

2001TRML 個人賽之解法

楊明雯

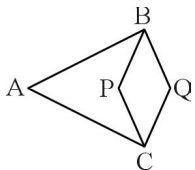
國立宜蘭高級中學

一、引言

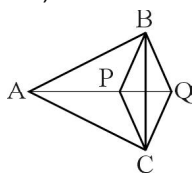
今年暑假 8 月 18、19 日由九九文教基金會主辦的 TRML 競賽在台灣大學、國立台灣科技大學、國立台北商業技術學院及市立金華國民中學熱鬧展開，當時吸引全台灣多所高中學生參加，本人當時帶領學生參加此競賽，回來後，為了增進學生對於數學競賽的興趣，針對個人賽的部分進行解法研討，發現當時每兩個題目只能做 10 分鐘，和之後研討後的解法有多處不同，思考方式也更加嚴密，也發現一個問題有時不會只有一種解法，在學生與老師的互相激勵下，往往衍生出多種解釋，學生也因此擁有腦力激盪的機會，利用這次個人賽的題目，討論出問題的解答。

二、題目

第一題 . 如圖所示， $\overline{AB} = \overline{AC} = 6$ 、 $\overline{BP} = \overline{BQ} = \overline{CP} = \overline{CQ} = 4$ 。求 $\overline{AP} \cdot \overline{AQ}$ 之值。



(解一)



連接 \overline{AP} 、 \overline{PQ} 、 \overline{BC} 因為 BQCP 為菱形，所以對角線互相垂直平分， \overline{PQ} 、 \overline{BC} 相

交於 M，假設 $\overline{AP} = x$ ， $\overline{PM} = \overline{MQ} = y$ ， $\overline{BM} = \overline{MC} = h$ 可得

$$(x+y)^2 + h^2 = 36 \cdots \cdots (1)$$

$$y^2 + h^2 = 4^2 = 16 \cdots \cdots (2)$$

$$(1) - (2) \quad x^2 + 2xy = 20$$

$$\text{而 } \overline{AP} \cdot \overline{AQ} = x(x+2y) = 20$$

(解二)

假設 $\overline{AM} = x$ ， $\overline{PM} = \overline{MQ} = y$ ， $\overline{BM} = \overline{MC} = h$ 得到

$$x^2 + h^2 = 36 \cdots \cdots (1)$$

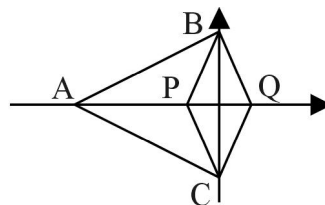
$$y^2 + h^2 = 16 \cdots \cdots (2)$$

$$(1) - (2) \quad x^2 - y^2 = 20$$

$$\overline{AP} \cdot \overline{AQ} = (x+y)(x-y) = x^2 - y^2 = 20$$

分析：解一和解二其實為同一種類型，但是屬於觀察直角三角形各股長與 \overline{AP} 和 \overline{AQ} 的關係，才能看出結果，多數同學了解此題可設未知數，也能了解菱形對角線會互相垂直平分的性質。

(解三) 利用解析幾何做法



假設 \overline{PQ} 、 \overline{BC} 的交點 M 座標為 (0, 0) 設 $P(-x, 0)$ ， $Q(x, 0)$ ， $A(-y, 0)$ ， $B(0, h)$ 得到

$$(-x)^2 + h^2 = 4^2 \cdots \cdots (1)$$

$$(-y)^2+h^2=6^2\cdots\cdots\cdots(2)$$

$$(2)-(1) \quad y^2-x^2=20$$

$$\overline{AP} \cdot \overline{AQ} = (-x+y)(x+y) = y^2 - x^2 = 20$$

分析：以上三種做法，但是我也發現如果對於分析不佳的學生，會試著使用第三種解法(解析幾何)設立坐標軸，一樣能解出答案。

第二題 . 設數列 $\{a_n\}_{n=1}^{\infty}$ 滿足： $a_1=2$ ， $a_2=500$ ， $a_3=2000$ ，並設 $\frac{a_{n+2} + a_{n+1}}{a_{n+1} + a_{n-1}} = \frac{a_{n+1}}{a_{n-1}}$ ， $n=2, 3, 4, \dots$ 。求 $\frac{a_{2001}}{a_{1999} \cdot a_{2000}}$ 之值。

(解一)

