中華民國第 57 屆中小學科學展覽會

作品說明書

國中組　數學科

030416

「線」出原形——加密五重奏

學校名稱：高雄市立大義國民中學

作者：	指導老師：
國二 侯又瑜	謝志強

關鍵詞：不完全加密、干擾式加密、密碼學

摘要

密碼學分為密碼術與破密學，而本次的研究重點在密碼術的部分。密碼術的研究在於加密的複雜性與解密的可逆性，而一個加密系統的好壞取決於它的安全性。本次研究運用了國中的幾何概念與高中的矩陣發展出新的加密方式。並透過合成函數的概念結合五重不同的加密方式，增加其加密的安全性，分別為改良式改撒密碼、不完全加密法(一維度不完全鏡射法、二維度分別不完全鏡射法、二維度不完全鏡射法、二維度不完全點射法、二維度改良式不完全映射法，高維度不完全加密法)、煙霧彈加密法(改良式維吉尼亞密碼、干擾加密法)、連分數加密法與 RSA 公鑰演算法，以各自加密法的優點截長補短，使這五重加密方式能相互配合，奏出和諧優美的「加密五重奏」。

壹、 研究動機

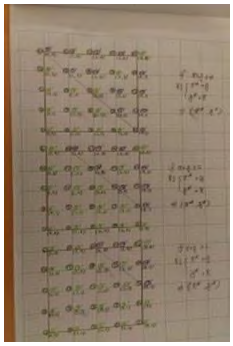
有一天，我在家中的書架上找書，找著找著卻無意間發現隱身書架深處，已沾了厚厚一層灰塵的《數學小魔女》。在好奇心的驅使下翻開封面，翻著泛黃的頁面，一不小心就掉進了書中密碼學的綺麗世界。閱讀完這本書後，我便希望能以「密碼學」當主題參加科展，並藉此機會見見課本外的天空。

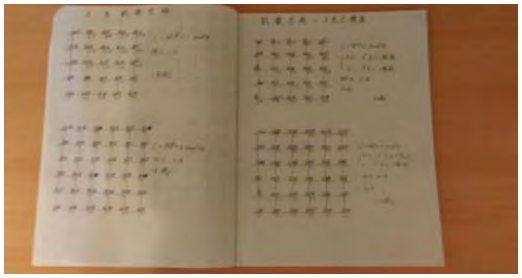
貳、研究目的

一、課程中所學的內容與工具是否能應用於密碼學中?
二、怎樣的密碼才能以比較複雜，而有安全性的形式呈現?
三、新的加密法要如何在高維度上加以延伸與推廣?

參、研究設備及器材

紙、筆、方格紙





肆、文獻探討

一、改良式凱撒密碼

改良式凱撒密碼			
	公式	原理	舉例
加密	f_1 C=mP+s(mod t) （P：明文，C：密文，s 為向後推移數）	密碼學家們為增加推移空間所提出二參數鑰匙的加密方式。 名詞定義; K_e:改良式凱撒密碼加密的鑰匙。 K_d:改良式凱撒密碼解密的鑰匙。 條件限制： m：必須不等於 0，且與 t 互質。【反例 1】【反例 2】 s：必須在 m=1 時，不等於編碼【反例 3】 【相關定理】設 a、b 表二正整數，則必定存在適當的整數 m、n,使得(a,b)=ma+nb。(其中 ma+nb 叫做 a、b 的線性組合) 【說明 1】m 必須與 t 互質是因為透過歐幾里得演算法找乘法逆運算數時，只能求得 m 和 t 的公因數，但無法求得 1，它的可逆性遭破壞，所以無法成為鑰匙。 【說明 2】因為 m 必須與 t 互質，所以若 t 為一大質數，m 符合的數字總數就遠超於 t 是合數時 m 符合的數字總數。這使密碼有更多種的組合，有助於增加安全性。	（P：明文，C：密文，s 為向後推移數） 【例 1】Ke=<m , s>=<5,0>,P=3 $C = 5 \times 3 + 0 (\mathrm{mod}\ 7)$=1 【例 2】Ke=<m , s>=<1,3> $C = 1 \times 3 + 3 (\mathrm{mod}\ 7)$=2 【反例 1】（所有密碼相同） Ke=<m , s>=<0,2>,P_1=3,P_2=4 C_1=$0 \times 3 + 2$(mod 7)=2, C_2=$0 \times 4 + 2$(mod 7)=2 【反例 2】（部分密碼相同） Ke=<m,s>P1=3,P2=5,P3=6,x=4, C_1=$2 \times 3 + 0$(mod 4)=2, C_2=$2 \times 5 + 0$(mod 4)=2, C_3=$2 \times 6 + 0$(mod 4)=0 【反例 3】（密文與明文相同） Ke=<m , s>,P=3 C=$1 \times 3 + 7$(mod 7)=3

<table>
<tr>
<td>解
密</td>
<td>f_1^{-1}
P=nC+w(mod t)</td>
<td>利用歐幾里得演算法的快速算法找到 m 的乘法逆運算。接下來 w 的部分利用移項的方式求出就行了。

格式
<table><tr><td>X1</td><td>Y1</td><td>R1</td><td></td></tr><tr><td>X2</td><td>Y2</td><td>R2</td><td></td></tr><tr><td>X3</td><td>Y3</td><td>R3</td><td>A1</td></tr><tr><td>X4</td><td>Y4</td><td>R4</td><td>A2</td></tr><tr><td>X5</td><td>Y5</td><td>R5</td><td>A3</td></tr></table>
原理
<table><tr><td>X1R1+Y1R2</td><td>R1</td><td>R2</td><td>X2R1+Y2R1</td></tr><tr><td>A1X2R1+A1Y2R2</td><td>A1R2</td><td></td><td></td></tr><tr><td>(X1-A1X2)R1+(Y1-A1Y2)R2
$\equiv X3R1 + Y3R2$</td><td>R3</td><td></td><td></td></tr></table>
步驟
1.先令 X1=1,Y1=0,X2=0,Y2=1
2.$R1 \div R2 = A1 \cdots R3$
則 X3= -(A1X2)+X1,Y3= -(A1X2)+Y2
3. $R2 \div R3 = A2 \cdots R4$
直到 Rn 出現 1，則停止。</td>
<td>加密公式：C=7P+3(mod26)
先求 C=7P(mod26)的乘法逆運算數。
<table><tr><td>1</td><td>0</td><td>26</td><td></td></tr><tr><td>0</td><td>1</td><td>7</td><td></td></tr><tr><td>1</td><td>-3</td><td>5</td><td>3</td></tr><tr><td>-1</td><td>4</td><td>2</td><td>1</td></tr><tr><td>3</td><td>-11</td><td>1</td><td>2</td></tr></table>出現 1
3 和-11 代表
$3 \times 26 + (-11) \times 7(\text{mod } 26)$
$=-11 \times 7(\text{mod } 26)$
=-77(mod 26)=1，
7 的乘法逆運算數是-11，
-11(mod 26)=15，
7(mod 26)的乘法逆運算數是 15。
由此得：
C=7P+3(mod 26),
7P=(C-3)(mod 26),
P=15(C-3)(mod 26),
P=15C-45(mod 26),
-45mod 26=17,
P=15C+17(mod 26)
Ke=＜m,s＞=<7,3>,
Kd=＜n,w＞=<15,17></td>
</tr>
</table>

二、連分數加密法

<table>
<tr><th colspan="2">連分數加密法</th></tr>
<tr><th>定義</th><th>定理</th></tr>
<tr><td>【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】
$\{q_0 : q_1, q_2 \cdots, q_{n-1}, q_n\} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}$</td><td>【定理 1: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 ∈ Z 且 0 ≤ r ＜ b 使得 a = qxb + r 。

【定理 2 :a、b 的線性組合】設 a、b 表二正整數，則必定存在適當的整數 m、n,使得(a,b)=ma+nb。

【定理 3】 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 $\{q_0 : q_1, q_2 \cdots, q_{n-1}, q_n\}$使得</td></tr>
</table>

	$\frac{a}{b}=\{q_0:q_1,q_2\cdots,q_{n-1},q_n\}$。 【定理 4】 設$\{q_0:q_1,q_2\cdots,q_{n-1},q_n\}$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$\frac{a}{b}=\{q_0:q_1,q_2\cdots,q_{n-1},q_n\}$

加密(利用【定理 4】加密)	解密(利用【定理 3】解密)	
步驟一，將明碼字母轉換成字元數值數列 步驟二，將字元數值數列進行分組，每 q 個分為一組(避免電腦 overflow) 步驟三，利用【定理 4】轉換成最簡假分數$\frac{a}{b}$ 步驟四，傳送 r 組數對(a,b)給 RSA 公鑰加密系統 r = $\frac{\text{字元數值數列之項數總數}}{q}$ 【例 1】:{2 : 3, 4,5} = $2+\frac{1}{3+\frac{1}{4+\frac{1}{5}}}=\frac{157}{68}$	【例 3】 輾轉相除法: 2 | 157 | 68 | 1 136 | 63 4 | 21 | 5 | 1 20 | 5 1 | 0	【例 3】改寫過程: $157=2\times68+21\rightarrow\ \frac{157}{68}=2+\frac{21}{68}$ $68=3\times21+5\ \rightarrow\ \frac{68}{21}=3+\frac{5}{21}$ $21=4\times5+1\ \rightarrow\ \frac{21}{5}=4+\frac{1}{5}$ *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}

由定理 1 與定理 2 可推論得定理 3 與定理 4 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 $\frac{a}{b}$ 與簡單假分數之 1 對 1 對應函數關係，也保證研究方法中的第 4 層加密(連分數加密法)是可行的。

三、RSA 公鑰演算法

RSA 公鑰演算法						
名詞定義	公鑰	公布出來的加密關鍵。				
	私鑰	私下保存的解密關鍵。				
	單向陷門函數	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），此即所謂陷門。				
演算方式	鑰匙產生	1.隨意產生兩個極大的質數 p、q　2.$N=p\times q$ 3.$\varphi(N)=(p-1)(q-1)$　4.$\gcd(e,\varphi(N))=1$，$e<\varphi(N)$ 5.依歐幾里得演算法找出 $ex-\varphi(N)y=1$裡的 x 和 y 公鑰：$<e,N>$，私鑰：x	加密	$C\equiv P^e(\text{mod } N)$	解密	$P\equiv C^x(\text{mod } N)$
使用	發送訊息者用接收訊息者公布的公鑰將訊息加密，傳給接收訊者。接收訊息者用自己的私鑰解密。					
舉例	鑰匙產生	$N=3\times5=15$ ， $\varphi(N)=(3-1)(5-1)=8$ 取 $e=7$,使得$(e,\varphi(N))=1$，由歐幾里得演算 $ex-\varphi(N)y=1$ 中 $x=13,y=6$ 公鑰：$<e,N>$ $=<7,15>$ 私鑰：$x=13$	加密	P=2 $C\equiv2^7(\text{mod } N)$ $\equiv8$	解密	C=8 $C\equiv8^{13}(\text{mod } N)$ $\equiv2$

四、維吉尼亞密碼

<table>
<tr><td colspan="6">維吉尼亞密碼</td></tr>
<tr><td>表格法</td><td colspan="2">在藍色字母行找到明文字母，並找到紫色字母行與明文相對應的鑰匙字母，兩者對應下來的字母及為密文。</td><td>舉例</td><td>明碼: LETTER
關鍵詞: LAST
鑰匙: LASTLA
密碼: W E L M P R</td><td rowspan="3">表格</td></tr>
<tr><td rowspan="2">算式</td><td>加密</td><td>將字母 A～Z 用數字 0～25 代替，$C_i \equiv P_i + K_i (\mathrm{mod} 26)$</td><td rowspan="2">舉例</td><td rowspan="2">明文: 11 4 19 19 4 17
關鍵詞: 11 0 18 19
鑰匙: 11 0 18 19 11 0
密文: 22 4 11 12 15 17</td></tr>
<tr><td>解密</td><td>將字母 A～Z 用數字 0～25 代替，$P_i \equiv C_i - K_i (\mathrm{mod} 26)$</td></tr>
</table>

五、希爾密碼

希爾密碼	
相關定理	在模 t 之下，方陣 M 可逆的充分必要條件為方陣 M 之行列式值與 t 互質；亦即， $M^{-1} \exists \Leftrightarrow \gcd(\det(\mathrm{M}), \mathrm{t}) = 1$
加密	步驟一，選定一個在模 t 之下的 n 階方陣，在此表示為 M。 步驟二，將訊息以 n 為單位分組，無法湊成時加入 x 補滿，令每組$1 \times \mathrm{n}$矩陣為 v。 步驟三，$\mathrm{M} \times v^T (\mathrm{mod\ t})$ 即為密文。
解密	步驟一，將訊息以 n 為單位分組，令每組$1 \times \mathrm{n}$矩陣為 w。 步驟二，$M^{-1} \times w^T (\mathrm{mod\ t})$ 。 步驟三，所得的數字再刪掉最後無意義的 x 即為明文。

伍、名詞定義

一、不完全加密：不完全加密是指只在一個條件下使某部分加密，保留某個部分不加密。

陸、研究方法與內容

一、一維度加密法

(一)一維度不完全鏡射法

1. 一維度完全鏡射法

一維度完全鏡射法	
想法	透過一條對稱軸，使一維的數字做位置上的鏡射。
鑰匙 討論	假設原始數字為 012345，對稱軸在 2 和 3 之間，經由鏡射使得加密數字能變成 543210，接下來比較原始數字與加密數字，發現上下的數字相加皆等於 50+5=5，1+4=5，2+3=5…， 原始數字:012345 加密數字:543210 因此鑰匙定為 5，並以 K=5 表示。
加密解密	C 為密文，P 為明文，K=(t-1)，其中 t 為編碼數。 加密: C=K−P，解密: P=K−C

【發現】一維度完全鏡射法是改良式凱撒密碼的特例，即

$K_e =< m, s >=< (t-1, K) >$，即$\mathrm{C} = (\mathrm{t}-1)\mathrm{P} + \mathrm{K}$以下以舉例來驗證:

一維度鏡射法	改良式凱撒密碼
t=6 K=5, P=012345 C_1=543210	Ke=<(t -1),K>,t=6,P=012345 $5 \times 0 + 5(\mathrm{mod}6) = 5$， $5 \times 1 + 5(\mathrm{mod}6) = 4$， $5 \times 2 + 5(\mathrm{mod}6) = 3$， $5 \times 3 + 5(\mathrm{mod}6) = 2$， $5 \times 4 + 5(\mathrm{mod}6) = 1$， $5 \times 5 + 5(\mathrm{mod}6) = 0$ C_2=543210
〔結論〕一維度鏡射法是改良式凱撒密碼的特例。	

2.一維度不完全鏡射法

<table>
<tr><td colspan="3">改良式一維度鏡射法(一維度不完全鏡射法)</td></tr>
<tr><td>想法</td><td colspan="2">透過一條軸，使它某些部分保留原狀不做鏡射，某部分做鏡射，即為不完全鏡射。如【圖二】。
 
【圖二】
說明:
整條線段為鏡射範圍，橘線為對稱軸，以它做鏡射。藍色線為有鏡射部分，較細線段為保持原狀的部分。</td></tr>
<tr><td>鑰匙討論</td><td colspan="2">(1)決定是否鏡射
是否鏡射在於 K−P 的值是否在編碼數(在此以 t 代表)的範圍內。如果在範圍內，就進行鏡射，如果不在範圍內，就不進行鏡射，故決定 K 值是間接決定是否鏡射。
(2)範圍
$K \in \{1,2,3,4,\cdots,2(t-2)+1\}$ ，若不在 K 值範圍內，則加密結果將與明碼相同。</td></tr>
<tr><td>加密
解密</td><td>加密</td><td>解密</td></tr>
<tr><td></td><td>$\begin{cases} C = K - P, if\ K - P \in \{0,1,2,\cdots,t-1\} \\ C = P, if\ K - P \notin \{0,1,2,\cdots,t-1\} \end{cases}$</td><td>$\begin{cases} P = K - C, if\ K - C \in \{0,1,2,\cdots,t-1\} \\ P = C, if\ K - C \notin \{0,1,2,\cdots,t-1\} \end{cases}$</td></tr>
</table>

