密碼學於網路應用簡介

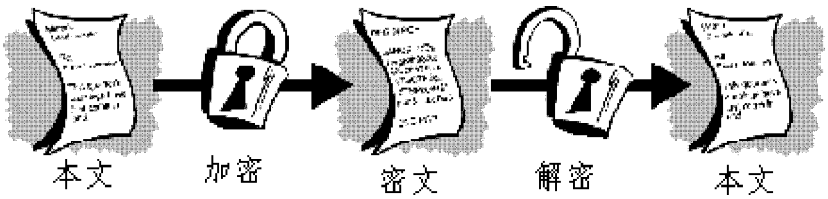
劉政彥

透過網路來傳遞資料，已日漸成爲不可或缺的管道，在愈來愈倚賴網路的情形下，不可不知網路傳輸的不安全，並利用現有的工具來做補強，使網路成爲較可靠的傳輸媒介。

所謂網路傳輸的不安全，係因爲Internet是開放性的，所傳的資料可輕易地被攔截下來，內容便被獲取者讀取，毫無保密性可言；另一方面，電腦文字資料可以輕易地修改內容，並以任何名義傳遞，那麼如何確認所發出的資料，就是該人所發出，並且未遭竄改？如何解決網路上的隱私及身份確認的問題？主要是透過密碼學的運用，來加強網路使用的可靠度。

基本密碼學觀念：

一般原始可讀的文件叫「本文」（Plaintext 或 Cleartext），經過「加密」（Encryption）後的文件叫做「密文」（Ciphertext）；所謂的「加密」是指用某種的方法來暫時替代本文，而不被看出原來本文內容的一種方法，而只讓知道這種方法的人，經過「解密」（Decryption）使密文還原成本文。



簡易的密碼學使用：

古代凱撒大帝要傳訊息給將軍，不信任傳訊息者，怕被洩密，便將訊息中所有的A字母替代爲D，所有的B替代爲E，以此類推，那麼只要有人知道「把字母移3位」這規則，便能正確解讀凱撒所傳遞的訊息內容；例如「SECRET」加密後變成「VHFUHW」，而此加解密的關鍵的複雜度（移3位字母）及所需要處理的時間（把字母置換回來），決定了是否眞的安全的要素。

較嚴密的密碼學：

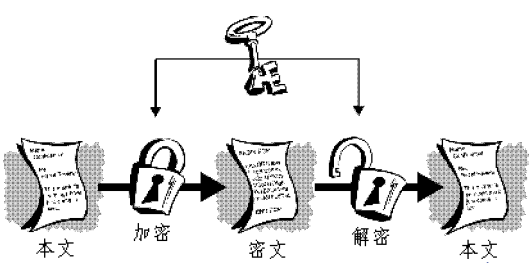
現代的密碼學（Cryptography）是利用數學來對資料加密解密，而達到保護資料安全目的的一種領域。判斷一個是否爲良好的加解密方式，是從所需花的時間及資源而決定的，好的加解密方式是不易在短時間或有限時間內被破解的。

密碼學如何運作？

加解密的機制是複雜的數學函式，並加上使用者提供一鑰匙（Key），使本文構成密文，這Key可能是一個字或字母或一串句子；同樣的本文可以依所給不同的Key形成不同的密文。所以被加密的密文是否眞的安全，在於兩個條件：極不易破解的加解密方式及Key的機密性。

傳統的密碼系統：

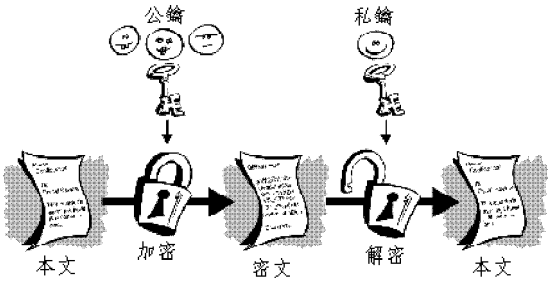
傳統的密碼系統又稱爲秘鑰（Secret-key）或對稱式鑰（Symmetric-key）密碼系統，加密和解密的Key是同樣的。優點是速度快，在資料沒有傳遞的考量下使用是方便的；但是當加密的資料要傳遞出去，在要用同一把Key的要求下，如何安全地傳遞Key是無法解決的問題。



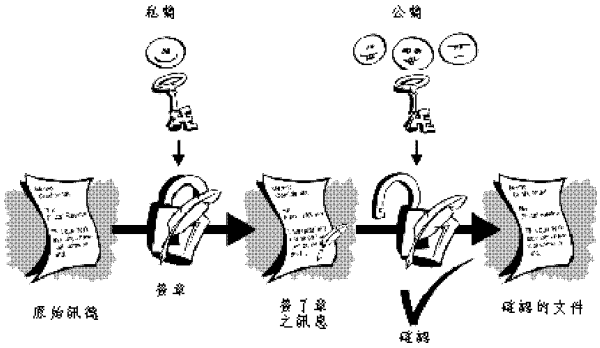
公鑰加解密系統：

爲解決 Key 傳遞的問題，而發展出「公鑰密碼學」（Public key cryptography），使用者需要產生一對 Key ，分別是「公鑰」（Public key）與「私鑰」（Private or Secret key）。公鑰是公開的，用來對資料加密的；相對的私鑰是自行保有，不可洩露的，用來解密回復本文用的。換句話說，用公鑰加密的密文，只有該私鑰可以解密；這就解決了 Key 怎麼傳佈的問題。

所以在網路的環境中，只要每一個使用者，產生公鑰和私鑰，每個人的公鑰置放於公眾可採信並可存取的地方，私鑰個人妥善的保存著；當別人要寄給你密文之時，拿到你公開的公鑰，來加密訊息內容，以密文傳遞給你，你再用你的私鑰使之還成本文；這樣便能使訊息的內容不被非收件者獲知。



電子簽章基本概念：



除此之外，公鑰加解密系統提供了「電子簽章」（Digital Signatures）的機制；所謂電子簽章是讓收訊息者確認，訊息是否確實沒被僞造竄改，是否正是該人所傳遞。另一方面，也是防止寄件者宣稱這不是他發的訊息的證明。這種效力是相當於在一般紙上用白紙黑字簽名的效力。

基本的運作方式是：用私鑰把資料加密，如果資料可被其公鑰解密，那麼就能確認該訊息是產生於原作者。

單向雜湊函式：

要把所有的訊息用私鑰加密，速度慢是不易解決的問題，因爲加密會產生至少比原訊息多一倍的資料量，而且訊息長短不一，因此發展出了單向雜湊函式（One-way hash function），此作用是不管原訊息長度有多少，透過此運算便會產生同樣固定長度大小的訊息出來，具產出稱爲「訊息摘要」（Message digest）。

寄件者把原文的摘要訊息，利用私鑰產生「簽章」的動作，把這被簽章的資訊摘要和該文件一同傳遞出，收件者利用寄件者的公鑰去確認其簽章，來確定其文件是否確實寄件者所寫之內容。

其他認證的問題：

上述所提的基本運作方式，可解決資訊保密及資訊一致性的問題，但是公鑰怎麼被管理，以及怎麼確認所獲得的公鑰就是你所想要寄的人。甚至怎麼確認，要寄給一個素未謀面的人，就是所要寄給的人；這些確認需要有猶如戶政機關般的認證中心（Certificate Authority）來確認並管理公鑰的可靠性；還有認證中心間怎麼建立及溝通，都是當前重要的建置方向。