檔案樂活情報 ALOHAS Archives 35
訂閱 / 取消訂閱
發刊日：99年5月16日
http://alohas.archives.gov.tw
發行機關：檔案管理局

探尋國家寶藏
國外檔案新知
檔案小智囊

檔案小智囊

友善列印

檔案上好鎖，資料不外洩

隨著Notebook、PDA等行動裝置及USB隨身碟、外接式硬碟等可攜式儲存裝置逐漸普及，因裝置遺失、遭竊而導致所存放在這些裝置上機敏資料外洩的風險也日漸升高。面對資料外洩的威脅，想保護好您的電子檔案，就讓檔案小智囊來告訴您如何鎖好檔案。

檔案管理局檔案資訊組設計師 黃俊銘

一、前言

隨著公文製作、管理與交換的電腦化腳步，政府機關的檔案媒體類型也逐漸由紙質檔案轉為電子檔案(electronic record)。無論電子檔案是以電子檔(electronic file)或資料庫(database)型式儲存，都需存放在電子儲存媒體上，才可供電腦存取使用。

因電腦軟硬體的發展迅速及應用普及化，電子儲存媒體技術演進迅速，儲存容量不斷增大，體積也越來越小。現在一小片拇指般大小的快閃記憶體（俗稱拇指碟或隨身碟）已經可以存放數10GB的數位資料，1個如手掌大的2.5吋外接式硬碟機也已發展到可存放達1TB的數位資料。如果這些數位資料都是很重要的電子檔案的話，我們是不是應該考慮它的安全性呢？因此，如何防止存放在磁碟機或隨身碟裡須被保護的電子檔案被隨意取得與竊用，是確保電子檔案安全的重要工作。本文將介紹軟體式的加密方法，希望日後大家可以利用它鎖好您的電子檔案。

二、以加密方式保護電子檔案

何謂加密？透過特定的數學公式(稱演算法)及特定長度的數值(稱金鑰或密鑰)將電子檔案中的數位資料重新計算或排列組合成另一種資料型式內容，就稱為加密。當他人拿到經過加密的資料，即使電腦軟體可以開啟這個電子

HOT! 哈燒新鮮貨

高雄市政府民國38年以前檔案入庫囉~

該批檔案產生於民國36年至38年，內容為剿匪清鄉、懲治土豪劣紳、財政統計及稅務人員移交等相關資料，共計14卷，

歡迎多加利用！

國家檔案現有館藏介紹

國家檔案典藏新訊

法務部調查局、國防部海軍司令部及臺北地方法院等檔案即將移轉！

法務部調查局及國防部海軍司令部有關戒嚴時期涉政治偵防及不當審判案件檔案計157卷，預定99. 5.30前移轉本局。另臺北地方法院、臺中醫院以及行政院農業委員會所屬林業試驗所、畜產試驗所、家畜衛生試驗所、桃園及臺東區農業改良場、種苗改良繁殖場等機關民國38年以前檔案，計約2236卷，預定99. 6.15前移轉本局。

本局檔案移轉資訊

NEW! 獨家報導

我是檔案探險家－檔案教

檔案，但看到的只是一群亂碼而已。下圖以簡單的流程圖描述數位資料加密及解密的過程。

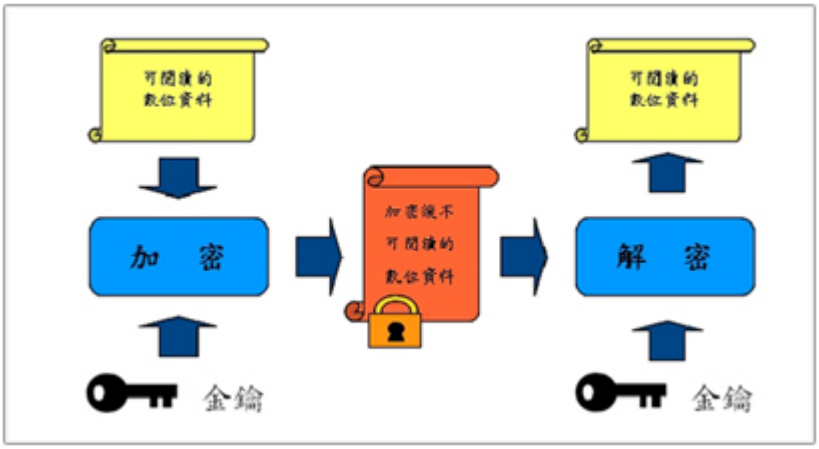

圖1 數位資料加密與解密流程圖 資料來源:作者自行整理

圖中，金鑰除了用來加密，也用來將已加密的數位資料轉換回原來可開啟及閱讀的數位資料，這個步驟也就是所謂的解密。金鑰的長度是以位元計，長度越長代表加密的強度越強，目前最廣泛使用加密演算法就是先進加密標準(AES, Advanced Encryption Standard) ，依金鑰長度又分為128位元（AES-128）、192 位元（AES-192）及256位元（AES-256）。

數位資料的加密處理可分硬體及軟體二種方式，其中加密軟體因取得成本低，故使用普及率高於硬體加密模式，以下讓大家認識幾種電腦作業系統常用的加密軟體。

（一）BitLocker

itLocker磁碟機加密，是微軟公司Windows作業系統提供用戶端電腦的資料保護功能。使用BitLocker磁碟機加密保護是透過整個 Windows 磁碟區加密的方式達成，只要將電子檔案存放在 BitLocker 保護之下的磁碟區，就會受到加密的保護，沒有金鑰是無法解開已加密的磁碟區，該電子檔案就無法以原來可閱讀的格式被開啟，而目前採用的加密演算法有AES-128及AES-256二種。

