第一章 安全性資訊系統簡介

本章以建立一套安全性資訊系統為主題，探討如何整合資訊與網路安全的相關技術，期望能讓讀者對本書內容有概括性的認識。

1-1 何謂安全性資訊系統

資訊系統是電子化企業（或政府）的命脈，無論由 2~3 位員工的小型店家到上萬人以上的大型公司（或組織），皆需昂賴資訊系統來管理整個公司的業務。資訊系統已是目前公司行號的最大資產，它運作得妥當能為公司牟取豐富利潤；但它如有任何瑕疵也可能造成公司巨大的損失，甚至導致公司倒閉。由此可見，如何建立一套『安全性資訊系統』（Secure Information System）是目前工業界上非常重要的課題。

利用資訊系統取代人工作業，已有一段不短的時日了，為何目前才被突顯它的安全性呢？早期資訊系統大多屬於封閉性環境，僅侷限於組織內運作，鮮少與公司外其他系統連線，或共同處理事務。但近年由於網路科技發達，公司行號之間講求合作生產、銷售，減低成本並提高效率。目前幾乎沒有一套資訊系統可以置身自我環境之內，而必須隨時透過網路與其它系統連線，並共同處理事務。譬如，目前國際化商業系統裡，講求產銷夥伴之間共同合作，各個公司之間必須建立生產鏈管理系統。當上游公司輸入某一張訂單明細表之後，各個生產夥伴公司及時收到零件訂單，並排定生產日期表。這些公司也許分散於全球各地，它們之間的資訊系統必須整合連線，並共同處理這些業務，當然需要一套安全性較高的資訊系統來承擔。

總而言之，由於網路的方便性，由原組織內的管理系統，跨越到多個組織之間的電子化管理環境。一般公司行號透過網路結合全球各地分公司或商業夥伴成為一個電子化公司；政府單位透過網路提供許多服務項目，讓人民可透過網路請求辦理各項事務，成為一個完整的電子化政府。由此可見，網路應用不僅是電子商務或電子化辦公室，已延伸到人民的生活領域時，它的安全性更不容忽視。我們相信沒有盡善盡美的安全技術，唯有不斷的研究及改良新的技術，才能嚇止網路犯罪的破壞與入侵行為。尤其，網路通

訊已成為國家最重要的經濟動脈，癱瘓網路系統的破壞力，已不亞於飛彈的攻擊。因此，無論是網路工作者、電子商務者、軍事工作者、或情報者等等，都必須具備網路安全的基本常識。本書僅著重於網路安全與資訊安全技術的介紹，至於相關法律問題，讀者應該多多參考網路犯罪法令規章，以及其他防護制度的規範，畢竟『人事』管理才是網路安全的最大漏洞。

如何建立一套『安全性資訊系統』？許多文獻裡提出很多關於『網路安全』(Network Security) [2, 6, 11, 17, 18, 64, 65, 82, 135, 136, 138]的相關技術。作者依據這些網路安全技術為基礎，提出一個簡單的構想，如圖 1-1 所示。也就是說，欲建構一套安全性資訊系統，應由下列 5 個重點來考量：

- 安全性作業系統：作業系統本身是否提供有安全性機制，或安全性等級如何。譬如，用戶認證、資源授權、日誌管理或稽核檢視等等。
- 安全性私有網路：企業網路是否具有防範被入侵與攻擊之能力，譬如建構防火牆或入侵偵測系統。
- 安全性電子化系統：電子化系統是否具有訊息隱密性、完整性、確認性、以及不可否認性功能。
- 安全性電子商務：電子商務系統是否具有防範偽造、篡改、確認交易雙分身分之能力。
- 安全性系統管理：各個安全性系統皆需要一套自動化管理系統，隨時監視系統的運作情形，並檢視可能出現的不安全交易行為。

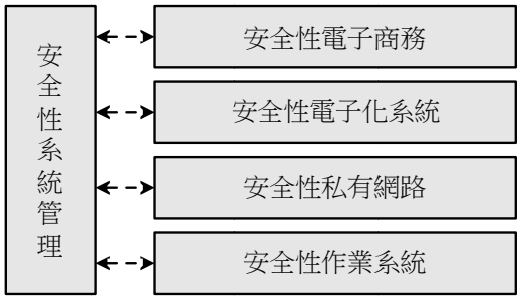


圖 1-1 安全性資訊系統的內涵

至於安全技術而言，大略可區分為『資訊安全』(Information Security，或稱訊息

安全）與網路安全。前者較著重於防護攻擊者詐騙、竄改、偽造、與否認交易等行為；然而網路安全則較重視防盜的行為。也就是說，攻擊資訊安全者大多是尋合法路徑（以技術層面而言）來達成目的，至於攻擊網路安全大多循非法路徑來達成。由此可見，資訊安全較屬於隱形的安全措施，不像網路安全的目標那麼顯著，兩者之間的重要性並沒有所謂的孰重孰輕，僅是從事的技術不同而已，但依然存在許多相似地方，兩者是不可以分開的，必須整合在一起。接下來，依照圖 1-1 簡略介紹，建構『安全性資訊系統』的相關技術如何。

1-2 安全性工具

既然安全性系統須達到隱密性與不可否認性等等功能，則須密碼學相關工具輔助才能達成，以下將簡略介紹之。

1-2-1 密碼系統

無論介紹何種安全性系統環境，『密碼學』（Cryptographic）[88, 129, 133, 136]總是離不開的課題。『密碼系統』（Cryptosystem）即是利用密碼學理論發展出來的資訊安全工具。密碼系統將明文編碼成一些沒有意義的文字或數字的密文之後，再傳送給接收端；接收端再依據原來雙方協議好的編碼方式，將密文解碼回原來的明文。攻擊者不知道編碼技巧（或編碼鑰匙，Key），則無法得知盜取訊息中的傳輸內容。如此達到隱密性的傳輸功能，但它的功能並非僅如此而已，其他功能本書還會陸續介紹。利用密碼學製作出來的隱密性功能的運作如下表示：

明文（Plaintext）：M

密文（Ciphertext）：C

加密編碼（Encryption）：E

解密編碼（Decryption）：D

加密鑰匙（Encryption Key）： K_1

解密鑰匙（Decryption Key）： K_2

編碼與解碼的過程如下：

加密過程：$C = E_{K1}(M)$

解密過程：$M = D_{K2}(C) = D_{K2}(E_{K1}(M))$

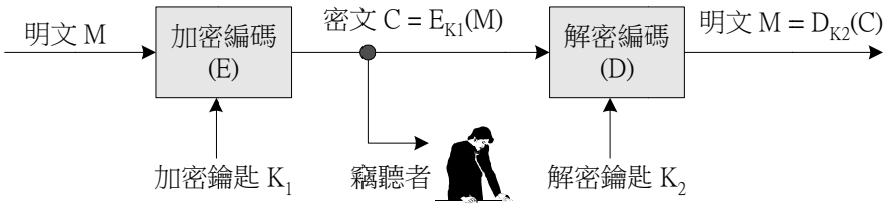


圖 1-2 典型密碼系統的功能圖

然而，發送與接收兩者之間所採用的加密/解密編碼技巧必須是互相搭配的，鑰匙的規格也必須是一致的。因此，隨著不同應用系統的需求，『密碼系統』（Cryptosystem）主要可區分為下列兩大類。

