Linux 伺服器環境下 IC 卡安全電子郵件系統的設計與具體實現

楊中皇
國立高雄第一科技大學 資訊管理系
chyang@computer.org
http://www.nkfust.edu.tw/~chyang
許舫瑋、邱億陞、謝劭杰
國立高雄第一科技大學 資訊管理系
http://www.crypto.nkfust.edu.tw

摘 要

電子郵件一直是國人使用網際網路的服務中最常被應用的，但目前使用上多只停留在一些個人或企業較不重要的訊息傳遞方面，而要提升電子郵件的應用至個人隱密資料、商業機構間的交易訊息甚至是政府公文的傳遞，則有賴在傳遞過程中訊息的保密。本研究修改 Linux 作業系統環境下免費且開放原始碼的 Sendmail 電子郵件伺服器，在其原始碼中加入 AES 加解密的功能，以確保郵件傳輸時的保密性。在用戶端我們製作了一個 IC 卡安全電子郵件收發系統，在 SMTP 電子郵件協定上，加入 AES 加解密的功能，並採用 IC 卡或自製內含金鑰的硬體設備來儲存與管理 AES 私密金鑰。

關鍵字：電子郵件、AES、IC 卡、保密、網路安全

Abstract – Electronic mail or email system is by far one of the most widely used applications in the Internet services. However, due to the lack of communication security services, sensitive official document of government organizations could not be transited securely over open networks using off-the-shell email systems. In this paper, we present our effort in the design of a secure email system that is based on enhancing the *sendmail* server with AES encryption and decryption functions. At the email client side, we add AES encryption/decryption on the SMTP email protocol and use smartcard to provide cryptographic key management.

Keywords：electronic mail, AES, IC card, confidentiality, network security

壹、前言

如果電腦的發明是人類世界的第三波革命，那麼無疑的 Internet 的建立則是再一次”Revolutionize”我們的生活型態和生活方式。網路的蓬勃發展拉近了人與人之間的距離，使得”世界村”、”地球村”不再只是一個口號。無論處在何地的兩方只要各有一個 E-mail 帳號就能在彈指間互遞訊息，這樣快速和便利的傳播方式使得許多人利用電子郵件來取代傳統的傳播媒介（如實體信件、電話）作為溝通的管道，而政府機關和一般公司更可使用電子郵件來作為公文和訊息傳遞的媒介，如此可節省其實體紙張的浪費又可加快公文或訊息傳遞的速度。

但電子郵件真是百利而無一害嗎？相信很多人都有透過郵件來申請進入某一商業網站或訂閱電子報，但在傳送的過程中，你我的個人資料很可能已被有心人士截取。一般電子郵件收發軟體以帳號與通行碼(password)方式做權限控制，但通行碼權限控制有其缺點，意即若使用者為了增加其安全性而設定長度較長之通行碼，以防止他人在旁窺伺進而記取盜用，相對的使用者本身亦難以記住密碼，甚或有人將其寫下以便使用，如此便會失去保密意義；相反的，若使用者為了便於熟記，而使用如生日、身份證編號・・・等易記之通行碼，則相對的亦容易被有心人士利用各種方式盜取。有心人士甚至只要利用簡單的網路封包掃

瞄工具就可在傳輸雙方途中截取使用者帳號與通行碼或信件內容，這就好比如我們現在使用的明信片一樣，只要想看內容就可輕易的觀看，不會在明信片上留下任何的痕跡。

如果我們對於電子郵件的要求只停留在一般個人非重要訊息的傳遞或商業機構的廣告信函那麼電子郵件的安全性就不值一顧了，但我們如果想將電子郵件如前文所述的應用在商業機構與顧客的交易訊息或政府公文資訊的傳遞，那麼電子郵件的安全性[1-3]就不容我們忽視了。所以我們探討 Unix/Linux 作業系統上最常被採用的電子郵件伺服器 Sendmail [4]，為其加上所缺乏的安全機制，使其不論是被公司或政府機構所使用都能保障使用者個人資料的安全性。選擇 Sendmail 郵件伺服器進行安全實作的主要理由是因為在 Web 環境下電子郵件傳送代理服務以 Sendmail 的佔有率最高，同時 Sendmail 為免費且開放原始碼的軟體，使本研究可在無智慧財產權的考量下分析其內部流程和運作機制，進而加入適當的安全機制。

