中華民國第四十三屆中小學科學展覽會參展作品專輯
高中組

數學科

科別：數學科

組別：高中組

作品名稱：簡單函數在密碼學之應用－三重加密法

關鍵詞：換位加密法、公開金鑰、資料壓縮

編號：040415

學校名稱：

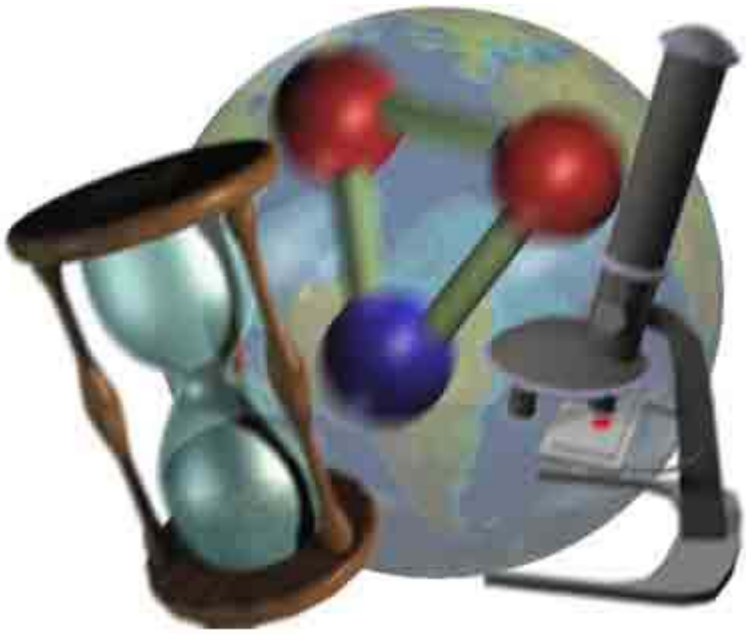
嘉義縣私立協同高級中學

作者姓名：

黃箴理、賴宜璟、許庭瑋、趙傳真

指導老師：

黃明正



摘要

在高一下學期三角函數課程中我們學到正餘弦疊合函數，$f(x)=a\sin x+b\cos x$，我們發現給予不同之參數 a、b 與 x 值除了可以得到不同之 $f(x)$ 之外，若藉著一系列之疊代獲得之 a、b 與 x 亦可求得一系列之 $f(x)$ 當作換位加密時之移位使用，其優點是可以讓資料之換位次序非常凌亂，提高資料保密之安全性。

在高一上學期整數單元中學到輾轉相除法原理，輾轉相除法除了求得兩個較大正整數之最大公因數之外，利用輾轉相除法之求解過程中，可以將一個最簡假分數化為簡單連分數型式。因此可以利用此簡單技巧作為一個正整數數列與最簡假分數的應對工具達成明文與密文之轉換作為加密與解密工具。

另外整數單元中也學到同餘運算，可以解一些較大正整數之間除法運算的餘數問題，RSA 加密方法即利用此方法達到增加解密之困難度。

我們將以上三種方法適當結合而提出我們新的加密與解密方法，稱為「三重加密法」，其優點可達成資料壓縮與資料保密之效果。

壹、研究動機與目的

去年老師曾給我們看過一部片子叫「美麗境界」，裡頭的男主角—奈許，是一位很有名的數學家，他對密碼有非常特殊的興趣。所以我們對密碼學產生了濃厚的興趣。我們試著找出適當的數列來作為與明文對應的數列，當上完輾轉相除法課程後才發現連分數是一個適當的工具，於是就開始我們的研究。

這個研究之目的在於了解現代密碼學研究方法與加密技術，並發掘一些簡單常見之函數在日常生活之應用。

貳、文獻概述

密碼學是一門研究如何隱藏秘密並能安全傳遞資訊給接受者的學問，因此如何加密與不容易被非資訊接受者解密為首要研究之課題。自從 1976 年史丹佛大學位學者 Diffie 和 Hellman 提出公開金鑰理論之後，密碼學在觀念與應用上均有重大突破[5]。

所謂公開金鑰與其對應之私密金鑰理論簡述如下：

一個資訊使用者某甲可以公開自己的加密金鑰給所有使用者，每一個使用者依據某甲的公開金鑰將資訊加密傳送給某甲，某甲再利用本身之私密金鑰配合其公開金鑰輕易將加密之資訊解密還原為原文。其理論基礎是建立在資訊安全之基礎上，每一個資訊使用者手上握有一對金鑰；其中一個為公開金鑰，是公開給其他使用者使用，作為加密處理使用。當資訊收受者接受到一篇密文，利用自己手上之一對金鑰可輕易解開密文成原文。非收受者就是連原始加密者都不容易解密還原為原文。例如：鴿子能夠簡單進入鴿舍而無法自由出入，但是鴿舍主人有一把鴿舍大門金鑰匙當然可輕易打開鴿舍取出鴿子。此概念用數學術語表示即所謂單向活門函數，如果一個函數 y＝f（x）滿足給定 x 很容易計算求得 y，但是很難由 y 求得 x＝f^{-1}（y）此即所謂單向，但是若掌握了函數 y＝f（x）的相關訊息即可輕易求得 x＝f^{-1}（y），此即所謂活門。

