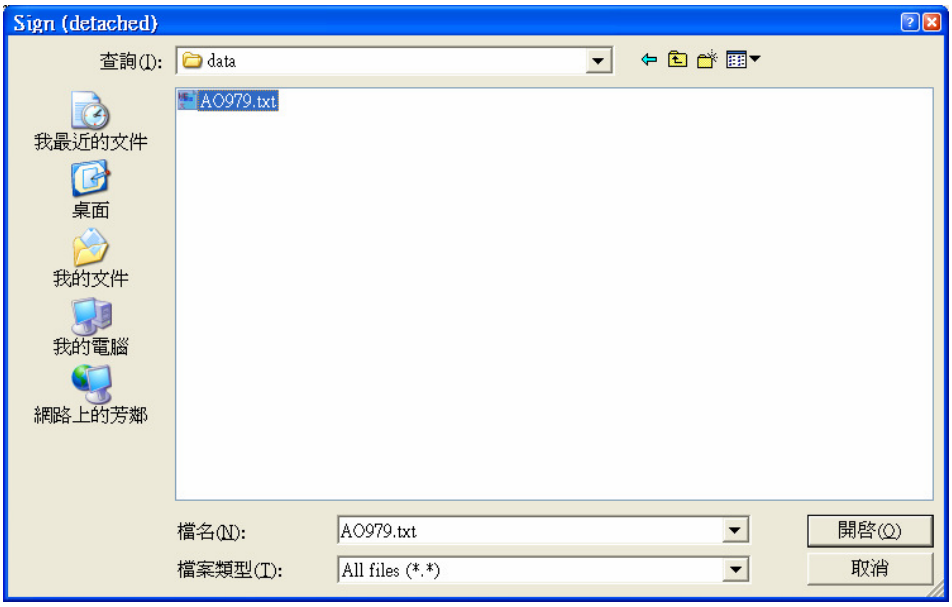
1.點選程式集之 GPGshell 下選擇 GPGtools。



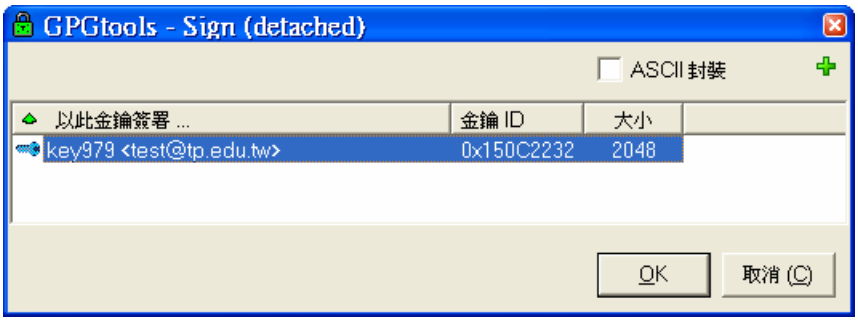
2.螢幕出現如下畫面，點選第 3 個項目。



3.點選要簽章的文件（如本範例 AO979.txt），選擇【開啟】。



4.選擇簽章鑰匙 key??? (如本範例 key979)，按【OK】鍵。



5.輸入「密碼(密語)」（產生鑰匙對時設定的密碼）後，按【Enter】鍵。

6.完成後，指定目錄中會產生簽章檔 AO???.txt.sig（如本範例 AO979.txt.sig）。