（二）FileVault

FileVault是蘋果電腦Mac OS作業系統用來保護電子檔案的功能，作用與微軟公司的BitLocker磁碟機加密軟體相同，它採用AES-128加密演算法，目前Mac OS X 10.3以上版本均內含該軟體功能。 使用FileVault時，並不會整個磁碟都加密，只有存放在使用者目錄下的電子檔案才會受到加密保護。

（三）TrueCrypt

TrueCrypt磁碟加密軟體是1套免費下載使用的自由軟體，目前支援作業系統有Windows、Mac OS 及Linux等，它比前面2種軟體支援更多種類的加密演算法，如AES-256、Serpent、Blowfish、CAST5等。使用TrueCrypt可以在硬碟或拇指碟上建立一個或多個虛擬的磁碟機，只要將電子檔案存放在該磁碟機上就會被自動加密，將來要開啟電子檔案時，就必須使用金鑰登入成功後，才可以讀取該磁碟機中的電子檔案內容。

育學習館探險之旅」已經啟動，多項大獎等您拿！

替代役公共行政役（檔案）第**81**梯次役男專業訓練

替代役公共行政役（檔案）第81梯次役男專業訓練自99.4.19-4.26假漢翔航空工業股份有限公司辦理，並於99.4.26由本局分發撥交各服勤單位。

99年度電子檔案管理教育訓練展開囉！

本局自99.4.26至7.23分別於臺北、臺中、高雄、花蓮辦理25場次之電子檔案管理教育訓練，相關資訊請瀏覽https://erecords.cisanet.org.tw。

小故事特蒐STORY

石牌與原住民的關係

居住在臺北市的市民對於「石牌」這個地名應該不陌生，這個地區不僅有著名的榮民總醫院，更因為是進入早年溫泉之鄉～北投的必經之地，因此，大多數的人都聽過這個地名；但是為什麼此地會叫「石牌」呢？其實是有一段與原住民有關的故事.....詳全文

TOP

三、如何鎖好您的電子檔案

目前TrueCrypt支援多種作業系統且取得容易，以下就該加密軟體進行簡要說明，如何使用它來保護您的可攜式磁碟或隨身碟中之電子檔案。

（一）下載安裝軟體

1.自http://www.truecrypt.org下載TrueCrypt軟體。

2.執行安裝檔。

3.接受授權聲明。

4.依安裝精靈逐步執行安裝作業。

（二）中文化

1.自http://www.truecrypt.org/localizations下載繁體中文套件。

2.將檔案解壓縮至TrueCrypt所在目錄，例如'C:\Program Files\TrueCrypt'。

3.執行TrueCrypt，並在「Settings」的功能選單裡選擇「Language」將語系改用「繁體中文」，即可完成中文化。

（三）使用TrueCrypt建立加密區

1.開啟TrueCrypt之後，選擇「建立加密區」。在出現「TrueCrypt加密區建立精靈」對話視窗後，預設為「Create an encrypted file container」，並按「下一步」。預設值「標準TrueCrypt加密區」，再按下「下一步」。

2. 選擇「加密演算法」，輸入「加密區大小」，輸入「加密區密碼」，最後到了「加密區格式化」，請依對話視窗內的訊息敘述：「請在此視窗內儘可能的移動滑鼠，移動的時間越長越好，這將會增強金鑰的加密強度」，決定後按「格式化」，並等待格式化完成。

3.建好TrueCrypt加密區後，還需經過掛載步驟。先任意點選一個磁碟代號，接著按下「選擇檔案」，並選擇剛製作出來的「TrueCrypt加密區」檔，最後再按下「掛載」即可。

4.輸入加密區所建立的密碼，再按「確定」。當成功載入TrueCrypt加密區後，在檔案總管中看起來就是一個可用的磁碟機，之後我們只要將電子檔案存放在該磁碟機，就可受到加密保護了。

四、結語

要防止電子檔案機敏資料的外洩，加密軟體確實是個好幫手。但在可攜式電腦及電子儲存媒體的使用上，仍需仰賴個人良好的使用習慣，電腦不使用時儘量關機，並妥善保存金鑰密碼及儲存裝置，並使用具複雜度的密碼，才能確保資料安全無虞。

參考資料

1.Wikipedia contributors, " Comparison of disk encryption software," Wikipedia, The Free Encyclopedia, http://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software（accessed April 19, 2010）.

2.Wikipedia contributors, " Advanced Encryption Standard," Wikipedia, The Free Encyclopedia, http://en.wikipedia.org/wiki/Advanced_Encryption_Standard（accessed April 19, 2010）.

3.Windows 用戶端技術中心, "Windows 7：資訊安全與防護", http://technet.microsoft.com/zh-tw/library/dd571075%28WS.10%29.aspx（accessed April 19, 2010）.

4.Wikipedia contributors, " FileVault," Wikipedia, The Free Encyclopedia, http://en.wikipedia.org/wiki/FileVault（accessed April 19, 2010）.

5.TRUECRYPT, FREE OPEN-SOURCE ON-THE_FLY ENCRYPTION, http://www.truecrypt.org/docs/（accessed April 19, 2010）.

TOP

徵稿訊息 | 精采回顧 | 訂閱 / 取消訂閱 | 聯絡我們

若您對檔案樂活情報有任何建議或疑惑，請聯絡：alohas@archives.gov.tw

檔案管理局 National Archives Administration