數論在密碼上的應用(下)

楊重駿　楊照崑

四、瑞未斯特、希米爾、愛得曼(Rivest, Shamir, Adleman)法

這個方法是上列三位科學家在 1978 所發表的，其步驟如下（又如圖 2 ）

1. 收報者取兩個相異的大質數 p 、q 及另一與 $(p-1)(q-1)$ 互質的數 a ，且 $a<w$ ，令
$w=(p-1)(q-1)$ ，
$m=pq$
及 p 、q 之較小者的位數（十進位）爲 k 。
2. （公開）告訴發報者 k ，m與 a 。
3. 發報者將他的信號分成許多段，每段含 $k-1$ 位數(十進位)

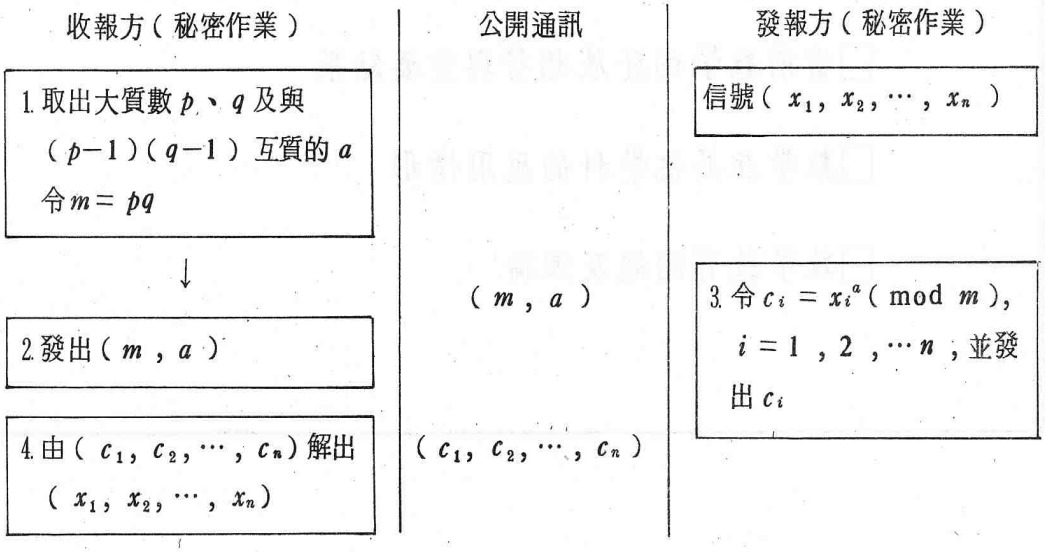

圖 2　（RSA 製碼法）在此作業程序中，m ，a ，c_1，⋯⋯ c_n 是公開的。

（若 $k=3$（即 p、q 均爲不小於二位的數），則信號

331414320001

則應分成

33,14,14,32,00,01

一個一個的考慮發出），設發報者的信號之一爲 x（$k-1$ 位數，即上例中之33, 或 14, 或 32, …），則他將它作成

$$c \equiv x^a \pmod{m}$$

發出。

4. 收報者收到 c 之後，即可把原有的 x 求出來，因 a 與 w 互質，由定理2.2及系知，我們可找到二整數 d、e；$d>0$ 使得

$$ad + we = 1$$

令

$$y \equiv c^d \pmod{m}$$

則此 y 即發報者之 x。我們先證明 $y=x$。

$$\begin{aligned} y &\equiv c^d \equiv (x^a)^d \equiv x^{ad} \\ &\equiv x^{1-we} \\ &\equiv x(x^{-we}) \pmod{m} \end{aligned} \tag{4.1}$$

但因 w、a、d 均爲大於1之整數，故 e 必爲一負數，即 $-e$ 爲一正數，又因 x 小於質數 p、q，故 x 同 m 互質，由定理2.3之系得

$$\begin{aligned} x^w &\equiv x^{(p-1)(q-1)} \\ &\equiv 1 \pmod{m} \end{aligned}$$