將 $\frac{a_{n+2} + a_{n+1}}{a_{n+1} + a_{n-1}} = \frac{a_{n+1}}{a_{n-1}}$ 交叉相乘，得到 $(a_{n+2} + a_{n+1}) a_{n-1} = (a_{n+1} + a_{n-1}) a_{n+1}$ 可以得到 $a_{n+2} a_{n-1} = a_{n+1} a_{n+1} + a_{n-1} a_{n+1}$ (其中 $a_{n+1} a_{n-1}$ 相消) 列出一連串漸進式

$$\begin{aligned} a_{2001} a_{1998} &= a_{2000} a_{2000} \\ a_{2000} a_{1997} &= a_{1999} a_{1999} \\ a_{1999} a_{1996} &= a_{1998} a_{1998} \\ &\dots\dots\dots \\ &\dots\dots\dots \\ a_5 a_2 &= a_4 a_4 \\ a_4 a_1 &= a_3 a_3 \end{aligned}$$

等式兩邊連乘，相同的消去，得到

$$\text{所以 } \frac{a_{2001}}{a_{1999} \cdot a_{2000}} = \frac{a_1}{a_1 \cdot a_2} = \frac{a_2 = a_3}{a_3} = \frac{a_{1999} a_{2000}}{2 \cdot 500} = 2$$

(解二)

先算出 $a_4=2000000$ ，再從 $\frac{a_3}{a_1 \times a_2} = 2 = \frac{a_4}{a_3 \times a_2}$ ，依此類推答案可能為 2，進而證明正確性，從解一中將 $\frac{a_{n+2} + a_{n+1}}{a_{n+1} + a_{n-1}} = \frac{a_{n+1}}{a_{n-1}}$ 交叉相乘，可以得到 $a_{n+2} a_{n-1} = a_{n+1} a_{n+1} + a_{n-1} a_{n+1}$ (其中 $a_{n+1} a_{n-1}$ 相消)

等號兩邊同乘 a_n 得到 $a_{n-1} a_n a_{n+2}$

$$\begin{aligned} &= a_n a_{n+1} a_{n+1} \\ &\Rightarrow \frac{a_{n+1}}{a_n \cdot a_{n-1}} = \frac{a_{n+2}}{a_{n+1} \cdot a_n} \text{類推} \\ &\frac{a_3}{a_1 \cdot a_2} = \dots = \frac{a_{n+1}}{a_n \cdot a_{n-1}} = \frac{a_{n+2}}{a_{n+1} \cdot a_n} = \frac{a_{n+3}}{a_{n+2} \cdot a_{n+1}} \\ &= \dots = \frac{a_{2000}}{a_{1999} \cdot a_{1998}} = 2 \end{aligned}$$

分析：這一部分是第一冊中遞迴式的部分，但是學生所學的過程中並沒有看過連續四項的關係式，所以看到分式，習慣將它交叉相乘化簡，從中看出遞迴關係式，此題就是以此種方法起步。

第三題 . 設 $x > 1$ ， $y > 1$ ，且 $(\log_{10} x)^2 + (\log_{10} y)^2 = \log_{10} x^2 + \log_{10} y^2$ ，求 $x^{\log_{10} y}$ 的最大值。

(解一)

求 $x^{\log_{10} y}$ 的最大值，相當於先求 $\log_{10} x \log_{10} y$ 的最大值方便起見，令 $\log_{10} x = a$ ， $\log_{10} y = b$ ，得到 $a^2 + b^2 = 2a + 2b$

$$\Rightarrow (a-1)^2 + (b-1)^2 = 2 \text{ 利用圓的參數式}$$

$$(a, b) = (1 + \sqrt{2} \cos q, 1 + \sqrt{2} \sin q)$$

$$ab = 1 + \sqrt{2}(\cos q + \sin q) + 2 \sin q \cos q$$

令 $t = \cos q + \sin q$ ， $-\sqrt{2} \leq t \leq \sqrt{2}$ (由三角函數的疊合得知)

$$\begin{aligned} ab &= 1 + \sqrt{2}t + t^2 - 1 = t^2 + \sqrt{2}t \\ &= \left(t + \frac{\sqrt{2}}{2}\right)^2 - \frac{1}{2} \end{aligned}$$

得到 $t = \sqrt{2}$ 時有最大值 $ab=4$

所以 $x^{\log_{10} y}$ 的最大值為 $10^4=10000$ 。

(解二)

