密碼學教學系統之建置

吳昌憲
沈俊仲
國立虎尾科技大學資訊管理系助理教授
國立虎尾科技大學資訊管理系研究生
cswu@nfu.edu.tw

摘要

在生活周遭時常聽到，我的電腦資料被盜、遊戲帳碼、銀行密碼和個人資料被竊取…等，但有多少人注意到這方面的問題？有誰會擔心下一個可能會是自己？大家時常說這個是機密、秘密，但下一秒就輕易洩漏出去，他們並沒有對資料做任何保護動作，來增加它們的安全性，如：用密封容器包裝起來，你認為這樣可以防止竊盜？本研究是以 MATLAB 來建置密碼學教學系統，密碼學演算法又分很多種，我們由淺至深，透過互動 GUI 畫面設計，逐步瞭解相關領域的知識。

關鍵字：資訊安全、密碼學、Matlab

一、 緒論

1.1 研究背景和動機

現今使用 3C 產品人數逐漸上升和範圍廣闊，小至幼稚園，大至的 80、90 歲的長者，沒有人不跟 3C 扯上關係。因此，人們再傳送訊息是非常方便，也快速傳遞至目的地，不管是私底下的傳訊，還是利用網路傳遞訊息…等，這些功能對現今 3C 產品來講都不是問題，像在家要靠桌上型電腦上網，才能在網路上發佈訊息，但現在不用侷限在家裡了，因為從筆記型電腦可以帶著跑後，陸陸續續也有智慧型手機和平板電腦，如果沒有使用強大功能，筆記型電腦開始慢慢被取代了，在聊天和上網部分，它們攜帶性便利在使用上也縮短時間。再傳送訊息便利的時代裡，這個過程裡充滿不知的變數，訊息是否送達目的地、是否只有指定的人才收的到、這過程是否安全呢？這些種種的問題又有多少人了解呢？當您在傳達機密或秘密時，您或許會很注意周遭環境和傳達的過程，但在一般簡單的對話或訊息卻不在意，大家對訊息的保密和認知還有段路要走，因為在新聞報導下，常聽到個人資料外漏或者帳號密碼被盜的新聞案件，這有些都是自己疏忽下所造成的，這裡我們不考慮人為因素。如果我們可以加強資訊安全的重要性，這樣我們就可以預防被盜的可能性。

1.2 研究目的

本研究是以資訊安全為基礎，再針對密碼學這部分做整合，讓更多人可以了解密碼學歷史，和有哪些加密技術是目前有在使用的…等，如何在科技發達底下防止資料外漏，就算不小心洩漏出去後，又有幾個人可以正確讀出內文呢。從基本的密碼學為基礎做起，慢慢整合其它密碼學成為一套系統，可以幫助對這項技術有興趣的研究者，也希望可以在密碼學課程中，短暫的使用在教學上，可以幫助學生們學習。

二、 文獻探討

2.1 資訊安全

1. 資訊安全問題演進

科技技術越來越進步，人們對資訊科技產生了依賴性，而這種現象到處可見，不管是坐著、躺著、趴著，甚至到行駛中的駕駛，也無時無刻看著智慧型手機。資訊科技如此的發達，有人利用這項資訊進行破壞，而這種行為對個人生活與社會造成很大的衝擊。因此，資訊安全問題隨著資訊科技的不斷創新而越趨複雜。

資訊科技是個新領域，從 1960 年代電腦才開始市場化，直到 1980 年代初期，電腦還在比較封閉的環境中，只有少數人家擁有，所以安全風險不高。在大型電腦主機的時代，資訊安全事件大多是人為操作錯誤所造成的資料遺失，或是內部人員操守問題所造成的洩密。

1980 年代個人電腦逐漸普及化，資訊安全事件也開始浮現。早期個人電腦的設計並未考慮存取控制，因此無法保護資訊的保密性與完整性。除此之外，交換使用軟碟讓電腦病毒開始出現。Elk Cloner 被視為最早的電腦病毒，在 1982 年由一位十五歲的美國學生 Rich Skrenta 寫在 Apple II 電腦上。感染媒介是軟碟，使用受感染的軟碟開機五十次，螢幕上就會出現一首打油詩。