故(4.1)式成爲

$$\begin{aligned} y &\equiv x(x^w)^{-e} \equiv x \cdot 1 \\ &\equiv x \pmod{m} \end{aligned}$$

但因 y 與 x 均取小於 m 之數，故 $y=x$。故本程序之正確性得證。

這種密碼之關鍵在於 p、q 爲兩大質數時，分解 m 成爲 p、q 爲一件極費時的工作，若分解不開 m，則找不到 w 與 d，因此就無法從 c 解得 x，在不久以前，要分解一個數的因子仍停留在近乎硬試的階段，即要從2，3，5，7，…，一直試到 $\sqrt{n}$ 附近才停止。若 n 是50位數而 p、q 均近25位數，則分解 m 要除約 10^{25} 次，若以電子計算機以每秒 10^6 次的高速運算，這仍是一個 10^{11} 年的工作，目前由於大家對這方面的重視，分解一個 50 位數的時間已可縮斷至 10^{10} 次運算。下面的表中列出了目前（1980年），分解一個大數大概所需的時間。

m的位數	分解 m 的最少運算次數	最快（1980年）電腦所費的時間
50	1.4×10^{10}	3.9 小時
70	9.0×10^{12}	104 天
80	1.3×10^{13}	150 天
100	2.3×10^{17}	74 年
200	1.2×10^{23}	3.8×10^{9} 年

若取 pq 各爲 40 位數在目前已經十分安全了，即使是 25 位數，在商業上也十分安全，因爲 3.9 小時最快電腦的計算費用也是一筆大的財富。

讀者也許要問這種大質數是否很多，而且容易找到？答案是：大質數既多而又容易找，前面已談到找一個大質數不宜用硬除的辦法，但因找它們所用的定理比我們已證明的幾個要難，我們將在下節中才介紹出來。我們只談一下質數之多，依據質數定理在 1 與 n 之間的質數約有 $n/\log e^n$ 個，因此小於 10^{40}（即 40 位）的質數約有