【舉例】P = safe → 18 0 5 4 , K = 15 , C = 18 15 10 11

【測試】一維度不完全鏡射法單獨使用時不夠安全，因此我們嘗試將它與改良式凱撒密碼一同使用，以下是實際測試的結果:(詳細狀況請參見附錄)

加密法 / 編碼數	改良式凱撒密碼	改良式凱撒密碼＋ 改良式一維度鏡射法
5	20 種組合	60 種組合
6	12 種組合	48 種組合

〔結論〕改良式凱撒密碼搭配上不完全鏡射法能有效增加安全性。

【發現】因改良式凱撒密碼 m 與 s 的條件，以及改良式一維度鏡射法中 K 的條件，當編碼數是一個很大的質數時，m 與 s 的範圍就能很廣，K 因為編碼數很大，所以範圍也很廣。

〔結論〕改良式凱撒密碼加上不完全鏡射時，編碼數為質數且愈大愈安全。

(二)煙霧彈式加密法

雖然不完全鏡射法與改良式凱撒密碼加密方式一起並用時能增加一些組合數，提升安全性，但只要利用頻率解析法便可破密，整體來說還是不夠安全，因此我們透過維吉尼亞密碼中給人”一對多，多對一”錯覺的發想，結合國中所學的數列，發展出煙霧彈式加密法。而煙霧彈式加密有著第三方無法發現的玄機，令人彷彿置身於茫茫煙霧中，無法單純使用頻率解析法準確解密，在此，我們提出兩種加密方式，分別為改良式維吉尼亞密碼和干擾式加密法。

1.改良式維吉尼亞密碼

改良式維吉尼亞密碼	
想法	維吉尼亞密碼的給人一種「非一對一可逆函數」的錯覺，相同的明文經由不同的鑰匙，能使相同的字母被加密成不同的字母，於是較改良式凱撒密碼安全，但不斷重複的特性造成了他遭破譯的危險性。因此我們提出應用一些常用數列（等差數列、等比數列、費波納契數列）與無理數為鑰匙加密的方法。但考慮到目前電腦運算無理數所能求得的位數，所以我們在使用無理數當鑰匙加密時，會使用兩個以上的鑰匙作加密並視情況照一定的規律使用。
鑰匙討論	加密、解密時的鑰匙可分為三種: (1)$\{K_i\}$:是一組常用的數列或是無理數小點後第 2i-1 位與第 2i 位所組的數列，使用時兩兩分組一組對照一個明文。 (2)$\{K_{ni}\}$:第 n 把鑰匙的K_i。

		加密	解密
加密解密	數列	$C_i \equiv P_i + K_i (\text{mod t})$	$P_i \equiv C_i - K_i (\text{mod t})$
	無理數	$C_i \equiv P_i + K_i (\text{mod t})$	$P_i \equiv C_i - K_i (\text{mod t})$
	交錯	步驟一，選定 r 個 Key 驟步二，i (mod r)=n(n = 1,2,⋯ r)，使用 Key_n 步驟三， $C_i \equiv P_i + K_{n(\frac{i+r-n}{r})} (\text{mod t})$	$P_i \equiv C_i - K_{n(\frac{i+r-n}{r})} (\text{mod t})$

【舉例】

鑰匙	以明文 safe 為例(t=26)
數列: 【使用等差數列(a_1=3,d=7)】 表示為: 定 K=(a_1,d) =(3，7)	明文:18 0 5 4 鑰匙: 3 10 17 24 密文:21 10 22 2
無理數: 【使用$\sqrt{5}$】 $K = \sqrt{5} = 2.23606797\cdots$ $K = \sqrt{5}$ ⇒ 23 60 67 97⋯	明文:18 0 5 4 鑰匙:23 60 67 97 密文:15 8 20 23
交錯: 【使用$\sqrt{3}$、$\sqrt{5}$ 與a_1=3,d=7 的等差數列】 $\{K_{1i}\} \Rightarrow 73\ 20\cdots$, $\{K_{2i}\} \Longrightarrow 23\ 60\ \cdots$, $\{K_{3i}\} \Longrightarrow\ 3\ 10\cdots$	明文: 18 0 5 4 鑰匙: 73 23 3 20 密文: 23 23 8 24 不同的明文經由鑰匙加密後形成了相同的明文，能維持著維吉尼亞密碼給人”一對多，多對一”的錯覺。

【延伸】使用一無理數小數點後的數或一數列透過(mod r)來決定鑰匙要使用哪一把。例:如上例使用三把鑰匙(r=3)，e = 2.71828⋯為選擇的無理數。鑰匙使用順序與數點後的數的關係如右:

e = 2.71828⋯
7(mod 3)=1→使用K_1
1(mod 3)=1→使用K_1
8(mod 3)=2→使用K_2
⋮

2.干擾式加密

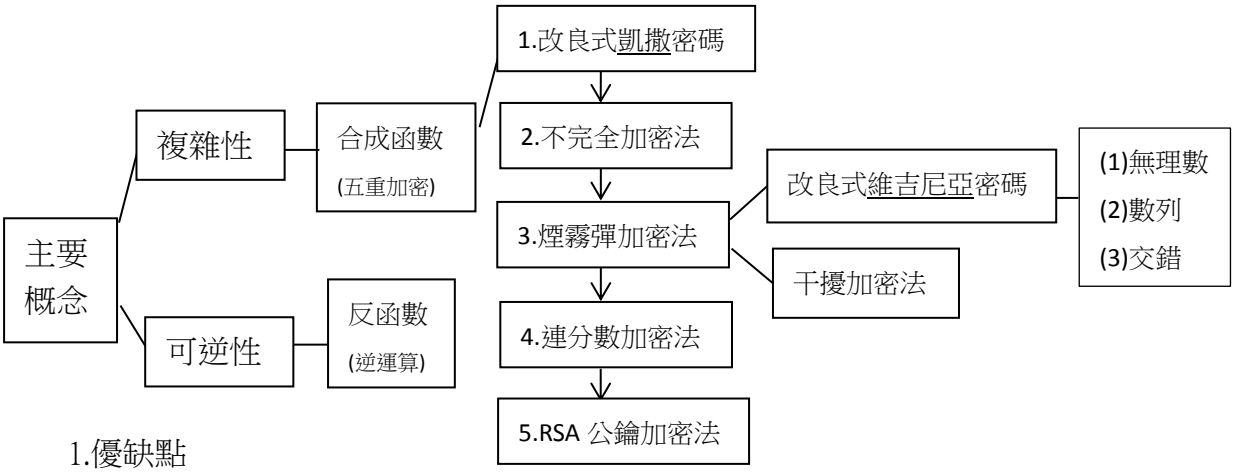
<table>
<tr><td colspan="3">干擾式加密</td></tr>
<tr><td>想法</td><td colspan="2">干擾式加密是在密碼中加上一些具規律性的干擾，於是我們希望在已加密文中以數列$\{a_n\}$的方式插入一組干擾的數字即$\{b_n\}$。每間隔a_i，放置一個干擾數b_i，即逐一在第 i + S_i項放置b_i。</td></tr>
<tr><td>鑰匙討論</td><td colspan="2">不同數列$\{a_n\}$即代表不同鑰匙。
限制：$\{a_n\}$須為正整數列
定義 $\{P_n\}$：明碼。 $\{a_n\}$：鑰匙。
$\{b_n\}$：由一組隨意數字組成的干擾數列。 $\{c_n\}$：密文。
S_i=a_1+a_2 + ⋯ + a_i</td></tr>
<tr><td rowspan="2">加密解密</td><td>加密</td><td>解密</td></tr>
<tr><td>$C_j = P_j \ \ if\ j < 1 + S_1$
$C_j = b_i$ if j = i + S_i,
$C_j = P_{j-i}\ if\ j \neq i + S_i$,
$i + S_i < j < (i+1) + S_{i+1}$</td><td>逐一刪掉$C_{S_i+1}$</td></tr>
</table>

【舉例】實際加密的狀況會如下:

<table>
<tr><td></td><td>符號舉例</td><td>數字舉例</td></tr>
<tr><td>加密</td><td>鑰匙：$\{a_n\} = \{1,2,3,\cdots\}$,
則$S_i = \frac{i(1+i)}{2}$
明文：$P_1\ P_2\ P_3\ P_4\ P_5\ P_6 \cdots$
密文： P_1 b_1 P_2 P_3 b_2 P_4 P_5 P_6 b_3⋯
➡$C_1\ C_2\ C_3\ C_4\ C_5\ C_6\ C_7\ C_8\ C_9 \cdots$</td><td>$\{a_n\} = \{1,2,3,\cdots\}$
$\{b_n\} = \{4,1,4,2,1,3,5,\cdots\}$
$S_i = 1 + 2 + 3 + \cdots + a_i$
$\{P_n\}$=safe → 18 0 5 4 ,
$\{C_n\} = 18\ 4\ 0\ 5\ 1\ 4$
→ 18 4 0 5 1 4</td></tr>
<tr><td>解密</td><td>鑰匙：$\{a_n\} = \{1,2,3,\cdots\}$,
則$S_i = \frac{i(1+i)}{2}$
密文：$C_1\ C_2\ C_3\ C_4\ C_5\ C_6\ C_7\ C_8\ C_9 \cdots$
➡ P_1 b_1 P_2 P_3 b_2 P_4 P_5 P_6 b_3⋯
⇓逐一刪掉C_{S_i+1}
明文：$P_1\ P_2\ P_3\ P_4\ P_5\ P_6 \cdots$</td><td>$\{a_n\} = \{1,2,3,\cdots\}$
$\{b_n\} = \{4,1,4,2,1,3,5,\cdots\}$
$S_i = 1 + 2 + 3 + \cdots + a_i$
$\{C_n\} = 18\ 4\ 0\ 5\ 1$
→ 18 4 0 5 1
⇓逐一刪掉C_{S_i+1}
$\{P_n\}$=18 0 5 4 → safe</td></tr>
</table>

(三)一維度五重加密法

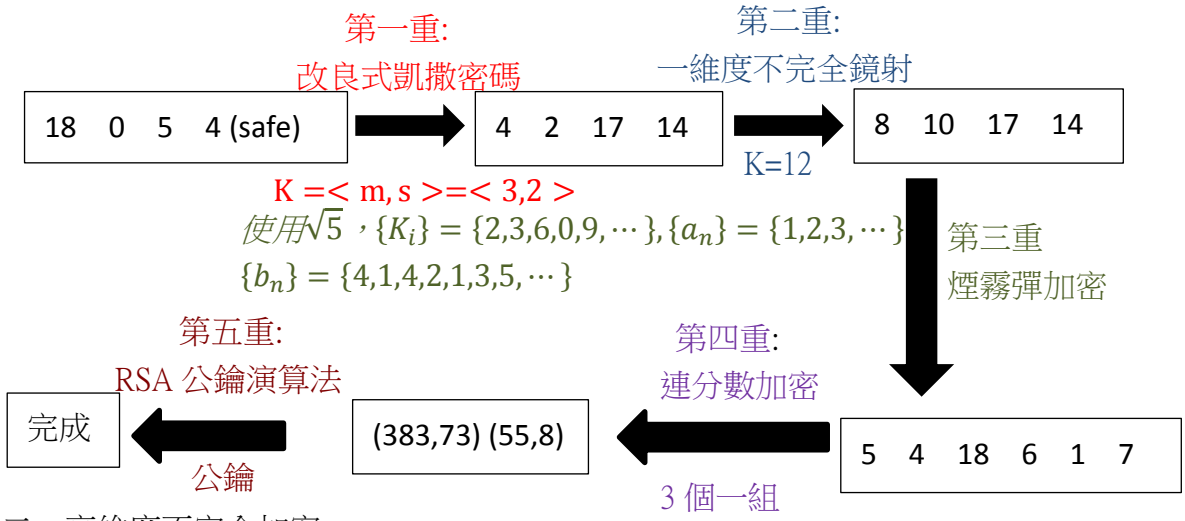
雖然不完全鏡射法在測試中已顯出它的優點，但單單使用一維度不完全鏡射法與煙霧彈加密法不夠安全，因此我們結合了一開始的測試中用到的改良式凱撒密碼，並在最後加上連分數加密法與 RSA 公鑰演算法，形成了一維度五重加密法，其架構如下:



1.優缺點

不完全鏡射法與煙霧但是加密能避開被頻率解析法破譯的危險，連分數加密法與 RSA 公鑰演算法因加密的方式能相互配合的很好，加上這兩重加密還能減少電腦的使用空間及增加整體安全性。

2.實例說明

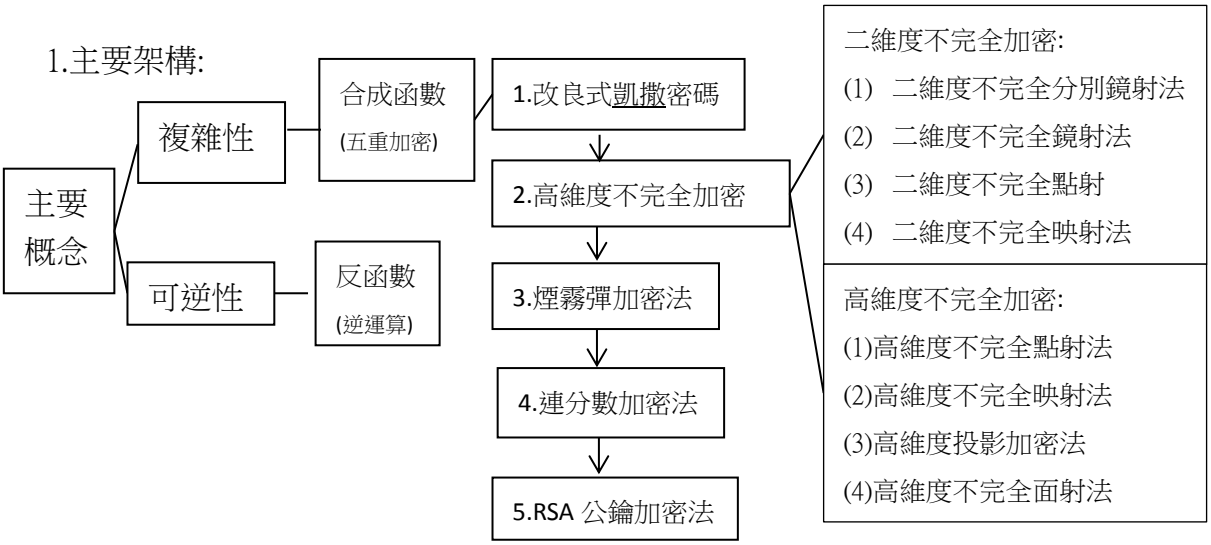


二、高維度不完全加密

(一)高維度五重加密法

我們想將一維度不完全鏡射法中一部分加密，一部分不加密的方式做延伸，因此對一維度五重加密中的第二重加密進行進一步的探討，並提出它在二維度、三維度和高維度空間中的應用；同時，沿用一維度加密法的概念，形成高維五重加密法。

1.主要架構:



2.使用時機與方法(以二維度為例)

