# 密碼學…電子時代的新顯學

知己知彼，百戰不殆；不知彼而知己，一勝一負；不知彼，不知己，每戰必殆。

從人類學會溝通後，便不斷尋找更為巧妙複雜的方式來隱藏訊息，以防敵人識破。例如：古代中國會用明礬水寫保密書信；義大利人則發現用明礬調配出來的墨水，可以滲透蛋殼，在裡面的熟蛋白留下痕跡，但是從蛋殼外表卻看不出來；甚至遠在波斯王朝時，剃光信差的頭髮，將訊息刺在信差的光頭上，等頭髮長出來了，就派他去傳遞秘密訊息。事實上，語言與文字就是最早的秘語與暗碼，使用不同語言或文字的兩個人是很難溝通的，除非比手劃腳。在比賽場上，特別是雙打，要溝通時，經常發現隊友會用手遮住嘴巴講話，用意是怕被對方識破，但若知道對手不懂我隊的語言，遮住嘴巴的動作就可以免了。上述這些隱匿法都是古代傳遞秘密訊息的方法，算是密碼學的早期雛形，而密碼學的歷史就是幾世紀以來編碼者與解碼者之間的戰爭史。

古代也會在文字上做文章，大搞隱藏訊息手法，例如破譯「青鵝」兩字的故事是說「唐朝時，武則天稱帝，地方官員徐敬業準備起兵造反，中書令裴炎給徐敬業等人寫了一封書信，只有『青鵝』兩個字，被人告發了，朝中大臣誰都不知道這是什麼意思。武則天說：『青』字可以拆成『十二月』，『鵝』字可以拆成『我自與』，這說的是『十二月我自與』。馬上殺掉了裴炎，徐敬業等人的造反也很快失敗了」。凱撒在高盧戰爭期間使用凱撒移位法與將領們通訊，他們的作法是把每個字母順移同樣的數目，例如：順移的數目為 3，*a* 就變成 *d*，*b* 就變成 *e*。有時候還採取比較複雜的調換字母順序來作為隱藏訊息的方法。當我們無法得知這調換順序時，就很難破解密碼。因此在一段很長的時期內，這種隱藏訊息的方法是很管用的，直到伊斯蘭先知穆罕默德的可蘭經出現，解密的工作才出現大幅度的進步。事情是這樣的，伊斯蘭神學家仔細計算可蘭經各個單字在每一篇啟示出現的頻率，發現這頻率有很高的穩定性。這項看似無關緊要的觀察結果，日後卻造成了密碼分析學的第一次大突破。

我們無法確知是誰先意識到字母出現頻率的差異可以用來破解密碼，就目前所知，這項技術的說明最早見於西元 9 世紀的科學家津帝：「倘若我們知道加密訊息所使用的語言，有一種破解它的方法是：找出一篇至少一頁長的相同語言的明文文章，數算每個字母的出現次數。把最常出現的字母稱為『1 號』，次常出現的字母稱為『2 號』，再次常出現的字母稱為『3 號』，以此類推，直到這篇明文樣本的所有字母都如此整理完畢。接下來，就輪到我們要解密的密碼文了，我們也將它的符號如此分類。找到最常出現的符號後，將它替換成明文範本的『1 號』字母，次常出現的符號換成『2 號』字母，再次常出現的符號依例換成『3 號』字母，以此類推，直到密碼文的所有符號都替換完畢為止」。

津帝的說明，以英文字母為例比較容易解釋。首先，為了確立每個英文字母的出現頻率，我們必須分析一篇或甚至數篇普通的英文文章。英文字母出現頻率最高的是$e$，接下來是$t$，然後是$a$，……。再來，檢視我們要處理的密碼文件，也把每個字母出現的頻率整理出來。假設密碼文件內出現頻率最高的字母是$j$，那麼它很可能是$e$的替身；如果密碼文件內出現頻率次高的字母是$p$，那它可能就是$t$的替身，於此類推。這樣我們就可以破解密碼文件了。