傳統上，密碼學(Cryptography)之技術主要用於軍事與外交方面，研究成果也常因所謂的〝國家安全〞因素，而無法公開。然而九０年代以後，隨著網際網路(Internet)與全球資訊網(WWW)的極速成長，網路安全問題也一再浮現出來。早期的網路安全措施多是倚賴封閉式的網路與隱藏系統設計的細節，並未在系統設計時便考量其安全性。然而隨著上網人口的增加，新聞群組(newsgroup)與電子佈告欄系統(Bulletin Board System, BBS)的風靡，使得全球性駭客族可以立即交換資訊、分享經驗。也因此近年來電腦網路被入侵、資料被竄改的情事在國內外不斷地發生。

使用密碼學技術對網路提供最佳的安全防禦，目前微軟公司(Microsoft)與網景公司(Netscape)的全球資訊網瀏覽器(WWW browser)也都配備這種技術。密碼系統中如果加密金匙與解密金匙兩者中有一者可以公開，則稱之公開金匙密碼系統 (public-key cryptosystem)。如果加密金匙與解密金匙兩者皆須保密，則稱之為私密金匙密碼系統(private-key cryptosystem)，其中最著名的系統為 DES (Data Encryption Standard)[5]。早期的密碼系統都是私密金匙密碼系統，而公開金匙密碼系統則是到 1976 年才被發明。西元 2000 年 10 月美國政府機構 NIST 正式宣布選用 Rijndael 演算法作為 AES (Advanced Encryption Standard)，且於 2001 年成為美國聯邦資訊處理加密標準[6]，逐步取代行之已久且近年來安全性受到質疑之 DES。但是世界上多數高科技國家，如美國、日本、法國，仍然對具備加解密保密功能的軟硬體裝置實施出口管制，或僅允許安全性較差之產品輸出。而國內進口的兼具保密功能的產品的安全性也一再令人質疑。所以我們確實有必要建立本土化的資訊安全基礎建設(Information Security Infrastructure)。

密碼學技術是目前所知唯一能有效地在不安全的網路上安全傳遞訊息的工具，在加入 AES 保密機制後的電子郵件伺服器與用戶端，就能確保兩端通訊間電子郵件訊息的保密性，使得電子郵件的應用方式能簡潔而又安全。

貳、電子郵件系統簡介

在現今電子郵件系統，主要由三類程式互相搭配而組成，這三類程式分別為 MDA、MTA、MUA 程式，下列分別說明三類程式的用途：

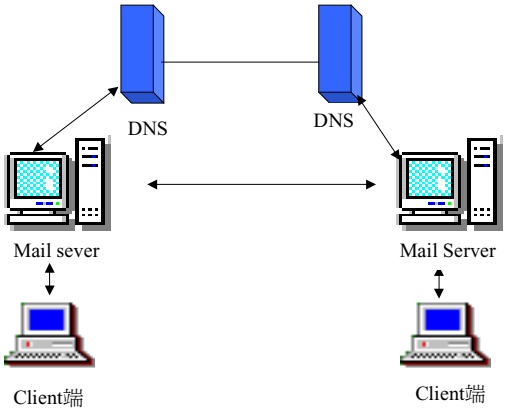
(1)MDA（Mail Delivery Agent）：郵件寄發代理者，此程式是負責 E-mail 的實際寄發。當 Mail Server 欲寄出 E-mail 之前，首先須將 E-mail 送交給 MDA 處理。MDA 如發現收件者是本機上的使用者則直接將郵件送至使用者的帳號目錄下，若發現為外部使用者，則將 E-mail 暫送至郵件佇列（mail queue），等候 MTA 傳送郵件。

