

中華民國第四十四屆中小學科學展覽會

作品說明書

國中組 生活與應用科學科

030806

臺北市立龍山國民中學

指導老師姓名

洪瑞甫

馮悅麗

作者姓名

王柏崴

中華民國第四十四屆中小學科學展覽會
作品說明書

科別：應用科學

組別：國中組

作品名稱：

終極密碼戰

關鍵詞：密碼學、數學、資訊安全

編號：

目錄

共 14 頁

壹、摘要	P.1
貳、研究動機	P.1
參、研究目的	P.1
肆、研究設備器材	P.1
伍、研究過程與方法	P.1
陸、實驗結果	P.2
柒、討論	P.9
捌、結論	P.10
玖、參考資料及其他	P.10
附錄一 (ASCII 碼表)	P.11
附錄二 (核心程式碼)	P.12
附錄三 (操作介面與執行結果)	P.14

壹、摘要

嘗試研究、整理、並介紹有關密碼學的知識，再破解一套傳統加解密系統，整理出弱點，並且因應舊系統的問題創造出一套新的密碼系統「神奇加密法」、「神奇文藏圖」，寫出程式，並實際應用。

貳、研究動機：

在電腦的世界裡，有很多文字皆要經過加密，來保護自己的資料及著作，像是在帳號密碼的處理方面，大多要經過加密才保險。正常的一段文字經過加密之後，為什麼會變的如此複雜呢？一段文字如何加密才能讓頂尖的破解者無法破解呢？這引起我很大的興趣。

作品與教材相關性說明：

7年級電腦課程：資訊安全與倫理。7年級在上電腦課時，老師常常提醒我們要注重網路安全，資料保密，不要隨意洩漏自己的帳號密碼給陌生人知道，也提及了電腦中的資料常是經過加密的，這引起了研究密碼學的動機。

8年級上學期數學第4章「二元一次方程式」內，提及了「方程式」這個名詞，就像豬肉罐頭製造機一樣，把數字（豬肉）丟進去，就會跑出來另一個數字（豬肉罐頭），這個精神跟密碼學一樣，把文章丟進去轉換器裡，就會跑出相關的密文。

參、研究目的：

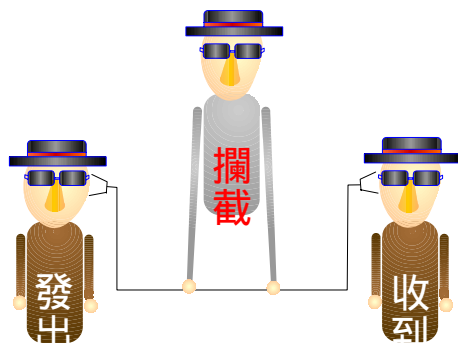
研究密碼的起源演變過程、加解密的方式、密碼的過去以及未來，嘗試破解一套現行的密碼系統，並且針對錯誤，發展出一套新的密碼系統，寫出程式，並實際操作於生活中。