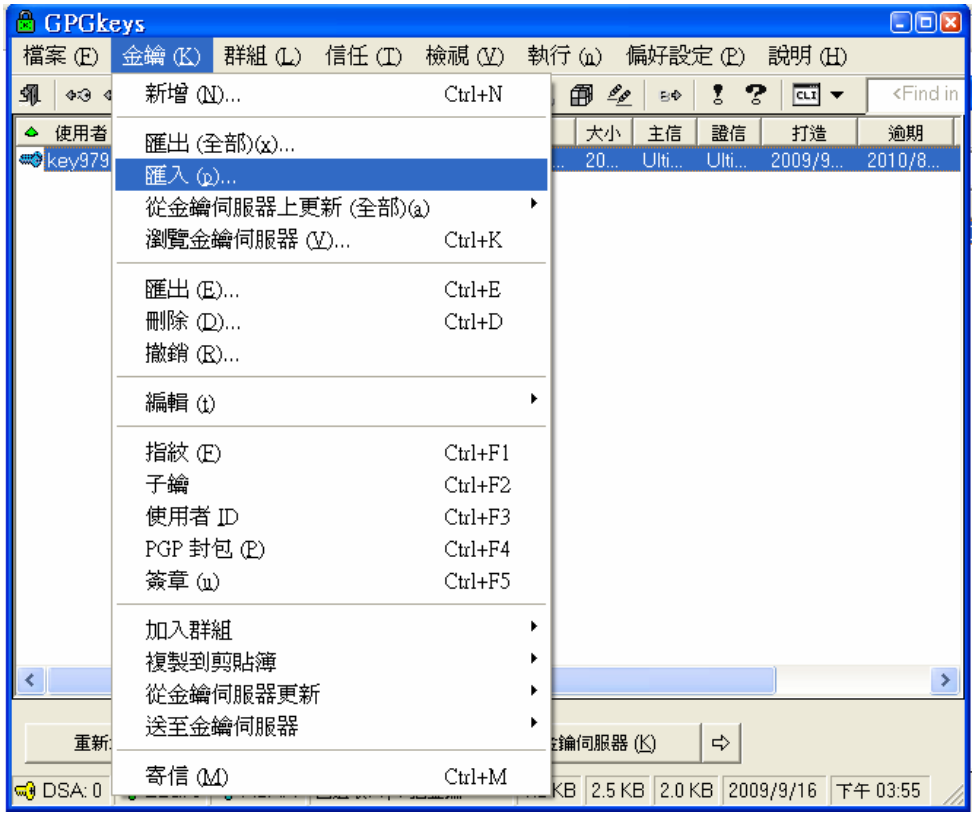
三、資料驗證

本中心傳送各項試務資料檔案（如准考證清冊及試場分配表檔案）及成績檔時，均使用電子簽章，各報名單位須使用本中心**「考試專用公鑰」**(以 ceec??.asc 命名，??為西元年度，例 ceec2011.asc)來核驗並確認檔案。**使用報名作業軟體完成安裝 GPG 者，已內含本中心「考試專用公鑰」**，或請洽本中心第二處取得本中心公鑰，並將其匯入貴單位之簽章軟體內。

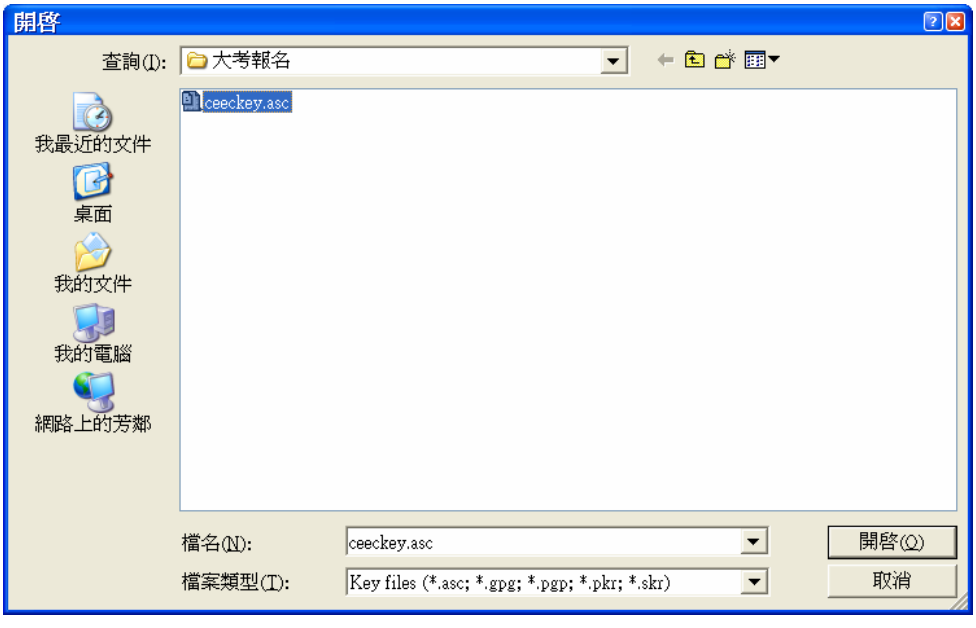
(一)匯入大考中心考試專用公鑰 (下列說明以 ceeckey.asc 為例)