【秘密鑰匙系統】

『秘密鑰匙密碼系統』（Secret Key Cryptosystem，或稱為秘密金鑰系統或密鑰系統）表示加密與解密是使用同一把鑰匙（如圖 1-2 中 $K_1 = K_2$），而這把鑰匙必須隱密地分送給通訊雙方；參與通訊者必須安全的保護這把鑰匙，絕不可洩漏給其他不相干的人，故而稱之。然因為加密與解密是採用同一把鑰匙，又可稱為『對稱式密碼系統』（Symmetric Cryptosystem）或『單一鑰匙密碼系統』（One-Key Cryptosystem）；然而秘密鑰匙密碼系統係採用傳統式的替代與移位技術來組成，此系統又稱為『傳統密碼系統』（Conventional Cryptosystem）其特性歸類如下：

◈ 訊息隱密性：此系統主要用於資料加密使用，以達到訊息隱密性功能。

◈ 鑰匙隱密性：此系統的鑰匙絕不可以洩漏給他人知道，否則便失去隱密性功能。

◈ 鑰匙長度短：雖然鑰匙的長度越長安全性越高，但為了提高加密與解密演算法效益，一般都不會採用太長的鑰匙長度。

◈ 鑰匙分配困難：欲將秘密鑰匙傳送給通訊的對方，是一件非常困難的事，必須仰賴其他裝置或協定運作才可達成。

◈ 訊息確認的功能：在雙方共享一把秘密鑰匙的情況下，可確認訊息的完整性與鑑定

性，但無法達到不可否認性。

◈ 常見的演算法：DES、DESX、Triple-DES、Blowfish、IDES、RC2、RC4、RC5 與 AES。

秘密鑰匙密碼系統是資訊安全最基本的工具之一，但它究竟是專門的研究領域，本書將以最簡潔的方式，讓讀者了解密碼系統的特性及功能，並於第二、三章介紹幾個較常用的秘密鑰匙系統。

【公開鑰匙系統】

『公開鑰匙密碼系統』(Public-Key Cryptosystem，或簡稱為公開金鑰系統、公鑰系統)表示系統 (或使用者) 中的鑰匙是成雙成對的，一把為『公開鑰匙』(Public Key，或稱公開金鑰)，它可以在網站或公開目錄上 (如電話簿功能) 公佈給他人知道，甚至愈多人知道愈好；另一把為『私有鑰匙』(Private Key，或稱私有金鑰)，持有人必須完全隱藏著這把鑰匙，絕對不可洩漏給他人知道。兩把鑰匙互為加/解密功能，亦即，如果利用公開鑰匙向資料加密，則必須利用相對應的私有鑰匙才可以解密，反之亦然。因為加密與解密鑰匙不相同，此系統又稱為『非對稱式密碼系統』(Asymmetric Cryptosystem) 或『雙鑰匙密碼系統』(Two-Key Cryptosystem)。

我們將公開鑰匙密碼系統的特性歸類如下：

◈ 資料隱密性功能：可以使用公開或私有鑰匙對資料加密，再利用相對應的公開或私有鑰匙解密；但因鑰匙長度較長，加密與解密的時間較長，因此僅限制於對短訊息加密使用。

◈ 鑰匙長度較長：一般在公鑰系統的應用之下，明文、密文、密碼演算法、以及公開鑰匙都是長時間暴露於公眾之下；為了克服暴力攻擊，鑰匙長度不得不較長一點。

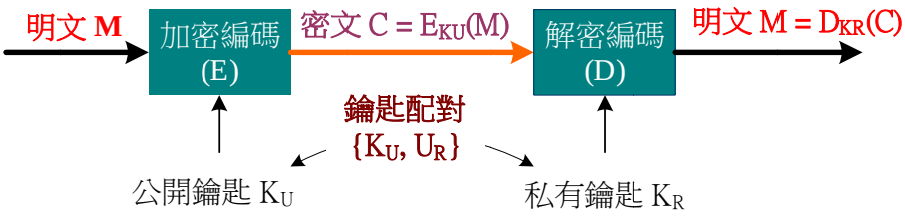
◈ 鑰匙分配容易：鑰匙持有人必須將公開鑰匙公佈出來，任何人都可以索取所欲通訊對象的公開鑰匙，因此，鑰匙分配問題較為容易。

◈ 可達到不可否認性的功能：這也是公鑰系統最主要的應用之一，可利用公鑰系統來簽署數位簽章，達成訊息的完整性與不可否認性。

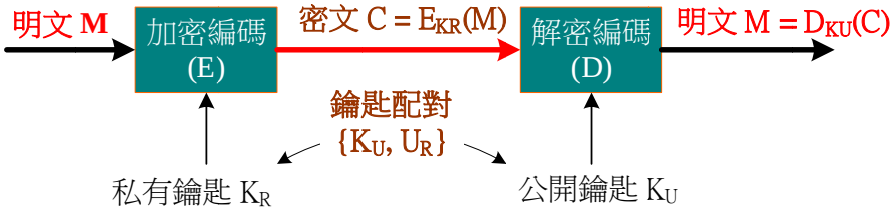
◈ 常見的密碼系統：RSA 演算法、Diffie-Hellman 鑰匙交換演算法、DSA 演算法、

ElGamal 與 DSS 演算法等等。

(a) 利用公開鑰匙加密



(b) 利用私有鑰匙加密



公開鑰匙密碼系統已不再採用傳統式的移位與取代技巧，而是以數論（Number Theory）理論中的指數同餘運算，來推演出加密演算法，因此，又稱為『現代密碼學』（Modern Cryptosystem）。本書將在第四章提出幾個較常用的演算法，說明公開鑰匙系統的基本原理。

1-2-2 雜湊函數

除了密碼系統之外，『雜湊函數』(Hash Function)乃是資訊安全中不可或缺的工具。雜湊函數是將一個不定長度的訊息，轉換成一個固定長度的雜湊碼(如圖 1-3 所示)。而此雜湊碼可以代表著原來訊息，進一步亦可作為完整性檢查或數位簽章使用。雜湊碼是由訊息的內容演算而來的，一般又稱為『訊息摘要』(Message Digest, MD)。我們以 M 表示輸入的訊息、H 表示雜湊函數、h 表示演算後的雜湊碼，其關係為：

$$h = H(M)$$

我期望輸出的雜湊碼 h，能隨輸入訊息 M 而改變，並且該值是無法仿冒的，類似人類『指紋』的功能一樣，當然要達到這個功能，主要關鍵在於雜湊函數的複雜度。因此，雜湊函數必須具備下列功能：