二維度	直接使用。	
一維度	字元數為偶數	兩兩分組後直接使用。
	字元數為奇數	兩兩分組，不夠的補上 x(解密時刪掉無意義的 x 即可)後使用。

(二)二維度五重加密法

1.二維度不完全加密法的延伸探討

(1) 二維度不完全分別鏡射法

想法: 我們試著將前面所提的「改良式一維度鏡射法」，透過下列的加密法，放到直角座標圖中，以 t=4 K_1=4 為例：

$$\begin{cases} x' = K_1 - x, if\ \ K_1 - x \in \{0,1,2,\cdots,t-1\} \\ x' = x, if\ K_1 - x \notin \{0,1,2,\cdots,t-1\} \end{cases} \text{ and } \begin{cases} y' = K_1 - y, if\ \ K_1 - y \in \{0,1,2,\cdots,t-1\} \\ y' = y, if\ K_1 - y \notin \{0,1,2,\cdots,t-1\} \end{cases}$$

m(0,3)	n(1,3)	o(2,3)	p(3,3)
i(0,2)	j(1,2)	k(2,2)	l(3,2)
e(0,1)	f(1,1)	g(2,1)	h(3,1)
a(0,0)	b (1,0)	c(2,0)	d(3,0)

【圖 3】

e’	h’	g’	f’
i’	l’	k’	j’
m’	p’	o’	n’
a’	d’	c’	d’

【圖 4】

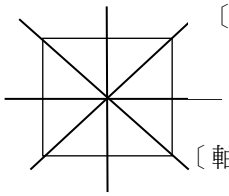
說明

(1)x’ 表示 x 透過改良式一維度加密法(分別鏡射法)加密的位置。

(2)【圖 4】是【圖 3】經由改良式一維度鏡射法加密後的結果。發現加密後的【圖 3】只是行列互換而已，所以， 我們改用以下介紹的加密法來做二維圖形上的加密。

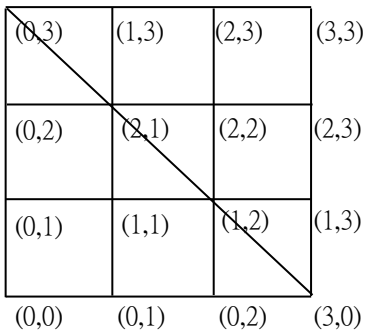
(2)二維度不完全鏡射法

(ⅰ)二維度完全鏡射法

二維度完全鏡射			
想法	分別鏡射法出現行列互換的結果，可視為鏡射的軸是鉛直與水平的那兩條對稱軸，於是針對剩下的兩條45 度的對稱軸進行鏡射。如【圖 5】  【圖 5】		
鑰匙討論	定$K_2 = -(t-1)$、$K_3 = 0$，其中 t 為編碼數。		
加密 解密	加密		解密
	軸 1:x+y+K_2=0	(x,y) → (x',y') =($-y$+(t − 1),$-x$ + (t − 1))	(x,y) → (x',y') = (-y'+(t-1), -x'+(t-1))
	軸 2:x-y+K_3=0	(x,y) → (x',y')= (y, x)	(x,y) → (x',y') = (y', x')
缺點	二維度完全鏡射法的組合方式不夠多，因此我們將提出二維度不完全鏡射法。		

【二維度完全鏡射法舉例】

【例 4】t=4 K2=-3

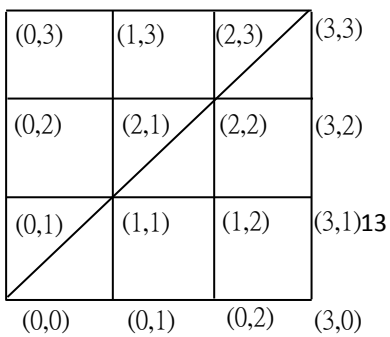


軸: x+y-3=0		
(x , y)		(x',y')
(0,0)	→	(3,3)
(0,1)	加密	(2,3)
(0,2)		(1,3)
(1,0)	←	(3,2)
(2,0)	解密	(3,1)
(1,1)		(2,2)

(3,0)、(1,2)、(2,1)、(0,3)為對稱軸，所以不鏡射。

【例 5】t=4

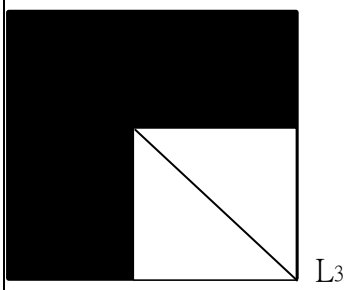
K3=0

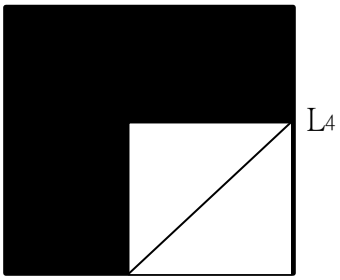


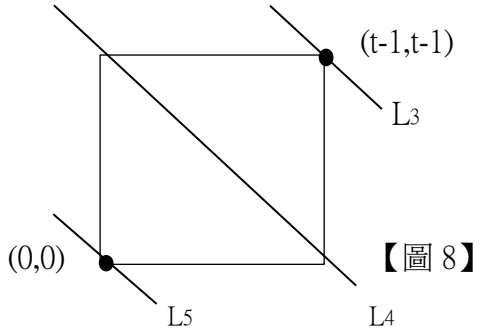
軸: x-y=0		
(x , y)		(x',y')
(3,0)	→	(0,3)
(3,1)	加密	(1,3)
(3,2)		(2,3)
(2,0)	←	(0,2)
(1,0)	解密	(0,1)
(2,1)		(1,2)

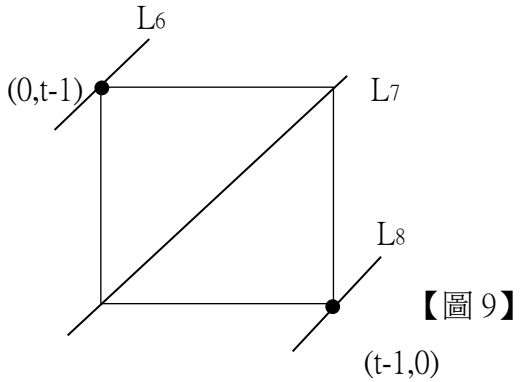
(0,0)、(1,1)、(2,2)、(3,3)為對稱軸，所以不鏡射。

(ii)二維度不完全鏡射法

<table>
<tr><td colspan="2">二維度不完全鏡射法</td></tr>
<tr><td>想法</td><td>此方法需要先找一條與 x 軸夾角為 45 度的線性方程式。在這樣的形況下，會有兩種方程式可使用，分別是 $x+y+K_2=0$ 和 $x-y+K_3=0$。接下來加密的部分就運用高中的對稱公式做計算。若超出了座標圖範圍，就不做鏡射。
以【圖 6】、【圖 7】說明:
 

【圖 6】
 

【圖 7】
說明:兩圖中黑色部分為不鏡射範圍，白色部分為鏡射範圍。L_3 和 L_4 兩條軸的方程式分別為:
L_3: $x+y+K_2=0$，
L_4: $x-y+K_3=0$。</td></tr>
<tr><td>鑰匙討論</td><td>定義: K_2、K_3 在此為加密的鑰匙。
公用: K 值(K_2、K_3)是在這個二元一次方程式中決定對稱軸的位置，也就是間接決定加密後點的位置和鏡射與否。
範圍: $x+y+K_2=0, K_2$：$-2(t-1)<K_2<0$ 且 K_2 為正整數
$x-y+K_3=0, K_3$：$-(t-1)<K_3<(t-1)$ 且 K_3 為正整數
若超出範圍，密文會與明文相同。如【圖 8】【圖 9】:
 

【圖 8】
鏡射範圍須在 L_3 到 L_5 之間
 

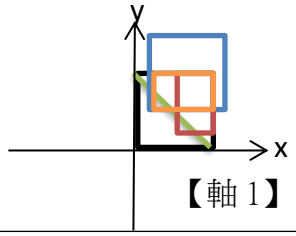
【圖 9】
鏡射範圍須在 L_6 到 L_8 之間</td></tr>
</table>

		加密	解密
加密解密	軸 1: $x+y+K_2=0$，	當 $x+y+K_2=0$ 時, 如果 $x'=-y-K_2 \in \{0,1,2,\cdots(t-1)\}$ 且 $y'=-x-K_2 \in \{0,1,2,\cdots(t-1)\}$ 則 $(x,y) \xrightarrow{g_2} (x',y')$ 即 $\begin{bmatrix}x\\y\end{bmatrix} \to \begin{bmatrix}x'\\y'\end{bmatrix}$ $= \begin{bmatrix}0 & -1\\-1 & 0\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix} + \begin{bmatrix}-K_2\\-K_2\end{bmatrix}$ if $x' \in \{0,1,2,\cdots,t-1\}$ and $y' \in \{0,1,2,\cdots,t-1\}$	當 $x+y+K_2=0$ 時, 如果 $x'=-y-K_2 \in \{0,1,2,\cdots(t-1)\}$ 且 $y'=-x-K_2 \in \{0,1,2,\cdots(t-1)\}$ 則 $(x,y) \xrightarrow{g_2^{-1}} (x',y')$ 即 $\begin{bmatrix}x\\y\end{bmatrix} \to \begin{bmatrix}x'\\y'\end{bmatrix}$ $= \begin{bmatrix}0 & -1\\-1 & 0\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix} + \begin{bmatrix}-K_2\\-K_2\end{bmatrix}$ if $x' \in \{0,1,2,\cdots,t-1\}$ and $y' \in \{0,1,2,\cdots,t-1\}$
	軸 2: $x-y+K_3=0$，	當 $x-y+K_3=0$ 時, 如果 $x'=y-K_3 \in \{0,1,2,\cdots(t-1)\}$ 且 $y'=x+K_3 \in \{0,1,2,\cdots(t-1)\}$ 則 $(x,y) \xrightarrow{g_3} (x',y')$ 即 $\begin{bmatrix}x\\y\end{bmatrix} \to \begin{bmatrix}x'\\y'\end{bmatrix}$ $= \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix} + \begin{bmatrix}-K_3\\K_3\end{bmatrix}$ if $x' \in \{0,1,2,\cdots,t-1\}$ and $y' \in \{0,1,2,\cdots,t-1\}$	當 $x-y+K_3=0$ 時, 如果 $x'=y+K_3 \in \{0,1,2,\cdots(t-1)\}$ 且 $y'=x+K_3 \in \{0,1,2,\cdots(t-1)\}$ 則 $(x,y) \xrightarrow{g_3^{-1}} (x',y')$ 即 $\begin{bmatrix}x\\y\end{bmatrix} \to \begin{bmatrix}x'\\y'\end{bmatrix}$ $= \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix} + \begin{bmatrix}-K_3\\K_3\end{bmatrix}$ if $x' \in \{0,1,2,\cdots,t-1\}$ and $y' \in \{0,1,2,\cdots,t-1\}$

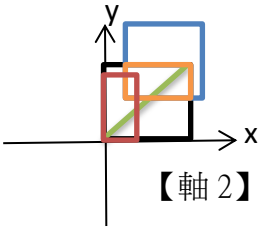
【發　現】軸 1 的加密情況其實是鏡射矩陣$\begin{bmatrix}cos2\theta & sin2\theta\\sin2\theta & -cos2\theta\end{bmatrix}$中$\theta = 135°$，再沿軸 2 方向平移的加密方式；軸 2 的加密情況其實是鏡射矩陣中$\theta = 45°$，再沿軸 1 方向平移的的加密方式。

【新發想】①調整θ，使鏡射矩陣中的 sin 值與 cos 值同時維持為整數，2θ只能是$90°$、$180°$、$270°$，即須$\theta = 45°$(軸 2 加密情況)、$\theta = 90°$(類似二維度不完全分別鏡射法中的行列互換)、$\theta = 135°$(軸 1 加密情況)

②調整平移方式，以圖示說明。



【軸 1】



【軸 2】

說明
在編碼範圍內(黑色正方形)以軸 1 或軸 2(綠色線)做鏡射，並進行平移到藍色正方形，平移後在編碼範圍內的便進行加密(橘色長方形)，發現紅色和橘色兩個長方形區塊，加密後都會在橘色長方形區塊，即有相同的加密結果，呈現多對一的現象。

【結果】以軸 1 加密時平移的方向必須沿著軸 2；以軸 2 加密時平移的方向必須沿著軸 1，若任意平移則明文與密文會出現多對一的情形，此加密方式便不可逆，故此加密法不成立，因而無法成為加密的工具。

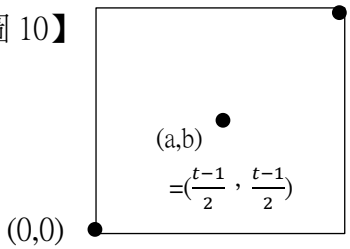
【心得】雖然兩個新發想都無法成為新的加密方式，但過程中我們發現了不完全鏡射法平移遵循的規律，以及不遵循平移規律即不能成為加密工具的結果，也算一種另類的發現。

【二維度不完全鏡射法舉例】

	加密 P=18 0 5 4 → [18 0][5 4]	解密
軸 1 K_2=-6 t=26	P=safe→18 0 5 4 → $\begin{bmatrix}18\\0\end{bmatrix}\begin{bmatrix}5\\4\end{bmatrix}$ $\begin{bmatrix}x'\\y'\end{bmatrix}=\begin{bmatrix}0&-1\\-1&0\end{bmatrix}\begin{bmatrix}18\\0\end{bmatrix}+\begin{bmatrix}-(-6)\\-(-6)\end{bmatrix}$ $=\begin{bmatrix}6\\-12\end{bmatrix}\Rightarrow$維持$\begin{bmatrix}18\\0\end{bmatrix}$ $\begin{bmatrix}x'\\y'\end{bmatrix}=\begin{bmatrix}0&-1\\-1&0\end{bmatrix}\begin{bmatrix}5\\4\end{bmatrix}+\begin{bmatrix}-(-6)\\-(-6)\end{bmatrix}=\begin{bmatrix}2\\1\end{bmatrix}$ ， C= 18 0 2 1	C= 18 0 2 1→ $\begin{bmatrix}18\\0\end{bmatrix}\begin{bmatrix}5\\4\end{bmatrix}$ $\begin{bmatrix}x\\y\end{bmatrix}=\begin{bmatrix}0&-1\\-1&0\end{bmatrix}\begin{bmatrix}18\\0\end{bmatrix}+\begin{bmatrix}-(-6)\\-(-6)\end{bmatrix}$ $=\begin{bmatrix}6\\-12\end{bmatrix}\Rightarrow$維持$\begin{bmatrix}18\\0\end{bmatrix}$ $\begin{bmatrix}x\\y\end{bmatrix}=\begin{bmatrix}0&-1\\-1&0\end{bmatrix}\begin{bmatrix}2\\1\end{bmatrix}+\begin{bmatrix}-(-6)\\-(-6)\end{bmatrix}=\begin{bmatrix}5\\4\end{bmatrix}$ ， P= 18 0 5 4
軸 2 K_3=3 t=26	P=safe→18 0 5 4→ $\begin{bmatrix}18\\0\end{bmatrix}\begin{bmatrix}5\\4\end{bmatrix}$ $\begin{bmatrix}x'\\y'\end{bmatrix}=\begin{bmatrix}0&1\\1&0\end{bmatrix}\begin{bmatrix}18\\0\end{bmatrix}+\begin{bmatrix}-3\\3\end{bmatrix}=\begin{bmatrix}-3\\21\end{bmatrix}$ ⇒維持$\begin{bmatrix}18\\0\end{bmatrix}$ $\begin{bmatrix}x'\\y'\end{bmatrix}=\begin{bmatrix}0&1\\1&0\end{bmatrix}\begin{bmatrix}5\\4\end{bmatrix}+\begin{bmatrix}-3\\3\end{bmatrix}=\begin{bmatrix}1\\8\end{bmatrix}$ C=$\begin{bmatrix}18\\0\end{bmatrix}\begin{bmatrix}1\\8\end{bmatrix}$ → 18 0 1 8	C=18 0 7 5→ [18 0][1 8] $\begin{bmatrix}x\\y\end{bmatrix}=\begin{bmatrix}0&1\\1&0\end{bmatrix}\begin{bmatrix}18\\0\end{bmatrix}+\begin{bmatrix}-3\\3\end{bmatrix}=\begin{bmatrix}-3\\21\end{bmatrix}$ ⇒ 維持$\begin{bmatrix}18\\0\end{bmatrix}$ $\begin{bmatrix}x\\y\end{bmatrix}=\begin{bmatrix}0&1\\1&0\end{bmatrix}\begin{bmatrix}1\\8\end{bmatrix}+\begin{bmatrix}-3\\3\end{bmatrix}=\begin{bmatrix}5\\4\end{bmatrix}$ P=$\begin{bmatrix}18\\0\end{bmatrix}\begin{bmatrix}5\\4\end{bmatrix}$ →18 0 5 4