今以 RSA 密碼系統說明，此系統在 1978 由麻省理工學院三位學者 Rivest、Shamir、Adleman 所提出[6][3]。

以下說明 RSA 密碼系統稗能更能了解公開金鑰與私密金鑰之運作原理：

資訊適用者某甲，為了本身收受之資料不容易被解密，隨機選出兩個足夠大的質數 P_1 與 P_2。

令 n＝P_1×P_2，令比 n 小且與 n 互質之整數共有 $\varphi(n)$ 個，可得知 $\varphi(n)=(p_1-1)(p_2-1)$。再隨機選取一數 e，滿足 gcd(e，$\varphi(n)$)＝1，再求得一數 d，滿足 $ed\equiv 1(\mathrm{mod}\,\varphi(n))$。此時某甲即可公開(e，n)為其公開金鑰給所有資訊使用者，作為傳遞訊息給某甲時加密使用。任一使用者，若欲將明文數碼 M 傳遞給某甲時，利用下列函數將 M 加密成 C。

$$C\equiv M^{e}\ (\mathrm{mod}\ n),$$

處理後傳遞 C 給某甲。當某甲收到資訊 C 後利用私密金鑰 d 與下列函數將 C 解密還原成 M,

$$M\equiv C^{d}\ (\mathrm{mod}\ n)。$$

當任一資訊用者利用數對(e，n)做加密處理之後的密文，也只有某甲本身可以利用手上未公開之私密金鑰 d 配合著已公開金鑰 n 輕易地將密文還原成原文。

其原理由以下之數學式之推導即可明白。

先找出 e 對模 $\varphi(n)$ 的乘法反元素 d，亦即 $ed\equiv 1\ (\mathrm{mod}\ \varphi(n))$，所以 $\exists k\in z$ 滿足 $ed=k\varphi(n)+1$。再利用尤拉公式， $\gcd(M,n)=1\Rightarrow M^{\varphi(n)}\equiv 1\ (\mathrm{mod}\ n)$ [4]。即可推導如下：

$$\begin{aligned} C^{d} &\equiv M^{ed}\ (\mathrm{mod}\ n)\\ &\equiv M^{K\varphi(n)+1}\ (\mathrm{mod}\ n)\\ &\equiv M\ (\mathrm{mod}\ n)。\end{aligned}$$

另外值得一提的是算術編碼法，此方法在資料壓縮上是一個有名的方法。算術編碼法是將明文當做是一個位於 $[0,1)$ 的數。它的方法略述如下：

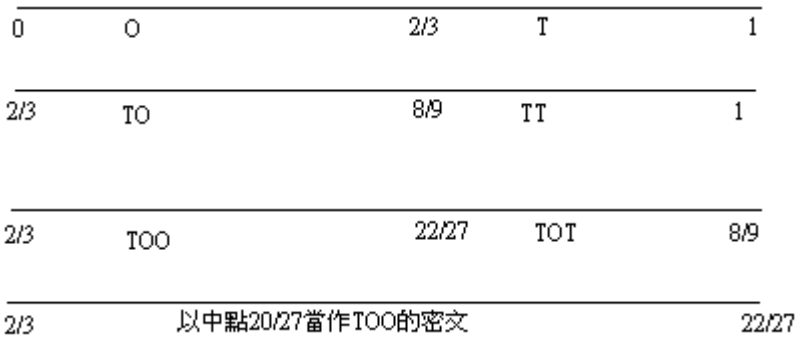
步驟 1：將明文中各字元出現之頻率統計出來。然後依據某一順序將字元排列在 $[0,1)$ 內，且讓各個字元對應的子區間長度與字元出現頻率成正比。

步驟 2：由明文的第一個字元將明文對應在第一個字元所屬的區間。再將此子區間依據步驟 1 的方法將各字元排列在該被選取的子區間內。

步驟 3：由明文的第二個字元將明文對應在第二個字元所屬的更小子區間。再將此第二次被選取子區間依據步驟 1 的方法將各字元排列在第二次子區間內。

步驟 4：重複步驟 3 直到明文字元均對應完畢。最後選取所在區間之中點所對應的有理數當作密文即可。

以明文 TOO 說明，字元 O 頻率是字元 T 的 2 倍，每一個區間分割為更小子區間時以長度 2：1 分割，字元 O 佔 2 份，字元 T 佔 1 份。如下圖



至此我們已將近代密碼學之概念做簡要之陳述。

參、研究方法與過程

一、輾轉相除法與連分數之關係

在各出版社所出版的高中數學課本(一)均提到輾轉相除法之原理，老師還告訴我們，一個最簡假分數可經由輾轉相除法輕易表示成一個連分數。因此我們想利用一個數列與一個假分數做 1 對 1 之對應處理，即可當做明文與密文之間的對應關係。

首先我們複習一些必需的數學定理與一些適當之定義：

【定義 1】：[簡單連分數]

一個連分數每項分子均 1 者稱之為簡單連分數。

【定義 2】：[$\{q_0 : q_1, q_2, ..., q_{n-1}, q_n\}$]