利用算數平均數大於等於幾何平均數

$$\frac{(\log_{10} x)^2 + (\log_{10} y)^2}{2} \geq \sqrt{(\log_{10} x)^2 (\log_{10} y)^2}$$

$$= \log_{10} x \cdot \log_{10} y \cdots\cdots\cdots(1)$$

因為 $(\log_{10} x)^2 + (\log_{10} y)^2 = \log_{10} x^2 + \log_{10} y^2$

(1)可改成 $\frac{\log_{10} x^2 + \log_{10} y^2}{2} \geq \log_{10} x \cdot \log_{10} y$

$$\log_{10} x + \log_{10} y \geq \log_{10} x \cdot \log_{10} y$$

等號成立發生在 $\log_{10} x = \log_{10} y (x > 1, y > 1)$
 得到 $x = y$ ，代回原式 $(\log_{10} x)^2 + (\log_{10} y)^2 = \log_{10} x^2 + \log_{10} y^2$ 得到 $x = y = 100$ ，所以 $\log_{10} x \log_{10} y$ 的最大值為 4， $x^{\log_{10} y}$ 的最大值為 $10^4 = 10000$ 。

(解三)

利用柯西不等式

$$[(\log_{10} x)^2 + (\log_{10} y)^2](2^2 + 2^2) \geq$$

$$(2\log_{10} x + 2\log_{10} y)^2$$

$$\text{因為 } (\log_{10} x)^2 + (\log_{10} y)^2 = \log_{10} x^2 + \log_{10} y^2$$

$$8(\log_{10} x^2 + \log_{10} y^2) \geq 4(\log_{10} x + \log_{10} y)^2$$

$$\text{令 } \log_{10} x + \log_{10} y = t \quad t > 0$$

$$16t \geq 4t^2$$

$$t^2 - 4t \leq 0$$

$$t(t - 4) \leq 0$$

$$0 \leq t \leq 4 \text{ 且 } t > 0 \Rightarrow 0 < t \leq 4$$

$$\text{又 } t^2 - 2\log_{10} x \log_{10} y = 2t$$

$$\log_{10} x \log_{10} y = \frac{1}{2}(t - 1)^2 - \frac{1}{2}$$

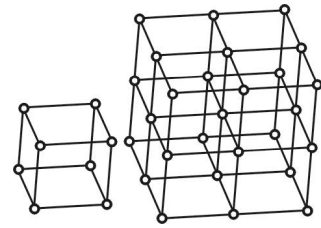
所以當 $t = 4$ 時， $\log_{10} x \log_{10} y$ 有最大值 4

$x^{\log_{10} y}$ 的最大值為 $10^4 = 10000$ 。

分析：這個題目所能用到的方法很多，有算幾不等式甚至三角函數，或是柯西不等式(向量上)，也可以利用幾何學來解釋，起因於算極大與極小值的方法本來就有很多，學生可以比較不同的解法，了解其中的差異。

問題四．如右圖所示的立方架，利用 1 單位長的鐵桿焊接而成， $1 \times 1 \times 1$ 立方架需要 12 根鐵條， $2 \times 2 \times 2$ 立方架需要 54 根，試問 $10 \times 10 \times 10$ 的立方架需要多少根這種鐵條焊接？

(解一)



分別從長、寬、高來討論所需要的根數，發現 $n \times n \times n$ 立方架需要 $n \times (n+1) \times (n+1)$ 根構成所有長，同理也需要 $n \times (n+1) \times (n+1)$ 根構成寬與高，因此 $n \times n \times n$ 的立方架共需要 $n \times (n+1) \times (n+1) \times 3$ 根，所以 $10 \times 10 \times 10$ 的立方架共需要 $10 \times 11 \times 11 \times 3 = 3630$ 根鐵條。

分析：此題為數學遊戲中的一種，利用分析長、寬、高的規律就可以得出共需要多少鐵條，此題對於學生而言，是屬於容易的一題。

(解二)

