密碼戰爭

◎ 劉祝宏

暢銷書「達文西密碼」改編的電影上映後，雖然引起許多爭議，然而從全球票房熱賣的氣勢，更顯示一般大眾對隱藏訊息的好奇，無論是「聖經密碼」到「達文西密碼」的窺探熱潮，甚至是國防上的秘密通訊需求，以及推動數位式密碼到量子密碼的精進發展，其實都在我們生活中扮演重要角色。

在「達文西密碼」一書中，有一段這樣的文字：「你可能也知道…警方會利用螢光燈去搜尋犯罪現場的血跡和其他鑑識證據。所以你就可以想像我們的驚訝…」忽然間，他把那盞燈指向屍體…鑲木地板上潦草的紫色字…寫著：「13-9-2-21-1-1-8-5　啊，嚴峻的魔鬼！　啊，跛足的聖人！」

國防大學中正理工學院電算中心婁得權主任表示，類似「達文西密碼」這種將資訊以不同形式隱藏的藏密技術，最早刊載在西元前五世紀古希臘學者希羅多德的歷史著作，當時為將波斯即將入侵希臘的情報通知斯巴達，又擔心半路被到處巡邏的波斯警衛攔截，曾把秘密訊息刻寫在木頭上，表面再用蠟質掩蓋，以躲過搜查。

同一時期，米利部的統治者希斯提艾奧斯被圍困時，為了聯絡女婿，將一名奴隸的頭髮全部剪掉，在頭皮上以刺青方式寫下訊息，等到奴隸頭髮長出來完全掩蓋訊息後，再派奴隸外出聯絡，對方就是捉住奴隸，如果不知道要剃掉奴隸的頭髮，可能就不會發現他頭髮下暗藏的訊息了。

除了上述案例之外，在二次世界大戰時，德國人在普通文件的「句點」中暗藏微縮照片，由於手法精細，被美國聯邦調查局局長胡佛譽為「敵人最傑出的諜報作品」。雖然最後還是被美國人發現，德國人早就藉此手法，成功傳送過好多情報了。

「達文西密碼」的開頭，法國羅浮宮館長利用夜光筆在地上留下訊息，而這是隱形墨水的應用，二戰中的隱形墨水成分，從果汁、牛奶、醋，甚至是尿液都有，只要對信紙加熱就可以顯影。更專業的則是使用光學顯影劑，必須在化學實驗室中進行解密。

這些傳統的藏密方式，面對前衛發達的現代數位科技，就顯得粗糙又老套了，取而代之的是電子資訊隱藏技術。例如幾年前流傳的「愛機程式（Love Machine）」，可利用軟體將色情圖片附加在正常的影片後，來躲避系統對色情圖片的檢查與攔截。而要破解高段的「資訊隱藏技術」，宛如大海撈針一樣困難，把機密資訊加密後，再隱藏於多媒體資訊中傳達，就像生物保護色般多了一層安全機制，例如用軟體將一張敵方機場照片，和一張不相干的美國航艦照片合成在一起，別說對方根本想不到裡面藏有情報，就算知道，如果沒有正確的解密金鑰，也只能盯著這張航艦照片猛搖頭，猜不透這張「有圖」天書。

自九一一事件後，美國國安當局曾經委託民間研究機構，企圖從網路世界中找出恐怖組織互通訊息的蛛絲馬跡，經偵查了數百萬張多媒體圖片後，毫無所獲。顯然，要從浩瀚難測的密碼世界中順利解碼，真的比大海撈針還難。

密碼戰爭自古至今一直是「絞盡腦汁的編碼者」和「嘔心瀝血的解碼人」的拔河較勁，有時影響了政權，有時左右了戰爭成敗，例如十六世紀蘇格蘭瑪莉女王，因企圖暗殺英格蘭伊莉莎白女王的信件密碼被破解，而走上斷頭台；兩次世界大戰時，情報密碼更攸關戰局。

在情報戰上，最傳統、最常用的解密方式有三種：第一種是「窮舉法」推估該密碼內的所有可能性，然後逐一輸入密文去比對，直到大意浮現；不過，這也是耗時最久的方法。

「統計攻擊法」則是利用「字母或是符號」出現的頻率，依最高頻率逐一代入密文之中，直至該密文的大意浮現，再進行解密分析，例如根據統計，英文字母「Ｅ」的出現機率爲一成三，是英文字母中出現頻率最高者，再以出現機率接近一成的「Ｔ」代入，找出有意義的組合。

「字典攻擊法」則是運用「常用的關鍵字」，例如古今中外較著名，或是普及性較高的人名（約翰、麥可）、地名（巴黎、華盛頓）、或是日期（九一一）逐一代入密文之中，找出加密的邏輯。

資訊時代的密碼大多靠著數學運算的複雜程度來維持它的安全性，例如 RSA 加密法用來加密訊息的金鑰，可能是由幾百位數的質數相乘所組成，要破解金鑰需要用因數分解回推，即使是用超級電腦運算，算出答案的時間可能遠超過你我壽命了。

如果遵循量子力學原理的「量子電腦」真能問世，就能輕易打破這種密碼法的防護罩，因爲依照理論推估，傳統超級電腦需要一百億年才能計算出的因數分解問題，量子電腦可能只要 30 秒就能解決。然而，世間萬物都有相生相剋之道，能夠與「量子電腦」相抗衡的正是「量子密碼」。其原理是運用微觀量子奇妙的「測不準」特性，以一長串的量子狀態作爲資訊加密與解密的密鑰，任何非法測量竊取量子密鑰的動作，都會改變量子狀態，竊取者因此只能得到一長串無意義的資訊，發訊者和合法接受者則能察覺密鑰是否曾被竊取過。

正因有許多製造技術待克服，2001 年底 IBM 宣佈建造出的量子電腦雛型機，還只能分解「15＝3×5」而已；相形之下量子密碼的發展腳步較快，根據美國科學人雜誌的報導，瑞士、美國和日本都已有傳輸量子密鑰的產品，只是還不到廣泛運用的階段。

總而言之，進步的資訊科技雖然便利了你我的日常生活，但是稍不謹慎，小則洩漏個人資料，大則影響國家安全。因此，我們平時不論在處理公務上或是個人言行上，均要無時無刻注意並養成習慣。畢竟，再精密的儀器最後使用的還是人。