將一個簡單連分數，型如 $q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots_{+\frac{1}{q_{n-1}+\frac{1}{q_n}}}}}$ 者，

記為 $\{q_0 : q_1, q_2, ..., q_{n-1}, q_n\}$，亦即

$$\{q_0 : q_1, q_2, ..., q_{n-1}, q_n\} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots_{+\frac{1}{q_{n-1}+\frac{1}{q_n}}}}}。 \quad (1)$$

【例 3】：$\{2 : 3, 4, 5\} = 2 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{5}}}$。

輾轉相除法與簡單連分數之關係：

【例 4】：利用輾轉相除法將$\frac{157}{68}$改寫成簡單連分數。

2	157	68	3
	136	63	
4	21	5	5
	20	5	
	1	0	

在上面得輾轉相除法式子中，表達的意思如下所述：

$$157=2\times 68+21\Leftrightarrow \frac{157}{68}=2+\frac{21}{68}$$

$$68=3\times 21+5\Leftrightarrow \frac{68}{21}=3+\frac{5}{21}$$

$$21=4\times 5+1\Leftrightarrow \frac{21}{5}=4+\frac{1}{5}$$

所以 $$\frac{157}{68}=2+\frac{21}{68}$$

$$=2+\frac{1}{3+\frac{5}{21}}$$

$$=2+\frac{1}{3+\frac{1}{4+\frac{1}{5}}}$$

因此$\frac{157}{68}$表示成簡單連分數為$\{2:3,4,5\}$。

接著定理 5 將保證兩個互質之正整數利用輾轉相除法求得 gcd 之過程表法是唯一的，因此一個最簡假分數改寫成簡單連分數表法也是唯一的。我們將以例 6 證明之。

【定理 5】：[除法原理]：

a，b 為兩個正整數，則唯一存在一組 q 與 r，其中 q，$r\in Z$ 且 $0\le r<b$ 使得 $a=q\times b+r$。

【證明】：

設有二組(q，r)與(q'，r')滿足 $a=q\times b+r$，其中 q，$r\in Z$ 且 $0\le r<b$ 又 q'，$r'\in Z$ 且 $0\le r'<b$。

$$\begin{cases} a=q\times b+r \\ a=q'\times b+r' \end{cases}$$

兩式相減

0=$b(q-q')+(r-r')$

$\Rightarrow (r'-r)=b(q-q')$

Case1：若 $r'-r=0$

因為 $b\neq 0$，所以 $q-q'=0$

因此 $q=q'$，$r=r'$，q 與 r 唯一存在。

Case2：若 $r'-r\neq 0$

因為$0\leq r<b$且$0\leq r'<b$

所以$-b<r'-r<b$

$\Rightarrow -b<(r'-r)=b(q-q')<b$

同除以b , (因為$b\neq 0$)

$-1<\frac{r'-r}{b}=q-q'<1$

又因為 q，q'同為整數，故 $q-q'\in Z$,

介於-1 與 1 之間唯有一個 0 為整數,

因此 $q-q'=0\Rightarrow \frac{r'-r}{b}=0\Rightarrow r'-r=0$ 矛盾,

故 除法原理得證。

由除法原理可知，兩互質整數利用輾轉相除法做最大公因數之求解過程表示方法是唯一的，因此一個最簡假分數表示為最簡連分數表法也是唯一的。由於最簡假分數的分子與分母互質且分子大於分母，由以上定義 2、例 3 與例 4 可知，其最大公因數即等於連分數中最末一項 a_n 的分子 1。這個道理在緊接著的例 6 將會很明確地告知。

【例 6】：設 a、b 為兩個互質正整數且 $a>b$。由除法原理知：

$a=q_0b+r_0$,其中$q_0,r_0\in Z,\ 0\leq r_0<b$,

$b=q_1r_0+r_1$,其中$q_1,r_1\in Z,\ 0\leq r_1<r_0$,

$r_0=q_2r_1+r_2$,其中$q_2,r_2\in Z,\ 0\leq r_2<r_1$,

$r_1=q_3r_2+r_3$,其中$q_3,r_3\in Z,\ 0\leq r_3<r_2$,

……..

$r_k=q_{k+2}r_{k+1}+r_{k+2}$,其中$q_{k+2},r_{k+2}\in Z,\ 0\leq r_{k+2}<r_{k+1}$,

…….

最後一式稍有不同,

$r_{n-2}=q_nr_{n-1}+r_n$,其中$q_n=r_{n-2},r_{n-1}=\gcd(a,b)=1,r_n=0$。

另外由輾轉相除法原理可知：

$$\frac{a}{b}=q_0+\frac{r_0}{b}$$

$$=q_0+\frac{1}{q_1+\frac{r_1}{r_0}}$$

$$= q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{r_2}{r_1}}}$$

……

$$= q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots_{+\cfrac{1}{q_{n-1}+\cfrac{r_{n-1}}{r_{n-2}}}}}}, \ r_{n-1} = \gcd(a,b) = 1, \ r_{n-2} = q_n,$$

$$= q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots_{+\cfrac{1}{q_{n-1}+\cfrac{1}{q_n}}}}}。$$