(2)MTA（Mail Transfer Agent）：郵件傳輸代理者，此程式的用途是直接或根據對方 DNS 的 MX 紀錄與遠方的郵件伺服主機進行連結，並且以 SMTP 協定傳遞郵件給對方的 Mail Server。當對方郵件伺服主機的 MTA 程式收到郵件後，則先轉存到 Mail box 等候使用者取用郵件。

(3)MUA（Mail User Agent）：郵件使用者代理者，此程式的功能為在用戶端幫助使用者接收、發送和管理郵件的操作介面。目前較知名的 MUA 軟體有 Microsoft 的 Outlook Express 和 Unix-like

下的 pine 等等。

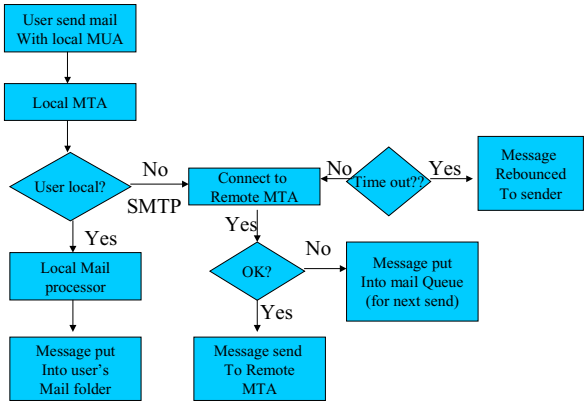
目前因為 MDA 和 MTA 工作性質關連性很強，所以現今的郵件伺服系統大都將此兩類程式整合在一起，而目前 MTA 軟體就泛指伺服器端的郵件伺服軟體，除本研究所使用的 Sendmail 其它還有 qmail、Postfix 等，其作用皆是負責寄發、接收、儲存和轉送郵件。



圖一：現今電子郵件系統架構

SMTP（Simple Mail Transfer Protocol）[7] 是 Internet 上主要的電子郵件通訊協定，當用戶端郵件軟體或伺服器端的 MTA 將郵件傳送出去時，就是使用此協定做為彼此溝通的媒介，才能在 Internet 上傳遞郵件。此協定是一種 Push 式的郵件通訊協定，把不屬於自己的郵件推送出去，逐漸的讓郵件越來越靠近目的主機，傳到預定的 Server 中。

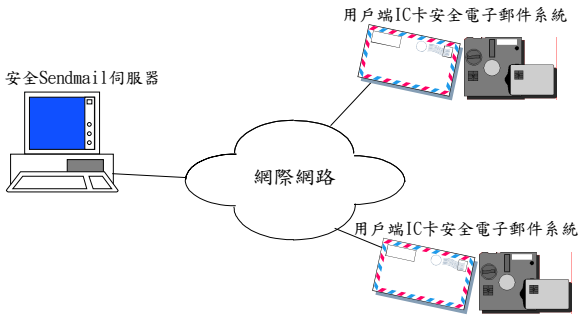
SMTP 協定是以數字與>>>字元開頭的訊息組成一筆交談記錄，本地端對遠端機器所說的話是以>>>字元做為開頭，而遠端機器所答覆的訊息則是以數字開頭。我們簡要說明交談之內容：首先傳送方連上了遠端的主機時，它會等遠端的機器啟始彼此間的交談，遠端機器送出 220 的數字和它完整合格的主機名稱，表示它已經準備好了，如果遠端機器也在執行 sendmail，它會說明程式的名稱與其版本。它還會表示已經準備好，並且提供該地區的日期與時間。接下去本地端送出 EHLO 這個字與它的主機名稱，EHLO 的 E 表示本地端的 sendmail 也可使用 ESMTP，然後遠端機器回覆 250，表示你的機器已經被接受了，然後列舉它所支援的 ESMTP 服務項目，再來本地端機器送出是那位傳送者要送出郵件，而目的方會送出 Sender ok 讓交談持續下去。再下去本地端表示要傳送到對方主機上的那一位使用者，假如目的方主機有這位使用者則送出 Recipient ok，否則會送出 User unknown 的錯誤訊息，此時本地端則可利用 DATA 指令表明要開始傳送郵件內容了，最後目的會分配一個佇列識別碼給它所接受的郵件，並將該識別碼顯示出來。圖二說明一般電子郵件的傳送流程。



