密碼兩三事

◎張敬昇

密碼的起源很早，古希臘、羅馬時期，便有利用文字符號轉換的密碼，作為傳遞軍情之用。近代數學與電腦蓬勃發展，對於密碼的編碼與解碼便更為講究，透過運算，資訊系統可輕易地產生對資訊加解密的鎖與鑰匙，讓想竊取資料的外人難以破解。相關技術在重視安全的電子商務與易於接收電磁波、開放的無線網路環境中被廣泛地使用。

拜網際網路的崛起，電子化的個人服務也如雨後春筍般出現，為了鑑別不同使用者並避免被人冒用，獨一無二的帳號與其對應之密碼便是最常被使用的模式。而在設計選擇密碼上人們總是矛盾的：既希望密碼簡單好記，但又希望密碼不為外人破解。我們要有個最基本的認知：沒有一種密碼是一定不會被破解的。再複雜的密碼也可能被破解、竊取，因此在密碼的保護與設計上，必須保持高度的警覺以維護個人隱私。

密碼學中有個專有名詞稱為「密碼強度」，定義了一組密碼被外人或電腦程式破解的難度，通常用「強」或「弱」來表示；強弱是相對的，不同的服務（資訊系統）對於密碼強度的要求便有所不同。密碼強度「弱」的意思是指此密碼易被猜測與破解，具有下列這些特徵：（一）順序或重複的字元：如「abcdef」、「qwerty」、「111111」等。（二）使用數字或符號在相似字元間替換，如用數字 1 代替小寫 L 等。（三）密碼為帳號的片段或完全相同，如帳號為 Tommy123，密碼是 Tom。（四）常用的單詞：如自己或熟人名字的縮寫；寵物的名字或常用的單字，就像 apple、monkey 等。（五）常用的數字：如生日、證件編號，以及這些數字與名字、稱號的簡單組合。

反之，密碼強度「強」則是指密碼不易被猜測與破解，主要的特色包含兩項：（一）長度足夠長。（二）密碼排列隨機，無單詞意義或不為常用的單詞。以下舉一些密碼強度強的例子：Tpftcits4Utg!（一串隨機的字元，

包含大小寫與數字及標點符號）、helloilikeappleandpiemicrosoftohmygodddd（很長的單詞密碼串，難以破解）。一般來說，鍵盤上常用的按鍵有 95 個，若使用的是隨機的８碼密碼，那麼便有約６千６百兆組的可能，外人難以在短時間內透過程式列舉破解。許多專家建議，一組強密碼的長度至少應在８碼以上，並包含大小寫字母、數字與標點符號之組合。筆者對使用中文注音鍵盤的讀者提供一種設計強密碼的作法：利用中文鍵盤上的注音符號順序，使用中文單詞或短句記憶，並用英數輸入法打出來。例如「我喜歡吃燒肉」，若不使用中文輸入法而使用英數輸入法就會變成「ji3vu3cjO t gl b.4」如此便是看似隨機卻有特殊意義的好記密碼。

最後的重點是維護密碼的習慣。人們有時使用一項新的資訊服務時，系統會給予用戶一組預設的密碼，若因偷懶而不進行更換，有心人士將可輕易從網路上找到此系統的預設密碼而予以破解。另外專家們建議，不要在不同的帳號使用相同的密碼，否則若因某些因素而洩漏密碼，使用者將有財務損失風險。此外，不要將密碼寫在他人容易窺視的地方，例如在辦公室的電腦旁使用便利貼記下自己的帳號密碼。

由於電腦運算與程式能力的進步，有心人士將更有能力透過不同的方法來探知使用者的密碼。在網路資訊發達的時代，我們更應小心維護個人的密碼，進而保護自身的隱私，以防被不肖人士利用。