因此最簡假分數$\frac{a}{b}$可以以簡單連分數唯一表示為$\{q_0 : q_1, q_2, ..., q_{n-1}, q_n\}$,

亦即$\frac{a}{b} = \{q_0 : q_1, q_2, ..., q_{n-1}, q_n\} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots_{+\cfrac{1}{q_{n-1}+\cfrac{1}{q_n}}}}}$。 (2)

【定理 7】設 a、b 為兩個互質正整數且 $a>b$, 則唯一存在一個簡單連分數

$\{q_0 : q_1, q_2, ..., q_{n-1}, q_n\}$ 使得$\frac{a}{b} = \{q_0 : q_1, q_2, ..., q_{n-1}, q_n\}$。

【定理 8】設$\{q_0 : q_1, q_2, ..., q_{n-1}, q_n\}$表示一個簡單連分數, 則唯一存在兩個互質正整數 a、

b 且 $a>b$, 使得$\frac{a}{b} = \{q_0 : q_1, q_2, ..., q_{n-1}, q_n\}$。

由定理 5 與例 6 可推論得定理 7 與定理 8 同時成立, 因此我們不再重複證明。這兩個定理保證最簡假分數$\frac{a}{b}$與簡單連分數之 1 對 1 對應關係, 也保證章節編號肆、四節當中所主張的連分數加密法是可行的。

二、換位式加密法

將字元字碼表依照某一約定的順序重新排列之後轉換成密文字碼表, 將明文依照密文字碼表重新改寫成密文。今以 ABCDE 五個字元的換位說明,

$\begin{pmatrix} A & B & C & D & E \\ B & C & D & E & A \end{pmatrix}$表示將字元順序向左移一位, 第一位移至最末一位。

例如中國廣播公司簡稱 BBC 經過轉換後密文為 CCD。事實上就 ABCDE 五個字元的換位模

式可以有 120 種。一般使用者都是依照某種幾何圖形設定順序。以下介紹我們所提的換位模式，稱為隨機換位法。

將 ABCDE 五個字元的換位順序隨機設定為$\begin{pmatrix} A & B & C & D & E \\ C & D & B & E & A \end{pmatrix}$。若以矩陣來表示此轉換即為：

$$\text{字元矩陣 } A=\begin{pmatrix}1\\0\\0\\0\\0\end{pmatrix}, B=\begin{pmatrix}0\\1\\0\\0\\0\end{pmatrix}, C=\begin{pmatrix}0\\0\\1\\0\\0\end{pmatrix}, D=\begin{pmatrix}0\\0\\0\\1\\0\end{pmatrix}, E=\begin{pmatrix}0\\0\\0\\0\\1\end{pmatrix}, \tag{3}$$

$$\text{加密矩陣 } En=\begin{pmatrix}0&0&0&0&1\\0&0&1&0&0\\1&0&0&0&0\\0&1&0&0&0\\0&0&0&1&0\end{pmatrix}, \tag{4}$$

$$\text{解密矩陣 } De=En^T=\begin{pmatrix}0&0&1&0&0\\0&0&0&1&0\\0&1&0&0&0\\0&0&0&0&1\\1&0&0&0&0\end{pmatrix}。 \tag{5}$$

當加密或解密時只要分別做一個矩陣乘法運算即可，舉例說明如下：

En A = C，*De C = A*，*En B = D*，*De D = B*，……等。

以矩陣作為明文與密文之轉換算子在記錄的方便性上並不佔有優勢，但是相同的換位順序模式我們可以利用一個四次多項式函數作為轉換算子，改善上述之缺失。我們的想法很簡單，利用經過 5 個定點(1, 3), (2, 4), (3, 2), (4, 5), (5, 1)的最低次多項式函數，當作加密函數。同理利用經過 5 個定點(3, 1), (4, 2), (2, 3), (5, 4), (1, 5)的最低次多項式函數，當作解密函數。

設轉換字元表為$\begin{pmatrix}1&2&3&4&5\\3&4&2&5&1\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\s_1&s_2&s_3&s_4&s_5\end{pmatrix}$，利用因式定理可以如下方式寫出加密函數 *f*(*x*)[1]。

$$\text{另加密函數 } f(x)=\sum_{j=1}^{5} t_j \prod_{i=1,i\neq j}^{5}(x-i) \tag{6}$$

可以算出特定的係數

$$t_j=\frac{s_j}{(-1)^{5-j}(j-1)!(5-j)!} \tag{7}$$

使函數 $f(x)=\sum_{j=1}^{5} t_j \prod_{i=1,i\neq j}^{5}(x-i)$ 通過五個定點(1, s_1), (2, s_2), (3, s_3), (4, s_4), (5, s_5)，亦即 $f(1)=s_1$, $f(2)=s_2$，$f(3)=s_3$，$f(4)=s_4$ 與 $f(5)=s_5$。同方法，令解密函數

$$g(x)=\sum_{i=1}^{5}\frac{i}{(-1)^{5-s_i}(s_i-1)!(5-s_i)!}\prod_{j=1,j\neq b_i}^{5}(x-j), \tag{8}$$