$$10^{40}/\log e 10^{40} = \frac{10^{40}}{92.1} \geqslant 10^{38} \text{ 個}$$

這又是一個天文數字，因爲一個一千頓電子計

算機中所含的原子數不過 10^{31} 左右，可見這種密碼之難以捉摸了。現取兩個用來做密碼的十五位質數以饗讀者：

p = 5862031427 1421210354 0772438083

q = 7976488510 8326808223 7297393713

要分解

$m = pq$

= 4675842632 8739231725 4879360844

8514393251 3976539392 0565972179

若不懂數學與計算機，則是談何容易。在本節結束之前，我們也舉一個例子，當然我們不會用上列的大質數，我們且取 p、q 均爲兩位數，令

$$p = 47 , \quad q = 59$$

則

$$m = pq = 47 \times 59 = 2773$$

$$w = (p-1)(q-1) = 2668$$

取 $a = 157$，由輾轉相除可得

$$17a - 1w \equiv 1$$

故

$$d = 17$$

故收方發出的密碼法是

$$m = 2773 , \quad a = 157 , \quad k = 2$$

此時發方必須一位一位的發出信號，設第一個要發的信號是 3，則他要發出的是

$$c \equiv x^a \equiv 3^{157} \pmod{2773}$$

c 之求法主要在將 157 分成 2 進位數並用定理 2.1 即

$$x^2 \equiv (x \pmod m)^2 \pmod m$$

因 $157 = 2^7 + 2^4 + 2^3 + 2^2 + 1$，而

$3 \equiv 3 \bmod (2773)$

$3^2 \equiv 9 \bmod (2773)$

$3^{2^2} \equiv 9^2 \equiv 81 \pmod{2773}$

$3^{2^3} \equiv 81^2 \equiv 1015 \pmod{2773}$

$3^{2^4} \equiv 1015^2 \equiv 1442 \pmod{2773}$

$3^{2^5} \equiv 1442^2 \equiv 2387 \pmod{2773}$

$3^{2^6} \equiv 2387^2 \equiv 2027 \pmod{2773}$

$3^{2^7} \equiv 2027^2 \equiv 1916 \pmod{2773}$

故

$$3^{157} \equiv 1916 \times 1442 \times 1015 \times 81 \times 3 \pmod{2773}$$

$$\equiv 964 \times 1015 \times 81 \times 3 \pmod{2773}$$

$$\equiv 2364 \times 81 \times 3 \pmod{2773}$$

$$\equiv 441 \pmod{2773}$$

因此 $c = 441$ 即發方發出之信號，當收方收到 441 之後，用同樣的運算法可得 c^d 爲

$$441^{17} \equiv 441^{2^4+1} \pmod{2773}$$

$$\equiv 371^{2^3} \times 441 \pmod{2773}$$

$$\equiv 1764^{2^2} \times 441 \pmod{2773}$$

$$\equiv 390^2 \times 441 \pmod{2773}$$

$$\equiv 3 \pmod{2773}$$

解碼完成：由上面的運算可知若沒有電子計算機，則解與做這種密碼是何等的辛苦。

五 如何尋找大質數

現在也許你有興趣學一點難一些的數論定理了。

定理 5.1 設 a，m 互質，且

$$ab \equiv ac \pmod m$$

則

$$b \equiv c \pmod m$$

證明 因 $a(b-c) \equiv 0 \pmod m$ 而 a 不含 m 之因子，故 $b-c$ 必爲 m 之倍數，即 $b-c \equiv 0 \pmod m$ 本定理得證。

定義 設 m 爲任何一正整數，定義 $\phi(m)$ 爲所有小於 m 且與 m 互質的自然數的數目，例如取 $m = 5$，則小於 m 又與 m 互質的數爲 1，2，3，4，故 $\phi(5) = 4$，又如取 $m = 12$，則小於 m 而又與 m 互質的數爲 1，5，7，11，故 $\phi(12) = 4$。$\phi(m)$ 一般稱爲尤拉函數，是數論中一個重要的函數。

定理 5.2 設 m 爲一自然數 $\phi(m)$ 表示所有小與 m 且與 m 互質的自然數，又以 r_1, r_2

，…，$r_{\phi(m)}$ 表示這些自然數。如果 a 與 m 互質，則 $ar_1, ar_2, \cdots ar_{\phi(m)}$ 對（mod m）而言是 $r_1, r_2, \cdots, r_{\phi(m)}$ 的一個排列。

證明 令 $x_i = ar_i$（mod m）

且 $0 \leqslant x_i < m$

則 $ar_i = qm + x_i$

因 ar_i 與 m 互質，故 x_i 必與 m 互質，因此 x_i 是 $r_1, r_2, \cdots, r_{\phi(m)}$ 中的一員，但由定理 5.2 知 $x_i \equiv x_j$（mod m）之充要條件爲 $r_i = r_j$，故所有的 x_i 皆不相同，本定理得證。

定理 5.3 （費馬、尤拉定理）設 w 與 m 爲兩互質之自然數，ϕ 爲尤拉函數，則

$$w^{\phi(m)} \equiv 1 \ (\text{mod } m)$$

證明 由定理 5.2 知

$$r_1 r_2 \cdots r_{\phi(m)} \equiv (wr_1)(wr_2)\cdots(wr_{\phi(m)}) \ (\text{mod } m)$$

即 $$r_1 r_2 \cdots r_{\phi(m)} \equiv w^{\phi(m)} r_1 r_2 \cdots r_{\phi(m)} \ (\text{mod } m)$$