(3)二維度不完全點射法

(ⅰ)完全點射法

完全點射法		
想法	在平面上的對稱方式除了線對稱，還有點對稱，於是想用點對稱的方式來進行座標圖上的鏡射。	
鑰匙討論	鑰匙是座標圖上的中心點，以(a,b)表示，(a,b)=($\frac{t-1}{2}$，$\frac{t-1}{2}$)而 a、b 不一定為整數。如【圖 10】  【圖 10】	
加密解密	加密	解密
	(x',y') = (2a-x,2b-y)	(x',y') = (2a-x,2b-y)

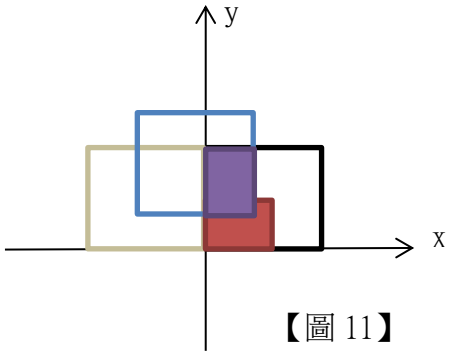
(ⅱ)不完全點射法

不完全點射法		
想法	概念與二維度不完全鏡射法相同，不過只有某部分讓它鏡射過去，保留某個部分不做鏡射，而作法仍可使用中點座標公式。	
鑰匙討論	鑰匙以 K_4 =(a,b)表示。 範圍：a= $\frac{N}{2}$, $N \in \{1,2,3,4,\cdots,2(t-2)+1\}$，b= $\frac{N}{2}$, $N \in \{1,2,3,4,\cdots,2(t-2)+1\}$	
加密解密	加密	解密
	$(x,y) \longrightarrow (x', y')$ if $\begin{cases} 2a-x \in \{0,1,2,\cdots(t-1)\} \\ 2b-y \in \{0,1,2,\cdots(t-1)\} \end{cases}$ 即為 $\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix}$ $= \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} 2a \\ 2b \end{bmatrix}$ if $\begin{cases} x' \in \{0,1,2,\cdots(t-1)\} \\ y' \in \{0,1,2,\cdots(t-1)\} \end{cases}$	$(x,y) \longrightarrow (x', y')$ if $\begin{cases} 2a-x \in \{0,1,2,\cdots(t-1)\} \\ 2b-y \in \{0,1,2,\cdots(t-1)\} \end{cases}$ 即為 $\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix}$ $= \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} 2a \\ 2b \end{bmatrix}$ if $\begin{cases} x' \in \{0,1,2,\cdots(t-1)\} \\ y' \in \{0,1,2,\cdots(t-1)\} \end{cases}$

【發　現】不完全點射法是旋轉矩陣$\begin{bmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{bmatrix}$中$\theta = 180°$，再平移的加密方式。

【新發想】

二維度不完全點射法是旋轉矩陣旋轉180°後再平移的加密方式，
我們由此想試試利用旋轉矩陣旋轉90°與旋轉270°再平移的加密方式是否可行。【圖 11】以旋轉90°做說明。



【圖 11】

【新發現】紫色長方形加密後因超出範圍，因此保持原來的位置。紅色長方形透過旋轉、平移後的位置會和紫色長方形相同，出現了多對一的加密結果。

【結果】利用旋轉矩陣旋轉90°或旋轉270°後再平移會產生明文與密文多對一的狀況，無法進行解密，故此加密方式不成立。

【心得】雖然利用旋轉矩陣旋轉90°與旋轉270°再平移的加密方式不存在，讓我們心中有著淡淡的失落感，但我們依然認為矩陣是一個很好的加密工具

【二維度不完全點射法舉例】

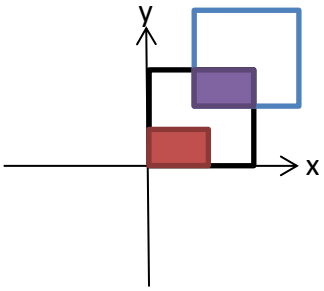
舉例	加密〔P=18 0 5 4→[18　0][5　4]〕	解密〔C=18 0 11 22→[18　0][11　22]〕
(t=26) (a,b) =(8,13)	$\begin{bmatrix} x' \\ y' \end{bmatrix}$ $= \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 18 \\ 0 \end{bmatrix} + \begin{bmatrix} 2\times 8 \\ 2\times 13 \end{bmatrix}$ $= \begin{bmatrix} -2 \\ 26 \end{bmatrix} \Rightarrow$ 維持 $\begin{bmatrix} 18 \\ 0 \end{bmatrix}$ $\begin{bmatrix} x' \\ y' \end{bmatrix}$ $= \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 5 \\ 4 \end{bmatrix} + \begin{bmatrix} 2\times 8 \\ 2\times 13 \end{bmatrix}$ $= \begin{bmatrix} 11 \\ 22 \end{bmatrix}$ $C = \begin{bmatrix} 18 \\ 0 \end{bmatrix}\begin{bmatrix} 11 \\ 22 \end{bmatrix} \rightarrow 18\ 0\ 11\ 22$	$\begin{bmatrix} x' \\ y' \end{bmatrix}$ $= \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 18 \\ 0 \end{bmatrix} + \begin{bmatrix} 2\times 8 \\ 2\times 13 \end{bmatrix}$ $= \begin{bmatrix} -2 \\ 26 \end{bmatrix} \Rightarrow$維持$\begin{bmatrix} 18 \\ 0 \end{bmatrix}$ $\begin{bmatrix} x' \\ y' \end{bmatrix}$ $= \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 11 \\ 22 \end{bmatrix} + \begin{bmatrix} 2\times 8 \\ 2\times 13 \end{bmatrix}$ $= \begin{bmatrix} 5 \\ 4 \end{bmatrix}$ P=$\begin{bmatrix} 18 \\ 0 \end{bmatrix}\begin{bmatrix} 5 \\ 4 \end{bmatrix} \rightarrow 18\ 0\ 5\ 4$

(4)二維度不完全映射法

（ｉ）改良式希爾密碼

我們想將文獻中的希爾密碼結合不完全加密的概念進行一些改良。若明文 P 為一個1×2矩陣，M 為一個溪二密碼中在限制條件下的加密矩陣，則 MP^T(mod t)後，再加上$\begin{bmatrix} s \\ q \end{bmatrix}$進行位移，即 C=M$P^T$(mod t)+ $\begin{bmatrix} s \\ q \end{bmatrix}$，若加密後超出編碼範圍變保持原狀不加密，若還在編碼範圍內便以運算結果為密文。

【以圖示說明】



說明:
明文經由希爾密碼加密後再平移到藍色正方形的位置。紫色長方形因加密後超出範圍而保持未加密前的原位，而紅色長方形(已經希爾密碼加密)再經平移加密後的位置會與紫色長方形相同，出現多對一的現象。

【以實例說明】$t = 26 \quad M = \begin{bmatrix} 1 & 2 \\ 7 & 11 \end{bmatrix}, \begin{bmatrix} s \\ q \end{bmatrix} = \begin{bmatrix} 16 \\ 16 \end{bmatrix}, \begin{bmatrix} x_1 \\ y_1 \end{bmatrix} = \begin{bmatrix} 20 \\ 7 \end{bmatrix} \begin{bmatrix} x_2 \\ y_2 \end{bmatrix} = \begin{bmatrix} 24 \\ 25 \end{bmatrix}$

$$\begin{bmatrix} x_1' \\ y_1' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 7 & 11 \end{bmatrix} \begin{bmatrix} 20 \\ 7 \end{bmatrix} (mod\ 26) + \begin{bmatrix} 16 \\ 16 \end{bmatrix} = \begin{bmatrix} 24 \\ 25 \end{bmatrix}$$

$$\begin{bmatrix} x_2' \\ y_2' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 7 & 11 \end{bmatrix} \begin{bmatrix} 24 \\ 25 \end{bmatrix} (mod\ 26) + \begin{bmatrix} 16 \\ 16 \end{bmatrix} = \begin{bmatrix} 38 \\ 17 \end{bmatrix} \Rightarrow 保持 \begin{bmatrix} 24 \\ 25 \end{bmatrix}$$

【發現】透過以上的例子，我們法發現利用改良式希爾密碼加密明文與密文會出現多對一的情況。此加密方式不可逆，故無法成為加密的工具。

【心得】雖然改良式希爾密碼無法成為加密工具，使我們有那麼一點的失落，但也因這個加密方式行不通，我們又產生了另一種不完全加密的想法。

(ii)二維度不完全映射法

由於改良式希爾密碼不成立，因此我們改變想法，透過將矩陣切割的方式，再結合希爾密碼，發展出不完全映射的加密方式。

<table>
<tr><td colspan="3">二維度不完全映射法</td></tr>
<tr><td>想法</td><td colspan="2">以前面文獻中的希爾密碼為基底，再選定一個鑰匙$\{K_i\}$，以 mod 2 的方式決定鏡射與否，結果為 0 的不做映射，結果為 1 的則做映射，即將加密的矩陣做切割，一部分映射，一部分透過單位矩陣，保留原狀，不進行映射，以符合不完全加密的概念。</td></tr>
<tr><td>鑰匙討論</td><td colspan="2">一個2×2的加密用矩陣 M(加密中的 M 須符合希爾密法中的限制條件)。
一個決定是否加密用的$\{K_i\}$:數列或無理數小數點後的數字第 i 位。</td></tr>
<tr><td rowspan="2">加密
解密</td><td>加密</td><td>解密</td></tr>
<tr><td>將明文以 2 為單位分組，無法湊成時加入 x 補滿，令每組1×2矩陣為v_i，共分為 l 組。其C_i為對應密文 。
$\begin{cases} {C_i}^T = M \times {v_i}^T \ (mod\ t)\ \ if\ K_i \equiv 1(mod\ 2) \\ {C_i}^T = {v_i}^T\ \ if\ K_i \equiv 0(mod\ 2) \end{cases}$
⇓
$[C_1 \quad C_2 \quad \cdots \quad C_l]^T$
$= \begin{bmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & A_l \end{bmatrix} [v_1 \quad v_2 \quad \cdots \quad v_l]^T (\text{mod t})$
其中$A_i = \begin{cases} M\ if\ \ K_i \equiv 1(mod\ 2) \\ I_{2\times 2}\ \ if\ \ K_i \equiv 0(mod\ 2) \end{cases}$</td><td>將密文以 2 為單位分組，令每組1×2矩陣為w_i，共分為 l 組。其P_i為對應明文 。
$\begin{cases} {P_i}^T = M^{-1} \times {w_i}^T (mod\ t)\ if\ K_i \equiv 1(mod\ 2) \\ {P_i}^T = {w_i}^T\ if\ K_i \equiv 0(mod\ 2) \end{cases}$
⇓
$[P_1 \quad P_2 \quad \cdots \quad P_l]^T$
$= \begin{bmatrix} {A_1}^{-1} & 0 & \cdots & 0 \\ 0 & {A_2}^{-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & {A_l}^{-1} \end{bmatrix} [w_1 \quad w_2 \quad \cdots \quad w_l]^T (\text{mod t})$
其中${A_i}^{-1} = \begin{cases} M^{-1}\ if\ \ K_i \equiv 1(mod\ 2) \\ I_{2\times 2}\ \ if\ \ K_i \equiv 0(mod\ 2) \end{cases}$
最後刪掉無意義的 x</td></tr>
<tr><td>延伸</td><td colspan="2">可選定 r 把鑰匙，運用類似改良式維氏密碼中用無理數為鑰匙的方法加密，相信在複雜度上會有一大提升，但速度的部分需要使用者自己斟酌。</td></tr>
</table>

【心得】分割矩陣的想法，可視為另類的不完全加密法，亦分割矩陣可使用在先前的各類不完全加密法中。

【二維度不完全映射舉例】

鑰匙決定	n=2，$\{K_i\} = \pi = 3.14159 \ldots.$，$M = \begin{bmatrix} 1 & 2 \\ 7 & 11 \end{bmatrix}$ 取 1(mod 2)≡1，4(mod 2)≡0 $\Rightarrow K_1 = 1$，$K_2 = 0$
加密	明文:18 0 5 4$\Longrightarrow {v_1}^T = \begin{bmatrix} 18 \\ 0 \end{bmatrix}$，${v_2}^T = \begin{bmatrix} 5 \\ 4 \end{bmatrix}$ $K_1 = 1$，故 $\begin{bmatrix} 1 & 2 \\ 7 & 11 \end{bmatrix}\begin{bmatrix} 18 \\ 0 \end{bmatrix}(mod\ 26) = \begin{bmatrix} 18 \\ 22 \end{bmatrix}$ $K_2 = 0$，故$\begin{bmatrix} 5 \\ 4 \end{bmatrix}$不加密 密文:$\begin{bmatrix} 18 \\ 22 \end{bmatrix}\begin{bmatrix} 5 \\ 4 \end{bmatrix} \rightarrow 18\ 0\ 5\ 4$
解密	密文:$18\ 22\ 5\ 4 \Rightarrow {w_1}^T = \begin{bmatrix} 18 \\ 22 \end{bmatrix}$，${w_2}^T = \begin{bmatrix} 5 \\ 4 \end{bmatrix}$，$M^{-1} = \begin{bmatrix} 5 & 18 \\ 11 & 17 \end{bmatrix}$ $K_1 = 1$，故 $\begin{bmatrix} 5 & 18 \\ 11 & 17 \end{bmatrix}\begin{bmatrix} 18 \\ 22 \end{bmatrix}(mod\ 26) = \begin{bmatrix} 18 \\ 0 \end{bmatrix}$ $K_2 = 0$，故$\begin{bmatrix} 5 \\ 4 \end{bmatrix}$不解密 明文:$\begin{bmatrix} 18 \\ 0 \end{bmatrix}\begin{bmatrix} 5 \\ 4 \end{bmatrix} \rightarrow 18\ 0\ 5\ 4$

(iii)二維度改良式不完全映射法

我們想將不完全映射法與改良式凱撒密碼的一些想法進行結合，在家密過程中，既加上平移的概念，同時也能克服改良式希爾密碼不

改良式不完全映射法	
想法	加密時將明文乘上加密矩陣 M，進行平移後再 mod t，使密文全都在編碼範圍內。再以選定一個鑰匙$\{K_i\}$，用 mod 2 的方式決定鏡射與否，結果為 0 的不做映射，結果為 1 的則做映射。
鑰匙討論	M:一個2×2的加密用矩陣(加密中的 M 須符合希爾密法中的限制條件)。 $\{K_i\}$一個決定是否加密用的數列或無理數小數點後的第 i 位數字。 $N = \begin{bmatrix} S \\ q \end{bmatrix}$:是一個$2 \times 1$的平移矩陣。

