# 密碼世界

游書海

今期首先要爲大家介紹的書，書名喚作《數學小魔女》，是台灣天下遠見出版股份有限公司出版的新書。不過，這書名跟原來的英文書名：《In code —— A Mathematical Journey》委實相去甚遠。

這本書的好處，該是讓家長們認識到，如何可以讓子女樂於接近科學以至數學，又如何讓他們具有充足的自信去自己解決問題。再者，本書的主角是位女孩子，這對於傳統觀念中女性總難以在數學領域做出成績，不啻是一次顛覆。而對於教師來說，他們在本書中看到的該會是：良好的教育環境能激發青少年的科學天賦，可惜，香港的青少年大部份都沒能夠處身在這樣良好的教育環境裏。

《In code —— A Mathematical Journey》是由 Sarah Flannery 與她的父親 David Flannery 合著的，內容描述她怎樣進行有關密碼學的研究，並因而奪得 1999 年愛爾蘭、歐洲青少年科學家大獎。

書的第一章就告訴我們，本書的主人翁 Sarah Flannery 之所以對數學有興趣，喜歡獨立思考，是因爲她有一個好父親，他從來不會逼她背數學公式，做數學作業，他只是出些好玩的數學謎題讓她猜，這樣猜呀猜，就教她猜出對數學的興趣。

所謂「趣題引智」，對於小孩子，適度的數學謎題確能起到啓導他們對數學的興趣，使他們敢於獨立思考，同時亦鍛鍊他們解決問題的毅力。這本書裏就介紹了好些有趣的數學謎題，讀者大可讓自己的子女或學生嘗試解決。

由於本書的主人翁是因爲研究與密碼有關的數學方法而得獎的，所以本書的大部份篇幅都談到密碼數學，而筆者覺得，書中所談的這些東西都能做到深入淺出，讓讀者很快明白現代密碼學中的數學原理。例如書中談到『單向函數』和『陷門』的概念，就反覆地舉了好些生動有趣的例子作比喻，使讀者能夠非常了解這些概念的內函。這是本書另一值得稱讚的地方。

說到密碼，相信誰也不會否認是很好玩的東西，用密碼遊戲來把青少年以至小學生引向數學，肯定是個好方法。所以，筆者今期除了介紹《數學小魔女》這本書外，還想多介紹幾本談密碼數學的書供讀者參考：

## SOS——編碼縱橫談

**談祥柏編著　上海教育出版社出版**

本書由四十多個短篇綴合而成，以輕鬆的筆調講述中外的許多有趣的密碼故事，中學生應可以自行閱讀。小學老師則不難挑選某些小學生也能理解的故事來說給他們聽。

## 密碼傳奇——從軍事隱語到電子芯片

**Rudolf Kippenhahn 著　鄧白樺、姚文俊、滕峻輝譯**

**上海譯文出版社出版**

這本書固然是科普讀物，但也可說是一本很好的西方密碼發展史。作者涉古通今，旁征博引，通過敘述發生在加密者和解密者之間的故事，揭示許多耳熟能詳的典故背後的內幕，讀來趣味盎然。正如譯者所說，這本書不但爲數學愛好者和喜歡玩弄數字符號的人提供了一個充滿遊戲和謎語的遐想空間，也爲一般讀者了解密碼王國打開了一扇知識之窗。

## 計算密碼學

**盧開澄著　湖南教育出版社出版**

本書是『走向數學』叢書中的一冊，較多較深入地從數學的角度來介紹近代的密碼學的知識。相比起上述的幾本書，這本《計算密碼學》是專門得多難讀得多，但有一定數學修養的讀者應可讀懂書中大部份的內容。

全書分兩部份，首部份介紹密碼學中幾個基本概念，第二部份介紹近代密碼學研究中的許多著名問題，如 RSA 公鑰密碼系統、數字簽名、概率加密、零知識證明等等。在有關的論述中，涉及的數學分支包括概率統計、信息論、數論、置換群、有限域、組合學以及算法複雜性理論等，可見密碼學涉及的數學的分支實在是多種多樣的。