雖然 $g(x)$不恆為 $f^{-1}(x)$, $f(x)$的反函數，但是 $g(x)$恆通過 5 個定點(s_1, 1), (s_2, 2), (s_3, 3), (s_4, 4), (s_5, 5)，亦即 g(s_1)=1，$g(s_2)$=2，$g(s_3)$=3，$g(s_4)$=4 與 $g(s_5)$=5，因此 $g(x)$可以當作解密函數使用。

由式(6)與式(8)可以知道，針對五個字元的換位加密與解密均需要一個四次多項式函數。我們知道英文字元分成大寫小寫再加上一些常用標點符號、數學符號與空白字元大約有一百個字元符號可能出現在任何一篇文章，包括科學性文章、報章雜誌文章等。因此需要一個九十九次多項式函數當作加密函數，另外還需要一個九十九次多項式函數當作解密函數。這個理由使得這個模式在實務上很難運作。因此我們想出一個讓換位順序足夠亂而且可以改寫成次數相對很小的多項式加密函數，也就是下一節所提的正餘弦疊合法。

三、正餘弦疊合法

在高中一年級數學課程有提到正餘弦疊合[2]。我們想利用正餘弦疊合函數跑出一組很亂的數列作為換位加密使用。

【定義 9】[字元數值]

將明文各個字元依照字碼表順序賦予各個字元一個整數值稱為字元數值。

$$\text{若令}\begin{cases} y_k=\alpha_k\sin x_k+\beta_k\cos x_k, \\ \gamma_k=\text{int}((y_k-\text{int}(y_k))*100), \end{cases}\quad \forall k\in N\cup\{0\}, \tag{9}$$

其中取 y_k 的小數點以下之十分位與百分位組成之二位整數當作 γ_k，其目的當作字元換位數值使用，然而為了使數列 $\{\gamma_k\}_{k=0}^{n}$ 更亂，在式(9)中的 α_k, 與 β_k 將採取遞迴數列方式產生，則我們有一個經過正餘弦疊合函數作用後的二位正整數數列 $\{\gamma_k\}_{k=0}^{n}$。如果我們的明文字元數值以另一個數列 $\{c_k\}_{k=0}^{n}$ 表示,

再令 $q_k=c_k+\gamma_k$, (10)

則數列 $\{q_k\}_{k=0}^{n}$ 是經過第一次換位加密處理的字元數值數列。

解密時也是利用式(9)與相同的 α_k, 與 β_k 得到數列 $\{\gamma_k\}_{k=0}^{n}$,

再令 $c_k=q_k-\gamma_k$, (11)

則可將密文字元數值數列 $\{q_k\}_{k=0}^{n}$ 還原成明文字元數值數列 $\{c_k\}_{k=0}^{n}$。

四、連分數加密法

【定義 10】[字串數值]

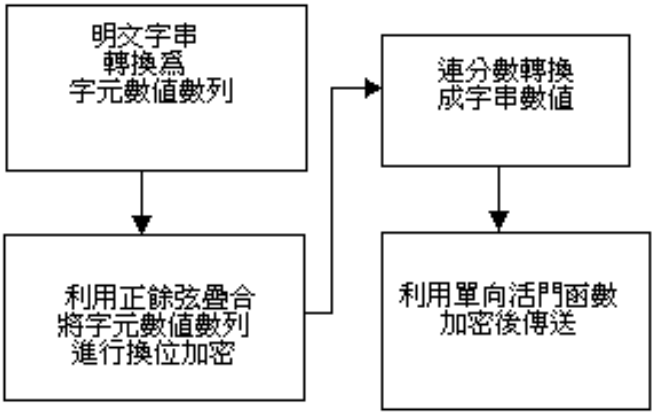
當一個有理數 a 代表一些字元所組成之字串 A$時，該有理數 a 稱為字串 A$的字串數值。

加密時利用定理 8，將式(10)所得的第一次加密處理的字元數值數列$\{q_k\}_{k=0}^{n}$轉換成最簡假分數$\frac{a}{b}$。這個假分數$\frac{a}{b}$是一個經過第二次加密處理的密文字串數值，它只是一個大於 1 的有理數，卻代表著一串字元，這意味著連分數加密法可以有效地壓縮文字檔。我們將在最後討論的章節中討論資料的壓縮比率。

解密時利用定理 7 與例 6，即使用輾轉相除法，將最簡假分數$\frac{a}{b}$轉換成字元數值數列$\{q_k\}_{k=0}^{n}$。

五、三重加密法

這是我們提出的加密新方法，流程圖如圖一。



圖一

步驟一、將字元字碼賦予數值，例如："A"為 1、"B"為 2、….、"Z"為 26、"句點"為 27、"空白字元"為 28。如圖二所示。

$$\begin{pmatrix} A & B & C & D & \cdots & Z & \square & blank \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \cdots & \updownarrow & \updownarrow & \updownarrow \\ 1 & 2 & 3 & 4 & \cdots & 26 & 27 & 28 \end{pmatrix}$$