◈ 固定長度輸出：雜湊函數必須對任意長度的訊息，產生固定長度的雜湊碼。

◈ 單向雜湊：如果給予雜湊碼 h，在計算上無法找出一個訊息 M，使其符合 h = H(M)；

此特性稱之為『單向雜湊』(One-way Hash)。即是訊息可經由雜湊函數計算出雜湊值，但無法由雜湊值反向推算出原訊息。

◈ 雜湊碼碰撞率低:對於一個訊息 M_1，在計算上是無法找出另一個訊息 $M_2 \neq M_1$，使其 $H(M_1) = H(M_2)$，亦即，不同訊息之間產生相同雜湊碼的碰撞率要很低。

◈ 常見的演算法：MD4、MD5、SHA-1 等等。

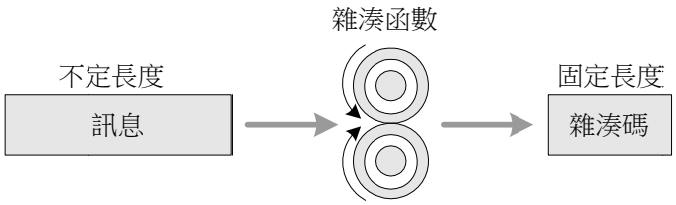


圖 1-3 雜湊函數的功能圖

基本上，我們要求每一筆訊息都有一個獨立的雜湊碼。亦即，不同訊息之間極不可能產生相同的雜湊碼，因此，有『數位指紋』(Digital Fingerprint) 之稱。研究雜湊演算法是一個非常有趣的課題，我們在第五章將會介紹到它。

1-2-3 亂數產生

在資訊安全領域中，『亂數』(Random Number，或稱 Nonce) 扮演著很重要的角色；簡單的說，亂數就是系統產生一個不可預測的數值，而且每次擷取時都會是不一樣的值。常使用到亂數的情況有：

◈ 交叉確認：通訊連線當中，某一方將一個亂數加密後傳送給對方，對方解密後將亂數加一，再加密後回傳給發送端，以確認雙方所握的鑰匙是否相同。

◈ 防止重播攻擊：訊息中加入一個亂數作為序號，每傳送一次便累計加一；如果收到重複的序號表示是重複攻擊。

◈ 產生通訊鑰匙：雙方確認身份之後（公鑰演算技巧），即可產生一個亂數作為通訊鑰匙（密鑰演算技巧）。

◈ 產生鑰匙參數：通訊雙方交換亂數（Nonce）來產生一個通訊鑰匙，例如 Diffie-Hellman 演算法。

◈ 計算鑰匙參數：許多演算法都利用亂數來產生鑰匙，譬如 RSA 演算法係利用亂數來產生公開與私有鑰匙。

由此可見，所產生的亂數必須是『不可預測性』，並且需要『隨機性』；否則所產生的亂數如被猜測出來，再好的演算法都是無用武之地。本書將於第五章介紹如何來產生可靠的亂數。

1-3 訊息的安全性

一般來講，我們針對傳輸訊息（或稱資訊）的安全性有下列四個層次：

◈ 隱密性（Secrecy or Privacy）：經過加密後的資訊在網路上傳輸，不至於被竊聽或盜取其內容（盜取成功也不了解其內容），以保持資料的隱密性。

◈ 確認性（Authenticity）：確定訊息來源的合法性；也就是說，訊息的確是來自發送端，而不是他人所偽造。

◈ 完整性（Integrity）：確定訊息在傳輸過程中沒有被竄改或部分訊息被取代。

◈ 不可否認性（Non-repudiation）：發送者事後無法否認發送該訊息的事實。

上述四種功能係利用雜湊函數、秘密鑰匙系統、以及公開鑰匙系統之間演變而來，以下分別介紹之。

1-3-1 訊息加密

訊息加密的主要目的是要達成資料隱密性功能。發送者將訊息加密後再傳送給接收者，接收者再依照雙方協議的方法及鑰匙，將訊息恢復成原來的格式。圖 1-4 有兩種訊息加密的方法，圖 1-4 (a) 為採用秘密鑰匙的加密演算法，雙方共享一把秘密鑰匙來通訊，不但可以達到資料隱密性的功能，也可完成確認性功能。可達到確認性功能的原因在於假設秘密鑰匙只有通訊雙方擁有，如果收到一份訊息而能夠以此鑰匙解密的話，則表示該訊息一定來自可信任的另一方。

圖 1-4 (b) 是利用公開鑰匙加密的方法，發送者利用接收者的公開鑰匙（K_{Ub}）對訊息加密，接收者再利用自己的私有鑰匙（K_{Rb}）解密；他人沒有接收端的私有鑰匙也

無法看到訊息內容，如此便能達到隱密性功能。

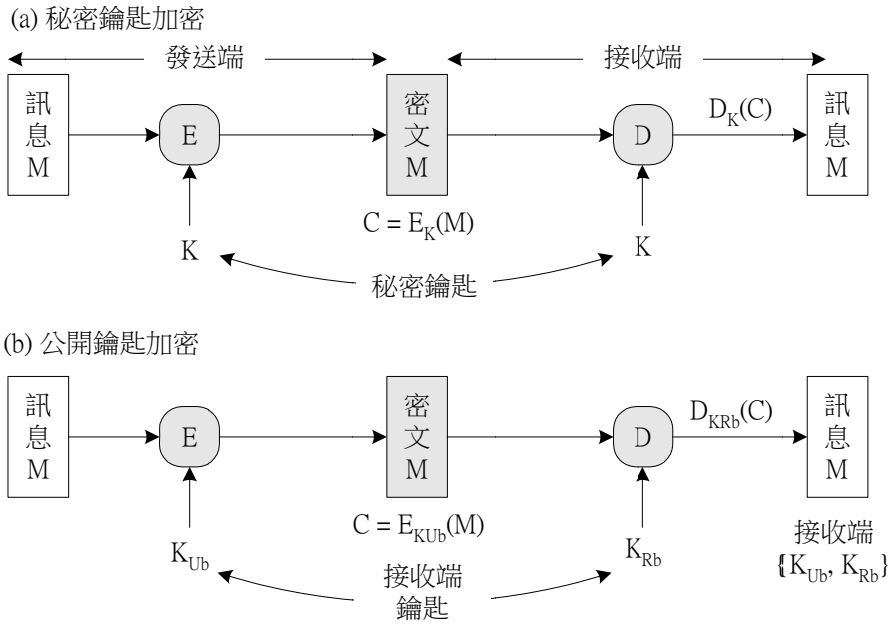


圖 1-4 訊息加密達到隱密性功能

1-3-2 訊息完整性檢查

圖 1-5 為訊息完整性檢查的運作程序，通訊雙方必須事先協議好使用何種雜湊函數（如 MD4、MD5）；發送者將訊息經過雜湊函數計算出雜湊碼，再將它附加於訊息之後傳送給接收者；接收者也利用相同的雜湊函數計算出另一個雜湊碼，如果兩個雜湊碼相同的話，表示訊息沒有發生錯誤，也沒有經過他人竄改。雜湊碼又稱為『完整性檢查值』(Integrity Check Value, ICV)，至於檢查能力如何，與雜湊函數的強度有關，本書第五章有詳細的說明。