因 $r_1 r_2 \cdots r_{\phi(m)}$ 與 m 互質，故

$$w^{\phi(m)} \equiv 1 \ (\text{mod } m)$$

本定理得證。

（此定理爲定理 2.3 之推廣，因 m 爲質數時 $\phi(m) = m - 1$）

我們又可以推廣定理 2.2，若以 (a, b) 表示 a，b 之最大公約數（公因子），若 $d = (a, b)$，則存在兩整數 x，y 可使

$$ax + by = d$$

這個證法與定理 2.2 極相似，求法也是用輾轉相除法。

定理 5.4 設 a，m 爲兩個互質之正整數且 $1 < a < m$，若 $a^k \equiv 1$（mod m），則 k 與 $\phi(m)$ 不互質。

證明 設 A 爲所有 $k \geqslant 1$ 且

$$a^k \equiv 1 \ (\text{mod } m)$$

之集合，因 $\phi(m) \in A$，故 A 非空集合。令 d 爲 A 中之最小一員，因 $a^1 \equiv a$（mod m），故 $1 \notin A$，即 $d > 1$。設 $a^k \equiv 1$（mod m），令 $k = qd + r$，$0 \leqslant r < d$，顯然由 $a^d \equiv 1$（mod m）可得

$$1 \equiv a^k \equiv a^{qd+r} \equiv (a^d)^q a^r \equiv a^r \ (\text{mod } m)$$

但因 d 爲此集合中之最小者，故 $r = 0$，即 k 必爲 d 之倍數，且因 $\phi(m) \in A$，可知 $(k, \phi(m)) \geqslant d > 1$，故 k 與 $\phi(m)$ 不互質。

現在我們終於走到了最後一個求證某數是質數的定理。

定理 5.5 （魯克斯（Lucas）定理）若 m 爲大於 1 之整數，a 爲任一與 m 互質之數，若 $a^{m-1} \equiv 1$（mod m），且對所有的（$m-1$）因子而言，$a^k \not\equiv 1$（mod m）則 m 必爲一質數。

證明 設 m 不是質數，則由 $\phi(m)$ 之定義可知 $\phi(m) < m - 1$，但由於 a，m 互質，由定理 5.3 知 $a^{\phi(m)} \equiv 1$（mod m），由已知條件及前定理知

$$(m - 1, \phi(m)) = d > 1$$

故 d 爲 $m-1$ 之一因子，由 (5.1) 知存在二整數 x，y 使得

$$(m-1)x + \phi(m)y = d$$

即

$$a^d \equiv a^{(m-1)x+\phi(m)y} \equiv (a^{m-1})^x (a^{\phi(m)})^y \equiv 1 \ (\text{mod } m)$$

故（$m-1$）有一因子使得 $a^d \equiv 1$（mod m），與假設相矛盾，故 m 必爲質數，本定理證畢。

這個定理若用來檢定一已知數 m 是否是質數並不容易，因爲 $m-1$ 的因子往往不易找到，前面已談過要分解一個大數的因子是件極費時的事，但這個定理來找一些大質數却很容易，例如我們令

$$m = 2^n + 1$$

則m的因子只有$2, 2^2 \cdots, 2^n$個，若我們能試一試一個可能與m互質的數a，像3，5，7之類的而且證得

$$a^{m-1} \equiv 1 \pmod{m}$$

但 $$a^{2^{n-1}} \equiv 1 \pmod{m}$$

則m必爲質數。原因是若

$$a^{2^{n-1}} \equiv 1 \pmod{m}$$

則對所有的$k < n-1$，a^{2^k}都不等於$1 \pmod{m}$。

（假如$a^{2^k} \equiv 1 \pmod{m}$）則

$$a^{2^{n-1}} \equiv \left(a^{2^k}\right)^{2^{n-1-k}} \equiv 1 \pmod{m}$$

對一個固定的a而言，這個整個檢驗過程不過一次驗定a與m互質，二次（mod m）而已，比硬除不只快了多少倍。

例 若令$m = 2^n - 1$，則我們若能試出一與m互質的數a像3，5，7，…而也證得

$$a^{m-1} \equiv 1 \pmod{m}$$

且 $$a^2 \not\equiv 1 \pmod{m}$$

及 $$a^{2^{n-1}-1} \not\equiv 1 \pmod{m}$$

則m必爲一質數（因$m-1 = 2^n - 2 = 2(2^{n-1}-1)$）目前最大的質數多半都是這樣求得的，在1979年納爾遜與斯羅溫斯基（H. Nelson & Slowinski）用電子計算機證明$2^{44497}-1$是一個13,395位的質數。若以100元一千字作稿費，把這個數寫出來就是一千三百元，「數播」一頁大約二千字，所以把這個字寫出來要佔去六頁半的篇幅。