圖二

步驟二、將明文字串 A$轉換為字元數值數列，例如："THE CAT IS CUTE."轉換成數列 $\{c_k\}_{k=0}^{15}$={20,8,5,28,3,1,20,28,9,19,28,3,21,20,5,27}。

步驟三、先徵求收受資訊方的公開金鑰$(\alpha_0, \beta_0, x_0, e, n)$，其中前三數$\alpha_0, \beta_0, x_0$在步驟三正餘弦疊合加密使用，後二數 *e,n* 在步驟五單向活門函數加密使用。

對第 *k* 個字元加密時

設 $y_k = \alpha_k \sin x_k + \beta_k \cos x_k$

$$= \sqrt{\alpha_k{}^2 + \beta_k{}^2} \sin(x_k + \varphi_k),\ \varphi_k = \sin^{-1} \frac{\beta_k}{\sqrt{\alpha_k{}^2 + \beta_k{}^2}}, \tag{12}$$

取 y_k 小數點以下前二碼，即十分位與百分位，當作換位加密用，並令其為 γ_k。

令第 *k* 個字元數值加密成為 q_k，即 $q_k = c_k + \gamma_k$。

接著計算下一步要使用的 α, β與 x 值，即 $\alpha_{k+1}, \beta_{k+1}, x_{k+1}$。

我們採取遞迴數列產生下一個數值，將 β_k 的數值存入新變數 α_{k+1}，φ_k 小數點以下前二碼加上 x_k 的數值和存入新變數 β_{k+1}。因為 γ_k 數值介於 0 與 99 之間，將 γ_k 乘以 $\frac{\pi}{200}$ 之數值存入 x_{k+1}，保證 $0 \le x_{k+1} < \frac{\pi}{2}$。步驟三的演算法如下：

input α_0, β_0, x_0

FOR K=0 TO 15

$$y_k = \alpha_k \sin x_k + \beta_k \cos x_k \tag{13}$$

$$\varphi_k = \sin^{-1} \frac{\beta_k}{\sqrt{\alpha_k{}^2 + \beta_k{}^2}} \tag{14}$$

$$\gamma_k = \text{int}((y_k - \text{int}(y_k)) * 100) \tag{15}$$

$$\alpha_{k+1} = \beta_k \tag{16}$$

$$\beta_{k+1} = x_k + \text{int}((\varphi_k - \text{int}(\varphi_k)) * 100) \tag{17}$$

$$x_{k+1} = \gamma_k * \pi / 200 \tag{18}$$

$$q_k = c_k + \gamma_k \tag{19}$$

Next K

以 $\alpha_0 = 9, \beta_0 = 180, x_0 = 1$ 帶入步驟三的演算法結果如下表三：

k	α_k	β_k	x_k	φ_k 的二碼	y_k 的二碼	明文	c_k	q_k
0	9	180	1	52	82	T	20	102
1	180	53	1.3	28	67	H	8	75
2	53	29.3	1.1	50	54	E	5	59
3	29.3	51.1	0.8	4	45		28	73
4	51.1	4.85	0.7	9	3	C	3	6
5	4.85	9.71	0	10	18	A	1	19

6	9.71	10	0.3	80	24	T	20	44
7	10	80.3	0.4	44	29		28	57
8	80.3	44.4	0.5	50	49	I	9	58
9	44.4	50.5	0.8	84	59	S	19	78
10	50.5	84.8	0.9	3	58		28	86
11	84.8	3.93	0.9	4	86	C	3	89
12	3.93	4.91	1.4	89	73	U	21	94
13	4.91	90.4	1.1	51	97	T	20	117
14	90.4	52.1	1.5	52	0	E	5	5
15	52.1	53.5	0	79	89	.	27	116

表三

步驟四、將數列$\{q_k\}$利用定理 8 轉換成最簡假分數$\frac{a}{b}$。

以表三數據得$\{q_0:q_1,\cdots,q_6\}=\frac{3799893419}{198259235}$，$\{q_7:q_8,\cdots,q_{11}\}=\frac{1975307288}{22191565}$，

$\{q_{12}:q_{13},\cdots,q_{15}\}=\frac{6401323}{55089}$，所以傳送三組數對(a, b)給步驟五。

步驟五、將步驟三所獲得的金鑰 *e,n*，應用 RSA 加密系統分別對分子，a，與分母，b，做加密動作，得到新分子 a'與新分母 b'。

$$a'\equiv a^e \pmod{n}, \tag{20}$$

$$b'\equiv b^e \pmod{n}。 \tag{21}$$

步驟五是借用三位學者 Rivest、Shamir、Adleman 的方法，在此不做驗證。

步驟六、傳送 a'與 b'給資訊收受方。我們考慮計算機將有理數以實數變數儲存資料若有效數字太少時資料會有誤失，因此以整數變數方式傳送確以保資料之正確。

解密時循加密之逆順序進行，即依照步驟五解密、步驟四解密、步驟三解密、步驟二解密進行。

步驟五的解密：取出私密金鑰$(\alpha_0,\beta_0,x_0,d,n)$，其中前三數$\alpha_0,\beta_0,x_0$在步驟三的解密使用，將後二數，*d*、*n* 代入解密運算式，

$$a\equiv (a')^d \pmod{n}, \tag{22}$$

$$b\equiv (b')^d \pmod{n}。 \tag{23}$$

步驟四的解密：將最簡假分數$\frac{a}{b}$利用定理 7 轉換成數列$\{q_k\}$。

步驟三的解密：

對第 *k* 個字元解密時

設$y_k=\alpha_k\sin x_k+\beta_k\cos x_k$

$$= \sqrt{\alpha_k{}^2 + \beta_k{}^2}\sin(x_k + \varphi_k),\ \varphi_k = \sin^{-1}\frac{\beta_k}{\sqrt{\alpha_k{}^2 + \beta_k{}^2}},$$