1.點選程式集之 GPGshell 選擇 GPGkeys。

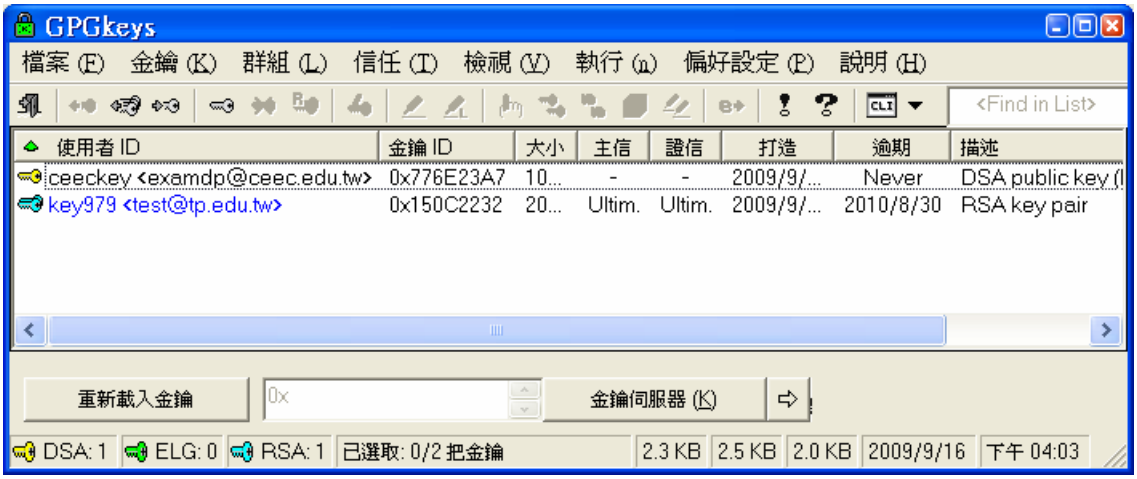
2.點選【金鑰】下拉選單，點選【匯入】。



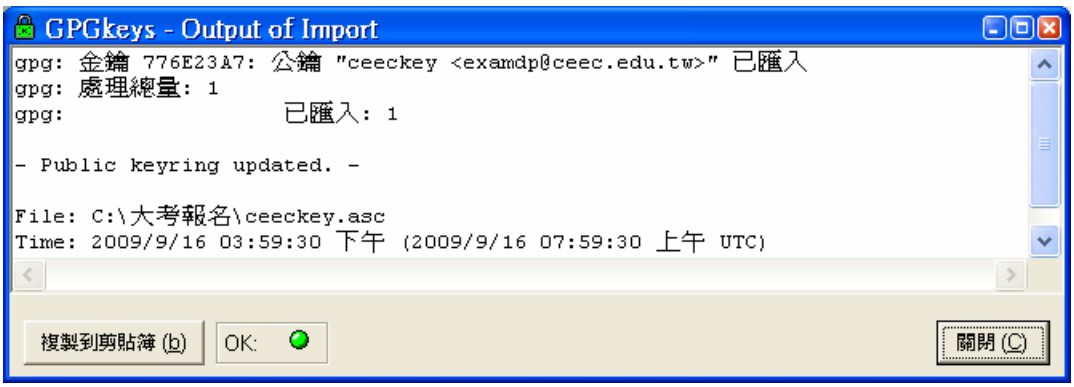
3.出現選取檔案視窗，選取 ceecKey.asc，按【開啟】。



4.出現如下畫面即表示成功匯入大考中心「**考試專用公鑰**」（如本範例 ceecKey）。



5.出現下列視窗，按【關閉】。



(二)檢查資料檔是否被更改

本範例中的資料檔為【SatL_979.xls】，簽章檔為【SatL_979.xls.sig】。

1.點選程式集之 GPGshell 下選擇 GPGtools。

2.螢幕出現如下畫面，點選最後一個項目（Deprypt/Verify）。

3.點選簽章檔（如本範例 SatL_979.txt.sig），按【開啟】。

4.出現圖一字樣表示資料檔 SatL_979.xls 未被更改過；圖二字樣則表示資料檔被更改過。

圖一：「完好的簽章…」表示資料未被更改過。