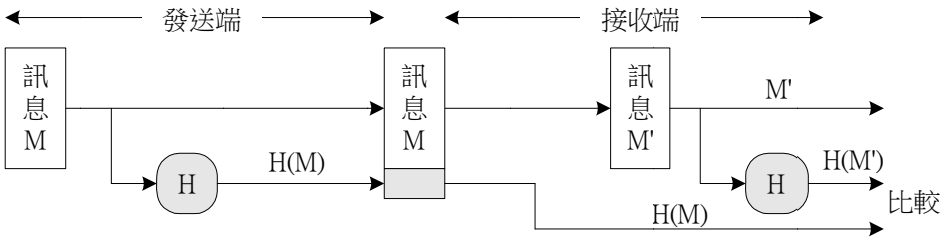


圖 1-5 訊息的完整性檢查

1-3-3 訊息確認

『訊息確認』(Message Authentication) 是為了達到資料的確認性與完整性功能。

也就是說，它能確定訊息的來源，是出自通訊的對方，而不是經由他人偽造的(確認性)；另一方面，它也能確定訊息在傳輸當中，沒有發生錯誤也未經他人竄改(完整性)。圖 1-6 為訊息確認的運作程序，事先通訊雙方都持有一把相同的祕密鑰匙(採用祕密鑰匙系統)。說明如下：首先傳送者將訊息經過雜湊函數計算出雜湊碼之後，再經過加密演算法加密 (使用秘密鑰匙)，得到一個稱之為『訊息確認碼』(Message Authentication Code, MAC)，發送時將 MAC 附加在訊息之後傳送給接收者；接收者將 MAC 解密 (同一把秘密鑰匙) 回原來的雜湊碼，也利用相同的雜湊函數計算所收到訊息的雜湊碼；如果兩者相同的話，便能確定訊息未被竄改過，更能確定來源無誤 (相同的秘密鑰匙)。本書於第六章會詳細說明有關訊息確認的技巧。

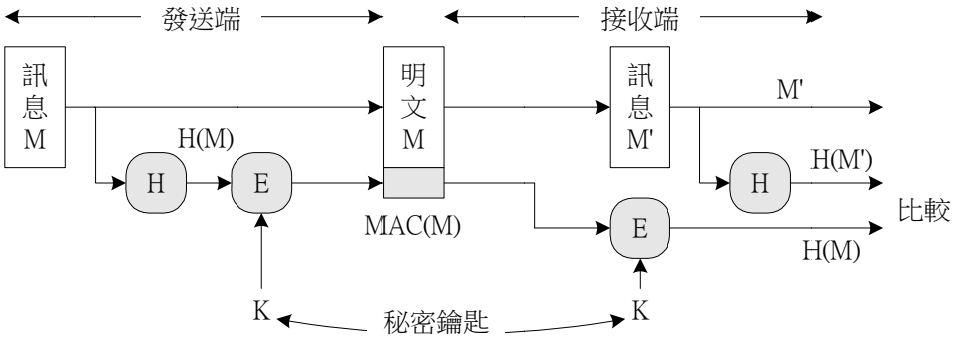


圖 1-6 訊息確認達到完整性與確認性功能

1-3-4 數位簽章

『數位簽章』(Digital Signature, DS) 屬於確認訊息來源的合法性與真實性，除了確認性與完整性的功能之外，還增加了不可否認性功能。看起來，數位簽章與訊息確認的功能很相同，但它們之間所採用密碼系統差異很大。訊息確認是採用秘密鑰匙系統，大多使用於安全連線下的傳輸 (如：IPSec)；然而，數位簽章是採用公開鑰匙系統，多半使用於沒有安全保護的連線上，主要從事於發送者身份的確認。圖 1-7 為數位簽章的運作程序，並假設接收者持有傳送者的公開鑰匙，說明如下：首先傳送者將訊息經由雜湊函數計算之後，再利用自己的私有鑰匙 (K_{Ra}) 加密 (簽署動作)，得到一個簽章碼 (DS)，再將簽章碼附加在訊息之後，發送給接收端；接收者則利用發送者的公開鑰匙 (K_{Ua}) 解開簽章碼的加密，得到原來的雜湊碼。也同時將所收到的訊息經由相同的雜湊函數計算出雜湊碼，如果兩者相同的話，表示訊息是正確的 (確認性功能)。另一方

面，簽章碼若可以順利使用發送者的公開鑰匙（K_{Ua}）解密的話，表示此加密鑰匙一定是發送者的私有鑰匙（K_{Ra}），接收者可以保留簽章碼，作為對方『不可否認』的依據。

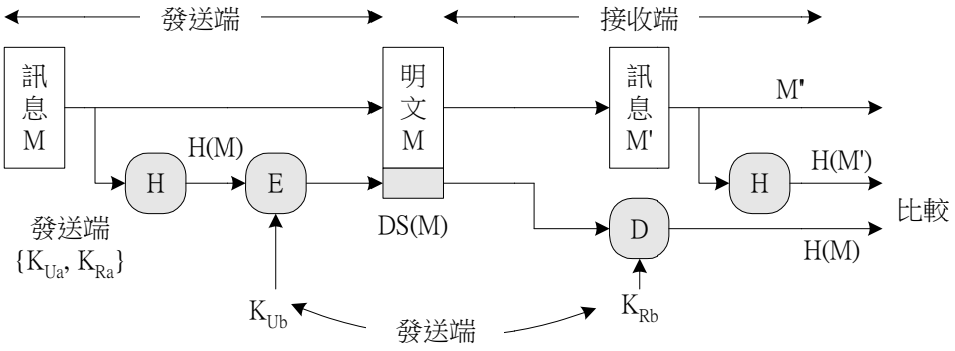


圖 1-7 數位簽章達成確認性與不可否認性功能

1-4 系統的安全性

一般所言的『電腦安全』（Computer Security）或『系統安全』（System Security），大多屬於『作業系統』（Operating System）的安全範疇。但目前資訊系統的運用大多透過網路傳輸，與其它系統之間共同處理，因此，安全性並不僅侷限於『本地作業系統』（Local OS），而應該考慮到『網路作業系統』（Network Operating System, NOS）領域，以下將介紹其重點。