肆、研究設備器材：

電腦 × 1、Visual Basic 軟體 × 1

伍、研究過程與方法：

- 一. 尋找密碼的真正意義。
- 二. 查出密碼演變的歷史。
- 三. 破解一套密碼系統。
- 四. 自創密碼並以電腦程式寫出。

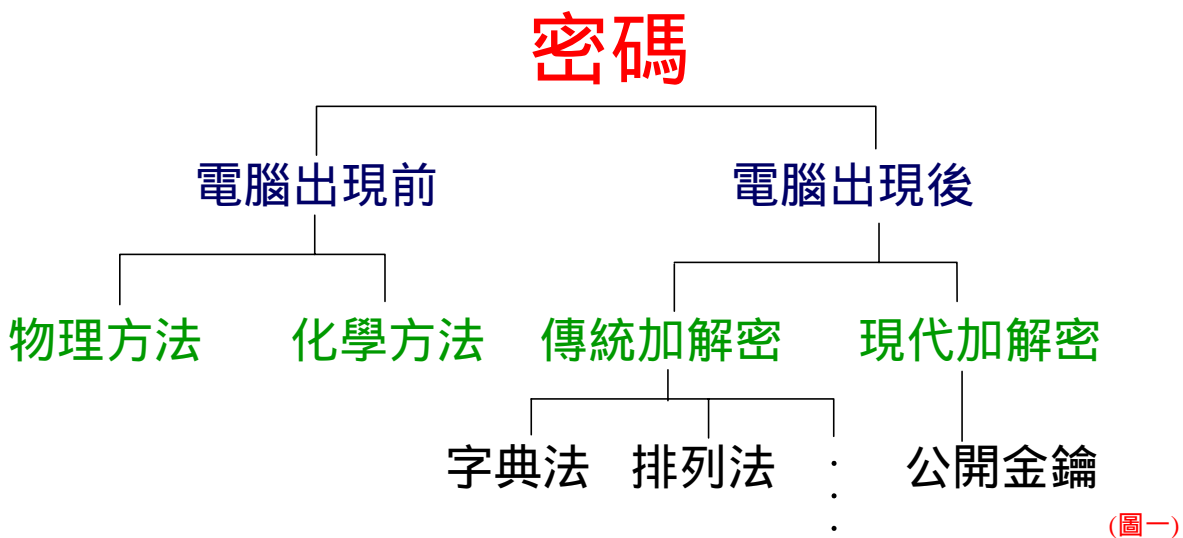


陸、實驗結果：

一、密碼的意義

密碼，顧名思義，是**加密**（註一）過的文字或數字，普遍存在於現代人類的生活中。從許多電影中可以得知，在戰爭時，軍隊常需要聯繫重要情報，為了避免敵軍知道情報內容，往往把文件以自訂方式**加密**，到了接收者手中時，再由密碼兵**解密**（註二）。但是有時候，**密文**會被敵軍攔截或奪走，這時敵軍就會想辦法**解密**，以獲得重要情報。為了減低被敵軍攔截並解密出重要情報的風險，密碼的加解密方式就日益複雜。現在是電腦網路的時代，許多事情都可以直接在網路上解決，像是網路納稅服務等，非常方便。但是像是這種攸關金錢的服務，如果沒有嚴格的保全，將會很容易被有心人士入侵，使民眾的權益受損，這時密碼系統就派上用場啦！另外在如果溝通不方便、距離太遙遠的時候，通常會用簡易密碼的方式傳遞訊息，例如「摩斯密碼」，就是這一種類型的**密文**（註三），它可以由光影的明暗，炊煙的有無來讓人們溝通。

二、密碼的演變歷史



密碼的演變有很多種。基本上，可分為電腦出現前與電腦出現後。

(一) 電腦出現前的加密方法

1. **化學方法**，這類型的密碼是運用化學變化構成的，舉例來說：

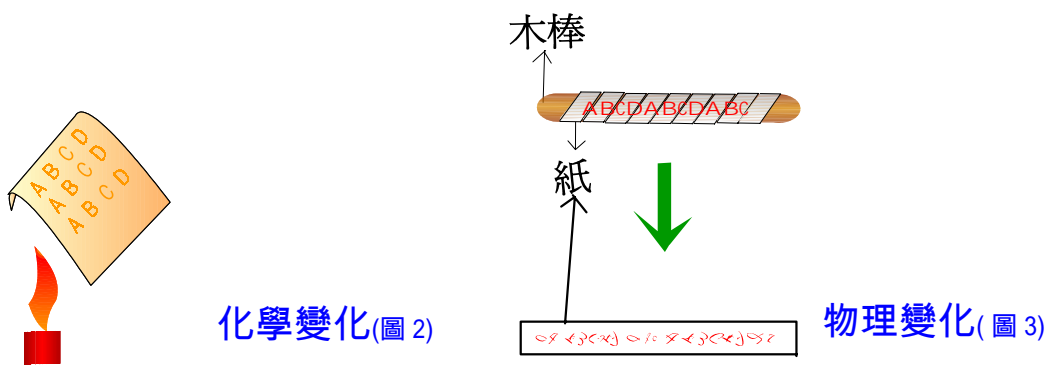
人們會把密文用沾了牛奶的筆寫在紙上，收到這張紙的人會把這張紙用小火烤熱，乳白色的牛奶起化學變化變成了棕色的，這時候收到紙張的人就知道紙張上的內容（圖2）。但是化學性質的變化不多，容易破解，漸漸被物理變化取代。

2. **物理方法**是以簡單的排列、組合、替換等方式來做簡單的加解密，像是將紙張捲在木棒上，並將密文寫在上面，這樣把紙張解下來後，密文便會變的無法辨識了（圖3）。