加密解密	加密	將明文以 2 為單位分組，無法湊成時加入 x 補滿，令每組1×2矩陣為v_i，共分為 l 組。其C_i為對應密文 。 $\begin{cases} {C_i}^T = (M \times {v_i}^T + N)(mod\ t)\ \ if\ K_i \equiv 1(mod\ 2) \\ {C_i}^T = {v_i}^T\ \ if\ K_i \equiv 0(mod\ 2) \end{cases}$ $\Downarrow$ $[C_1 \quad C_2 \quad \cdots \quad C_l]^T$ $= \left(\begin{bmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & A_l \end{bmatrix} [v_1 \quad v_2 \quad \cdots \quad v_l]^T + \begin{bmatrix} B_1 \\ B_2 \\ \vdots \\ B_l \end{bmatrix} \right) (mod\ t)$ $A_i = \begin{cases} M\ if\ \ K_i \equiv 1(mod\ 2) \\ I_{2\times 2}\ \ if\ \ K_i \equiv 0(mod\ 2) \end{cases}$ ， $B_i = \begin{cases} N\ if\ \ K_i \equiv 1(mod\ 2) \\ \begin{bmatrix} 0 \\ 0 \end{bmatrix}\ if\ \ K_i \equiv 0(mod\ 2) \end{cases}$
	解密	將密文以 2 為單位分組，令每組1×2矩陣為w_i，共分為 l 組。其P_i為對應明文。 $\begin{cases} {P_i}^T = \left(M^{-1}({w_i}^T - N)\right)(mod\ t)\ \ if\ K_i \equiv 1(mod\ 2) \\ {P_i}^T = {w_i}^T\ if\ K_i \equiv 0(mod\ 2) \end{cases}$ $\Downarrow$ $[P_1 \quad P_2 \quad \cdots \quad P_l]^T$ $= \left(\begin{bmatrix} {A_1}^{-1} & 0 & \cdots & 0 \\ 0 & {A_2}^{-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & {A_l}^{-1} \end{bmatrix} \left([w_1 \quad w_2 \quad \cdots \quad w_l]^T - \begin{bmatrix} B_1 \\ B_2 \\ \vdots \\ B_l \end{bmatrix} \right) \right) (mod\ t)$ 其中${A_i}^{-1} = \begin{cases} M^{-1}\ if\ \ K_i \equiv 1(mod\ 2) \\ I_{2\times 2}\ \ if\ \ K_i \equiv 0(mod\ 2) \end{cases}$ ，$B_i = \begin{cases} N\ if\ \ K_i \equiv 1(mod\ 2) \\ \begin{bmatrix} 0 \\ 0 \end{bmatrix}\ if\ \ K_i \equiv 0(mod\ 2) \end{cases}$

可逆的問題，故發展出二維度改良式不完全映射法。

【發現】

①二維度改良式不完全映射的加密方式與一維度改良式凱撒密碼 C=mP+s (mod t)相似，都是先做乘法的動作再進行推移，差別只在於是否結合不完全加密的概念，故二維度改良式不完全映射法可以視為一維度改良式凱撒密碼，再結合不完全概念所發展出的加密法。

②二維度不完全映射法是改良式不完全映射法的特例($\begin{bmatrix} S \\ q \end{bmatrix}=\begin{bmatrix} 0 \\ 0 \end{bmatrix}$)，能直接被改良式不完全映射取代。如右圖:

【二維度改良式不完全映射舉例】

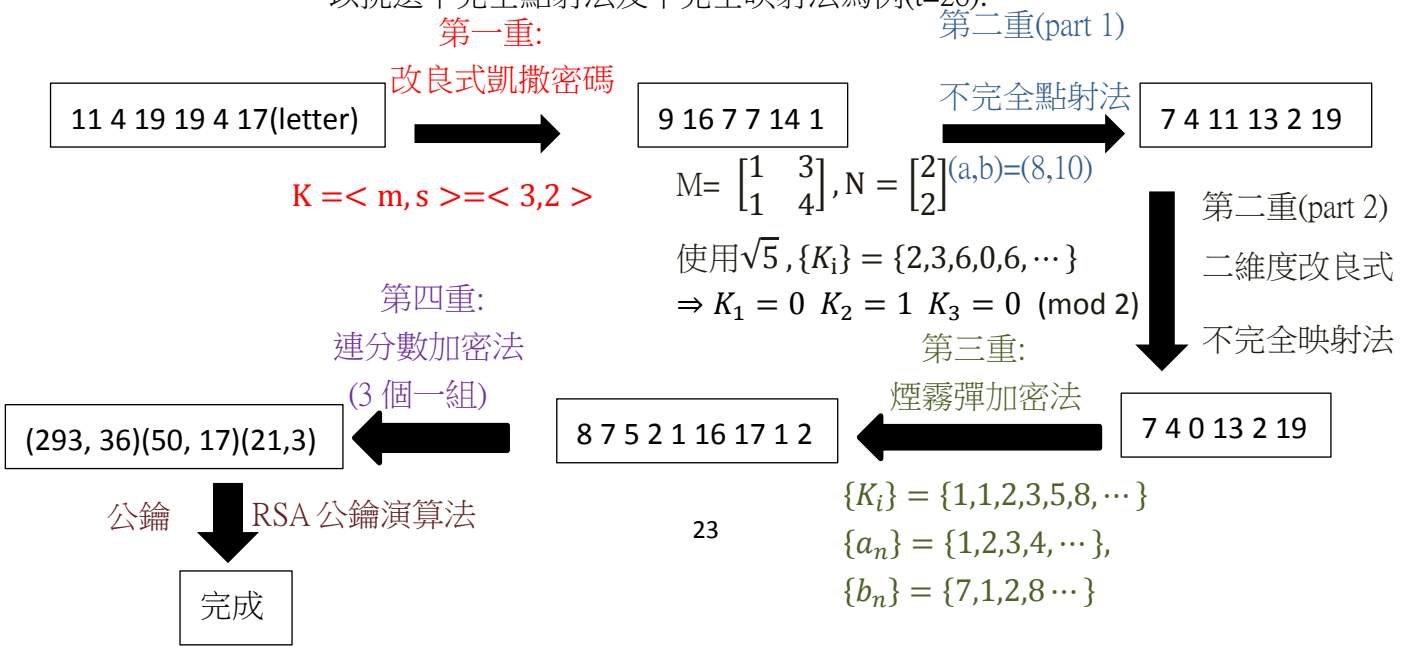
鑰匙決定	t=26 , n=2，$\{K_i\} = \pi = 3.14159 \ldots$，$M = \begin{bmatrix} 1 & 2 \\ 7 & 11 \end{bmatrix}$，$N = \begin{bmatrix} 2 \\ 2 \end{bmatrix}$ 取 1(mod 2)≡1，4(mod 2)≡0 $\Rightarrow K_1 = 1$，$K_2 = 0$
加密	明文:18 0 5 4$\Longrightarrow {v_1}^T = \begin{bmatrix} 18 \\ 0 \end{bmatrix}$, ${v_2}^T = \begin{bmatrix} 5 \\ 4 \end{bmatrix}$ $K_1 = 1$，故 $\left(\begin{bmatrix} 1 & 2 \\ 7 & 11 \end{bmatrix}\begin{bmatrix} 18 \\ 0 \end{bmatrix} + \begin{bmatrix} 2 \\ 2 \end{bmatrix}\right)(mod\ 26) = \begin{bmatrix} 20 \\ 24 \end{bmatrix}$ $K_2 = 0$，故$\begin{bmatrix} 5 \\ 4 \end{bmatrix}$不加密 密文:$\begin{bmatrix} 20 \\ 24 \end{bmatrix}\begin{bmatrix} 5 \\ 4 \end{bmatrix} \rightarrow 20\ \ 24\ \ 5\ \ 4$
解密	密文:20 24 5 4 $\Rightarrow {w_1}^T = \begin{bmatrix} 18 \\ 22 \end{bmatrix}, {w_2}^T = \begin{bmatrix} 5 \\ 4 \end{bmatrix}$，$M^{-1} = \begin{bmatrix} 5 & 18 \\ 11 & 17 \end{bmatrix}$ $K_1 = 1$，故 $\left(\begin{bmatrix} 5 & 18 \\ 11 & 17 \end{bmatrix}\left(\begin{bmatrix} 20 \\ 24 \end{bmatrix} - \begin{bmatrix} 2 \\ 2 \end{bmatrix}\right)\right)(mod\ 26) = \begin{bmatrix} 18 \\ 0 \end{bmatrix}$ $K_2 = 0$，故$\begin{bmatrix} 5 \\ 4 \end{bmatrix}$不解密 明文:$\begin{bmatrix} 18 \\ 0 \end{bmatrix}\begin{bmatrix} 5 \\ 4 \end{bmatrix} \rightarrow 18\ \ 0\ \ 5\ \ 4$

(5)二維度不完全加密法的選擇

可彈性挑選二維度不完全中的加密方式(不只使用一種二維度不完全加密法)應用於第二重加密。

2.二維度五重加密法實例說明

以挑選不完全點射法及不完全映射法為例(t=26):



3.三維度不完全加密、N 維度不完全加密之想法與使用

(1)高維度不完全點法

想法	我們想將二維度不完全點射法的想法與加密方式延伸至高維度空間，而我們發現高維度點射法不會受限於不同的維度空間，故是個不錯的加密方式。
使用	使用方式與二維度不完全點設法相似，在此便不多說明。

(2)高維度改良式不完全映射法

想法	基於我們認為矩陣是一種很好的加密工具，因此我們想將二維度改良式不完全映射法延伸至三維度及 N 維度空間。
使用	加密方式與二維度改良式不完全映射法相同，只需使要使用矩陣 M 的階數等於空間的為度數(N=n)。其缺點為皆數越高，運算數度越慢。

(3)高維度投影法

想法	我們想用投影的方式使高維度的空間能進行只能在二維度或三維度空間中進行的加密方式(二維度不完全鏡射法)。
使用	將空間投影到二維平面，或將 N 維度空間投影到三維空間。

【舉例】

我們以四維度空間(x,y,z,q)為例所產生的幾個鑰匙：

投影至二維平面:

K=(1,1,0,0):投影到 x-y ，K=(1,0,1,0):投影到 x-z 平面

K=(1,0,0,1):投影到 x-q 平面　　其他以此類推。

投影至三維空間:

我們以四維度空間(x,y,z,q)為例所產生的幾個鑰匙:

K=(1,1,1,0)投影到 x-y-z 平面 ，K=(0,1,1,1)投影到 y-z-q 平面

K=(1,0,1,1)投影到 x-z-q 平面　　其他以此類推。

4.高維度不完全面射法

(1)三維度不完全鏡射法

想法	我們想將二維度不完全鏡射法的想法直接延伸到三維度空間， 而二維度空間的線性方程式到了三維度空間中便會變成平面，因此產生了三維度不完全面射法。
使用	用平面方程式 M：ax+by+cz+d=0 進行加密，鑰匙:K=d

(2)高維度不完全面射法

想法	將高維度空間投影至三維度空間，在進行加密。
使用	以投影加密法的方式加密。

柒、研究結果

一、新發展的加密方式

(一)一維度的新加密法

1.一維度不完鏡射法

運用了課程中所學的對稱軸與線對稱圖形的概念。

一維度不完鏡射法優缺點分析表		
優點	速度快	因加密函數簡單，所以運算速度快。
	省空間	因運算速度快，所以不需耗費太大的電腦空間。
缺點	加密前後差別小	不完全鏡射法只是部分做明文位置的互換，若鑰匙選定不佳則有可能只有小部分鏡射，加密前後無多大差別。

2.煙霧彈式加密

煙霧彈式加密分成兩部分，分別為改良式維吉尼亞密碼及干擾加密法。

改良式維吉尼亞密碼是利用課堂上所學到的數列與無理數的概念改良原本維吉尼亞密碼鑰匙不斷重複，以致容易被算出的缺陷，並保留給人非一對一可逆函數的錯覺。

干擾式加密法的想法是從維吉尼亞密碼使人產生錯覺產生，並結所學的數列與無理數的概念所產生的新加密方式。

煙霧彈式加密優缺點分析表			
改良式維氏密碼	優點	避開普通頻率解析法	給人一種「一對多函數」的錯覺，明文與密文的對應關係並不是一對一，因此普通的頻率解析法在此不適用。
	缺點	速度慢	比原本的維是密碼多了一些步驟，也多花了一些時間運算。
干擾加密法	優點	抵擋頻率解析法	所插入的干擾數字會影響頻率分析的結果，進而無法準確又快速地解密。
	缺點	稍顯薄弱	用此加密方式加密的密文還是太「透明」。
		佔電腦空間	插入明文中的干擾數字會佔掉電腦的空間。

(二)二維度的新加密法(一維度不完全鏡射之概念延伸)

將不完全加密的想法，除了原本判斷平移後是否在編碼範圍內以外，也延伸了透過分割矩陣的作法，以達到不完全加密的效果。並結合了線對稱、點對稱以及矩陣的概念，在二維度平面上再發展出一些新的不完全加密方式。二維度不完全加密的優缺點與一維度不完全加密類似，但複雜性較一維度的不完全鏡射法高。

1.二維度分別鏡射法

將一維度不完全鏡射法的加密方式直接用於二維上，將 x 座標與 y 座標分開做鏡射。

2.二維度不完全鏡射法

運用平面中線對稱圖形的概念進行加密與解密，其加密方式如下:

軸 1 $x+y+K_2=0$:$\begin{bmatrix}x\\y\end{bmatrix} \rightarrow \begin{bmatrix}x'\\y'\end{bmatrix} = \begin{bmatrix}0 & -1\\-1 & 0\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix} + \begin{bmatrix}-K_2\\-K_2\end{bmatrix}$

if $x' \in \{0,1,2,\cdots,t-1\}$

and $y' \in \{0,1,2,\cdots,t-1\}$

軸 2 $x-y+K_3=0$:$\begin{bmatrix}x\\y\end{bmatrix} \rightarrow \begin{bmatrix}x'\\y'\end{bmatrix} = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix} + \begin{bmatrix}-K_3\\K_3\end{bmatrix}$

if $x' \in \{0,1,2,\cdots,t-1\}$

and $y' \in \{0,1,2,\cdots,t-1\}$ 解密方式詳見第 15 頁

其實，二維度不完全鏡射法的加密情況，就是透過鏡射矩陣

$\begin{bmatrix}cos2\theta & sin2\theta\\sin2\theta & -cos2\theta\end{bmatrix}$中$\theta = 135°$、$\theta = 45°$，再沿指定方向平移的加密方式。

3.二維度不完全點射法

運用中點座標公式與點對稱的概念進行加密與解密。加密方式如下:

$$\begin{bmatrix}x\\y\end{bmatrix}\rightarrow\begin{bmatrix}x'\\y'\end{bmatrix}=\begin{bmatrix}0&-1\\-1&0\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix}+\begin{bmatrix}2a\\2b\end{bmatrix}\text{if}\begin{cases}2\text{a}-\text{x}\ \in\{0,1,2,\cdots(t-1)\}\\2b-y\in\{0,1,2,\cdots(t-1)\}\end{cases}$$

解密方式詳見第 17 頁

換句話說，不完全點射法是旋轉矩陣$\begin{bmatrix}cos\theta&-sin\theta\\sin\theta&cos\theta\end{bmatrix}$中$\theta=180°$，再平移的加密方式。

4.二維度改良式不完全映射法

以希爾密碼的形式結合不完全加密的概念(矩陣分割)與改良式凱撒密碼的想法所發展出的新加密方式。加密方法如下:

