17 質數的應用與密碼學

有人將質數比喻爲數的原子。任何整數皆由質數組成由算術基本定理,任何正整數皆可表爲質數的乘積。”萬物唯數”,而質數正是數的原子,可見其在數學中的重要性。

過往,質數的應用,非常有限。可是,隨著資訊科技的發展,質數卻變得非常重要,數論的研究如雨後春筍,散佈數學的每一個角落,尤並在保密與加密的使用更爲顯著。

17.1 資訊年代

在當今資訊年代，每一件事物總得黏上一些訊息，而這些訊息亦或多或少會涉及到不欲爲第三者知道的資料和秘密，傳送這些訊息，便需要保密。過往，使用的保密的方法繁多，方法各異，例如:

1. 隱藏

   (a) 公元前 227 年，燕國的樊於期將軍，甘願將自己的頭臚交給荊軻，讓荊軻作爲進見秦王的手信，荊軻提著樊於期的首級，帶著督亢(古地名,今河北省涿州市附近)的地圖見秦王（代表割地督亢），地圖內藏暗格，藏有一把匕首，當他展開地圖給秦王看的時候，圖窮匕現，他便取出匕首，上前行刺秦王，惜最終事敗，被殺。

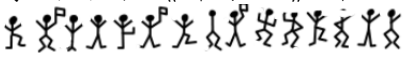
   (b) 據說古羅馬人亦有將信使的頭髮剃光，將密函寫在信使的頭頂，利用信使新長出的頭法來掩蔽密函。

   (c) 走私販子將走私物品隱藏,僞裝。有行李箱的暗格者,亦甚或收藏毒品於體內等。

   (d) 將密函用微縮的方法，縮影成一篇文章內的某個標點，據說是冷戰時期，美蘇間碟用的保密方法。

   (e) 使用隱形墨水。如使用酸性液體（如檸檬汁）寫在紙上，酸性液體乾透後,連同文字隱去，經加熱,可得回訊息。武俠小說《鹿鼎記》中的四十二章經,暗藏清朝龍脈的秘密,韋小寶不小心將四十二章經掉入火盤,從而發現秘密。

ii. 暗號的使用

- 電影中常見類似的橋段，如以摘柸爲號，打牌的時候打暗號示意叫胡的牌。
- 在比賽中,以暗號示意隊友進攻策略。
- 福爾摩斯探案《歸來記》中“跳舞的人“內，以不同舞者的形象圖案作密碼傳遞訊息。 
- 遠足時,在分叉路上,在樹枝上綁上顏色絲帶或在地上留下記號,示意隨後隊友行走方向。

- 在我國的兵書《六韜》亦談到如何以暗號傳遞軍令。《六韜》據說爲姜子牙所作,惟《六韜》的作者已不可考。全書以姜太公與周文王、周武王對話的方式編成。在《六韜》中的《龍韜》之「陰符」("陰"意指隱蔽)中，姜子牙講述如何用兵符的長度來傳遞有關戰況的訊息。

  武王問太公曰： 引兵深入諸侯之地，三軍卒有緩急 ，或利或害。吾將以近通遠，從中應外，以給三軍之用，爲之奈何？

  太公曰： 主與將有陰符 ，凡八等：有大勝克敵之符，長一尺；破軍擒將之符，長九寸；降城得邑之符，長八寸；卻敵報遠之符，長七寸；誓眾堅守之符，長六寸；請糧益兵之符，長五寸； 敗軍亡將之符，長四寸；失利亡士之符，長三寸。諸奉使行符，稽留若符事泄，聞者告者皆誅之 。八符者，主將秘聞，所以陰通，言語不泄、中外相知之術，敵雖聖智，莫之能識。