圖二：一般電子郵件的傳送流程

參、系統架構

本 Linux 伺服器環境下 IC 卡安全電子郵件系統是由安全 Sendmail 伺服器與用戶端安全電子郵件系統這兩部份所組合，其架構如圖三所示。

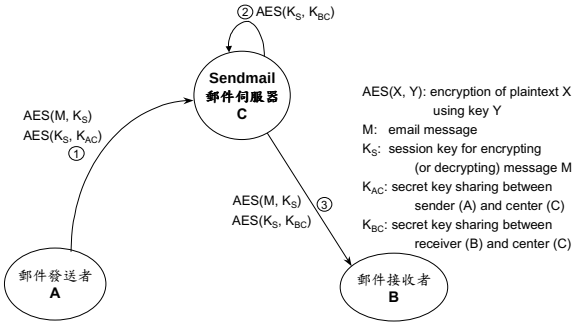


圖三：Linux 環境下 IC 卡安全電子郵件系統

本研究假設系統內所有的用戶的電子郵件帳號位於同一 sendmail 郵件伺服器上。這種假設猶如 VPN (Virtual Private Networking) [8-9] 使用公眾網路來模擬企業私用網路，達到方便而且安全的網路溝通。企業在外面拜訪客戶的銷售人員、在家上班的員工、出差在外的主管，可透過此安全電子郵件系統經由公眾網路與公司內部主管或同仁安全通信。電子郵件的收件人和寄件人必須事先在金鑰分配中心上面註冊自己的個人電子郵件帳號資料和取得自己與金鑰分配中心共享的私密金鑰。

金鑰分配中心（Key Distribution Center，KDC）[10]為具公信力第三者（Trusted Third Party），KDC 與系統內所有電子郵件的使用者共享有一把不為他人得知之 128 位元 AES 私密金鑰。為了提供郵件在傳輸時的隱密性，用戶端系統在郵件寄出之前會先產生一串 128 位元的隨機字串稱為會談金鑰 （Session Key, *Ks*），再以 AES-128 演算法對郵件內容加密。

寄件用戶端系統然後以其與KDC共享之金鑰將會談金鑰加密，加密過的電子郵件及加密過的會談金鑰一起送至 Sendmail 伺服器。修改後的Sendmail伺服器透過KDC解密取出會談金鑰後再以收件人與 KDC 共享之金鑰加密，然後直接將加密過的電子郵件及加密過的會談金鑰存送至使用者的帳號目錄下。寄件戶端系統加密過程如圖 4 所示，加強安全功能後的 Sendmail 伺服器同時扮演 KDC 的角色。



圖四：安全 sendmail 伺服器同時扮演 KDC 的角色

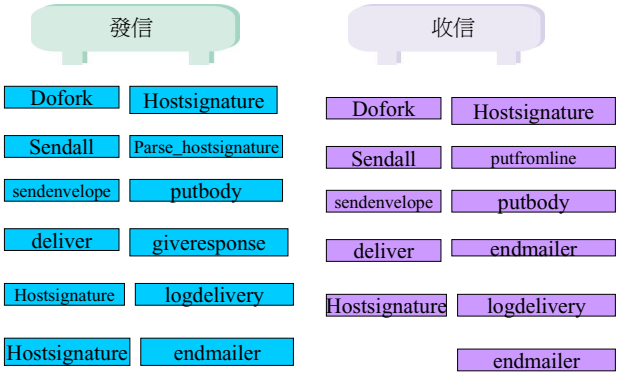
當收件人收到加密郵件時，先利用收件人與 KDC 共享的的私密金鑰來對會談金鑰解密，然後利用解密後的會談金鑰將被 AES-128 所加密的郵件內容予以解密。