M:一個2×2的加密用矩陣(加密中的 M 須符合希爾密法中的限制條件)。

$\{K_i\}$一個決定是否加密用的數列或無理數小數點後的第 i 位數字。

$N=\begin{bmatrix}s\\q\end{bmatrix}$:是一個$2\times1$的平移矩陣。

將明文以 2 為單位分組，無法湊成時加入 x 補滿，令每組1×2矩陣為v_i，共分為 l 組。其C_i為對應密文 。

$$\begin{cases}{C_i}^T=(M\ \times{v_i}^T+N)(mod\ t)\ \ if\ K_i\equiv1(mod\ 2)\\{C_i}^T={v_i}^T\ \ if\ K_i\equiv0(mod\ 2)\end{cases}$$

$$[C_1\quad C_2\quad\cdots\quad C_l]^T=\left(\begin{bmatrix}A_1&0&\cdots&0\\0&A_2&\cdots&0\\\vdots&\vdots&\ddots&0\\0&0&0&A_l\end{bmatrix}[v_1\quad v_2\quad\cdots\quad v_l]^T+\begin{bmatrix}B_1\\B_2\\\vdots\\B_l\end{bmatrix}\right)(mod\ t)$$

$$A_i=\begin{cases}M\ if\ \ K_i\equiv1(mod\ 2)\\I_{2\times2}\ \ if\ \ K_i\equiv0(mod\ 2)\end{cases}\quad B_i=\begin{cases}N\ if\ \ K_i\equiv1(mod\ 2)\\\begin{bmatrix}0\\0\end{bmatrix}\ if\ \ K_i\equiv0(mod\ 2)\end{cases}$$

解密方式詳見 22 頁

二、一維度五重加密法

新發展的一維度加密方式雖然明文與密文的差異性不大，安全性稍顯不足，但在改良式凱撒密碼結合一維度不完全鏡射法的測試下，發現**結合不完全鏡射法能提升改良式凱撒密碼的複雜度**。其測試結果如下:

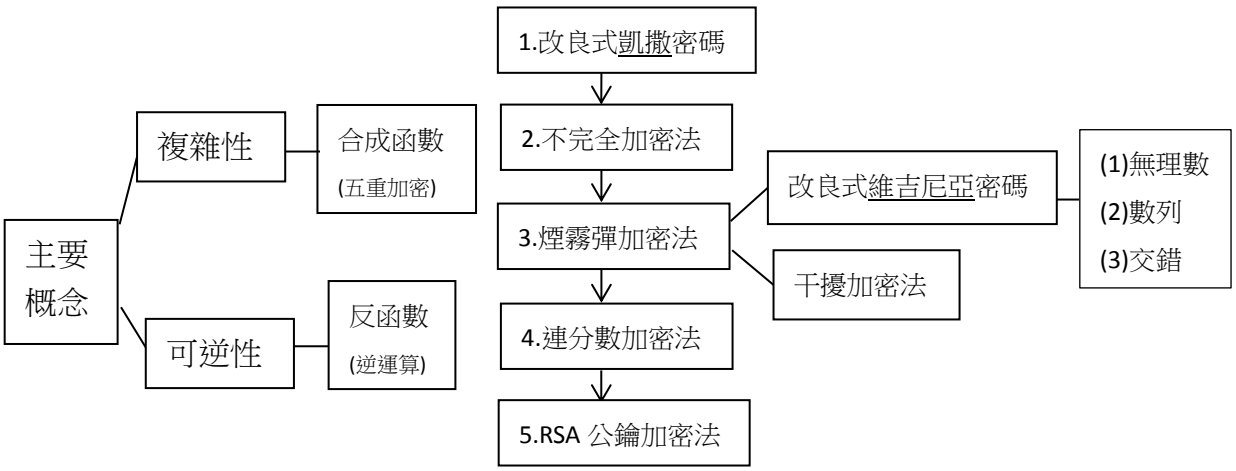
加密法 / 編碼數	改良式凱撒密碼	改良式凱撒密碼＋ 改良式一維度鏡射法
5	20 種組合	60 種組合
6	12 種組合	48 種組合

由此發現，在這兩種加密中，因改良式凱撒密碼 m 與 s 的條件，以及改良式一維度鏡射法(一維度不完全鏡射法)中 K 的條件，當編碼數是一個很大的質數時，m 與 s 的範圍就能很廣，K 因為編碼數很大，所以範圍也很廣。由此可知，**改良式凱撒密碼加上不完全鏡射時，編碼數為質數且愈大，就能愈安全。**

前三重加密方式的結合，雖提高了安全性，但煙霧彈加密法中的干擾加密法增加了字元數量，降低了傳送效率，而第四重的連分數加密法，能縮減字元傳送量，提高傳送效率。

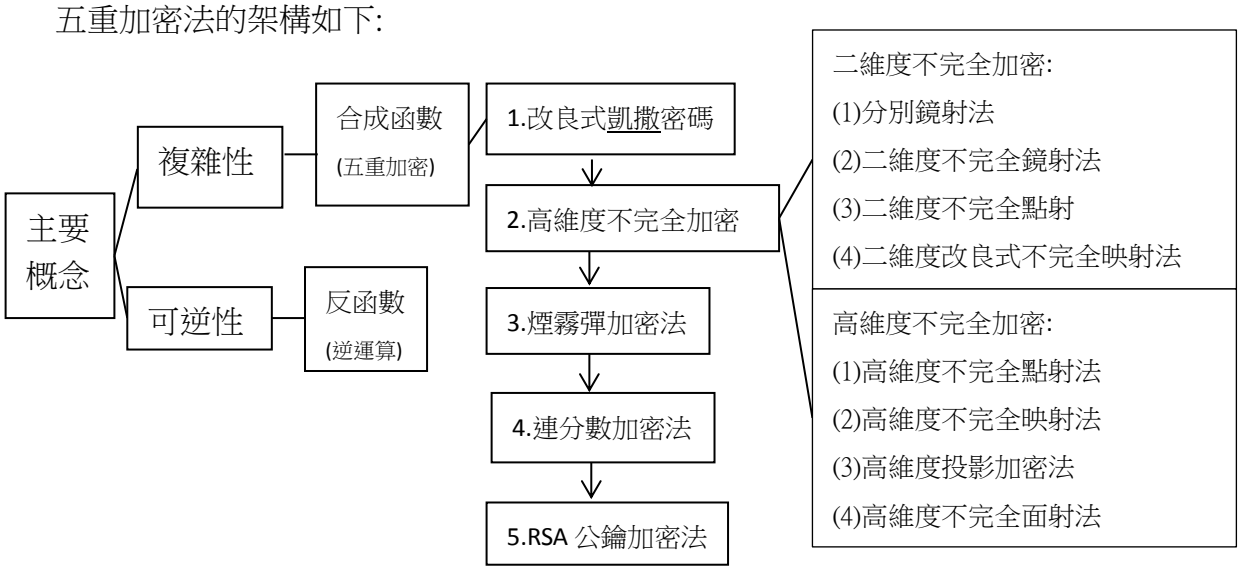
同時，因為前四重的加密方式加密解密的過程需要進行鑰匙的傳遞，因而容易落入鑰匙外流的險境，因此我們在四重加密法後，再結合 RSA 公鑰演算法，以避開鑰匙外流的危險。

簡言之，五重加密法就是以截長補短的方式，保留各種加密法的優點，避開各種加密法的弱點，進而得到安全的密碼。其架構如下:



三、高維度五重加密法

我們將一維度五重加密中一維度不完全鏡射法的想法延伸推廣至二維度平面(發展了二維度分別鏡射法、二維度不完全鏡射法、二維度不完全點射法、二維度改良式不完全映射法)及高維度空間(高維度不完全點射法、高維度不完全映射法、高維度投影加密法、高維度不完全面射法)，其高維度五重加密法的架構如下:



捌、結論與未來展望

在本次的研究中，我們利用合成函數的概念，發展了五重加密法，並透過反函數的概念分別對五重加密法運用其逆運算進行解密，其中，第二、三重加密是我們透過課程內容中異想天開所發展出的加密法:不完全加密法與煙霧彈加密法，這也是本次研究裡最令我感到興奮與成就感的。

在不完全加密法一維鏡射法裡，我們有進行密文組合的測試，發現有些密文組合雖與改良式凱撒密碼的加密結果有重複的現象，但依然增加了密文的組合數，也因此提供了更大的複雜度與安全性，對於重複的現象，在未來時間允許下，我會再繼續深入探討。

在高維度不完全加密的探討中，我們發現不完全鏡射法在二維平面、三維空間與其他高維度空間中是可行的，並從中提出不完全面射法。但因時間有限，所以無法更深入探討在三維度鏡射法的鑰匙選擇及平面方程式 M:ax+by+cz+d=0 中的 a、b、c 限制。也無法繼續思考四維空間等高維度空間的鏡射方式，只能暫時

使用投影加密的方式，將高維度空間投影到二、三維度，再使用不完全鏡射法或不完全面射法。但相信不完全鏡射法在其他高維度空間中依然適用。希冀以後能繼續探討。

這次研究因著時間有限，因而無法進行更多不同加密方式的探討，例如:在空間中直線與對稱點的鏡射關係、在三維度空間以及更高維度空間中的不完全加密、不完全映射中的矩陣變化。在未來求學的日子裡，我會繼續探討不同空間中各式各樣的加密方式和投影方式，使加密方式能呈現更多元的風貌，也會將高中、大學所學的新知識與新的數學工具應用於加密方式中，並學習編寫程式與資訊相關知識，進行實際應用上的測試，使得整個加密邁向更安全，更完備的美麗「鏡」界。

玖、參考文獻

九章出版社編輯群（譯）(1997)。**集的故事**（原作者：Vilenkin, N. Y.）。台北市：九章出版社。

木棉(2006)。**睡夢中，學三角**。台北市：天下遠見出版社。

沈淵源著（2016）。**不可能的任務：公鑰密碼傳奇**。台北市：三民。

吳篤承(2007)。**魔幻金鑰**。中華民國第 47 屆中小學科學展覽會參展作品專輯(編號：080405)。台北市：國立台灣科學教育館。

陳朕疆（譯）(2015)。**數學女孩秘密筆記圓圓的三角函數篇**（原作者：結城浩）。台北市：世茂。

許庭瑋、黃箴理、趙傳真、賴宜璟（2003）。**簡單函數在密碼學之應用－三重加密法**。中華民國第 43 屆中小學科學展覽會參展作品專輯（編號：040415）。台北市：國立台灣科學教育館。

葉偉文（譯）(2001)。**數學小魔女**（原作者：Sarah Flannery with David Flannery）。台北市：天下遠見出版社。(原著出版：2000 年)

【評語】030416

密碼學是十分實用而且有趣的。作者針對如何加密才能讓資訊更為安全給出了想法。利用之前已有的加密技巧，混合多種加密方式來得出一個更難被破譯的加密方法，想法還不錯。只是作者可能沒注意到的是，這些方法可能是在早期早已有人嘗試過的方法。傳統方式與現在發展的最大不同點在於，一旦得知加密方式，破譯並不困難。作者確實給出了一些有趣的想法，但是並沒有脫離早期密碼學的思維,有點可惜。如果能對密碼學較新的發展有更多的認識，可能可以避免重複前人的工作，也應該可以得出更好的結果。本文提出的方法，基本上是一些函數的合成。但是因為每個函數都已經是熟知的,合成後只是將步驟變多,因此在數學上的深度較為不足。此外，對密碼的複雜度以及合成順序是否會受影響可以進行探討。

作品海報

摘要

密碼學分為密碼術與破密學，而本次的研究重點在密碼術的部分。密碼術的研究在於加密的複雜性與解密的可逆性，而一個加密系統的好壞取決於它的安全性。本次研究運用了國中的幾何概念與高中的矩陣發展出新的加密方式。並透過**合成函數**的概念結合五重不同的加密方式，增加其加密的安全性，分別為**改良式凱撒密碼**、**不完全加密法(一維度不完全鏡射法**、**二維度分別不完全鏡射法**、**二維度不完全鏡射法**、**二維度不完全點射法**、**二維度改良式不完全映射法**，**高維度不完全加密法)**、**煙霧彈加密法(改良式維吉尼亞密碼**、**干擾加密法)**、**連分數加密法與RSA公鑰演算法**，以各自加密法的優點截長補短，使這五重加密方式能相互配合，奏出和諧優美的「加密五重奏」。

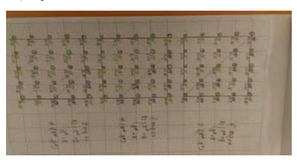
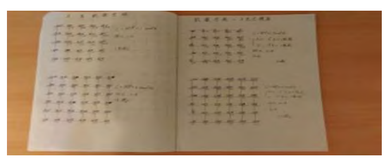
壹、研究動機

有一天，我在家中的書架上找書，找著找著卻無意間發現隱身書架深處，已沾了厚厚一層灰塵的《數學小魔女》。在好奇心的驅使下翻開封面，翻著泛黃的頁面，一不小心就掉進了書中密碼學的綺麗世界。閱讀完這本書後，我便希望能以「密碼學」當主題參加科展，並藉此機會見見課本外的天空。

貳、研究目的

一、課程中所學的內容與工具是否能應用於密碼學中?
二、怎樣的密碼才能以比較複雜，而有安全性的形式呈現?
三、新的加密法要如何在高維度上加以延伸與推廣?

參、研究設備及器材


肆、文獻探討

一、改良式凱撒密碼　二、維吉尼亞密碼　三、連分數加密法　四、RSA公鑰演算法　五、希爾密碼 (C為密碼，P為明文，K為鑰匙)

伍、研究方法與內容

一、一維度加密法

(一)煙霧彈式加密

1.改良式維吉尼亞密碼

想法:維吉尼亞密碼的給人一種「**非一對一可逆函數**」**的錯覺**，相同的明文經由不同的鑰匙，能使相同的字母被加密成不同的字母，於是較改良式凱撒密碼安全，但不斷重複的特性造成了他遭破譯的危險性。因此我們提出應用一些常用**數列**（等差數列、等比數列、費波納契數列）與**無理數**為鑰匙加密的方法。但考慮到目前電腦運算無理數所能求得的位數，所以我們在使用無理數當鑰匙加密時，會使用兩個以上的鑰匙作加密並視情況照一定的規律使用。

鑰匙: 加密、解密時的鑰匙可分為兩種:

(1)$\{K_i\}$:是一組常用的數列或是無理數小點後第2i-1位與第2i位所組的數列，使用時兩兩分組一組對照一個明文。

(2)$\{K_{ni}\}$:第n把鑰匙的K_i。

	加密	解密
數列	$C_i \equiv P_i + K_i (\mathrm{mod\ t})$	$P_i \equiv C_i - K_i (\mathrm{mod\ t})$
無理數	$C_i \equiv P_i + K_i (\mathrm{mod\ t})$	$P_i \equiv C_i - K_i (\mathrm{mod\ t})$
交錯	步驟一，選定r個Key 步驟二，i (mod r)=n(n = 1,2,⋯ r)，使用 Key_n 步驟三， $C_i \equiv P_i + K_{n(\frac{i+r-n}{r})}$ (mod t)	$P_i \equiv C_i - K_{n(\frac{i+r-n}{r})} (mod\ t)$

2.干擾式加密

想法:干擾式加密是在密碼中加上一些**具規律性的干擾**，於是我們希望在已加密文中以數列$\{a_n\}$的方式插入一組干擾的數字即$\{b_n\}$。每間隔a_i，放置一個干擾數b_i，即逐一在第 i + S_i項放置b_i。

鑰匙:不同數列 即代表不同鑰匙。$\{a_n\}$須為正整數列。$\{P_n\}$：明碼。 $\{a_n\}$：鑰匙。 $\{b_n\}$ ：由一組隨意數字組成的干擾數列。

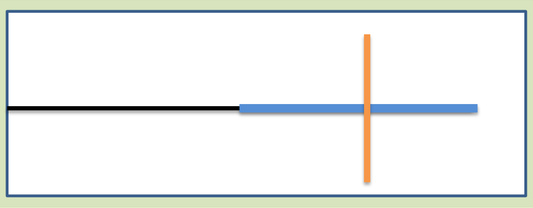
$\{C_n\}$ ：密文。 $S_i = a_1 + a_2 + \cdots + a_i$

加密	解密
$C_j = P_j \ \ if\ j < 1 + S_1, C_j = b_i$ if j = i + $S_i, C_j = P_{j-i}\ if\ j \neq i + S_i, i + S_i < j < (i+1) + S_{i+1}$	逐一刪掉C_{S_i+1}