註一. **加密**：將原始文章轉化成密碼的方式

註二. **密文**：加密過後的文章

註三. **解密**：將密文轉換成原始文章的方式



有了電腦以後，運算速度激增，又演變出了傳統式密碼與公開金鑰。

(二) 電腦出現後的加解密方法

電腦出現後，依加密的鑰匙又可分為現代加密法及傳統加密法。傳統加密法其加解密是同一隻鑰匙，故較容易被破解。現代加密法的加解密是使用不同的一隻鑰匙，即使你知道加密的鑰匙，你也無法從中推得解密的鑰匙。所以現代加密法會比傳統加密法來得安全。詳細介紹如下

1. 傳統式密碼：只要是加密跟解密是採用同一隻鑰匙或你可以從加密的方式推得出解密的鑰匙都算是傳統式密碼。這裡我們以字典法與排列法為例說明。

字典法舉例：在以前戰爭時有種簡單的「凱薩密碼」，它的規則是「A 變 B，B 變 C，C 變 D」(參照表一)，例如「I like math.」寫成「J mjlf nbui.」，不過因為變換方法太簡單了，很容易以『常用度法』(利用字母在文章中的常用度來猜出原文)猜出。字典法可以跟下面所介紹的排列法一齊使用。

原文	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
密文	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

圖表一：凱薩密碼

排列法舉例：利用改變字母的排列形成密文。

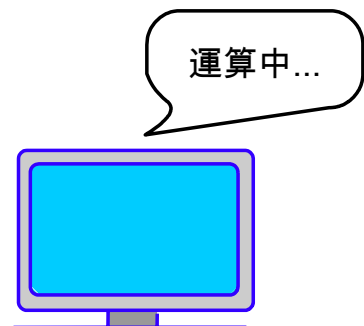
EX：第 1 個與第 2 個字母交換，第 3 個與第 4 個字母交換.....「I like math.」變成「Iilekm ta.h」

2. 現代加密法：又稱公開金鑰法，這是現代最安全的加密方法，發訊人利用收訊人的公開金鑰(註 4)加密，收訊人再使用自己的私密金鑰(註 5)解密以獲得訊息內容，這種方法比使用傳統加解密安全多了。著名的例子有 RSA 密碼系統。

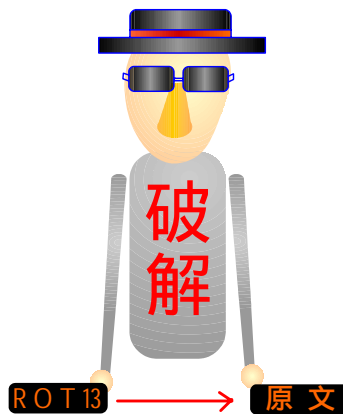
公開金鑰法就是加解密使用的是不同的鑰匙的方法！

註 4. **公開金鑰**：可以公開的加密鑰匙。縱使你有公開金鑰，也無法解出密文！所以可以公開此金鑰。

註 5. **私密金鑰**：用來解自己公開金鑰所加密的密文。公開金鑰及私密金鑰是配對的關係。自己公開金鑰所加的密文，只有自己的私密金鑰可以解開。所以每個人都要妥善保管自己的私密金鑰。



三、 加解密攻防戰：



上述的傳統加密法現在仍然廣泛流通於一般的網路中，但是傳統加解密法太有「規律性」了，破解者只要經過多份文件的比較之後，往往能夠很容易的解出原文內容，以下以「ROT13」這套加密方法實戰示範：

密文：V unir n qernz.

Gb fr gur jbeyq.

以上兩句是以 ROT13 加密法加密出來的文字，當破解者攔截到這兩句之後，會用三種方法來破解：1.常用字法 2.ASCII 法 3.排序法

1. 常用字法：

在英文的句子中，a 和 the 最常用到，所以先把密文中最常用到的字挑出來：第一句是 n，第二句是 e，由於 a 當定冠詞的機率也滿高的，當 a 是不定冠詞的時候有 a 跟 an 兩種變化，而第一句的 n 單獨出現的次數較多，所以原文部分先把 n 訂為 a，所以第一句原文是：* *a** a***a*。

(以*代表未知)

2. ASCII 法：

ASCII 是電腦中的一種編碼方式，每一個字或符號皆有它的 ASCII 值(見附錄 1)。由前一個步驟得知 a 對應到 n，很有可能是以 ASCII 法加密，由 ASCII 表上得知，a 的 ASCII 值是 97，n 的 ASCII 值是 110，兩者相差 13，由於這兩個句子中的字母是使用同一種加密方法，很有可能其他字的對應方法也有此種規律，
a→n, b→o, c→p, d→q, e→r, e→s, f→t, g→u, h→v, i→w, j→x, l→y, m→z, n→a, o→b, p→c, q→d, r→e, s→f, t→g, u→h, v→i, w→j, x→k, y→l, z→m

密文解密成原文：I have a dream. To see the world.