  使用愈長的兵符,表示愈好的消息,愈短的則愈凶。據說《六韜》爲公元前所作,可見古時已有使用長短來表示吉凶,日常有所謂"三長兩短"是否與此有關,又或是與無蓋的棺材板是三塊長,兩塊短有關,可待考證。

iii. 編碼或重組訊息

- 《六韜》中的「陰書」亦談及如何將訊息分拆送出,再將訊息重組解讀。內文亦很清楚地分析到,使用符號來傳遞訊息的局限,是以需用編碼的方法。

  武王問太公曰： 引兵深入諸侯之地，主將欲合兵，行無窮之變，圖不測之利。其事煩多，符不能明；相去遼遠，言語不通。爲之奈何？

  太公曰： 諸有陰事大慮，當用書，不用符。主以書遣將，將以書問主。書皆一合而再離，三發而一知。再離者，分書爲三部。三發而一知者，言三人，人操一分，相參而不相知情也。此謂陰書。敵雖聖智，莫之能識。

  陰書所描述的傳密方法可看作「整存零付」,將一整段訊息分拆,由數人運送,得到訊息的一方再將零散的訊息整合。例如,分別由三人送出以下三段文字:

  六一先事之的
  韜部秦思大著
  是集軍想成作

  將文字逐一由不同段落取出,便可得到:六韜是一部集先秦軍事思想之大成的著作。

- 某些網上的電子銀行,亦採用類似上述的「整存零付」方法,在每次輸入密碼時,只需用户輸入全組密碼中的某幾個字符(每次指定隨機的不同位置的字符),銀行再核對密碼。
- 某些網上的電子銀行,在每次輸入密碼時,回送一個重新編排過的鍵盤,讓用户以滑鼠在版面上點選字符,輸入密碼,銀行再在自己的終端將輸入的字符重組,核對密碼。
- 現今使用之密碼,如公鑰密碼等

17.2 郵遞問題

(一般會將以下問題冠名爲"俄羅斯郵遞問題",更有謂以前的俄羅斯郵遞人員,會盜取郵件內的物件,然而,實情是否如此,不得而知,但是,對俄羅斯人不太專重,所以抹去"俄羅斯"三字。)

> 在某地，郵務人員非常好奇，要是郵包不加上鎖，郵務人員總會打開郵包偷看。A 小姐欲將一個內藏情信的盒子寄給 B 先生，當然,將盒子密封寄給 B 先生是一個方法,可是不想只能破壞盒子才可將它打開,亦希望能再重用盒子,惟有將盒子上鎖,問他們如何可以，將盒子上鎖寄給 B 先生,使得盒子在上鎖後,不會被郵務人員 C 偷看，而 B 君可以順利地打開盒子呢？（A 小姐不可以將鎖匙寄出）。

現今銀行將提款卡及密碼分開寄出便是一個方法,以下是 A 小姐和 B 先生使用的方法：

1. A 小姐將盒子用 X 鎖鎖上,將盒子寄給 B 先生
2. B 先生收到盒子後，在盒子上加上另一把鎖 Y,再將盒子寄回給 A 小姐
3. A 小姐收到盒子後，用自己的 X 鎖匙解去 X 鎖，再將盒子寄回給 B 先生
4. B 先生收到盒子後，用自己的 Y 鎖匙解去 Y 鎖, 打開盒子

在密碼學中,習慣上稱送件人爲 Alice ，收件人爲 Bob，帶惡意的瞥伯（第三者）爲 Chuck (以前有稱爲 Carol, 但是對名爲 Carol 的人不大好，故改之）。

17.3 郵遞問題的應用

在日常生活中，類似郵遞問題的解決方法已廣爲應用，例如:

1. 網上繳費
   (a) A (客户) 由電腦發出繳費指令給 B (繳費服務中心)
   (b) B 由電話發出含有密碼的短訊給 A
   (c) A 由電腦輸入 B 的密碼完成交易
2. 網上電子銀行
   (a) B (銀行) 送一個密碼機給 A(客户) 長期保存,這個密碼機會隨著時間,產生不同的密碼,以時間作爲輸入來產生密碼的公式只有銀行知道。
   (b) A 以固定的個人密碼登入銀行網頁
   (c) B 要求 A 輸入時間密碼
   (d) A 輸入時間密碼完成登入個人賬户