依照加密時的過程取y_k小數點以下前二碼, 即十分位與百分位, 當作換位解密用, 並令其為γ_k。
令第 k 個字元數值解密成為 c_k, 即$c_k = q_k - \gamma_k$。
接著計算下一步要使用的α, β與x 值, 即$\alpha_{k+1}, \beta_{k+1}, x_{k+1}$。
依照加密時的過程產生下一個數值, 將β_k的數值存入新變數α_{k+1}, φ_k 小數點以下前二碼加上x_k的數值和存入新變數β_{k+1}。因為γ_k 數值介於 0 與 99 之間, 將γ_k 乘以$\frac{\pi}{200}$之數值存入x_{k+1}, 保證$0 \le x_{k+1} < \frac{\pi}{2}$。步驟三的解密演算法如下：

input α_0, β_0, x_0
FOR K=0 TO 15

$$y_k = \alpha_k \sin x_k + \beta_k \cos x_k \quad (24)$$

$$\varphi_k = \sin^{-1}\frac{\beta_k}{\sqrt{\alpha_k{}^2 + \beta_k{}^2}} \quad (25)$$

$$\gamma_k = \text{int}((y_k - \text{int}(y_k))*100) \quad (26)$$
$$\alpha_{k+1} = \beta_k \quad (27)$$
$$\beta_{k+1} = x_k + \text{int}((\varphi_k - \text{int}(\varphi_k))*100) \quad (28)$$
$$x_{k+1} = \gamma_k * \pi / 200 \quad (29)$$
$$c_k = q_k - \gamma_k \quad (30)$$

Next K

步驟二的解密：將$\{c_0 : c_1, c_2, ..., c_n\}$轉換為明文字串 A$。

依照之前說明即將$\{c_k\}_{k=0}^{15}$={20,8,5,28,3,1,20,28,9,19,28,3,21,20,5,27}轉換為明文字串"THE CAT IS CUTE."。

肆、討論

當我們研讀現代密碼學入門有關書籍時, 我們對單向活門函數最感興趣, 我們一再嘗試寫出新函數, 但是要寫出一個比 RSA 系統更難破解的方法實在不是目前能力所能解決。因此我們朝簡單函數當作換位加密用方向尋找, 正因為正餘弦疊合函數是有界且是週期函數因此很適合作為換位加密用。眾所週知的凱撒加密法就是基本換位法之一種[7], 它是利用同餘運算, 取其換位移位數值不致於過大以致於計算機產生 overflow 現象。所以使用式(13)的時候α_k, β_k與x_k的選取很重要。只要保持$\alpha_k > 0$和$\beta_k > 0$, 式(14)之$\varphi_k > 0$恆成立, φ_k必為第一象限角, 倘若再配合選取x_k也是第一象限角, 則$x_k + \varphi_k$必為第一或第二象限角, 因此y_k恆為正

值且小於正餘弦疊合函數的振幅 $\sqrt{\alpha_k{}^2+\beta_k{}^2}$ 不致於過大以致於計算機產生 overflow 現象。式(16)、式(17)與式(18)的目的只是要讓下一步的式(15)當中之 γ_k 很亂使移位數值難以預料，而我們也達成願望，可是當我們跑程式的時候卻發現式(17)中的 $\text{int}((\varphi_k-\text{int}(\varphi_k))*100)$，也就是 φ_k 小數點以下前二碼，大約在 k=20 之後呈現週期現象，這是我們始料未及的情形。這一點有待投入更多心力。還好式(15)在 k=20 之後 φ_k 呈現週期現象時用來做換位數值的 γ_k 依然很亂，資料保密之安全性還能接受。假若駭客不知道我們使用正餘弦疊合法將很難突破，所以很難估計被破解的機率。假若駭客知道我們使用正餘弦疊合法而且也知道參數 α_{k+1},β_{k+1} 與 x_{k+1} 如何由 α_k,β_k 與 x_k 選取，則駭客只要猜中 α_0,β_0 與 x_0 即可破解。若 α_0,β_0 與 x_0 均為 n 位正整數，則被破解機率為 $\frac{1}{10^{3n}}$。之前在肆、二節最末談及可以將正餘弦疊合法改寫為次數很小的多項式加密函數，方法是利用泰勒展開式即可以達成，這一部分我們計畫當作我們下一個研究目標。