很長一段時間，非洲下撒哈拉區使用鼓聲來傳遞資訊，鼓聲、號角和鐘聲一樣，有時能用來示意，傳遞簡單的訊息，例如：進攻、撤退和上教堂，但是我們無法想像鼓聲會說話，而且是非洲人利用鼓聲來傳遞資訊。非洲會說話的鼓就像華騷所勾勒的「鼓聲隆隆不息，響徹黑暗大陸，……，會說話的鼓，是莽林的無線電」。

高斯是第一位實驗電磁脈衝通訊的人，他架設了一條長一公里的電線，由位於哥廷根的韋伯實驗室連接到高斯居住的天文臺，用來互相傳遞訊息，這也開啟了電磁密碼的時代，直到 1838 年，美國人摩斯開發的電磁密碼最為成功，這套密碼和高斯及韋伯的密碼很像，只是把每個字母轉換為長短電波的組合。摩斯密碼擁有精簡、低成本與高效率的優點，所以在通訊科技昌明的今天，它仍然占有相當重要的地位。摩斯密碼的組成相當簡單，它是由點「・」(短音）與線段「－」(長音）所組成的，例如：數字 0、1、3、5，英文字母$Q$與運算符號＋、×的摩斯電碼分別為

**0** －－－－－
**1** ・－－－－
**3** ・・・－－
**5** ・・・・・
*Q* －－・－
＋ ・－・－・
× －・・－

電報與密碼的長期發展，促使人們對個人隱私的重視，例如：英國維多利亞時期的年輕情侶無法公然表達他們的愛意，甚至不能透過信函，因為他們的父母可能會攔截、閱讀信件內容。因此，有些情侶就透過報紙的個人啟事區傳送加密的訊息給對方。這些俗稱的「相思專欄」勾起解密專家的好奇心。有一次惠斯頓解譯了一名牛津學生刊在《泰晤士報》提議愛人與他一起私奔的啟示。幾天後，惠斯頓刊登他自己的啟事，也用同樣的密碼加密，勸告這對愛侶不要履行這項輕率、叛逆的計畫。稍後隨即出現第三則啟事，這次沒有加密，它是女方當事人發出的：「親愛的惠斯頓，不要再寫了。我們的密碼被發現了」。

每一本現代的書都有國際標準書碼（或稱 ISBN 碼），國際標準書碼一共有十碼，前九碼是 9 個數字，稱為「訊息碼」；第十碼可能是數字或是×這個記號，

稱為「檢查碼」。檢查碼是由訊息碼所決定的，將訊息碼的每個數字依序分別乘上 1、2、3、……、9，再將其總和除以 11，當所得的餘數是 10 時，規定檢查碼為×，餘數不為 10 時，就以此餘數當檢查碼。例如《阿草的葫蘆》這本書的訊息碼為 957-990-882，又

$$1\times9+2\times5+3\times7+4\times9+5\times9+6\times0+7\times8+8\times8+9\times2=259$$

除以 11 所得的餘數為 6，故檢查碼為 6，此書完整的 ISBN 碼為 957-990-882-6，如下圖的標籤所示：


婷婷從電腦上查得《幾何原本十三卷》這本書的 ISBN 碼，並用噴墨印表機將它印下。由於不小心觸摸，使得其中的第三碼數字模糊了，但是其他的數字還很清楚，書碼如下所示：

ISBN：04■-620-112-0

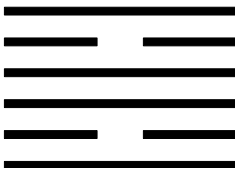
你能推得該書碼的第三碼應該是多少嗎？這是辦得到的，國際標準書碼具有神奇的功能：它會自我偵錯，而這偵錯的道理來自於 11 倍數的算術使用，算算看模糊的數字應該是多少。