有些學生是觀察 $a_1 = 12$ ， $a_2 = 54$ ， $a_3 = 144$ ， $a_4 = 300$ ， $a_5 = 540$ 則 $a_2 - a_1 = b_1 = 42$ ， $a_3 - a_2 = b_2 = 90$ ， $a_4 - a_3 = b_3 = 156$ ， $a_5 - a_4 = b_4 = 240$ ， $b_2 - b_1 = c_1 = 48$ ， $b_3 - b_2 = c_2 = 66$ ， $b_4 - b_3 = c_3 = 84$ ， $b_2 - c_2 - c_1 = 18$ ， $c_3 - c_2 = 18$ 所以依此類推出 $c_4 - c_3 = 18$ ， $b_5 - b_4 = 102$ ， $a_6 - a_5 = 542$ ，所以 $a_6 = 1082$ 得到 $a_{10} = 3630$

(解三)

從解二中，可以觀察出遞迴式，得到 $a_{n+3} - 3a_{n+2} + 3a_{n+1} - a_n = 18$ ，其中 $a_1 = 12$ ， $a_2 = 54$ ， $a_3 = 144$ ， $(a_{n+3} - a_{n+2}) - 2(a_{n+2} - a_{n+1}) + (a_{n+1} - a_n) = 18$
 令 $b_n = a_{n+1} - a_n \Rightarrow b_{n+2} - 2b_{n+1} + b_n = 18$
 其中 $b_1 = 42$ ， $b_2 = 90$
 令 $c_n = b_{n+1} - b_n \Rightarrow c_{n+1} - c_n = 18$
 其中 $c_1 = b_2 - b_1 = 48$

所以 $c_n = c_1 + 18(n-1) = 18n + 30$

$$b_n = b_1 + 18\left(\frac{(n-1) \cdot n}{2}\right) + 30(n-1) = 9n^2 + 21n + 12$$

$$a_n = a_1 + 9\left(\frac{(n-1) \cdot n \cdot (2n-1)}{6}\right) +$$

$$21\left(\frac{(n-1) \cdot n}{2}\right) + 12(n-1) = 3n^3 + 6n^2 + 3n \text{ 所以}$$

$$a_{10} = 3630$$

分析：這三種方法嚴謹度不同，多數學生可能先想到的是解二，但是較難找出其關係式，只能依次類推，所以短時間競賽中，解一不失為一種好方法。

問題五 . 設 $P(x)$ 為非負的實係數多項式，若 $P(1)=4$, $P(2)=5$, $P(3)=6$, 求 $P(90)$ 。

(解)

因為此題針對 $P(x)$ 為非負的實係數多項式，所以討論如此的 $P(x)$ 是否有可能 $\deg P(x) \geq 2$, 一般而言，看到 $P(1)=4$, $P(2)=5$, $P(3)=6$, 我們會假設 $P(x) = (x-1)(x-2)(x-3)Q(x) + x + 3$, 如此一來， $P(90)$ 成為未定數，所以我們證明 $\deg P(x) < 2$, 令 $p(x) = (x-1)(x-2)(x-3)Q(x) + x + 3 = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, 又 $P(x)$ 為非負的實係數多項式，所以 $a_n, a_{n-1}, \dots, a_2, a_1, a_0 \geq 0$ 再令 $F(x) = P(x) - x - 3 = (x-1)(x-2)(x-3)Q(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + (a_1 - 1)x + (a_0 - 3)$

$$F(1) = 0$$

$$\Rightarrow a_n + a_{n-1} + \dots + a_2 + (a_1 - 1) + (a_0 - 3) = 0 \dots \textcircled{1}$$

$$F(2) = 0$$

$$\Rightarrow a_n 2^n + a_{n-1} 2^{n-1} + \dots + a_2 \cdot 2^2 + (a_1 - 1) \cdot 2 + (a_0 - 3) = 0 \dots \textcircled{2}$$

$$F(3) = 0$$

$$\Rightarrow a_n 3^n + a_{n-1} 3^{n-1} + \dots + a_2 3^2 + (a_1 - 1) \cdot 3 + (a_0 - 3) = 0 \dots \textcircled{3}$$

所以 $\textcircled{2} - \textcircled{1}$

$$a_n(2^n - 1) + a_{n-1}(2^{n-1} - 1) + \dots + a_2(2^2 - 1) + (a_1 - 1) = 0 \dots \textcircled{4}$$

$\textcircled{3} - \textcircled{1}$

$$a_n(3^n - 1) + a_{n-1}(3^{n-1} - 1) + \dots + a_2(3^2 - 1) + (a_1 - 1) = 0 \dots \textcircled{5}$$