1-4-1 安全性措施

基本上，作業系統的安全性大多是由廠商所提供，近年來作業系統大多已將網路功能整合進入系統核心之內，成為名符其實的網路作業系統。因此，考量系統安全性之時，也需考量網路的安全性，即是，本書所介紹的各種安全技術大多也涵蓋在作業系統之內。我們將作業系統所需的安全技術歸類如下：

◈ 密碼與用戶認證：密碼為使用者進入系統的最後一道關卡，很不幸的，使用者密碼必須儲存在系統的某一個檔案之內（如 /etc/passwd）。當然，我們絕不會將密碼的明文儲存在檔案，而會經過特殊處理（如醃製法）之後，再存入檔案；然而，當客戶登入系統時，會以某一認證協定來判斷客戶的真偽，最簡單的方法是『盤問/回應』，當然有許多系統為了增加它的安全性而採用 Kerberos 認證協定。（第十章說明）

- 資源授權與分配：針對每一使用者（或群組）使用資源的權限，必須劃分清楚，尤其在分散式處理環境裡，我們很難預測使用者會來自何方。一般系統內都會針對每一個檔案維護一只完整的『存取控制表』(ACL)，當使用者存取檔案時，再比對是否在權限範圍之內。

- 安全稽核：安全的作業系統必須提供稽核檢查哪些檔案被不當存取，此為非常重要的安全機制。管理者必須隨時檢視稽核紀錄，由紀錄中找出隱形的入侵者；這方面本書第十四章會有詳細的介紹。

- 存取紀錄：可以針對使用者或檔案作存取的紀錄（或稱日誌檔案）。一般來講，此紀錄檔案可能非常的大，必須透過專屬的資料庫系統分析與統計；由統計出來的訊息可以了解檔案被存取的現象，從中也可以找出入侵者的蛛絲馬跡。

- 資源備份：資源備份是管理者例行的公事。然而安全性作業系統也必須提供每日異動資料備份、與週期性的整體備份之工具。

- 病毒防範：病毒防範是目前系統最不可或缺的事項，也是入侵者最直接進入系統的工具；這方面本書第十四章會有詳細的介紹。

各家廠商所發行的安全性作業系統，之間的管理方式都大異其趣，管理者必須詳讀他們的操作手冊，才能如魚得水般的順手管理。本書限於篇幅無法再闢一個章節來介紹系統安全，但相關技術也會出現在各章節之中。

1-4-2 安全性等級

許多廠商都將稱其具有安全機制的作業系統為『安全性作業系統』(Secure Operating System)，但安全性如何又另當別論了。美國國防部有鑑於此，因此發行一本俗稱為『橘皮書』(The Orange Book)來定義作業系統安全性的等級，其中包含了四個等級，如下：

- 等級 D：最低安全防護。

- 等級 C：隨意性的安全防護。

◈ 等級 B：強制性的安全防護。

◈ 等級 A：驗證性的安全防護。

最低等級 D 幾乎沒有什麼安全機制，這類等級的作業系統大多屬於個人電腦（PC），如 Windows Xp 系列。等級 D 的作業系統並不強制使用者遵循安全措施來操作，並且可隨意選擇哪些安全機制。等級 C 包含兩個子分類：C1 與 C2；C1 包括密碼使用、檔案存取限制、與防止意外傷害（如檔案損壞）等能力；C2 除了包含 C1 的能力之外，還增加稽核檢查能力。一般都將 Unix 與 Windows 2000 歸類於 C2 的等級，但從安全稽核的能力來看，Windows 2000 似乎比 Unix 能力強了一點（事實上很難評論）。

等級 B 包含三個子分類，基本上都會要求提供安全文件、主動防護的安全機制、以及系統故障時的安全維護。B1 包含了 C2 所有的功能，並能區分出與安全有關或無關的系統部分；B2 增加了安全系統的數學描述，且必須提供改變架構時的安全措施，並保證新的安全架構不會出現『後門』的現象；B3 系統更進一步，要求系統管理員必須負起安全職責，尤其當系統發生故障時也必須維護系統的安全。等級 A 為最高等級，必須以數學方式來驗證系統的安全性，以及提供安全政策是否合乎安全設計的明細表。

1-4-3 封閉性用戶認證

『用戶認證』（User Authentication）表示使用者登入系統時，系統如何去判斷登入者的身份，再授與登入者適當的使用權限。如果以單一主機系統而言，最基本方法是以『帳號 + 密碼』（Account + Password）來認證登入者的身份。但當公司內有多只伺服主機時，是否需要在每部主機上建立每位員工帳號？又員工同時存取多部主機上資源時，是否需要登入每部主機呢？尤其目前資訊化蓬勃發展之期，規模稍大的公司內，大多擁有多部主機系統，吾人必須發展一套特殊工具將系統資源與用戶整合管理，這就是用戶認證系統。目前最普遍使用的認證系統為 Kerberos，它使用較複雜的盤問/回應認證協定，來確認登入者的身份，其它運作程序如圖 1-8 所示，說明如下：

◈ 步驟 1：用戶端向 Kerberos 系統登入，並取得欲通往哪一個伺服器的通行證。

◈ 步驟 2：用戶端持著通行證，向伺服器要求給予服務。

◈ 步驟 3：伺服器向 Kerberos 確認通行證的合法性。

◈ 步驟 4：伺服器回應給客戶端是否給予服務。

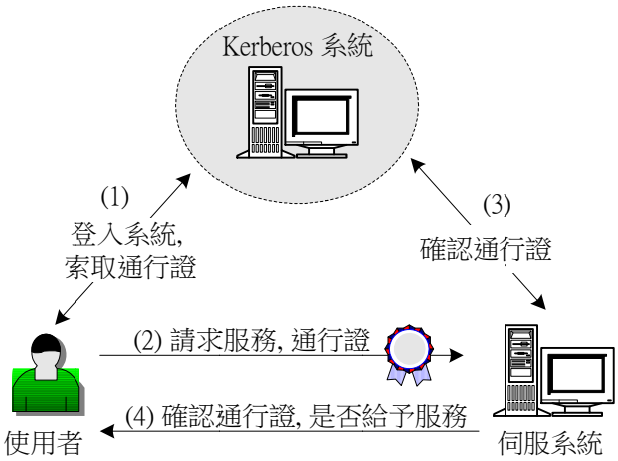


圖 1-8 用戶認證系統

並非每一次客戶要求服務之前，都必須向 Kerberos 系統索取通行證，而是每一張通行證都有註明持有人身分及有效期限。在這有效期限之內，持有人可以向任何系統資源提出服務要求。本書在第十章會詳細介紹到相關技術。