網際網路在 1990 年代以驚人的速度成長，由於大家電腦都連結再一起，使病毒散播與駭客攻擊更加方便有效。Melissa 是 1999 年由電子郵件傳播的 Word 巨集病毒，它利用受感染電腦的電子郵件通訊錄，再發出五十封病毒郵件，因此數小時內就可以傳遍全球。另外，像 Code Red 蠕蟲利用當時作業系統的瑕疵，在 2001 年七月十九日一天內感染全球 359,000 台電腦。該蠕蟲的攻擊速度與範圍皆駭人聽聞。

較早的電腦或網路破壞者大多以炫耀技術或惡作劇為主，但在電子商務蓬勃發展的二十一世紀，他們的目的已逐漸轉變為獲取非法利益。例如，有位十九歲的俄國駭客在 1999 年侵入 CD Universe 公司的網路，竊取三十萬筆信用卡資料。在勒索十萬美元贖金未遂後，就報復性地將其中數千筆資料公布在網際網路上。2000 年九月，全球首屈一指的金融服務機構 Western Union 關閉網站五天，因為它遭到駭客入侵並盜走一萬五千筆信用卡資料。經追查發現，駭客是利用系統維修時，沒有防火牆的十五分鐘空檔入侵。一個較新的案例是美國花旗銀行在 7-11 便利店的自動提款機 PIN 碼被竊賊破解，2007 年十月後的半年間至少 200 萬美元被盜領。據調查，由於銀行新安裝的系統允許透過網際網路的維修方式，一向受慎密保護的 PIN 碼資料，疑似就是操作人員未按照正常加密規定動作，在傳輸過程中洩漏。

近年來的木馬程式、間諜軟體、釣魚網站、垃圾郵件等，大多看中商業利益，而成為攻擊目標。它們也許不像蠕蟲那麼轟動地登上新聞頭版頭條，但卻造成更大的整體經濟損失，也更難使用單一種技術來防禦它們。

2. 資訊安全管理議題

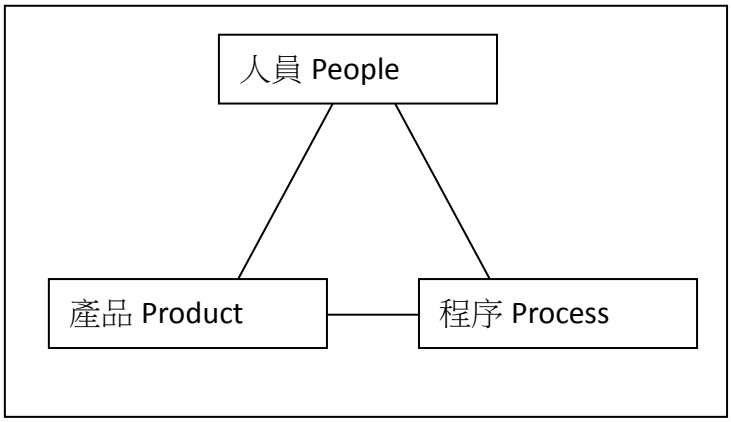

圖 1 資訊安全三 P 圖

資訊安全三個 P 的結合，用一句話來結合這三者的關係：人員必須遵守安全程序，產品才能發會最大效用。為什麼會把人員放進來，因為，人為部分的漏洞是很難避免的，常常把職業道德掛在嘴邊，雖然大多數人員都有做到，但還是要預防那小部分，教育訓練歸教育，發生後調查都是個人因素所引起。程序部分，公司有一套辦公安全機制流程，必須透過員工訓練來告知新進員工，讓人員可以實際遵守，以免發生不必要的缺失。產品部分，就是公司所引進的系統，靠這些強大的系統來維護，並在使用前舉辦職前訓練，操作人員可以融入系統裡，讓公司營運可以更加快速和順利。所以資訊安全並不是單靠科技面，還需要妥善的管理才能防範。可見這三個 P 的重要性，這過程是環環相扣的，缺一不可。

資訊安全的三元素，分別是實體安全(Physical security)、營運安全(operational security)、管理與政策(management and policies)，從這些範圍下去討論。