3. 排序法：

如果密文讀起來仍不通順的話，可用排序法再次排序，常用的排序方法有分組排序(abcdefg badcfeg)，首尾調換(abcdefg gfedcba)，如果排序之後閱讀起來正常的話，那就破解完成了。

四、自創密碼系統：

(一) 神奇密文：

前面所述的「傳統加密法」的防禦力薄弱，很容易破解，以下便把傳統加密法的弱點一列出：

1. 加密方法容易猜測
2. 能依密文長短判斷原文長短
3. 經過多重比較之後可以輕鬆的找到規律性
4. 經過排列組合以及一般的字母替換法則後容易找到原文為了克服這些困難，我想到了了一種新型的加密方法：

它有以下特性：

1. 亂數加解密（同樣的文章，每次加密的結果可以不同）
2. 原文在一定字數內，密文長短不會變
3. 無法由排列組合以及字母對照找到規律性

字母替代字典步驟如下：

Step1: 字母替代字典以 ATCG 四個英文字母排列組合（可以重複），總共有 4^4 共 256 種排列方法。

Step2: 把較常用的符號編入，剩下的做成一長串無意義的字串(圖表二)

字母替代表									
符號	加密成	符號	加密成	符號	加密成	符號	加密成	符號	加密成
空白	ACGC	q	ICCA	B	ICTA	N	ACCG	*	IGCA
a	AITG	r	GAGG	9	IAIC	O	AAGT	#	AACI
b	CTCA	s	IACC	0	AAIG	P	AGAT	\$	ACAG
c	ICGC	t	IGAC	.	CGAA	Q	IICI	%	ACGI
d	ACCA	v	CTAG	A	GICC	R	GCTG	&	GGGA
e	CGIA	w	CCGG	B	CGAA	S	GCGI	^	GGAC
f	IGIC	x	CAIG	C	CCGI	I	CGAI	@	ICTG
g	AGCI	λ	GGCI	D	IGAA	U	CIII	:	ACTC
h	IIGA	y	AIAT	E	IIIA	V	AGII	;	IITC
i	CTGG	z	ATCA	F	AGAC	W	AACC	-	CTCC
j	IIIG	l	ATCG	G	AIIA	X	IAGI	_	CGTG
k	CAGI	2	AIGC	H	IIGI	Y	GIAG	+	GTCC
l	CGCG	3	ACGA	I	CACC	Z	GATG	-	GTAI
m	IGCG	4	IIAI	J	ICCG	!	GACG	\	GCTA
n	CCTG	5	CTGA	K	CCCI	?	GGIC	(ICTI
o	GIIG	6	CAGA	L	ICAC	.	GCAC)	IAGG
p	GCCC	7	CCAI	M	IAAC	/	CAAG	[AICI

(圖表二)

加密步驟：

Step1: 把原文依對應的字典內容編碼成 ATCG 四種符號；

例：you 編成 ATATGTTGCTAG

Step2: 把加密過後的字串 4 個一組分組

Step3: 用電腦產生亂數，決定無意義的字串要放在哪裡，在字串組與字串組中隨機插入無意義的字串。使字數為 100 的倍數。

解密步驟：

Step1: 把密文四個一組分組，每次讀入四個碼，能翻譯的原文內容就依字典翻譯，不能翻譯的無意義文字內容則跳過。

例:

I have a dream.這段文字會轉換成

CCTA	TCGT	CACC	AAGA	ACGC	TTGA	AACG	ATTG	CCGG	CGTA	AACA	AACG	ACGC	ATTG	TCGT	TGGG	TGAA
亂數	亂數	I	亂數	空白	h	亂數	a	v	e	亂數	亂數	空白	a	亂數	亂數	亂數
ACCA	CCTA	GAGG	CGTA	ATGG	ATTG	TGCG	GCAC									
d	亂數	e	亂數	a	m											