由於書籍出版量龐大，ISBN 開始面臨無碼可用的局面，因此 2007 年 1 月 1 日起，ISBN 改為 13 碼，並將第 2、4、6、8、10 和 12 個數字相加後乘以 3，再加上第 1、3、5、7、9 和 11 個數字，最後選定第 13 個檢查碼，讓其總和為 10 的倍數，例如下圖所示：


就是一本書的國際標準書碼。

萊布尼茲發明了二進制，只用數字 0 和 1 表示數。當年他與在清朝的傳教士來往，世上至今仍然留有那時他們的書信。歷史記載，萊布尼茲在德國見過邵雍的方圓圖，他曾經用放大鏡仔細觀察八卦，發現八卦是由陽爻（實線）和陰爻（中斷的線）兩種符號組成。萊布尼茲的天才在於，他以數解卦。這個方

法開闢了溝通算術與易經的道路。按照他的觀點，所謂陰陽可以數字化，陽爻用數字 1 表示，陰爻用數字 0 表示。這樣每個卦都成了由 0 和 1 構成的六位數。特別的，他認為採用二進制來計算是最簡單的，例如：下圖是《易經》六十四卦中的第三十卦（離為火），由下往上讀可以得到二進位表示的 101101：

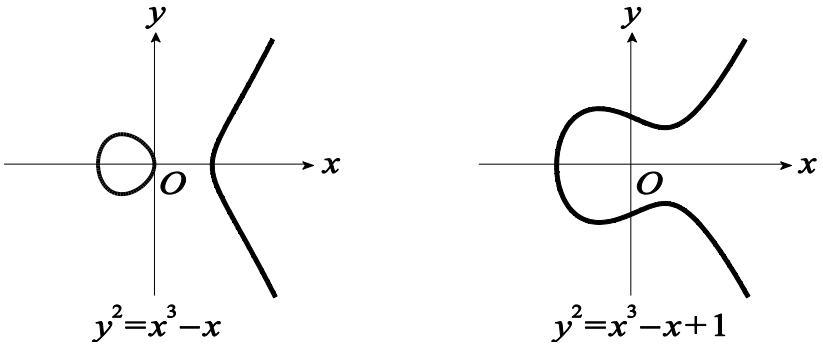


無論訊息加密與否，都需要找出由一地傳遞至另一地的方法。中國長城上的狼煙，水手使用的旗號系統，輪船打出的燈光訊號，一般書信傳遞，這些都是為了將訊息傳遞出去所想到的方法。身處 21 世紀的今日，網際網路無遠弗屆，幾乎取代一切傳遞訊息的方法。

來趟時空旅行，無論是回到過去，或者前往未來，總是令人嚮往與期待，如此我們就可以改變歷史或者讓預測未來變成簡單。在時空旅行尚未成熟之前，人類一直利用數學在偷窺未來，也利用數學在探知過去。既然偷窺，探知與揭開秘密的衝動是人類的天性，所以把重要的資料與訊息加密，不被盜取變為相當重要。所謂道高一尺魔高一丈，以其人之道，還治其人之身，我們也只能利用數學來防堵與加密，進行反制。維多利亞時代的密碼分析大師巴貝吉指出「解密技術最特別的一點，在於每個人都深信自己能設計出一套無人能解的暗碼，就連略懂皮毛的人也不例外。我還觀察到，愈聰明的人愈相信這一點」。

不管訊息如何加密，最終還是得把解密鑰匙送至對方，對方才能正確解讀訊息，運送解密鑰匙的過程出了差錯，再好的加密技術也沒用。如何不必運送解密鑰匙成為密碼學的一大難題，解決的方法是這樣的：「愛麗絲將一則極私密的訊息，加密之後送給巴伯，此時巴伯沒有解開它的密碼，但沒有關係，巴伯再將這訊息加第二道密碼，然後送還給愛麗絲，愛麗絲收到這加了兩道密碼的訊息之後，將第一道她所設的密碼解開，僅留下第二道密碼，然後再將訊息寄給巴伯，此時巴伯就可以解開他所設的第二道密碼，進而得知愛麗絲的私密訊息內容為何了」。在整個傳遞過程中，即使私密訊息被攔截，也無法解開訊息，這是近代密碼學加密而不必傳遞解密鑰匙的基本原理，妙不可言吧！