(二)一維度不完全鏡射法

想法:透過一條軸，使一維的數字做位置上的鏡射，並使鏡射後在範圍內的做鏡射，超出範圍的就保持原狀。

如圖:



說明:
整條線段為鏡射範圍，橘線為對稱軸，以它做鏡射。藍色線為有鏡射部分，較細線段為保持原狀的部分。

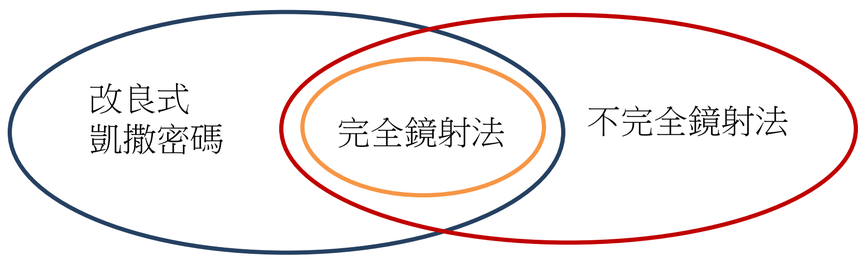
鑰匙:決定K值即決定是否鏡射。$K \in \{1,2,3,4,\cdots,2(t-2)+1\}$ ，若不在K值範圍內，則加密結果將與明碼相同。

加密	解密
$\begin{cases} C = K - P, if\ K - P \in \{0,1,2,\cdots,t-1\} \\ C = P, if\ K - P \notin \{0,1,2,\cdots,t-1\} \end{cases}$	$\begin{cases} P = K - C, if\ K - C \in \{0,1,2,\cdots,t-1\} \\ P = C, if\ K - C \notin \{0,1,2,\cdots,t-1\} \end{cases}$

此外我們也發現**完全鏡射法是不完全鏡射法及改良式凱撒密碼**

$K_e = < m, s > = < (t-1, K) >$，即$\mathbf{C = (t-1)P + K}$的特例，

如右圖:



二、二維度不完全加密

(一)二維度不完全分別鏡射法

想法:我們試著將前面所提的「改良式一維度鏡射法」，透過下列的加密法，放到直角座標圖中。

鑰匙:與一維度不完全鏡射法相同，在此訂為 K_1

加密	解密
$\begin{cases} x' = K_1 - x, if\ \ K_1 - x \in \{0,1,2,\cdots,t-1\} \\ x' = x, if\ K_1 - x \notin \{0,1,2,\cdots,t-1\} \end{cases}$ and $\begin{cases} y' = K_1 - y, if\ \ K_1 - y \in \{0,1,2,\cdots,t-1\} \\ y' = y, if\ K_1 - y \notin \{0,1,2,\cdots,t-1\} \end{cases}$	$\begin{cases} x' = K_1 - x, if K_1 - x \in \{0,1,2,\cdots,t-1\} \\ x' = x, if K_1 - x \notin \{0,1,2,\cdots,t-1\} \end{cases}$ and $\begin{cases} y' = K_1 - y, if K_1 - y \in \{0,1,2,\cdots,t-1\} \\ y' = y, if K_1 - y \notin \{0,1,2,\cdots,t-1\} \end{cases}$

(二)二維度不完全鏡射法

想法:**分別鏡射法出現行列互換的結果**，可視為鏡射的軸是鉛直與水平的那兩條對稱軸，於是針對剩下的兩條45度的對稱軸(x+y+K_2=0、x-y+K_3=0)進行鏡射。如【圖二】。接下來加密的部分就運用高中的對稱公式做計算。若超出了座標圖範圍，就不做鏡射。如【圖三】。

鑰匙:K_2、K_3在此為加密的鑰匙。-2(t-1)＜K_2＜0 且K_2為正整數,K_3：-(t-1)＜K_3＜(t-1)且K_3為正整數。

	加密	解密
軸1: x+y+K_2=0	$\begin{bmatrix} x \\ y \end{bmatrix} \to \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} -K_2 \\ -K_2 \end{bmatrix}$ if $x' \in \{0,1,2,\cdots,t-1\}$ and $y' \in \{0,1,2,\cdots,t-1\}$	$\begin{bmatrix} x \\ y \end{bmatrix} \to \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} -K_2 \\ -K_2 \end{bmatrix}$ if $x' \in \{0,1,2,\cdots,t-1\}$ and $y' \in \{0,1,2,\cdots,t-1\}$
軸2: x-y+K_3=0	$\begin{bmatrix} x \\ y \end{bmatrix} \to \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} -K_3 \\ K_3 \end{bmatrix}$ if $x' \in \{0,1,2,\cdots,t-1\}$ and $y' \in \{0,1,2,\cdots,t-1\}$	$\begin{bmatrix} x \\ y \end{bmatrix} \to \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} -K_3 \\ K_3 \end{bmatrix}$ if $x' \in \{0,1,2,\cdots,t-1\}$ and $y' \in \{0,1,2,\cdots,t-1\}$

【圖二】

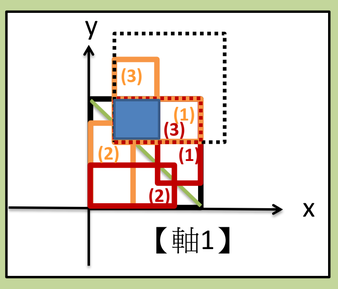
【圖三】

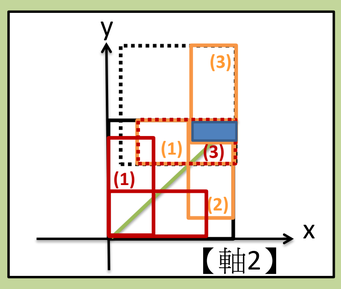
說明:
【圖二】
橘線為垂直與水平的對稱軸，綠線為兩條45度的對稱軸。
【圖三】
兩圖中黑色部分為不鏡射範圍，白色部分為鏡射範圍。
L_3和L_4兩條軸的方程式分別為:L_3: x+y+K_2=0，L_4: x-y+ K_3=0。

此外我們也發現**軸1的加密情況其實是鏡射矩陣** $\begin{bmatrix} cos2\theta & sin2\theta \\ sin2\theta & -cos2\theta \end{bmatrix}$**中**$\theta = 135°$，**再沿 軸 2 方向平移的加密方式；軸2的加密情況其實是鏡射矩陣中** $\theta = 45°$，**再沿軸1方向平移的的加密方式**。由此，我們有了以下兩個的新發想:

1.調整θ，使鏡射矩陣中的sin值與cos值同時維持為整數。
【結果】2θ只能是90°、180°、270°，即須θ = 45°(軸2加密情況)、θ = 90°(類似二維度不完全分別鏡射法中的行列互換)、θ = 135°(軸1加密情況)

2.調整平移方式，以圖示說明:





說明
紅色長方形與橘色長方形經由綠色的對稱軸鏡射後再平移，最後在藍色區塊出現明文與密文多對一的現象。(紅色長方形與橘色長方形的移動方式是沿著數字的順序)。

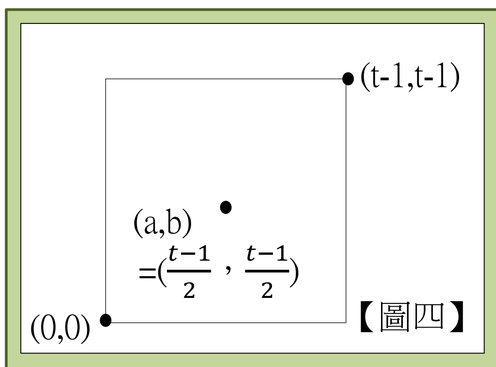
【結果】以軸1加密時平移的方向必須沿著軸2；以軸2加密時平移的方向必須沿著軸1，若任意平移則明文與密文會出現多對一的情形，此加密方式便不可逆，故此加密法不成立，因而無法成為加密的工具。

(三)二維度不完全點射法

想法:在平面上的對稱方式除了線對稱，還有點對稱，於是想用點對稱的方式來進行座標圖上的鏡射。只有某部分讓它鏡射過去，保留某個部分不做鏡射，而作法使用中點座標公式。 以【圖四】做說明:

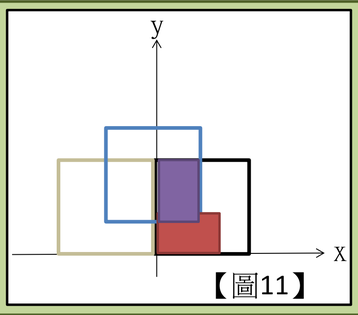
鑰匙:座標圖中的一點，以K_4 =(a,b)表示。a= $\frac{N}{2}, N \in \{1,2,3,4,\cdots,2(t-2)+1\}$，b= $\frac{N}{2}, N \in \{1,2,3,4,\cdots,2(t-2)+1\}$

加密	解密
$\begin{bmatrix}x\\y\end{bmatrix} \to \begin{bmatrix}x'\\y'\end{bmatrix}$ $= \begin{bmatrix}-1 & 0\\0 & -1\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix} + \begin{bmatrix}2a\\2b\end{bmatrix}$ if $\begin{cases}x' \in \{0,1,2,\cdots(t-1)\}\\y' \in \{0,1,2,\cdots(t-1)\}\end{cases}$	$\begin{bmatrix}x\\y\end{bmatrix} \to \begin{bmatrix}x'\\y'\end{bmatrix}$ $= \begin{bmatrix}-1 & 0\\0 & -1\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix} + \begin{bmatrix}2a\\2b\end{bmatrix}$ if $\begin{cases}x' \in \{0,1,2,\cdots(t-1)\}\\y' \in \{0,1,2,\cdots(t-1)\}\end{cases}$



說明:
以(a,b)為中點為例，(0,0)加密後會到(t-1,t-1)的位置， (t-1,t-1)解密後會到(0,0)的位置。

此外，我們也發現不完全點射法是旋轉矩陣$\begin{bmatrix}cos\theta & -sin\theta\\sin\theta & cos\theta\end{bmatrix}$中$\theta = 180°$，再平移的加密方式。由此，我們有了以下的新發想:
二維度不完全點射法是旋轉矩陣旋轉180°後再平移的加密方式，我們由此想試試利用旋轉矩陣旋轉90°與旋轉270°再平移的加密方式是否可行。
下圖以旋轉90°做說明:

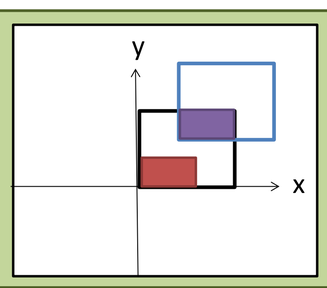


說明:
紫色長方形加密後因超出範圍，因此保持原來的位置。紅色長方形透過旋轉、平移後的位置會和紫色長方形相同，出現了多對一的加密結果。

【結果】利用旋轉矩陣旋轉90°或旋轉270°後再平移會產生明文與密文多對一的狀況，無法進行解密，故此加密方式不成立。

(四)二維度改良式不完全映射法

我們由改良式凱撒密碼得到了以下的新發想:
我們想將文獻中的希爾密碼結合不完全加密的概念進行一些改良。若明文P為一個1×2矩陣，M為一個希爾密碼中在限制條件下的加密矩陣，則MP^T(mod t)後，再加上$\begin{bmatrix}S\\q\end{bmatrix}$進行位移，即C=M$P^T$(mod t)+ $\begin{bmatrix}S\\q\end{bmatrix}$，若加密後超出編碼範圍變保持原狀不加密，若還在編碼範圍內便以運算結果為密文。
以下圖說明:



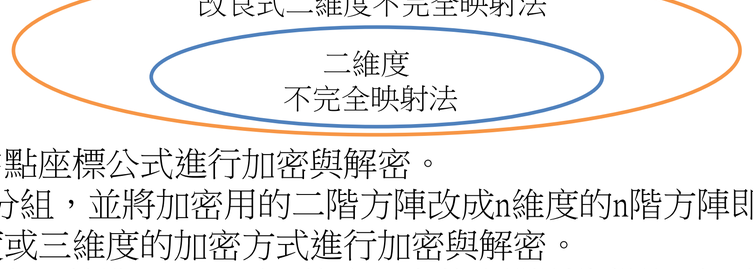
說明:
明文經由希爾密碼加密後再平移到藍色正方形的位置。紫色長方形因加密後超出範圍而保持未加密前的原位，而紅色長方形(已經希爾密碼加密)再經平移加密後的位置會與紫色長方形相同，出現多對一的現象。

【結果】透過以上的例子，我們法發現利用改良式希爾密碼加密明文與密 文會出現多對一的情況。此加密方式不可逆，故無法成為加密的工具。
想法:因為以上的加密方式不成立，所以我們改用矩陣切割的方式，發展出不完全映射法，並將其結合改良式凱撒密碼中的平移想法，發展出改良式不完全映射的加密方式。

鑰匙:M:一個2×2的加密用矩陣(加密中的M須符合希爾密法中的限制條件)。$\{K_i\}$一個決定是否加密用的數列或無理數小數點後的第i位數字。
$N = \begin{bmatrix}S\\q\end{bmatrix}$:是一個$2 \times 1$的平移矩陣。

加密	解密
將明文以2為單位分組，無法湊成時加入x補滿，令每組1×2矩陣為v_i，共分為 l 組。其C_i為對應密文 。 $\begin{cases}C_i{}^T = (M \times v_i{}^T + N)(mod\ t)\ \ if\ K_i \equiv 1(mod\ 2)\\C_i{}^T = v_i{}^T\ \ if\ K_i \equiv 0(mod\ 2)\end{cases} \Rightarrow [C_1\quad C_2\quad \cdots\quad C_l]^T$ $= \left(\begin{bmatrix}A_1 & 0 & \cdots & 0\\0 & A_2 & \cdots & 0\\\vdots & \vdots & \ddots & 0\\0 & 0 & 0 & A_l\end{bmatrix}[v_1\quad v_2\quad \cdots\quad v_l]^T + \begin{bmatrix}B_1\\B_2\\\vdots\\B_l\end{bmatrix}\right)(mod\ t)$ $A_i = \begin{cases}M\ if\ K_i \equiv 1(mod\ 2)\\I_{2\times2}\ \ if\ K_i \equiv 0(mod\ 2)\end{cases}$，$B_i = \begin{cases}N\ if\ K_i \equiv 1(mod\ 2)\\\begin{bmatrix}0\\0\end{bmatrix}\ if\ K_i \equiv 0(mod\ 2)\end{cases}$	將密文以2為單位分組，令每組1×2矩陣為w_i，共分為 l 組。其P_i為對應明文。 $\begin{cases}P_i{}^T = (M^{-1}(w_i{}^T - N))(mod\ t)\ \ if\ K_i \equiv 1(mod\ 2)\\P_i{}^T = w_i{}^T\ if\ K_i \equiv 0(mod\ 2)\end{cases} \Rightarrow [P_1\quad P_2\quad \cdots\quad P_l]^T$ $= \left(\begin{bmatrix}A_1{}^{-1} & 0 & \cdots & 0\\0 & A_2{}^{-1} & \cdots & 0\\\vdots & \vdots & \ddots & 0\\0 & 0 & 0 & A_l{}^{-1}\end{bmatrix}\left([w_1\quad w_2\quad \cdots\quad w_l]^T - \begin{bmatrix}B_1\\B_2\\\vdots\\B_l\end{bmatrix}\right)\right)(mod\ t)$ 其中$A_i{}^{-1} = \begin{cases}M^{-1}\ if\ K_i \equiv 1(mod\ 2)\\I_{2\times2}\ \ if\ K_i \equiv 0(mod\ 2)\end{cases}$，$B_i = \begin{cases}N\ if\ K_i \equiv 1(mod\ 2)\\\begin{bmatrix}0\\0\end{bmatrix}\ if\ K_i \equiv 0(mod\ 2)\end{cases}$ 最後刪掉無意義的x