但也可以是

CCTA	TCGT	CACC	AAGA	ACGC	TTGA	AACG	ATTG	CCGG	CGTA	AACA	AACG	ACGC	ATTG	TCGT	TGGG	TGAA
亂數	I	亂數	h	亂數	亂數	亂數	a	v	亂數	e	空白	a	空白	亂數	亂數	亂數
ACCA	CCTA	GAGG	CGTA	ATGG	ATTG	TGCG	GCAC									
d	e	e	亂數	a	亂數	m										

相同的原文，也可以有很多不同的結果喔！

破解率：1.未取得加解密器：暴力猜碼：機率 2.9×10^{224} 分之 1

2.已取得加解密器：反組譯：破解機率 1 分之 1 (必定破解！)

但是這種加密方法仍有破綻，如果敵人得到編碼器的話，就能很容易的去解碼，所以又想到了一奇計。

(二) 神奇文藏圖：

最近上網，發現現代最流行的生物科技中有一個難題叫做「基因密碼」，基因是細胞核內染色體上的一段的 DNA(去氧核糖核酸)，而且是由四種鹼基所構成，分別由 A、T、C、G 代表，這些鹼基的排列攸關著我們人身上的各種特徵的形成與否。而 DNA 的排列可以以圖形表達，也就是說可以用圖形來表達一串繁雜的密碼！如果能將文字藏在圖片中，分析每一張圖片的規律也是很費時間的。例如將文字藏在單一顏色的圖片中，讓人看不出是密文，就如同每個盒子的外表長的都一模一樣，但是裡面裝的東西可是皆不相同。

1.密文藏在單一顏色中

加密

Step1: 首先把原文依神奇密文之方式加密成 ATCG 四種符號。

Step2: 取得使用者輸入的 RGB 值，來畫出此 RGB 所產生的顏色圖形。

(註：電腦裡面的顏色是由 Red, Green, Blue 三色的光所組成的)

Step3: 訂出一個標準(表三)，讓電腦在讀取密文字串時能依文字內容來寫入圖片

加密	A 時	→ R 減 1, G 減 0, B 減 0	解密	R 減 1, G 減 0, B 減 0 時	→ A
	T 時	→ R 減 1, G 減 0, B 減 1		R 減 1, G 減 0, B 減 0 時	→ T
	C 時	→ R 減 0, G 減 1, B 減 0		R 減 1, G 減 0, B 減 0 時	→ C
	G 時	→ R 減 0, G 減 0, B 減 1		R 減 1, G 減 0, B 減 0 時	→ G

EX：當讀到 A 時 在圖片格裡面寫入一個點，其 RGB 值為： (圖表三)

(R 值 = 使用者輸入 R 值減 1, G 值 = 輸入的 G 值減 1, B 值 = 輸入的 B 值減 0)

當 R 或 G 或 B 值為 0 的時候，改減 1 為加 1 (避免出現 -1 的狀況)

Step4: 存檔

因為每一個點的 RGB 值只有加一或減一而已，所以肉眼看不出這樣的些微差別，以致於可以將密文藏在單一顏色的圖片中。

解密

Step1: 讀入圖檔

Step2: 使用者輸入標準 RGB 值

Step3: 一一讀取圖中的每一個點，將其 RGB 值與使用者輸入的標準直相減，將得到的值變成絕對值，依先前加密時定下的標準規則解密，轉成文字密文。

Step4: 依神奇密文方式解密，即大功告成

但是如果只有單一顏色的圖，防禦力仍太單薄，如果破解者使用軟體看出每一點的 RGB 值，又發現居然皆不相同的時候，應該也會心存懷疑吧！所以又改進成另一種較完美的加密方法

2.密文藏在一般圖片中

加密

Step1: 讀取一張自選圖片 (圖片內的點數要比加密的密文字數多)