I. 實體安全是保護資訊與資產，是讓未經授權人員無法輕易接觸實體，如：伺服器、磁碟機和偷接電纜等，就是那些看的到、摸的到和可能被偷的實體物品。維護實體安全三個重點：
   i. 讓你的實體物品遠離被攻擊目標。
   ii. 可以偵測入侵者，以防被盜發生。
   iii. 即使系統和資料被盜後，把傷害降到最低，能立刻恢復辦公機制。

II. 營運安全在確保組織能正常正確運作，大多數資訊安全人員工作範圍，應注意以下幾點：
   i. 電腦、有線網路和無線網路的運作。
   ii. 資料和檔案管理。
   iii. 存取控制、身分認證及網路的安全結構設計。
   iv. 經常性的維護、與其它網路連結、備份計畫與復原計畫等。

III. 管理與政策是組織直接領導它的管理方向，背後需要高層管理人員支持，才能發會最大效用。以下是資訊安全政策時應可慮的項目：
   i. 行政管理政策：系統及管理員制定的標準作業流程，如升級、監控、備份及稽核等。
   ii. 軟體設計需求：制定組織採購、外包或自行開發之相關安全要求。
   iii. 災害復原計畫：受到人為或外在因素，而影響到公司損失，必須透過此計畫，讓公司在短時間內恢復並上軌道。
   iv. 資訊政策：包括資訊存取、機密等級、儲存以及機密資訊的傳遞與銷毀。
   v. 安全政策：預防未經授權人可輕易進入內部和相關配套措施。

vi. 使用者管理政策：員工在受雇期間的資訊安全相關管理制度，包括新人訓練、存取權限的設定與取消等。

2.2 密碼學

密碼學是一種將資訊可以安全傳遞和接收的相關知識，並利用數學演算法來對資料進行加密和解密。它可以儲存訊息，並在公開的網路上傳遞訊息，任何不應該看到訊息的人也很難擷取和閱讀內文。

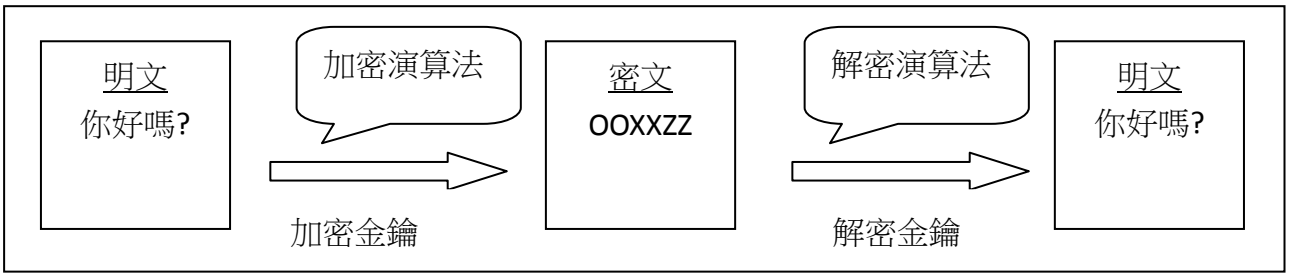

圖 2 加解密流程圖

密碼系統是由明文、密文、金鑰、加密和解密演算法所組成的。過程是由明文，經過加密金鑰加密為密文，在用密文傳遞至目的地，再透過解密金鑰解密而恢復明文。明文就是想要傳達訊息給下一個人，裡面可能含有重大機密，不能洩漏出去的資料。密文則是加密後的明文，也就是經過加密的資料，就算密文被盜竊後，必須知道加密演算法才知道如何解密，讓竊盜者不容易得知明文。加密演算法利用密鑰對明文進行加密的編碼動作的演算法。解密演算法利用金鑰對密文進行解密編碼動作的演算法。解密就是將密文還原到明文的過程。密碼破解是不需解密金鑰或者讓何偽造金鑰，就能夠將密文破解還原到明文。

1. 密碼學的目的

為什麼需要密碼學呢？密碼學可以確保資料的私密性，它也提供相關認證，可以偵測資料和訊息是否被竄改過，也可以針對傳送過程、目的地或者相關交易做身分驗證，為了背後的利益不被駭客所竊取。密碼學目的如下圖