接著討論連分數轉換部分，這一個加密最主要附加功能是資料壓縮。前一段提到當我們跑程式的時候卻發現式(17)中的 $\text{int}((\varphi_k-\text{int}(\varphi_k))*100)$，也就是 φ_k 小數點以下前二碼，大約在 k=20 之後呈現週期現象。由於利用連分數轉換將 $\{q_k\}$ 轉換成最簡假分數需要兩個整數變數儲存資料，若是 $\{q_k\}$ 數列項數過多將使得兩個整數變數數值過大產生 overflow 現象。因此無法如願將一整篇文章只壓縮成一個有理數，所以 k=20 之後 φ_k 小數點以下前二碼呈現週期現象並不妨礙我們的加密需求。因為式(19)的 q_k 介於 1 到 198 之間，以 100 為平均值計算，假設一個整變數佔用 4 bytes，一個字元佔用 2 bytes 大約每 4 個字元就要轉換成一組最簡假分數，平均壓縮率為 $\frac{4bytes\times 2}{2bytes\times 4}=100\%$。若 q_k 都是最小值 1 時，這時 45 個字元轉換成一組最簡假分數，壓縮率為 $\frac{4bytes\times 2}{2bytes\times 45}=\frac{4}{45}=8.89\%$。若 q_k 都是最大值 198 時，這時 4 個字元轉換成一組最簡假分數，壓縮率為 $\frac{4bytes\times 2}{2bytes\times 4}=100\%$。當使用長整數一個整變數佔用 6 bytes 時，壓縮率如下表四所示。所以長整數變數有較好的一壓縮率。但是比較 8 bytes 長整數時壓縮率沒有改善，因此我們建議使用 6 bytes 整數以符合效率。若從另一個角度看效率，為了讓 q_k 的值變小使平均數也變小，讓每次壓縮字元數提高。我們採取犧牲移位數值亂度讓 γ_k 數值變小，將式(15)變成

$$\gamma_k=\text{int}((y_k-\text{int}(y_k))*10) \tag{31}$$

γ_k 只取 y_k 小數點下第一位則式(19)的 q_k 值介於 1 到 109 之間，以 55 為平均值計算可求得平均壓縮率，另外最佳情形 q_k 都是 1，以及最不好情形 q_k 都是 109 的壓縮率均列在表四當中。由表四的數據可知，在犧牲移位數值亂度之下，我們以平均縮率的觀點考量仍然建議使用 6 bytes 整數以符合效率。

一個整變數佔用位元	數列$\{q_k\}$	壓縮一次字元數	壓縮率
8 bytes	設 q_k 都是 198	8	100%
8 bytes	設 q_k 都是 100	9	88.89%
8 bytes	設 q_k 都是 1	91	8.79%
6 bytes	設 q_k 都是 198	6	100%
6 bytes	設 q_k 都是 100	7	85.71%
6 bytes	設 q_k 都是 1	68	8.82%
4 bytes	設 q_k 都是 198	4	100%
4 bytes	設 q_k 都是 100	4	100%
4 bytes	設 q_k 都是 1	45	8.89%
以下考慮 γ_k 介於 0 與 9 之間情況			
8 bytes	設 q_k 都是 109	9	88.89%
8 bytes	設 q_k 都是 55	10	80%
8 bytes	設 q_k 都是 1	91	8.79%
6 bytes	設 q_k 都是 109	6	100%
6 bytes	設 q_k 都是 55	8	75%
6 bytes	設 q_k 都是 1	68	8.82%
4 bytes	設 q_k 都是 109	4	100%
4 bytes	設 q_k 都是 55	5	80%
4 bytes	設 q_k 都是 1	45	8.89%

表四　　$\text{壓縮率} = \dfrac{\text{一個整變數位元數} \times 2}{2\ bytes \times \text{壓縮一次字元數}}$

至於單向活門函數部分，我們還沒有任何貢獻，我們為了資料的安全性選擇 RSA 系統當作第三重加密，其目的只是給駭客更少的機會。我們仍然有很多問題尚未突破，這些個別問題將由我們四人日後一一解決。

伍、結論

為了增加資料之安全性，在正餘弦疊合換位加密部分，可以增加 α_0、β_0 與 x_0 之位數 n。n 值增大 α_0、β_0 與 x_0 三數被猜中機率變小，可以降底洩密之風險。因此 n 值越大越好。

在連分數轉換部分，利用 6 bytes 長整數轉換，有最佳壓縮率。

陸、參考資料

[1]余文卿主編，高中數學（一），龍騰文化，P.156。

[2]余文卿主編，高中數學（二），龍騰文化，P.135。

[3]官大智專題演講稿，因數分解與 RSA 密碼系統，國立中山大學應用數學系高中資優班專題講座。

[4]閔嗣鶴、嚴士健編，初等數論（第二版），凡異，P.62。
[5]楊吳泉編著，現代密碼學入門與程式設計，全華科技圖書，P.1-5。
[6]楊吳泉編著，現代密碼學入門與程式設計，全華科技圖書，P.3-29。
[7]楊吳泉編著，現代密碼學入門與程式設計，全華科技圖書，P.2-3。

評語

優點：透過本次參展得以瞭解到最基本的資料壓縮原理。
改進：作品採用正餘弦疊合函數似乎並不平凡，應該對於該函數的背景多一些說明。