IC 卡[11-14] 記憶容量可達數千位元組，資料可重複多次寫入或更新，具有發展為多目的、多功能卡的潛力。相對於 IC 卡，目前市場上較普遍之磁條卡的記憶容量僅約為一百多個位元組。所以 IC 卡與目前常用的磁條卡比較起來具有難以偽造與記憶體容量較高的優點，然而價位也較高。IC 卡在交通、金融、醫療等的應用日趨廣泛，一張 IC 卡不僅可用做身份識別，也可提供門禁管制、電子郵件(電子公文)、圖書借還書、成績輸入與查詢等功能，同時 IC 卡讀卡機的價格也日益便宜，這使得 IC 卡越來越適合網路安全應用。

我們將寄件人與收件人與KDC共享的私密金鑰儲存在個人的 IC 卡或軟碟片中。透過 IC 卡讀取私密金鑰時，系統會要求使用者輸入 IC 卡通行碼(password)，通行碼正確時才能獲得授權進入 IC 卡讀取資料。驗證通行碼的工作由 IC 卡內部完成，因此駭客無法單純的經由破解安全電子郵件收發系統來取得 IC 卡密碼以及使用者的私密金鑰。

肆、具體實現

Sendmail 是在 Unix 或 Linux 作業系統平臺下對電子郵件伺服器的實作。選擇 Sendmail 最主要一點是 Sendmail 是免費的，而且有完整的原始碼。而就目前的市面上商業或是免費 email 伺服器應用方案來看，Sendmail 被越來越多的企業界使用。本研究主要是將保密功能加入到原來的 Sendmail 郵件伺服器中，所以目前並不打算修改原有的程式流程，只將需用到的程式或變數加入保密功能後再將其放回原有的流程中，儘量不更動原有的流程。圖 5 為執行收發郵件時，Sendmail 伺服器程式之相關函式執行順序。

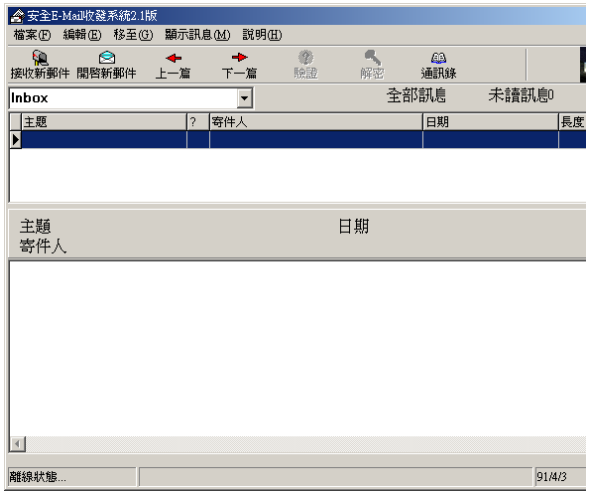


圖五：收發電子郵件時 sendmail 伺服器執行相關函式順序

由上圖五可見 Sendmail 伺服器程式收信或發信執行到的函數是非常相似，而在收發信時所共用的變數非常的多。我們主要修改傳送 mail 的子程式"**deliver.c**"原始碼，加入 AES 加解密及 KDC 的功能。

在用戶端我們採C++Builder 5.0 [15] 作為軟體主要開發工具，系統是在 Windows 98/2000 平台下發展。讀卡機我們採用兩種，一為 Fischer 公司的 Smarty IC 卡讀卡機[16]，它在形狀大小上跟 3.5 吋磁碟片一樣。只要將 IC 卡置入讀卡機後，再將此讀卡機插

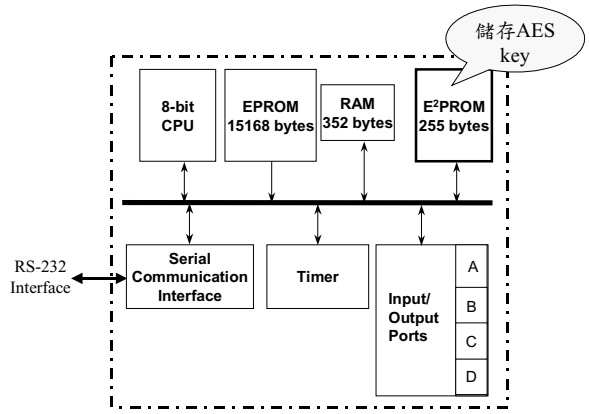
入電腦 3.5 吋軟碟機即可透過 PC 操作。另一種為符合 PC/SC 1.0 [17] 規格的讀卡機。前者使用較簡便，但因產品有專利故較貴；後者透過 RS-232 或 USB1.1 的介面纜線連接到電腦，價格較便宜。