例 若p爲一質數s，t爲兩正整數，$m = 2^s p^t + 1$則我們若能試出一個與m互質的數a並證得

$$a^{m-1} \equiv 1 \pmod{m}$$

且 $$a^{2^{s-1}p^t} \not\equiv 1 \pmod{m}$$

$$a^{2^s p^{t-1}} \not\equiv 1 \pmod{m}$$

則m爲一質數。

例 若p，q爲兩質數，$m = 2pq + 1$，則我們若能試出一個與m互質的數a並證得

$$a^{m-1} \equiv 1 \pmod{m}$$

$$a^{2p} \not\equiv 1 \pmod{m}$$

$$a^{pq} \not\equiv 1 \pmod{m}$$

及 $$a^{2q} \not\equiv 1 \pmod{m}$$

則m爲一質數。

如此這般，我們可以由小而大滾雪球式的很容易的找到許多大質數，由於走的路徑千變萬化，所可能找到的大質數也是一個天文數字。當然電子計算機是不可少的工具。在定理5.5中我們只要求任何一個與m互質的a，因此什麼與m互質的a都可以，根據一般的經驗，若m是質數，很快就可以找到一個小的a像3，5，7之類的滿足定理5.5，若不成功，就可以放棄另找了，反正候選的m多得不得了，最近有一個極巧妙的結果由Lehmer, Solorary與Shassen同時發現。即若m不是質數，則至少有一半以上的數從2，3，…，到$m-1$不能滿足$a^{m-1} \equiv 1 \pmod{m}$，可惜我們沒有辦法在本文中證明此一結果。這個結果在另一個角度看來，即一個不是質數的m只有很小的機會能通過許多小的a。我們最後舉一個數字的例子

例 $257 = 2^8 + 1$是不是質數？

因$m - 1 = 2^8$，故我們若能找到一個與m互質的a且

$$a^{2^8} \equiv 1 \pmod{m}$$

$$a^{2^7} \not\equiv 1 \pmod{m}$$

m即爲質數。$m = 275$不是3的倍數，我們先取$a = 3$，我們一步一步的求$3^{2^7} \pmod{m}$與$3^{2^8} \pmod{m}$。

k	2^k	$3^{2^k} \equiv ?\ (\mathrm{mod}\ 257)$
0	$2^0 = 1$	$3 \equiv 3$
1	$2^1 = 2$	$3^2 \equiv 9$
2	$2^2 = 4$	$3^4 \equiv 9^2 \equiv 81$
3	$2^3 = 8$	$3^8 \equiv 81^2 \equiv 136$
4	16	$136^2 \equiv 249$
5	32	$249^2 \equiv 64$
6	64	$64^2 \equiv 241$
7	128	$241^2 \equiv 256$
8	256	$256^2 \equiv 1$

故257是一個質數。

六、結尾的話

前面說過，在重賞或生死交關的情形下，至今尚很少不能破獲的密碼，在現今數論密碼一日千里的進展之下，我們剛才談到兩種密碼也許就要(已經？)落伍，但新的方法必然又會出現，並且在尋找新數論密碼的長途上，數學家一定可以用時在路邊揀到一些前人所未發現的珍珠，有一天人類也許可以坦誠相處到不要用密碼通訊的地步，但這些拾來的珍珠將永遠是數學史上的光輝。

參考資料

1. Rivest, R. L; Shcmir, A.; Adleman, L. "A method for obtaining digital signature and public-key cryptasystem" *Communication of ACM*, 1978, pp. 120-126.

2. Simmons, G. "Cryptology : The mathematics of sewre communication" *The Mathematical Intelligencer*, 1978, pp. 233-246.

3. Hellman, M. E. "The mathematics of public-key cryptography" *Scientific American*, August, 1979, pp. 146-157.

4. Pomerance, C. "The search for prime numbers" *Scientific American*, December, 1982, pp. 136-147.

本文作者：

楊重駿：現任職於美國海軍研究實驗所

楊照崑：現任教於美國佛羅里達大學統計系