Step2: 讀取圖中的每一個點，把讀到每一個的點的 RGB 值當作標準色，把密文中的字串一一讀取，依前述方法 (表三)，寫入第二張張圖片中

Step3: 把第二張圖片存檔

P.S. 可以支援將同段密文加密到多張圖片，安全性倍增！

解密

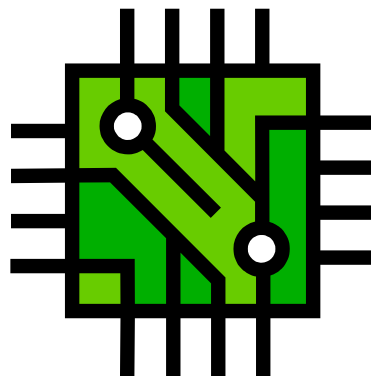
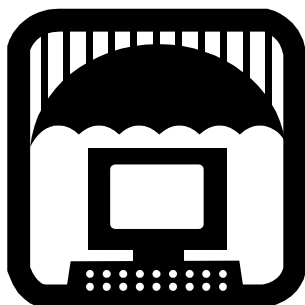
Step1: 讀取加密後的圖片

Step2: 讀取原來圖片

Step3: 讀取原圖跟密圖的點，把 RGB 值相互比較，依前述方法解密。

Step4: 依神奇密文方法解密成原文

好處：不易被發現，如果要破解，必定要有原圖 (解鈴還需繫鈴人)