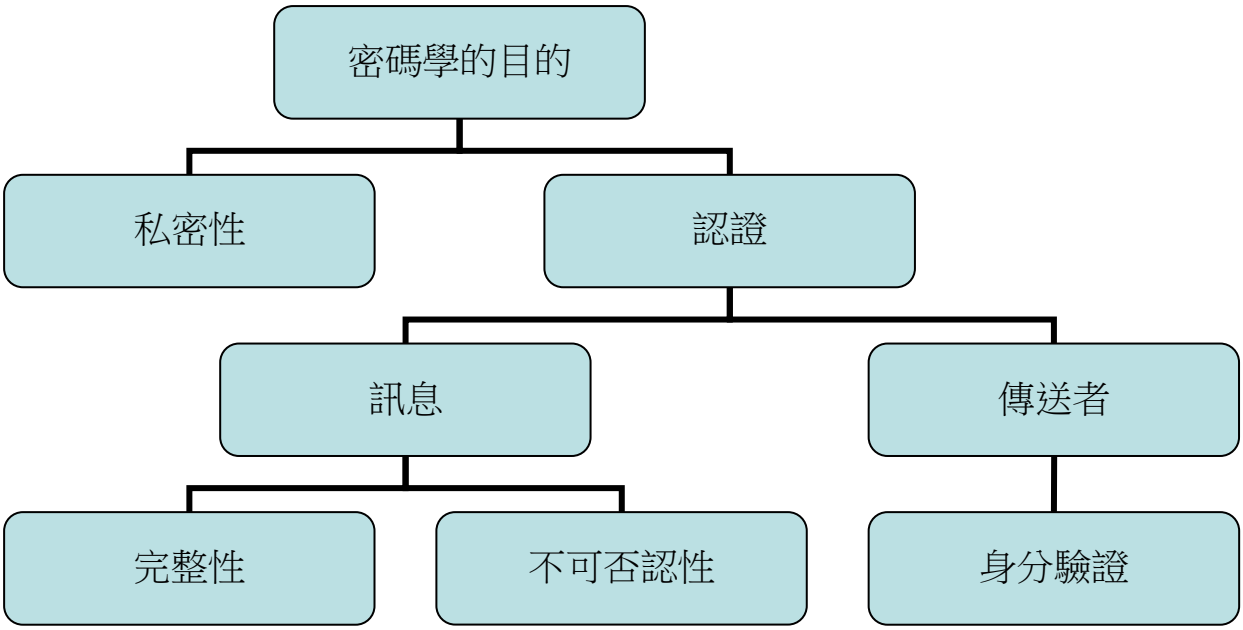

圖 3 密碼學目的樹狀圖

2. 密碼學分類

密碼學系統可跟據三種不同的觀點來分類：

I. 明文轉換密文所使用的運算方法：

i. 取代-是將明文內的每一個元素都被對應到另外一個元素，如：單字 apple 被對應到 dssoh，有時候被對應到的無法形成一個單字。

ii. 置換-將明文中的元素重新排列，如：單字 apple 經過重新排列後 apepl。

iii. 相乘-以取代與置換為基礎構成的複雜組合，達到更複雜的相乘效果。

II. 使用金鑰的個數：

i. 私密鑰匙，或傳統加密系統-加密與解密使用同一把金鑰。

ii. 非對稱性或公開鑰匙加密系統-加密與解密使用一對金鑰。

iii. 雜奏-不需要金鑰的加密技術。

III. 處理明文方法

i. 資料區段加密法-將明文分成數 n 個區段，並且對資料區段做相同的加密演算法。

ii. 資料流加密法-不會將明文切分為區段，而是一次加密資料流。常見作法將較短的加密鑰匙延展，近似亂碼的金鑰串流，再和原始資料經過 XOR 運算後，產生密文資料。

2.3 MATLAB

1. 簡介

科學研究和計算領域裡經常遇到一些複雜的數學運算，而這些運算如用計算機或手動運算的話，真是費時又費工且也不一定精確，如果可以透過電腦程式計算這些問題，能簡單又快速完成，精確度也會相對提高。MATLAB 就是解決這種複雜數學院算的強大軟體。