$\textcircled{5} - \textcircled{4}$

$$a_n(3^n - 2^n) + a_{n-1}(3^{n-1} - 2^{n-1}) + \dots + a_2(3 - 2) = 0$$

因為 $a_n, a_{n-1}, \dots, a_2, a_1, a_0 \geq 0$, 所以 $a_n = a_{n-1} = \dots = a_2 = 0$ 因此 $P(x)$ 只能為一次式， $P(x) = a_1 x + a_0$ 又 $P(1)=4$, $P(2)=5$, $P(3)=6$, 所以 $P(x) = x + 3$, $P(90) = 93$

分析：當初很多學生馬上就能看出答案為 93，但是並不知道理論為何，而現階段第一冊所學的若 $f(x)$ 為大於或等於 n 次多項式，而 $f(a_1) = f(a_2) = f(a_3) = \dots = f(a_{n+1}) = 0$ ，即可得到 $f(x) = 0$ ，但是此題並沒有說明為幾次式，問題著重在 $P(x)$ 為非負的實係數多項式，所以證明為何 $P(x)$ 不可能為二次以上的式子。

問題六 . 對任意一正整數 n ，定義多項式 $f_n(x)$ 如下：

$$f_1(x) = 1 + x^3, f_2(x) = 1 + 4x^9, \dots, f_n(x) = 1 + n^2 x^{3^n}$$

設 $f_1(x)f_2(x)\dots f_9(x) = 1 + a_1 x^{k_1} + a_2 x^{k_2} + \dots + a_m x^{k_m}$ 。其中每個 a_i 與 k_i 都是正整數，且 $k_1 < k_2 < \dots < k_m$ ，試求 a_{30} 之值。

(解)

將 $f_1(x)f_2(x)\dots f_9(x)$ 相乘，因為 $f_n(x) = 1 + n^2 x^{3^n}$ ，對所有 x^{3^k} 項中，前面 $x^{3^1}, x^{3^2}, \dots, x^{3^{k-1}}$ 項相乘並不會影響 x^{3^k} 的係數

所以 $f_1(x)f_2(x)\dots\dots f_9(x)$ 中並不會有係數進位的情況產生，求 a_{30} 相當於第 31 項的係數，(第一項為常數項)

利用二進位法， $31=1+2+4+8+16$

所以相當於 $x^3 \cdot x^9 \cdot x^{27} \cdot x^{81} \cdot x^{243}$ 相乘後的係數，即為 $1^2 \cdot 2^2 \cdot 3^2 \cdot 4^2 \cdot 5^2 = (1 \cdot 2 \cdot 3 \cdot 4 \cdot 5)^2 = (5!)^2 = 120^2 = 14400$

分析：此題下手的重點即在於認清 $f_1(x)f_2(x)\dots\dots f_9(x)$ 相乘後係數並不會進位造成困擾，而 $f_n(x) = 1 + n^2 x^{3^n}$ 皆為兩項，所以每一個數字皆可以用二進位表示法表示，得到係數為 $1^2 \cdot 2^2 \cdot 3^2 \cdot 4^2 \cdot 5^2$ 。

第七題 . 從五個不同的正整數中，任意選出四個數，並計算其乘積，結果發現這樣的乘積分別為：x，y，z，140 及 210。試求 xyz 之最小值。

(解一)

先分解 $140=2^2 \times 5 \times 7$ ， $210=2 \times 3 \times 5 \times 7$ ，觀察數字，發現這五位正整數中，必有兩個數字有 2，

由 $140=2^2 \times \dots$ 觀察出，代表從兩個正整數中分別抓出 2。

同理其餘數字由 3，5，7 所組成，所以 $xyz \times 140 \times 210 = 2^8 \times 3^4 \times 5^4 \times 7^4$

$$xyz = 2^5 \times 3^3 \times 5^2 \times 7^2 = 1058400$$

(解二)

設此五數 a,b,c,d,e,則 140×210 中間必有三數重複，假設為 a,b,c $\Rightarrow (abc)^2 de = 140 \times 210$
又 $140=2^2 \times 5 \times 7$ ， $210=2 \times 3 \times 5 \times 7$ ，
 $\Rightarrow 140 \times 210 = 2^3 \times 3 \times 5^2 \times 7^2$