過去的密碼學需要大家先面對面協商，用於網路交易是行不通的，幸好數學提供了解決的辦法。利用大質數、費馬小定理及橢圓曲線（非高中的橢圓）是近年來有效傳遞密碼的方法。



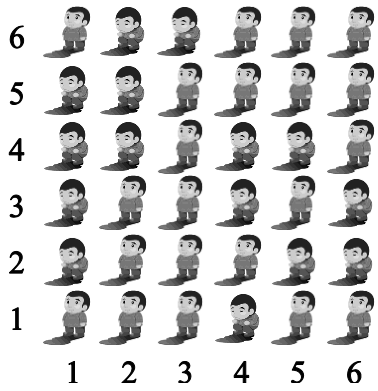

有人說，首度運用芥子氣與氯氣的第一次世界大戰，可稱之為化學家的戰爭，以原子彈結束的第二次世界大戰，可稱之為物理學家的戰爭。以此類推，有人相信第三次世界大戰將是數學家的戰爭，因為數學家將掌控下一場大戰的重要武器—資訊。

約翰・查威克在《線形文字 $B$ 的解譯》中說道「揭開秘密的衝動是人類根深蒂固的天性。就是最不好奇的心，也會為即將得知他人的秘密而悸動。有些幸運的人能以解謎為業，我們大部分的人卻得靠解開那些供消遣之用的矯造謎語來滿足這種慾望。對一般人而言，偵探故事或縱橫字謎便已足夠，極少數人則是以破解玄密的符號為志業」。

現在就讓密碼學家耍一道需要一點解密過程的《讀心術遊戲》，來滿足一般讀者的好奇心，也當成本章科學家餘興節目的內容：下圖中的左圖縱橫各六行列，一共有 36 位小朋友，每位小朋友只有站立或蹲下兩種情形，每按電腦的亂碼鈕一次，這 36 位小朋友會隨機設定成站立或蹲下。雖然是隨機，但是還是有某一種「特色」存在，請讀者從圖中解讀出這關鍵的「特色」是什麼？當我們點選圖中一位小朋友時，此小朋友及其前、後、左、右共 5 位小朋友的狀態都會改變，即站立者變成蹲下者，而蹲下者卻變成站立者。例如：點選左圖中坐標為 $(4,3)$ 的小朋友之後，就會變成右圖的小朋友站、蹲分布狀態。


讀心術遊戲是這樣進行的「讀心專家先閉上眼睛，被讀心的人在電腦上隨

意的按電腦的亂碼鈕，按愈多次愈好，這樣小朋友的站蹲分布才會很亂。然後，從圖中選定 1 位小朋友，並點選他，舉例來說，下圖中 36 位小朋友的站蹲分布就是某位被讀心人操作的結果」。接著讀心專家張開他的雙眼，看著 36 位小朋友的分布圖及傾聽被讀心人的心跳，讀心專家可以辨識出剛剛被點選的小朋友的坐標，你相信嗎？理由又為何呢？




最後，感謝臺灣商務印書館翻譯的科普書籍《碼書》（賽門・辛著，劉燕芬譯），讓我對密碼學的歷史有基本的認識，也謝謝我的研究生陳裕錫幫我撰寫 Flash 版的《許教授的讀心術》遊戲，關於密碼學的科普書籍也可以參閱天下文化出版的《數學小魔女》（夫蘭納里著，葉偉文譯）與衛城出版的《資訊》（詹姆斯・葛雷易克著，賴盈滿譯）。