破解密碼

黃文璋
國立高雄大學應用數學系

在沙朗史東與麥克道格拉斯合演的第六感追緝令那部電影中, 麥克道格拉斯爲了表示他很難被捉摸, 說"I am very unpredictable" 。結果擅長分析人性的沙朗史東與他同時說出unpredictable一字 。

在日常生活中, 我們常會用到密碼, 如號碼鎖 、提款卡及上網的密碼等 。如何挑選密碼? 用生日 、女兒名字或家裡門牌號碼? 不少人傾向挑選與自己相關的數字或文字 。如果提款卡與皮包一起遺失, 皮包中的身分證及記事本等, 便會透露不少關於遺失者的個人資料 。因此這樣設定密碼, 雖容易記憶, 卻很容易被破解 。

對於個人密碼, 隨機挑選數字或英文字母的組合（例如用抽籤產生數字或字母）最難被破解 。同樣的道理, 要藏貴重物品, 最好先將可藏的地點編號, 然後隨機地挑一個, 這樣才是最難被找到的 。不要藏在那些浮上你腦海中自認難找的地點 。

有些密碼的設定, 不是那麼難破解 。以國際書碼（簡稱ISBN）爲例 。爲了檢誤, 那一串10個數字, 依序分別乘上$1, 2, 3, \cdots, 10$相加後必須是11的倍數 。例如, 有一本書之編碼爲957-21-0686-4, $9 \times 1 + 5 \times 2 + \cdots + 4 \times 10$等於253, 的確是11的倍數 。收集夠多的書碼, 喜愛數字的人, 要看出這種編碼方式並非不可能 。當然書的編碼方式被知道, 影響倒不是那麼大 。

再看有些入學考試的彌封號碼, 爲將准考證號碼都加上一個固定的數。例如都加14號, 則1001成爲1015, 1002成爲1016, 依此類推。放榜會議時, 只顯示出彌封號以免有徇私。採用這種簡單的對照關係, 於放榜後比較容易將彌封號還原成准考證號碼, 且不易出錯。但長期參與試務工作者, 或有心人是很容易看出這種編碼方式。如果彌封號不是這麼有規律的產生, 還原時出錯就天下大亂了。

也許爲了維持一定的小獎中獎率, 北銀吉時樂小獎的中獎號碼採用類似由准考證號碼造出彌封號的原理(當然應較複雜些)。其實若設定一套亂數機制以產生中獎號碼, 機率的理論告訴我們, 實際中獎率與所設定的中獎機率相差不會太大。除非是像樂透彩頭獎號碼以隨機的方式產生, 只要不是隨機產生, 經過足夠時間的比對, 就沒有破不了的密碼。北銀如果每期更換規律還好, 若一直未更換, 幾期下來就變成very predictable。