此外，我們還發現不完全映射法其實就是改良式不完全鏡射法中
$N = \begin{bmatrix}S\\q\end{bmatrix} = \begin{bmatrix}0\\0\end{bmatrix}$的特例，如右圖:



三、高維度不完全加密
(一)高維度不完全點射法:與二維度不完全點設法相同，運用點對稱的想法及中點座標公式進行加密與解密。
(二)高維度改良式不完全映射法:與二維度改良式不完全映射相似，以n為單位分組，並將加密用的二階方陣改成n維度的n階方陣即可。
(三)高維度投影法:將空間投影至二維或三維空間，在對投影後的空間以二維度或三維度的加密方式進行加密與解密。
(四)高維度面射法:三維度空間可直接使用平面方程式M：ax+by+cz+d=0 進行加密，鑰匙:K=d。而三維度以上的空間則先投影至三維空間再加密。

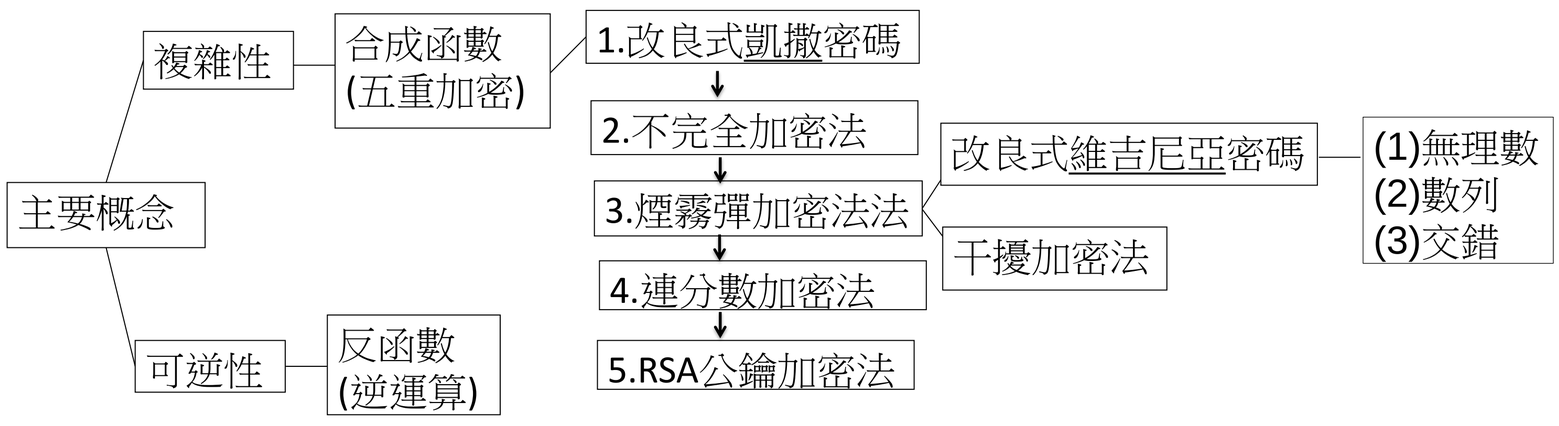
陸、研究結果

一、一維度五重加密

我們有將一維度不完全鏡射法與改良式凱撒密碼進行結合並測其密文組合數，其結果如右:

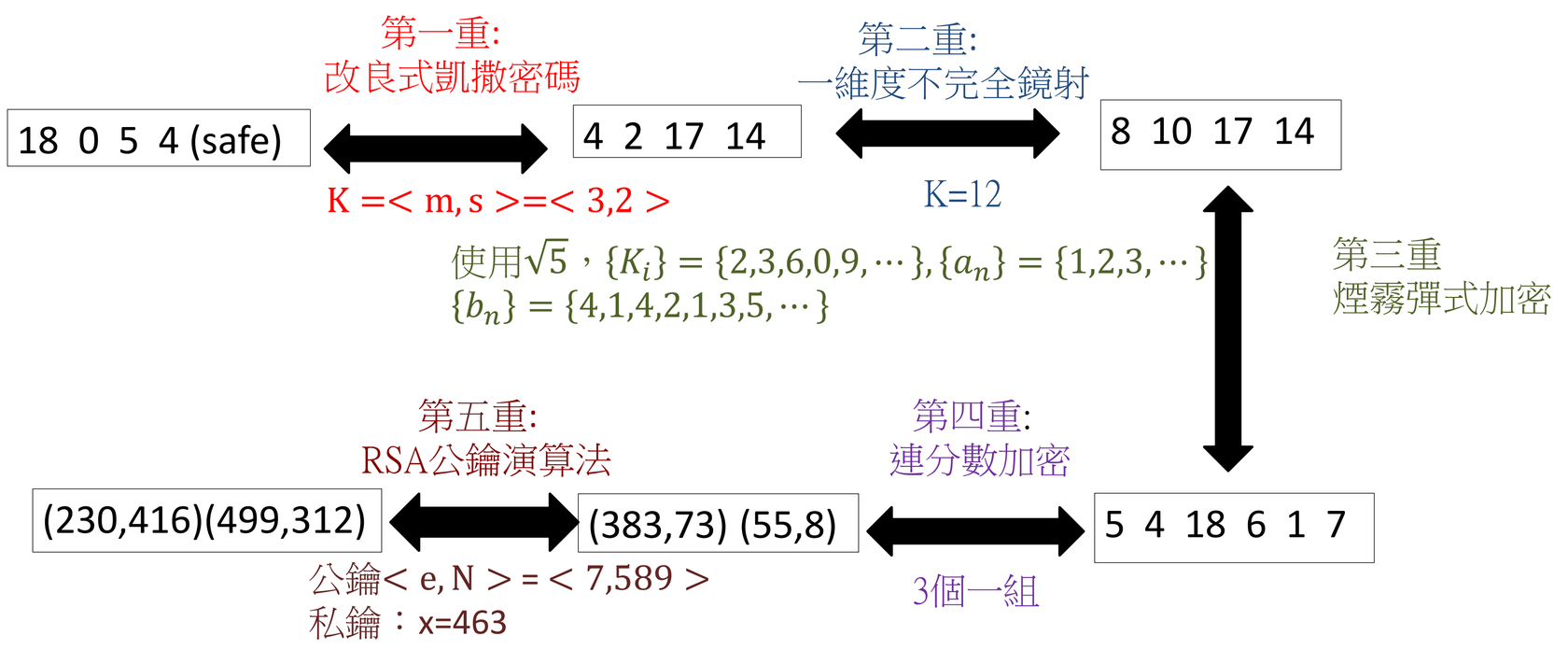
加密法 / 編碼數	改良式凱撒密碼	改良式凱撒密碼＋一維度不完全鏡射法
5	20種組合	60種組合
6	12種組合	48種組合

雖然不完全鏡射法在與測試中已顯出它的優點，但單單使用一維度不完全鏡射法與煙霧彈加密法不夠安全，因此我們結合了一開始的測試中用到的改良式凱撒密碼，並在最後加上連分數加密法與RSA公鑰演算法，形成了一維度五重加密法，其架構如下:



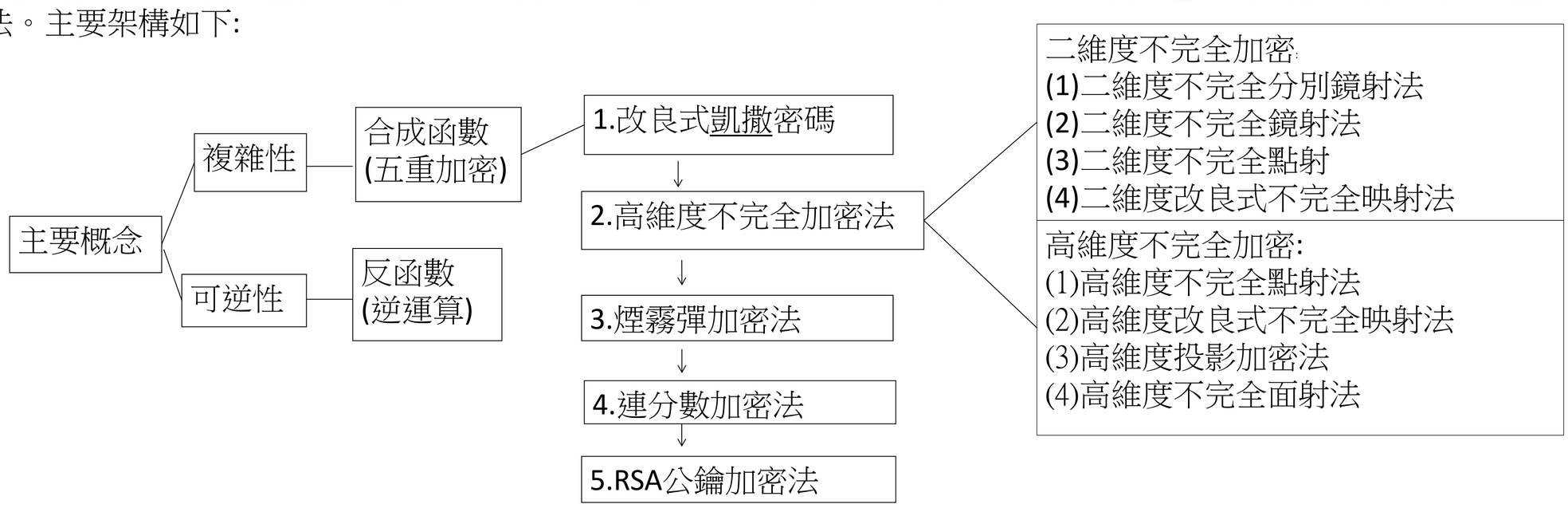
優缺點: **不完全鏡射法**已在測試中顯出優點，但還是**不夠安全**為此加入**煙霧彈式加密**來**避開被頻率解析法破譯的危險**但煙霧彈加密中的**干擾式加密**會**增加字元傳送量，減低傳送速度**，因此結合**連分數加密法**來**縮減傳送字，提高傳送速度**，最後結合**RSA公鑰演算法**來**增加整體安全性**。**五重加密**雖能增加**安全性**，但會降低處理速度，**增加處理時間**。

實例說明:



二、高維度五重加密

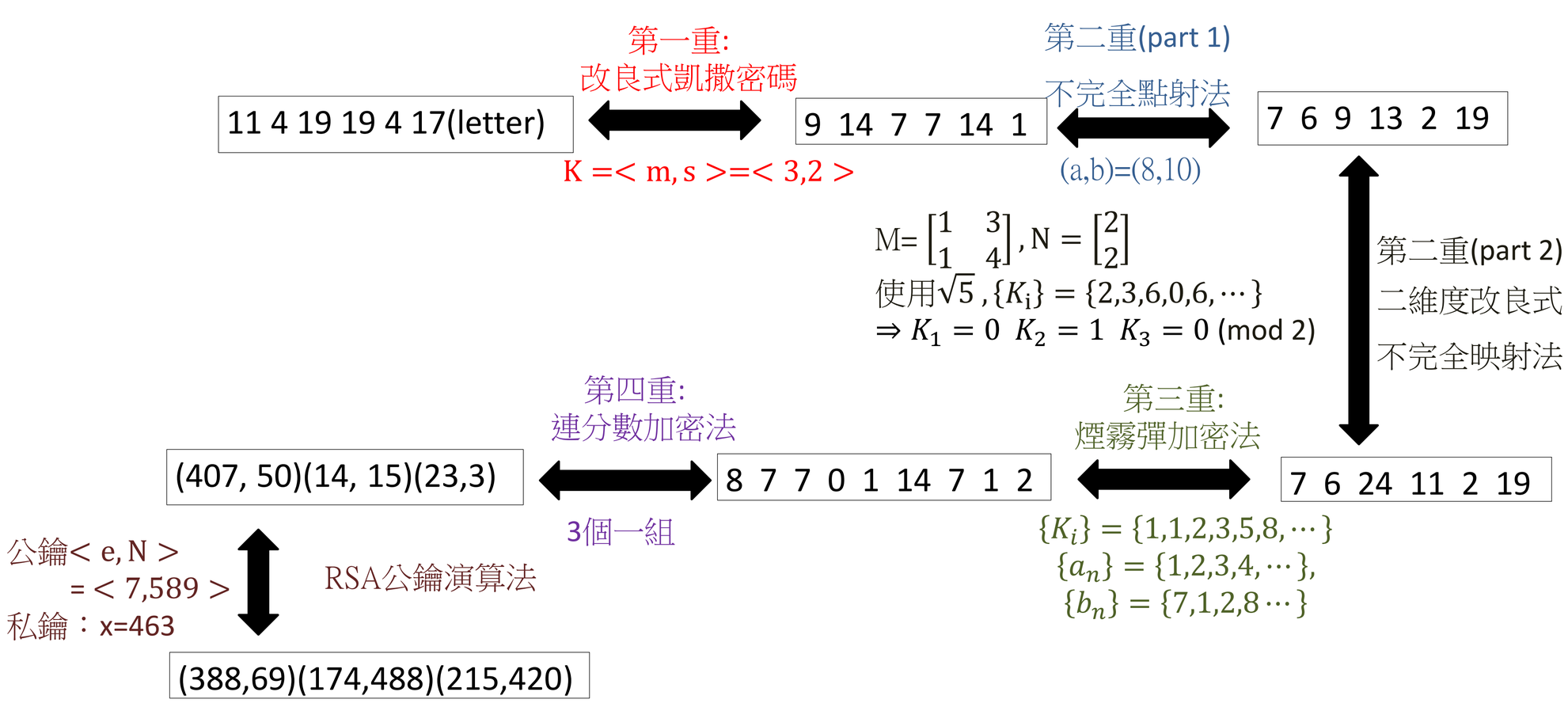
我們想將一維度不完全鏡射法中一部分加密，一部分不加密的方式做延伸，因此對一維度五重加密中的第二重加密進行進一步的探討，並提出它在二維度、三維度和高維度空間中的應用；同時，沿用一維度加密法的概念，形成高維五重加密法。主要架構如下:



使用時機與方法(以二維度為例):

二維度	直接使用。	
一維度	字元數為偶數	兩兩分組後直接使用。
	字元數為奇數	兩兩分組，不夠的補上x(解密時刪掉無意義的x即可)後使用。

實例說明:可彈性挑選二維度不完全中的加密方式(不只使用一種二維度不完全加密法)應用於第二重加密。以挑選不完全點射法及改良式不完全映射法為例(t=26):



柒、未來展望

一、繼續探討空間中不同的鏡射方式與投影方式。
二、將未來新到的數學工具運用於加密方式中，使其更多元豐富。
三、嘗試在安全性與時間成本的平衡間，找到更加合適的加密方式。
四、學習資訊相關知識，將研究進行實際運用。

捌、文獻資料

九章出版社編輯群（譯）（1997）。**集的故事**（原作者：Vilenkin, N. Y.）。台北市：九章出版社。

木棉(2006)。**睡夢中，學三角**。台北市：天下遠見出版社。

沈淵源著（2016）。**不可能的任務：公鑰密碼傳奇**。台北市：三民。

吳篤承（2007）。**魔幻金鑰**。中華民國第47屆中小學科學展覽會參展作品專輯（編號：080405）。台北市：國立台灣科學教育館。

陳朕疆（譯）（2015）。**數學女孩秘密筆記圓圓的三角函數篇**（原作者：結城浩）。台北市：世茂。

許庭瑋、黃箴理、趙傳真、賴宜璟（2003）。**簡單函數在密碼學之應用－三重加密法**。中華民國第43屆中小學科學展覽會參展作品專輯（編號：040415）。台北市：國立台灣科學教育館。

葉偉文（譯）（2001）。**數學小魔女**（原作者：Sarah Flannery with David Flannery）。台北市：天下遠見出版社。（原著出版：2000年）