1-4-4 開放性用戶認證

Kerberos 大多運用組織單位內的電子化系統，亦是，用戶端使用之前都必須在管理系統上建立帳號。更清楚的說，使用者都是熟人，多半不是陌生人。但在開放式的電子商務(或電子化公司、電子化政府)環境底下，通訊對象可能來自世界各地的陌生人，或久久才使用一次 (如申報綜合所得稅)。如何確認陌生人的身份與交易方法，這可必須仰賴以下介紹的數位憑證。

我們可以回想一下在公開鑰匙系統底下，每一個使用者都擁有一對公開鑰匙與私有鑰匙，並且向外公佈該公開鑰匙所代表持有人的身份；只要收到某一個數位簽章的訊息，如能夠由某一個人的公開鑰匙認證成功的話，則表示該訊息一定被持有人保證並簽署過的。此種現象就好像火車站的儲物櫃一樣，只認識鑰匙而不理會到底是何人持有鑰匙。在電子化的環境裡，僅以擁有鑰匙來確認持有人身分是不夠的，譬如高雄與台北都

有一個志明，各擁有一把公開鑰匙，我們很難去區分哪一把鑰匙是高雄志明或台北志明的。再說，任何人都可以公佈它的公開鑰匙的話，也很容易被偽造的；譬如，志明可以在網路上公開一把鑰匙，並宣稱該鑰匙為春嬌所有，我們又如何來辨別它呢？

由此可見，僅利用公開鑰匙來證明身份是不夠的，它必須經過權威單位來證明它的合法性，因此，便誕生了『數位憑證』(Digital Certificate)。數位憑證是一張電子性的文件，它裡面記載了持有人的姓名、郵政地址、電子郵遞地址、公開鑰匙、以及有效期限等等；使用者必須持有有效證件向權威單位 (譬如內政部) 申請，並經過權威單位審核無誤後，才會發憑證給予申請者，發行憑證的單位一般稱之為『憑證授權』(Certificate Authority, CA) 中心。CA 中心會利用它的私有鑰匙來簽署所發行憑證，以保證該憑證的合法性 (有如關防的功能)；然而，任何人都可以利用 CA 中心的公開鑰匙來認證所發行憑證的真偽。

簡單的說，數位憑證是虛擬網路上的合法『身分證』，在陌生的開放性環境裏確認身分的主要工具。圖 1-9 即是說明數位憑證如何在網路上顯示身份，與要求服務的運作程序，如下：

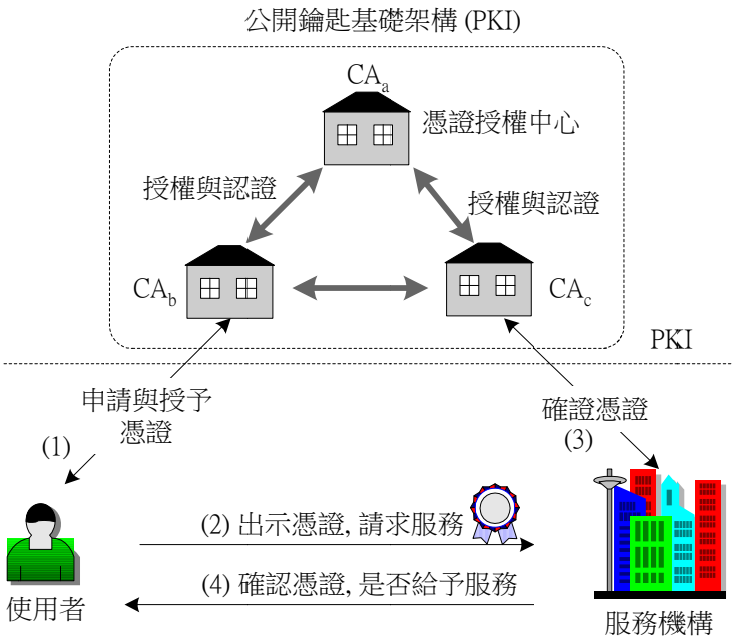


圖 1-9 數位憑證與 PKI 系統的運作程序

◈ 步驟 1：使用者持有效證件向憑證授權中心 (CA$_b$) 申請數位憑證，並經審核合格後取得憑證。

◈ 步驟 2：使用者出示憑證向服務機構請求服務。

◈ 步驟 3：服務機構收到使用者的憑證之後，可由憑證上的數位簽章來認證它的合法性（與確認性），並且觀察憑證內記載的有效期限是否過期；如果服務機構還需要更進一步確認的話，可將該憑證轉送給它直屬的 CA 中心（CA_c），請求它幫忙確認；該 CA 中心（CA_c）透過認證路徑找到原發行該憑證發行的 CA（CA_b），從中找尋有關該憑證的資料（如註銷或逾期等等），再回應給服務機構。

◈ 步驟 4：服務機構確認憑證之後，回應訊息給使用者表明是否給予服務。

目前網際網路上大多採用 X.509 v3 數位憑證，關於數位憑證與 PKI 系統，本書將於第七與第九章有更詳細說明。

1-5 電子化系統的安全性

本章到目前為止，由基本的演算法（密鑰演算法、公鑰演算法、雜湊演算法）延伸出來了許多資訊安全技術。接下來，我們將介紹這些安全技術如何應用在實際環境裡。

1-5-1 安全性網頁系統

『網頁系統』（Web System）是電子商務（或電子化公司、電子化政府）上最主要的應用系統之一，它的安全性決定電子商務的成功與否。另一方面，無論封閉系統或開放系統裡，利用數位憑證來確認身分是最可靠的途徑，但如何將它植入應用系統裡，『安全性網頁系統』（Secure Web）即是最佳的範例。圖 1-10 即是將認證工具植入『瀏覽器』的運作程序，首先它利用數位憑證（X.509）確認雙方身份後（訊號 (1) 與 (2)），再互相交換鑰匙材料（訊號 (3) 與 (4)）。雙方再利用所交換的材料來製作出一把會議鑰匙，協議會議鑰匙的方法大多採用 Diffie-Hellman 演算法，以後雙方便利用此鑰匙來通訊（訊號 (5)）。