圖二：「損壞的簽章…」表示資料被更改過。

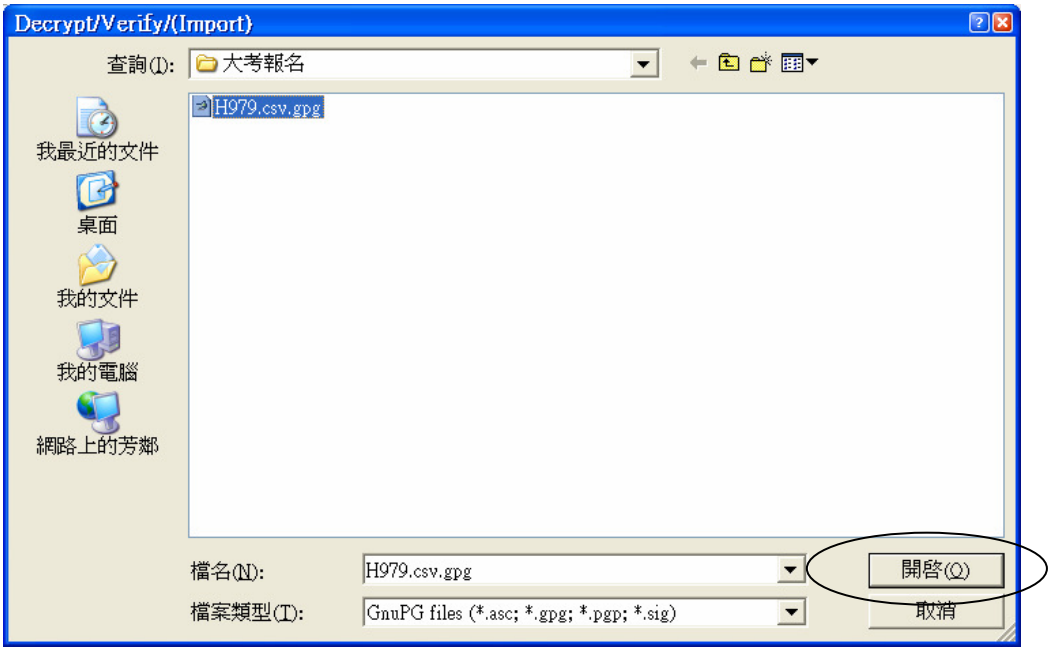
四、資料解密方式

本中心傳送之加密成績檔 H???.csv.gpg (???為單位代碼，例如：單位代碼為 979 的加密成績檔為 H979.csv.gpg)，係以各單位報名時之公鑰 key???.asc 加密，開啟檔案時需以各報名單位之鑰匙對及密碼解密。解密後之成績檔為 H???.csv，解密方式如下：

1.點選程式集之 GPGshell 下選擇 GPGtools。

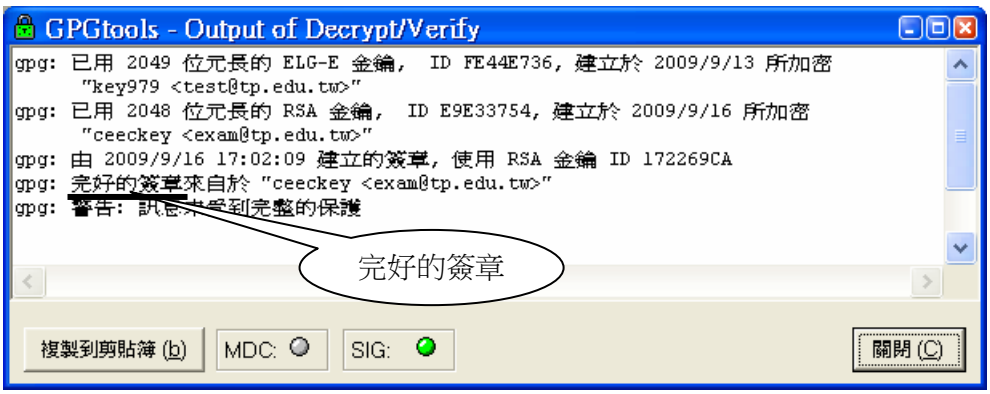
2.螢幕出現如下畫面，點選最後一個項目（Deprypt/Verify）。

3.點選要解密的檔案（如範例 H979.csv.gpg），點選【開啟】。



4.輸入「密碼(密語)」（產生鑰匙對時設定的密碼）後，按【Enter】鍵。

5.出現下圖字樣表示解密成功及簽章無誤，按【關閉】鍵。



6.完成後，在相同目錄下會產生 H???.csv（如範例 H979.csv）。