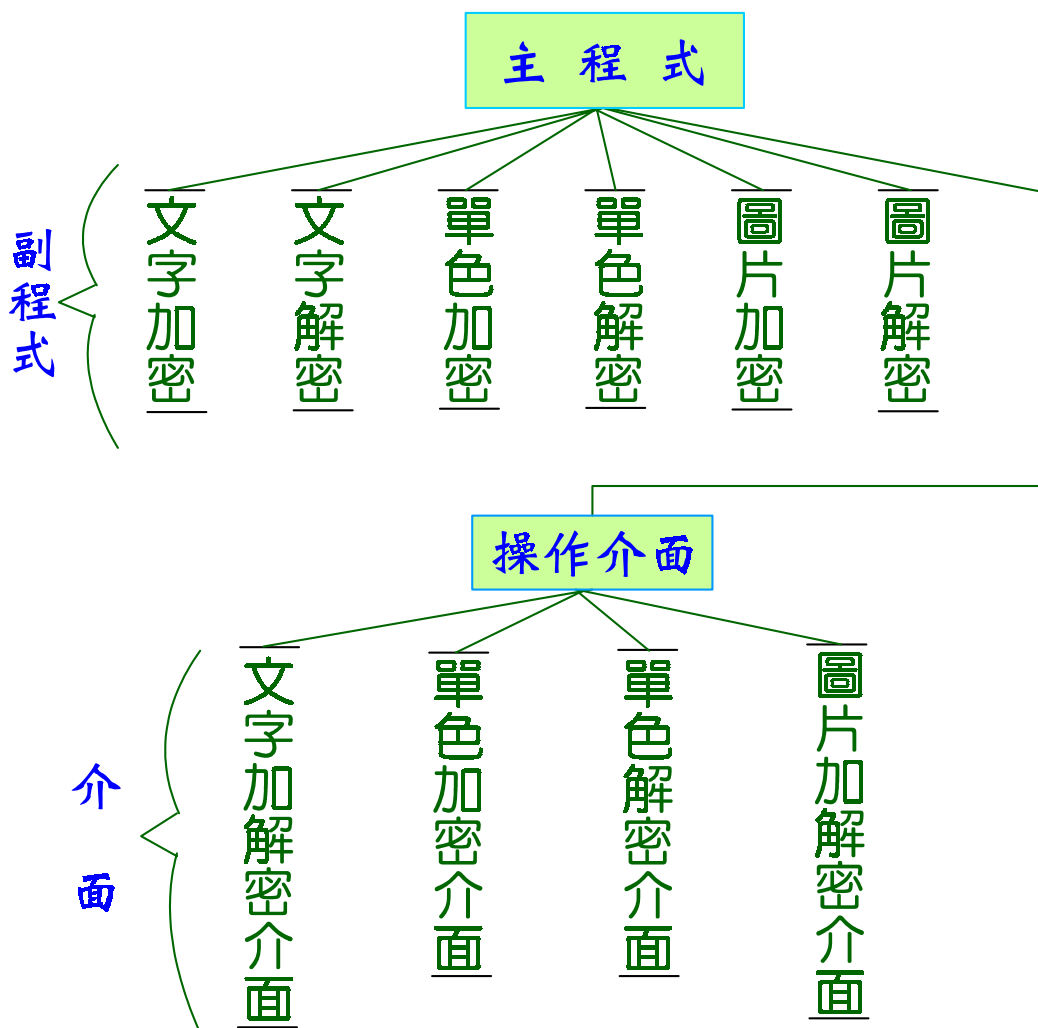
(三) 終極密碼戰 Final Version

- 1.採用亂數字典，改善神奇加解密字典產生方式，由固定 4^4 個元素對應變成 63^4 個元素取 256 個排列組合，也就是每一次加密用的字典都可以不一樣，解密時亦需取得字典檔才可以解密。
- 2.字典檔圖像化，隱藏字典內容，避免被破解。
- 3.可以加密中文字及與次常用符號。
- 4.能直接加解密一般檔案。
- 5.修改使用介面，使其更平易近人。

破解率：1.未取得加解密器：**暴力猜碼：**機率 $(63^4) ! / (63^4 - 256) !$ 分之 1 = $3.1 * 10^{1843}$ 分之 1，無法經由常用字法破解
2.已取得加解密器：**反組譯：**同未取得加解密器

程式運作

程式碼請見附錄二



(圖 4)

副程式：一種可以隨時呼叫的程式類型，就像是工具一樣。

柒、討論：

神奇加解密 & 神奇文藏圖 VS 傳統加解密

一、傳統加解密與神奇加解密的比較：

	傳統加解密	神奇加解密
字數	原文越長密文越長	原文在一定限度內，密文的長度與原文沒關係
對應	同一原文加密結果相同	同一原文加密結果不同
規律性	大，容易找到規律	小，有亂數，不易找到規律

二、傳統加解密與神奇文藏圖的比較：

	傳統加解密	神奇文藏圖
容易發現度	極易發現	不易發現
規律性	易找到	小，有亂數，不易找到規律
加解密方式	算式	圖片比較
被攔截到時	易破解	要蒐集完所有圖片才可破解，減低風險
可否經由多份密文比較找出規律	可，長串文字易比較	否，一般圖片加密中每一點的顏色不同，無法比較

三、單色加解密與一般圖片加解密的比較



	單色加解密	一般圖片加密
被發現難易度	難	難
破解難易	易	難
規律性	大	小
支援多張圖	否	是

捌、.結論：

這次創造了一個『神奇文藏圖』系統，製作期間問題重重，但是靠著努力思考，最後都一一克服。

一、程式出問題

在寫程式的時候，霹哩啪啦的一大串，難免會出錯。但是掉了一顆小螺絲，整個程式就沒辦法運轉啦！出錯時，就得要慢慢的『抓蟲』，需要極大的耐心。

二、太過理想化

這是許多初學者的共通病。想像使用者一定會依自己所設計的方式照步驟進行程式是不太可能的。所以最好設計多一點的使用提示，方便使用者。

三、單位的轉換

在 Visual Basic 的表單裡，是使用 Twip 為單位，在圖片中，卻使用 Px 為單位，這兩個單位的轉換是一個難題。後來發現表單中有「繪圖格式」這個選項終於解決。

四、邊框的大小

在程式進行中，如果圖片太小，則圖片欄不會有邊框。但如果圖片較大，則圖片欄會出現邊框，在讀取時會出問題。

五、字典法的配置

哪一些常用的字要配什麼代號，哪些代號要分配到亂數區域，也是一難題。到底要用不重複的 5 個字呢？還是重複的 4 個字？因為不重複的 5 個字只有 $5! = 120$ 個組合，4 個字重複共有 $4^4=256$ 種組合。因為英文文章中常用的符號共有 97 個字，且為了省空間，所以採用 4 字可重複的方式。

（終極密碼戰最終版本採用 63^4 個元素取 256 個對應成 ASCII 值）

密碼從古自今不斷的演變，每一個觀念的創新，也都是新的契機。就像開放式金鑰的觀念就令人拍案叫絕，居然能光明正大的公佈加密的方法及密文，而不用擔心被破解。這次自己發展出來的密碼系統是屬於一半傳統一半創新式的加解密系統，解密時，光是擁有儲存密碼的圖片是不行的，還得要擁有原圖。神奇加密裡文字對照密文的方法是傳統加解密類中的字典法，而神奇文藏圖的部分則是一種創新（只有密圖無法直接得到密文）。密碼學的未來充滿著光明，在人越來越倚重電腦的時代，越有機會使用到密碼來保密，當你體會到密碼的方便性時，就會知道什麼叫做「方便的複雜化」了！