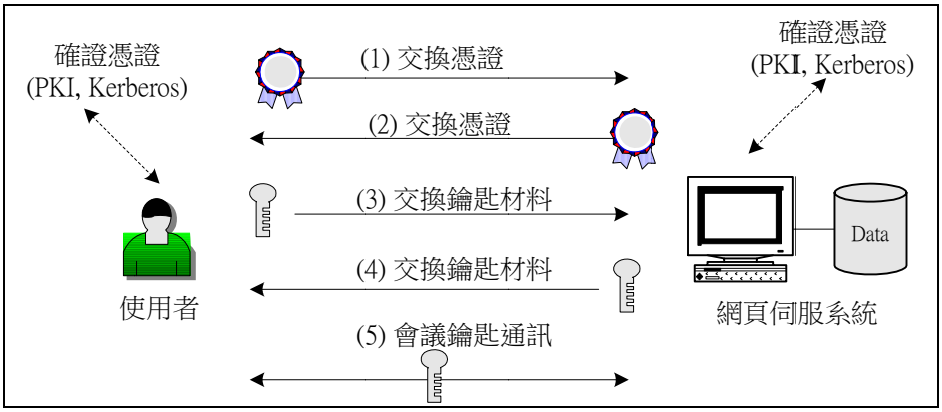


圖 1-10 安全性網頁系統的運作程序

雙方建立會議鑰匙之後，這把鑰匙便是雙方共享的秘密鑰匙，所採用的加密方法也是秘密鑰匙演算法(如 DES)。目前網際網路上有 SSL(Secure Socket Layer) 與 TLS (Transport Layer Security) 兩個主要的通訊協定，本書在第十一章會有詳細的說明。

1-5-2 安全性電子郵件

無論網際網路上的『伊媚兒』或辦公室自動化的『公文交換』都是屬於電子郵件的範圍。電子郵件的安全性最能表現出資訊安全的特色，一般『安全性電子郵件』(Secure E-mail) 的考量主要有：隱密性、確認性、完整性與不可否認性，幾乎是整合資訊安全的所有需求。目前安全郵件系統大多採用 S/MIME (Secure/Multipurpose Internet Mail Extension)，它將安全性因素嵌入信件之中。圖 1-11 為安全性郵件的運作程序，發信者將安全機制與數位簽章附加在信件之後傳送出去；接收者取出安全機制後，再依照安全機制的描述來拆解信件。當然這裡面的關鍵還是在於鑰匙的使用，無論信件的隱密性、確認性、以及不可否認性，都依照公開鑰匙演算法來製作加密、數位簽章等安全參數。

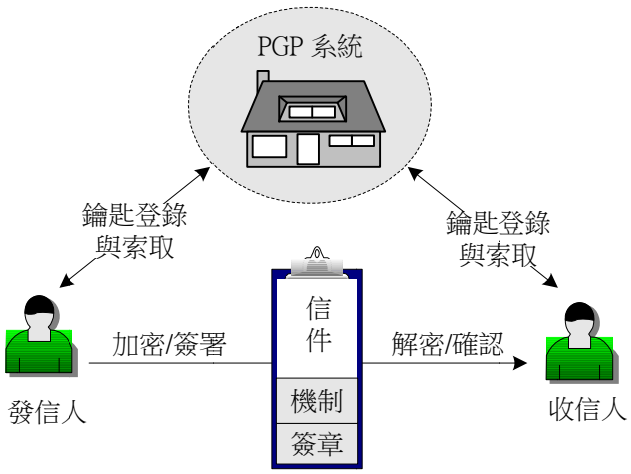


圖 1-11 安全性電子郵件的運作程序

同樣的，我們必須將安全性郵件可能使用到的安全機制整合一個完整系統，目前網際網路上使用最普遍的是 PGP (Pretty Good Privacy)。早期 PGP 有自己的數位憑證格式，但最近幾年來 X.509 v3 數位憑證漸成為公開的標準，因此，新版本的 PGP 系統已採用 X.509 v3 憑證。至於安全性郵件的相關技術，本書於第十二章內會有詳細的說明。

1-5-3 安全性電子交易

我們最終的目標還是希望在虛擬網路上建立安全的交易環境，並希望它的運作能比實際環境的交易更安全可靠。首先，我們以圖 1-12 作為範例來說明安全性電子交易的運作程序，如下：

- 步驟 1：客戶瀏覽網頁尋找所需的產品，並在網頁上訂購產品，其中會輸入相關資料、以及信用卡號碼。
- 步驟 2：客戶端電腦透過 Internet 連線將訂單傳送給 ISP 公司。
- 步驟 3：ISP 公司將訂單轉送給商家網站 (Internet 連線)。
- 步驟 4：商家網站收到訂單之後，依照信用卡號碼，通知客戶銀行及商家銀行，並將客戶帳戶內某些金額轉帳到商家銀行；以上程序都正確的話，則進行下一步驟；否則回應給客戶表明訂購失敗。
- 步驟 5：商家網站將訂單轉送到出貨倉庫，並回應給客戶端訂購成功。
- 步驟 6：倉庫收到訂單之後，便將所訂購的貨品送到客戶的郵政地址所在地；客戶簽收後，整個交易過程便算成功。

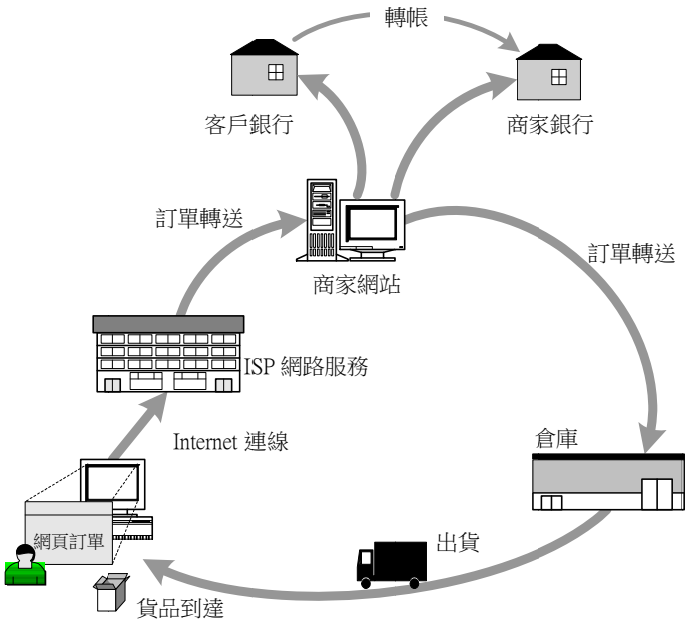


圖 1-12 電子交易的運作程序

在上述的交易過程之中，可以發現需要安全考量的地方，是當客戶輸入信用卡號碼時，絕對不允許他人窺視到信用卡號碼，因此必須要有特殊的安全機制來保護它才行。但無論如何，客戶還是在網頁上輸入信用卡號碼，亦即我們必須將安全機制嵌入網頁系統內。目前為了達到安全性的傳輸，大多採用 SHTTP(Secure HyperText Transfer Protocol) 協定，其中包含著 SSL v3 (TLS) 安全協定；這方面的相關技術將在第十一章內詳細說明。