所以 $(abc)^2 = (2 \cdot 5 \cdot 7)^2 = 70^2$
則 $de = \frac{140 \times 210}{(2 \cdot 5 \cdot 7)^2} = 6$

$$\text{又 } 140 \times 210 \times xyz = (abcde)^4$$

所以 xyz 之積最小應為

$$(abc)^2 (de)^3 = 70^2 \cdot 6^3 = 1058400$$

分析：此兩種解法皆由觀察四個數乘積應有的規律出發，學生多能看出此種關係。

第八題 . 已知有 $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots, \frac{1}{2001}$ 共 2001 個數，規定 "操作" 一次如下：拿掉其中任兩數 a，b 後，其餘不動，再加入一數 a+b+ab。經過 2000 次這樣的操作之後只剩下一數，求此數。

(解)

先考慮 $\frac{1}{p}, \frac{1}{q}, \frac{1}{r}$ 三數，先證明其分配律成立，即先操作 $\frac{1}{p}, \frac{1}{q}$ ，再操作 $\frac{1}{r}$ 或先操作 $\frac{1}{q}, \frac{1}{r}$ ，再操作 $\frac{1}{p}$ ，所得的結果是一樣的，才可知先操作任何數結果相同。

先操作 $\frac{1}{p}, \frac{1}{q}$ ，剩下 $\frac{1}{p} + \frac{1}{q} + \frac{1}{pq}$ 和 $\frac{1}{r}$ 得到 $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} + \frac{1}{pq} + \frac{1}{pr} + \frac{1}{qr} + \frac{1}{pqr}$
或先操作 $\frac{1}{q}, \frac{1}{r}$ ，剩下 $\frac{1}{q} + \frac{1}{r} + \frac{1}{qr}$ 和 $\frac{1}{p}$ 得到 $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} + \frac{1}{pq} + \frac{1}{pr} + \frac{1}{qr} + \frac{1}{pqr}$

同理類推至操作四數時，任兩數先操作其結果相同，類推至有限個(2001 個)代表 $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots, \frac{1}{2001}$ 這 2001 個數中，先操作哪一個結果相同。

而且觀察到 $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} + \frac{1}{pq} + \frac{1}{pr} + \frac{1}{qr} + \frac{1}{pqr}$
即為 $(x - \frac{1}{p})(x - \frac{1}{q})(x - \frac{1}{r}) - 1$ 而 x=1 帶入

所以操作 $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots, \frac{1}{2001}$ 這 2001 個數，即為 $(1 + \frac{1}{1})(1 + \frac{1}{2})(1 + \frac{1}{3})$

$$\begin{aligned} & \left(1 + \frac{1}{4}\right) \cdots \left(1 + \frac{1}{2001}\right) - 1 \\ &= \frac{2}{1} \cdot \frac{3}{2} \cdot \frac{4}{3} \cdots \frac{2002}{2001} - 1 = 2001. \end{aligned}$$

分析：此題多數同學利用前三個數字推出結果為 3，所以依次類推這 2001 個數也會得到結果為 2001，但並不知道其理論支持，但是在短時間競賽中，此種能以小類推大數字的方法，不失為解題法之一。

三、結語

從數學競賽中，學生可以藉此得到腦力激盪的機會，也可以測驗數學知識整合的程度，有時候老師的工作必須評量學生想法的邏輯性，從旁協助，因為光是學生的想法就千變萬化。以上可能只為解法的其中之一，想藉此拋磚引玉引起學生更多的解題想法，也希望先進多多指教。

(上承第 15 頁)

結語

紐約及華府遭受的恐怖攻擊凸顯了情報蒐集的重要，雖然蒐集情報所涉及的領域比密碼學要廣得多，但是密碼學在其中扮演著關鍵的角色；據報載，美國鎖定的頭號主嫌賓拉登平素對先進加密技術即抱持著高度的興趣；雙方的開打可以想見在密碼學領域將有一番較勁。

英文裡，研究加密的方法的學問稱為 Cryptography，研究如何破解密文的學問稱為 Cryptanalysis，這兩個領域合起來則稱為 Cryptology。

本文限於篇幅，只介紹了代換加密法的四種類型中的兩種，另外兩種有機會筆者將另文介紹。

參考資料

1. 許介彥(2001), 密碼學初步, 科學教育月刊, 第 239 期.
 2. Dorothy E. R. Denning, Cryptography and Data Security, Addison-Wesley, 1982.
 3. Martin Gardner, Codes, Ciphers, and Secret Writing, Dover, 1972.
 4. William Stallings, Cryptography and Network Security, 2nd edition, Prentice Hall, 1999.
- 作者信箱：chsu@mail.dyu.edu.tw