MATLAB 這個名詞是由矩陣(Matrix)和實驗室(Laboratory)這兩個單字的前三個字母所組成的，顧名思義，它是基於矩陣運算的軟體。它可以協助使用者輕鬆、有效率的完成資料分析及視覺化、應用程式開發、系統設計、模擬、產生程式碼以及硬體實現等繁雜工作。它像一種語言，透過

工程人員比較容易了解和學習，藉助積木般建構和解決問題的方式，透過工具箱化簡與解決目前工程和科學重要的問題。基礎是以 MATLAB 和 SIMULINK，但最強大的部分卻它是工具箱，在每一代的 MATLAB 開發上，都會新增一些工具箱，而且工具箱還不斷的在更新和改善。

2. GUI 介紹

Graphical User Interface 的縮寫是 GUI，意思是圖形使用者介面。隨著電腦技術的發展，使用者與電腦交換訊息的方式有重大改變，不只是傳統的指令方式輸入程式語言，已發展到圖形介面與使用者交換訊息。圖形化介面可以快速產生圖形和控制元件，可以隨心所欲的變更及擺設外觀。使用者不須熟悉大量的指令，只要使用滑鼠即可與電腦交換訊息，可選擇要運算的程序、控制的方式、及顯示圖形訊息的外觀，達到圖形使用者介面的程式設計。

圖形使用者介面是由按鈕、視窗、工具列、鍵盤動作等物件所構成的，藉由設計好的介面呼叫 MATLAB 來進行運算。GUI 對象通常包含三種：使用者介面控制元件、下拉式選單，和活動式選單。介面控制元件包含：按鍵、表框、工具列、文字顯示等。下拉式選單則是有各種選單和子選單。活動式選單是具有彈跳式的選單。

一個好的圖形使用者介面在設計時需有以下三個原則：

I. 簡單性：應力求簡潔、直接、清晰地呈現出介面的功能與特徵，避免在不同視窗之間進行切換。

II. 一致性：設計者保持一貫的設計風格，這樣使用者就會熟悉介面操作的環境，不用常常去適應新介面的操作。

III. 親和性：指在設計介面時，應儘量使用大家熟悉的符號與物件，就算使用者可能不了解介面的具體涵義或操作方法，但也可憑藉自己以往的經驗而自我學習來操作此介面。

應注意介面的動態性能，對於使用者操作的反應要迅速且連續，當出現運算時間比較長的情況，要有顯示等待時間的物件，並且允許使用者中斷運算。

一般在設計介面的步驟有：

I. 分析介面所要呈現的功能，明確地設計介面要達成的任務。

II. 構思與規劃介面架構，並站在使用者的角度來思考。

III.撰寫介面呈式。

測試介面程式，驗證是否有達到所需的功能。

三、 研究方法

3.1 研究流程

1. 了解資訊安全重要性：必須先去了解什麼是資訊安全，還有資訊安全的重要性。開發這套系統就是為了讓更多人了解資訊安全裡面的密碼學，讓大家對密碼學部分有一定認知。
2. 蒐集密碼學演算法：密碼學演變和創新，從凱撒使用替換密碼開始，之後分古典密碼學和現代密碼學等。
3. 規劃與設定開發環境：系統開發系統前，應先找到適當開發軟體，因程式設計軟體多樣化，所以選擇也會比較多，撰寫語言選擇也是很重要，用對了工具就可事半功倍。本系統是以 MATLAB 軟體設計開發，所以需安裝此套系統外，相關的網際網路、Win7 作業系統等不可或缺。
4. 密碼學系統開發階段：用 MATLAB 軟體去開發建置，必須是以圖形介面為主，在操作和表達面需要簡潔易懂，將繁雜的密碼學演算法，彙整成一套系統，從基本的演算法開始著手，建構好這些演

算法後，在朝更進階的部分去開發。

5. 測試、除錯及改善系統：等到系統開發完畢時，須進入測試階段，自己先做簡單的測試和除錯，等到自己確認完後，在請對密碼學有興趣的同好幫忙測試，如果有認識教師有資訊安全課程，也可詢問老師是否願意請學生幫忙測試系統，再針對這些問題下去一一解決，把系統出錯率降到最低。
6. 密碼學系統建置完成：系統建置完畢。如下圖：4