另外，對於商家、商家銀行、客戶銀行之間的信用卡付款機制，也必須有一個安全性的付款協定來製作。在這方面，銀行與發卡中心 (如 IBM、Visa、MasterCard) 已共同發展出一個『安全性電子交易』(Secure Electronic Transaction, SET) 協定。SET 除了建構一個較完整的交易環境之外，欲期望達成陌生人之間交易之後，能不留下雙方任何痕跡，因而發展出『電子錢包』(Electronic Wallet)。客戶向銀行購買電子錢包之後，便可直接在網路上購買任何物品，如同實際環境下，在菜市場購買東西一樣。這方面的詳細技術請參考 IBM 官方網站：

http://publib-b.boulder.ibm.com/Redbooks.nsf/RedbookAbstracts/sg244978.html

此為 IBM 公司的 Redbook 共計有 340 頁，包含 The Theory、The Practice 與 Installing and Configuring Net.Commerce 等三大部份。讀者有興趣的話，可以到該網站下載

這些規範，或參考相關書籍 [103]，本書侷限於篇幅不再另闢章節介紹。

1-6 網路的安全性

開放式網際網路有其方便性，但也存在許多危險性，任何人都可以利用它來傳輸訊息，並利用它來接收訊息。本質上，網際網路是不安全的，更何況它是屬於國際性的網路環境，攻擊者或竊取者也許會躲在世界上任何一個角落，要去挖掘它或防範它實非易事。

在廣泛的不安全網路上，欲分割或隔離某一領域內私有網路，並能使其具有安全性功能，可由三個方面來思考。第一個思考方向的『防火牆』(Firewall) 機制，是屬於『點』的安全考量，亦即某一地區網路安全性而言；然而第二思考方向是『虛擬私有網路』(Virtual Private Network, VPN)，是屬於『線』的安全考量，乃透過網際網路結合多地區網路的安全考量，最後，再結合『入侵偵測系統』(Intrusion Detection System, IDS)。以下分別介紹這些安全機制。

1-6-1 防火牆與入侵偵測

簡單的說，『防火牆』(Firewall) 是將不安全性網路與安全性網路之間隔開的一道防護牆；但它絕不是『鐵幕』政策，而必須保持合法性的進出。所謂不安全性的網路，意指允許各方人士任意進出與存取的網路。若我們限制某些訊息的進出，成為可預期掌握及控制的網路，便可稱之為安全性網路。換言之，城牆將包圍著居住的人民，保護居民不受城外盜匪或它國軍隊侵犯，即是將不安全環境裡建構一個安全性較高的居住環境。防火牆即是如同城牆的城門一樣，一方面保持居民進出的方便性，一方面保護居民的安全性，如圖 1-13 所示。

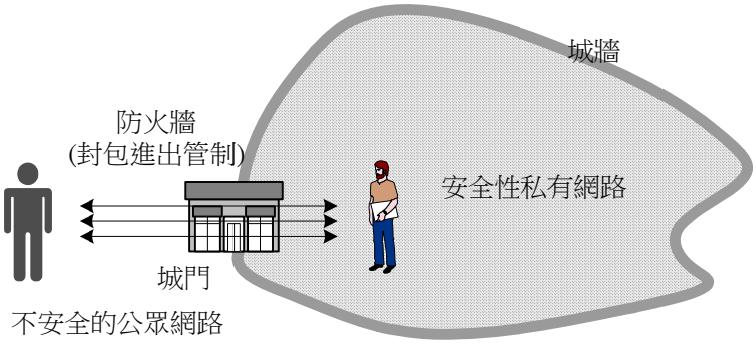


圖 1-13 防火牆架構圖

實現防火牆有：封包過濾器、代理器與網路位址轉譯等三種主要機制，本書第十三章將介紹其原理與製作方法。不幸有攻擊者突破防火牆防範，成功入侵私有網路時，吾人還是需要『入侵偵測』設備將其找出來，以維持私有網路的安全性，第十四章將告訴您偵測方法。

1-6-2 虛擬私有網路架構

當組織單位（或公司行號）分散在各地時，如何將各地區網路結合成一個完整的應用環境，的確是讓許多從事網路工作者頭痛的問題。早期幾乎都向中華電信公司承租專線來連結，但專線價格昂貴並且限制連線範圍。譬如，高雄與台北之間連線採用專線，價錢已非常昂貴，何況是國際間網路承租專線，實非一般單位所能承擔。話說回來，若能利用便宜的網際網路架設私有網路，實在非常方便，其費用無關地理環境。而『虛擬私有網路』（Virtual Private Network, VPN）就在此種需求下被發展出來，如圖 1-14 所示。

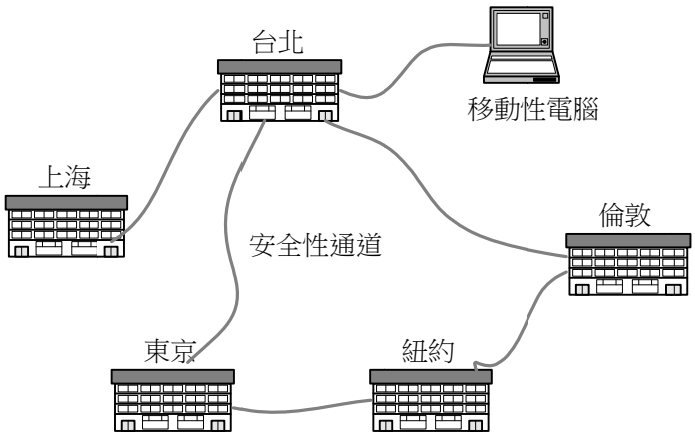


圖 1-14 虛擬私有網路架構

然而，私有網路內傳輸的資料多半屬於機密性的，如果沒有經過特殊處理便將資料放在網際網路上傳輸，公司內部的資料便會流露於外。又依照 TCP/IP 協定，封包在網際網路上傳送時，必須經過多個路由器的轉送才會到達目的地；當路由器收到一個 IP 封包時，必須拆解才知道應該往何路徑轉送，因此，封包內訊息將被一覽無遺。如何在不安全的網路連線下，建立成『安全性通道』，本書利用第十五、十六與十七章等三個

章節，介紹其相關技術與建構方法。

1-8 結論

我們利用這一章將本書的內容作一個簡單的描述，讓讀者可以儘快進入網路安全的領域裡；許多讀者開始研習網路安全時容易被密碼學所擊垮，到底密碼學祇不過是網路安全的一個重要工具而已，因此，本書儘量簡化密碼學的介紹，以更廣闊的空間來介紹其它技術，如果讀者欲更進一步的研究密碼學的話，請另外參考其它書籍 [1, 6, 10, 82, 135, 136]。