圖六：用戶端安全電子郵件系統主畫面

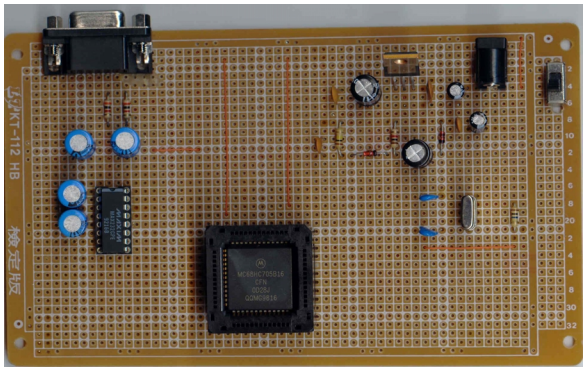
以 C++Builder 開發的用戶端的主畫面顯示於上圖六。用戶可設定電子郵件伺服器的 IP 位址及選擇郵件傳送時是否加密，也可設定通訊錄的內容。加密或解密電子郵件則需透過 IC 卡或是軟碟片的方式輸入正確的通行碼讀取與 KDC 共享的私密金鑰。

除了IC卡外。我們也於具備八位元6805中央處理位元之摩托羅拉公司 MC68HC705B16 [18] 單晶片微處理器(microcontroller)進行低成本硬體的具體實現。MC68HC705B16內部結構如圖七，提供八位元的6805微處理機，同時此單晶片內含 E^2PROM可動態儲存AES金鑰，甚至有一次燒錄(one-time programmable)裝置可由使用者自行燒錄韌體，且單價便宜。



圖七：MC68HC705B16微處理器內部結構圖

我們的硬體雛型說明於圖八。受限於Linux系統介面開發的困難，我們的硬體目前以RS-232介面與PC做AES加密資料交換。



圖八：以MC68HC705B16單晶片為基礎的安控硬體雛形

128位元金鑰之AES (AES-128)演算法的於MC68HC705B16具體實現也已完成[19]，金鑰安排(key schedule)時間為0.95 ms，每個128位元區塊加密時間則為4.3 ms。表一列出我們以組合語言撰寫AES-128程式於MC68HC705B16及MC68HC908AB32 [20]及H8/3113智慧卡晶片[21]的執行效率，其中我們假設MC68HC705B16晶片內部時鐘(clock)為允許之2.1MHz，MC68HC705B16為8MHz，而H8/3113 晶片內部時鐘假設為5MHz。

表一: 128位元金鑰之AES於三種單晶片微處理器上之執行效率

單晶片型號	金鑰安排(key schedule)時間	每個區塊(block)加密時間	加密處理速度
Motorola MC68HC705B16	0.95 ms 2000 cycles	4.3 ms 9000 cycles	30 Kbits/s
Motorola MC68HC908AB32	0.22 ms 1759 cycles	0.9 ms 7258 cycles	141 Kbits/s
Hitachi H8/3113 (IC卡)	0.43 ms 1080 cycles	1.67 ms 4180 cycles	76 Kbits/s

伍、結論

網際網路有著跨國界、跨地區、２４小

時全年無休的效率以及卓越的分佈性，但是除非能建立一套安全且便捷的制度，否則網路應用將難以有突破性的發展。本研究中實作了一套安全而易於實施的電子郵件系統，所有流通於用戶端與伺服器端二方之間的電子郵件資訊流，都使用密碼學技術將其保護。

雖然 56 位元的 DES 為目前全世界使用最廣泛相當強的加解密演算法，但隨著電子科技的發展與電腦運算速度的提升，設計破解 DES 的特殊硬體或以多部電腦合作破解 DES 的構想與實驗近幾年來一再被提出，使得 DES 系統的安全性受到質疑。這也使得以 DES 為密碼演算法機制的系統安全性堪虞，所以我們改用去年成為美國密標準的 128 位元 AES 加解密演算法。

