試務資料檔解密程式操作說明

本程式提供製作鑰匙對及資料檔解密等作業功能，並已內含大考中心 116 學年度考試專用公鑰(ceec2027.asc)，報名單位可於程式中執行產生(製作)鑰匙對、匯出公鑰檔、資料檔解密等作業。

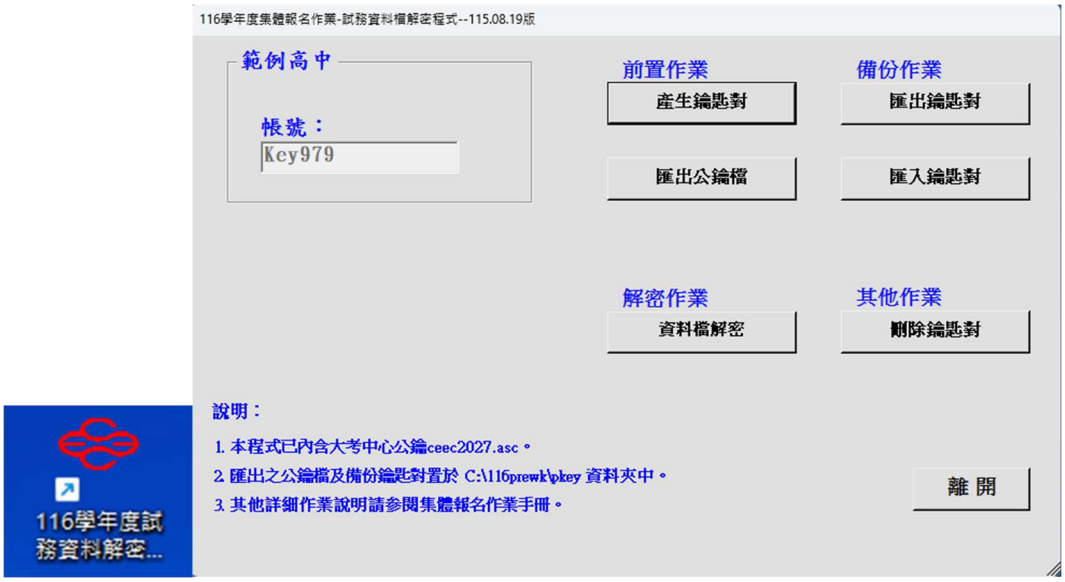
一、軟體安裝

※建議安裝前，應先行移除 C：\下之 11?prewk 資料夾 (11?表示非當學年度者)，若有需保留者，請將該資料夾(11?prewk)移出 C 槽，另行備份至其他位置保存，以利作業。

(一)自本中心網站下載專區下載試務資料檔解密程式【ceec116prewk.zip】置於 C：\，解壓縮後會自動產生 C：\ceec116prewk 資料夾。

(二)執行 C：\ceec116prewk 下之 CeecSetup.msi 按步驟依序安裝。

(三)安裝後會自動產生 C：\ 116prewk 資料夾。電腦桌面會出現「116 試務資料解密程式」圖示，即完成安裝程序。



二、作業說明

(一)前置作業

1.產生鑰匙對

(1)此功能僅須執行一次（產生的鑰匙對以**報名單位代碼**命名，如本範例中的 Key979），產生鑰匙對時**必須自行設定密碼，並務必牢記密碼**俾便於【資料檔解密】時使用。本學年度各項考試（學測、英聽、術科、分科測驗）均使用相同鑰匙對，請妥善保存。

(2)每一次產生的鑰匙對 均為獨立且唯一；當再次重新產生鑰匙對，即使名稱密碼不變，在使用上仍視為兩副不同的鑰匙對，亦即**重新產生的鑰匙對不能解開原有的加密檔**。

2.匯出公鑰檔

執行此功能後，將於 C：\ 116prewk \ pkey 下產生報名單位公鑰檔 Key???.asc。

(二)備份作業

1.匯出鑰匙對

產生鑰匙對後，請務必執行備份作業之【匯出鑰匙對】，並將匯出的備份鑰匙對檔案（Key???pub.asc 及 Key???sec.asc）另行妥善保存。

2.匯入鑰匙對

若原有鑰匙對不慎損毀遺失或電腦重整，可將保存之備份鑰匙對檔案（Key???pub.asc 及 Key???sec.asc）置放於 C：\ 116prewk \ pkey 下，並執行備份作業之【匯入鑰匙對】，即可回復原有鑰匙對。

(三)解密作業

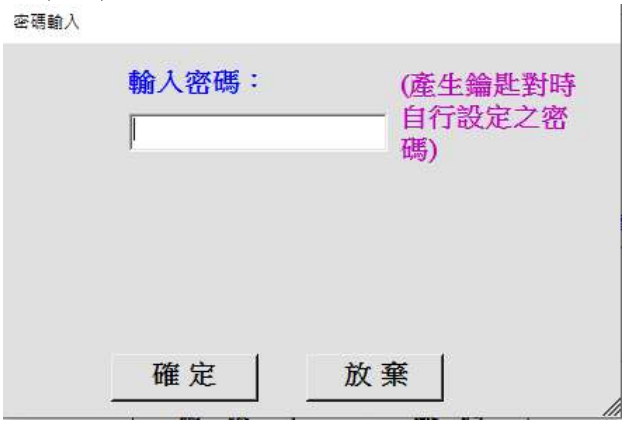
將本中心傳送至各報名單位之加密檔（副檔名為.gpg），含考生報考檔、應試號碼清冊及相關檔、試場分配檔及成績檔等，置放於自定之目錄下 (本範例置放於 C：\ 116prewk \ pkey 資料夾)。

※步驟如下：

點選【資料檔解密】→ (圖 1) 點選「瀏覽」選取檔案 → 點選【解密】→
(圖 2) 輸入密碼（產生鑰匙對時自行設定之密碼）→ 點選【確定】→ 完成解密，
解密後的檔案儲存於與加密檔相同資料夾，如本範例中 C：\ 116prewk \ pkey 資料夾。

(圖 1)

(圖 2)



(四)刪除鑰匙對

如須產生新的鑰匙對，須先執行【刪除鑰匙對】刪除原有鑰匙對，方能製作新的鑰匙對。建議每學年度使用新的鑰匙對，以降低資訊安全的風險。

※本中心傳送的加密檔（如：報考資料檔、應試號碼清冊檔、試場分配檔及成績檔等）是使用各報名單位於**報名時上傳的公鑰檔**加密，報名單位解密時必須使用同一副鑰匙對解密，因此，若報名單位重新產生鑰匙對，必須將新的公鑰檔寄給本中心，待本中心重新製作新的加密檔寄送報名單位，方可解密。