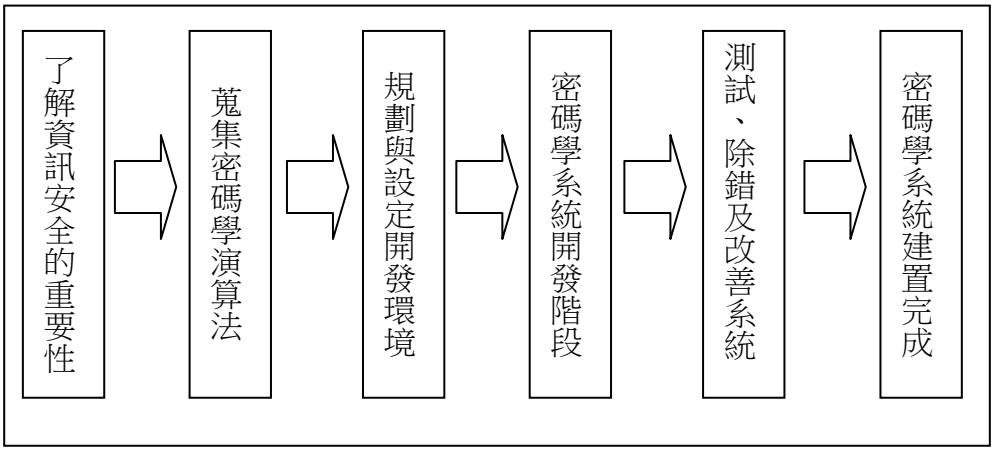

圖 4 研究流程圖

3.2 系統功能介紹

把演算法分類，針對每一種算法獨立運用，並點選上面的演算法運作，如圖 5。

1. 加密過程：在左邊的 Edit Text 輸入明文，在透過中間的加密按鈕，進行加密動作，加密後的密文會顯示在右邊的 Edit Text。
2. 解密過程：在右邊的 Edit Text 輸入密文，在透過中間的解密按鈕，進行解密動作，解密後的明文會顯示在左邊的 Edit Text。

圖 5 系統介面圖

四、 預期成果

希望這套系統建立完成時，可以幫助剛接觸的研究者上手外，或是老師在資訊安全課程中，能夠透過這套系統讓學生們了解密碼學，不會看到書上的演算法過於繁雜，而放棄資訊安全這塊重要的議題。讓更多的人了解密碼學過程，這是在建置這套系統的目的，希望大家養成習慣，可以在機密文件裡，多做一道加密的動作，並跟對方共同建立一套機制，在默契上選擇一個演算法下去做配合，或定期更換加密的方法，這樣才能增加被破解的困難度。

參考文獻

[1]三谷政昭、佐藤伸一。世界第一簡單密碼學，2009 年 5 月，世和印製企業有限公司。

[2]王后珍、張煥國、管海明、伍前紅。多變量代數理論及其在密碼學中的應用，北京工業大學學報，2010/05/01，P627~634。

[3]李軼昆、徐建波。基於密碼學的安全網絡文件系統設計，湖南城市學院學報(自然科學版)，2005/09/01，p69~71。

[4]林志賢。橢圓曲線 Pairings 之密碼應用理論，資訊安全通訊，2010/10，P32~44。

[5]郭姿君。MATLAB 程式設計與應用，2009 年 11 月，滄海書局，P1~14、P228~233。

[6]張堂賢、游上民、劉宜傑、張元瑞，ATMS 通訊安全動態加密技術研究，運輸學刊，2010/03，P51~74。

[7]潘天佑。資訊安全概論與實務，2008 年 12 月，碁峯資訊股份有限公司，P1-2~1-7。

[8]傅曉彤、張寧、肖國鎮。張 Chang 等人的消息可恢復式簽名方案的安全性分析，西安電子科技大學學報，2005/12，P920~921。

[9]羅婉平。現代計算機密碼學及發展前景，江西廣播電視大學學報，2009 年第 3 期。

魏薇。基於身份的電子郵件系統，徐州工程學院學報，2007/04，P14~17。

[10]http://avp.toko.edu.tw/docs/class/3/%E5%AF%86%E7%A2%BC%E5%AD%B8%E5%8E%9F%E7%90%86%E8%88%87%E6%8A%80%E8%A1%93.pdf