我們以 sendmail 這種開放式原始碼的軟體進行安全伺服器的具體實現。我們安全電子郵件的用戶端使用低成本的硬體自製設備或 IC 卡作為金鑰管理與儲存的工具，使得金鑰管理更完善，免去使用者直接保管金鑰的麻煩。

致謝

本研究部分成果承蒙國科會計畫（NSC 90-2213-E -327-008）的經費補助，特此致謝。

參考文獻

1. C. H. Yang, S. L. Yen, H. D. Liu, K. Liu , B. S. Jeng, K. Y. Chang, M. S. Chang, Y. L. Cheng, J. L. Liang, and D. M. Shien, “Secure Official Document Mail Systems for Office Automation,” *Proc. 31st Annual 1997 International Carnahan Conf. On Security Technology*, October 1997, Australia, pp. 161-164.
2. Stephen T. Kent, “Internet Privacy Enhanced Mail,” *Communications of the ACM*, Vol. 36, No. 8, August 1993, pp. 48-60.
3. Bruce Schneier, *E-Mail Security*, John Wiley & Sons, Inc., 1995.
4. Sendmail, http://www.sendmail.org/
5. National Institute of Standards and Technology, Federal Information Processing Standard (FIPS) 46-3, *Data Encryption Standard*, October 25, 1999, http://csrc.nist.gov/fips/ fips46-3.pdf.
6. National Institute of Standards and Technology, “Advanced Encryption Standard (AES),” Federal Information Processing Standard, *FIPS PUB 197*, November 26, 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
7. Jonathan B. Postel, *Simple Mail Transfer Protocol*, RFC 821, 1982.
8. Paul Ferguson and Geoff Huston，“What is a VPN?”, http://www.employees.org/~ferguson/vpn.pdf , 1998.
9. Naganand Doraswamy and Dan Harkins， *IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks*, Prentice Hall PTR,1999.
10. William Stallings, *Cryptography and Network Security: Principles and Practice*, 2nd edition, Prentice-Hall, Inc. 1999.
11. W. Rankl and W. Effing, *Smart Card Handbook*, 2nd edition, John Wiley & Sons, 2000.
12. 楊中皇，校園 IC 卡的資訊安全系統設計，*第十屆國際資訊管理學術研討會論文集*，1999 年 6 月，pp. 614-618。
13. 楊中皇，以智慧卡為基礎的安全 XML 文件交換，*第九屆全國資訊安全會議論文集*，1999 年 5 月，pp. 142-148。
14. Chung-Huang Yang, "On the Design of Dual-Interface Campus Smart Cards," *The 2000 Symposium on Cryptography and Information Security (SCIS 2000)*, January 26-28, 2000, Okinawa, Japan, Section D32.
15. Borland C++Builder, http://www.borland.com/bcppbuilder/
16. http://www.smartdisk.com/smarty.html
17. PC/SC Workgroup, http://www.pcscworkgroup.com/
18. *MC68HC05B4/705B5/05B6/05B8/(7)05B16/705B16N/(7)05B32 Technical Data*, Rev. 4, Motorola Ltd., January 1999. 參見 http://www.mcu.motsps.com/.
19. 楊中皇、蔡金鳳，新一代對稱式密碼學演算法於智慧卡上的具體實現，第十一屆全國資訊安全會議，2001， pp. 199-206。

20. *MC68HC908AB32 HCMOS Microcontroller Unit*, Rev. 1, Motorola Ltd., August 2000. http://www.mcu.motsps.com/ or http://e-www.motorola.com/brdata/PDFDB/docs/MC68HC908AB32.pdf.
21. *Hitachi Single-Chip Microcomputer H8/3113 Hardware Manual*, Hitachi Ltd., 1998. 参見 http://www.hitachisemiconductor.com/sic/jsp/japan/eng/products/mpumcu/816bit/index.html.