玖、.參考資料及其他：

- 一、 莎拉·夫蘭那里 / 數學小魔女 ISBN 957-621-795-4{310}
- 二、 布魯斯 施耐爾 / 秘密與謊言 ISBN 957667875-7
- 三、 川九保勝夫 / 基礎數學 ISBN 157-776-515-7
- 四、 吳權威、梁仁楷/ VB 入門與應用 / 2003 年 5 月初版 / 暮峰資訊
- 五、 小瓜瓜的 VB 研究小站 / <http://vb.infoserv.com.tw/>
- 六、 生計介紹*何謂基因 / <http://www.bmnews.net/big5/biotech/gene.html>
- 七、 摩斯密碼 / <http://www.contest.edu.tw/award/88/save/a871232/www/sos/s4.htm>
- 八、 ROT13 / <http://www.rot13.com>



ASCII 總表 (附錄 1)

0 = [null]	65 = A	105 = i
8 = [backspace]	66 = B	106 = j
9 = [tab]	67 = C	107 = k
10 = [linefeed]	68 = D	108 = l
13 = [enter]	69 = E	109 = m
31 =	70 = F	110 = n
32 = [space]	71 = G	111 = o
33 = !	72 = H	112 = p
34 = "	73 = I	113 = q
35 = #	74 = J	114 = r
36 = \$	75 = K	115 = s
37 = %	76 = L	116 = t
38 = &	77 = M	117 = u
39 = '	78 = N	118 = v
40 = (79 = O	119 = w
41 =)	80 = P	120 = x
42 = *	81 = Q	121 = y
43 = +	82 = R	122 = z
44 = ,	83 = S	123 = {
45 = -	84 = T	124 =
46 = .	85 = U	125 = }
47 = /	86 = V	126 = ~
48 = 0	87 = W	127 =
49 = 1	88 = X	128 = €
50 = 2	89 = Y	(128 之後是較不常用的符號 <略>)
51 = 3	90 = Z	
52 = 4	91 = [
53 = 5	92 = \	
54 = 6	93 =]	
55 = 7	94 = ^	
56 = 8	95 = _	
57 = 9	96 = `	
58 = :	97 = a	
59 = ;	98 = b	
60 = <	99 = c	
61 = =	100 = d	
62 = >	101 = e	
63 = ?	102 = f	
64 = @	103 = g	
	104 = h	

核心程式碼 (附錄 2)

Sub di()

'文字加密副程式開始

wi = Text1.Text '設定 wi 變數的內容為原文

lo = Len(wi) '令 lo 變數的值為原文長度

For i = 1 To lo '令 i 這個變數的值從 1 屬到 lo(記次變數)

ch = Mid(wi, i, 1) '取 wi 字串的第 i 個字為 ch

迴圈 {
 Select Case ch
 '搜尋字典中 ch 對應的密文並貼上<省略>
 End Select
Next 'i 遞增

wol = 100 - (Len(wo) Mod 100)

'當字串長不為 100 的倍數時

 bea = wol / 4 '令 bea 為 wol 的 4 分之 1

'補足百字程式開始

If Len(wo) Mod 100 <> 0 Then

Randomize

迴圈 {
 For i9 = 1 To bea
 rnd1 = Int(Rnd * 109) + 1 '找一個亂數值
 Randomize
 rnd2 = Int(Rnd * lo) * 4 + 1 '找一個亂數插入位置
 Randomize
 dta = rnddata(rnd1) '亂數插入陣列 rnddata 中的值
 wo = InsStr(wo, dta, rnd2) '執行插入動作
 lo = Len(wo) / 4 '再次偵測密文長
 Next 'i9 遞增

End If

'補足百字程式結束

Text2.Text = wo

End Sub '文字加密副程式結束



Sub dic()

‘文字解密副程式開始

wo = Text2.Text ‘令 wo 的內容為密文

lo2 = Len(wo) ‘令 lo 的值為密文字串長度

lo3 = lo2 / 4

For i2 = 1 To lo3 ‘令 i2 從 1 數到 lo3 (記次變數)

ch2 = Mid(wo, i2 * 4 - 3, 4) ‘逐一讀入密文一組 4 個字母

Select Case ch2

’搜尋字典中密文所對應的字母，並轉回原文<省略>

End Select

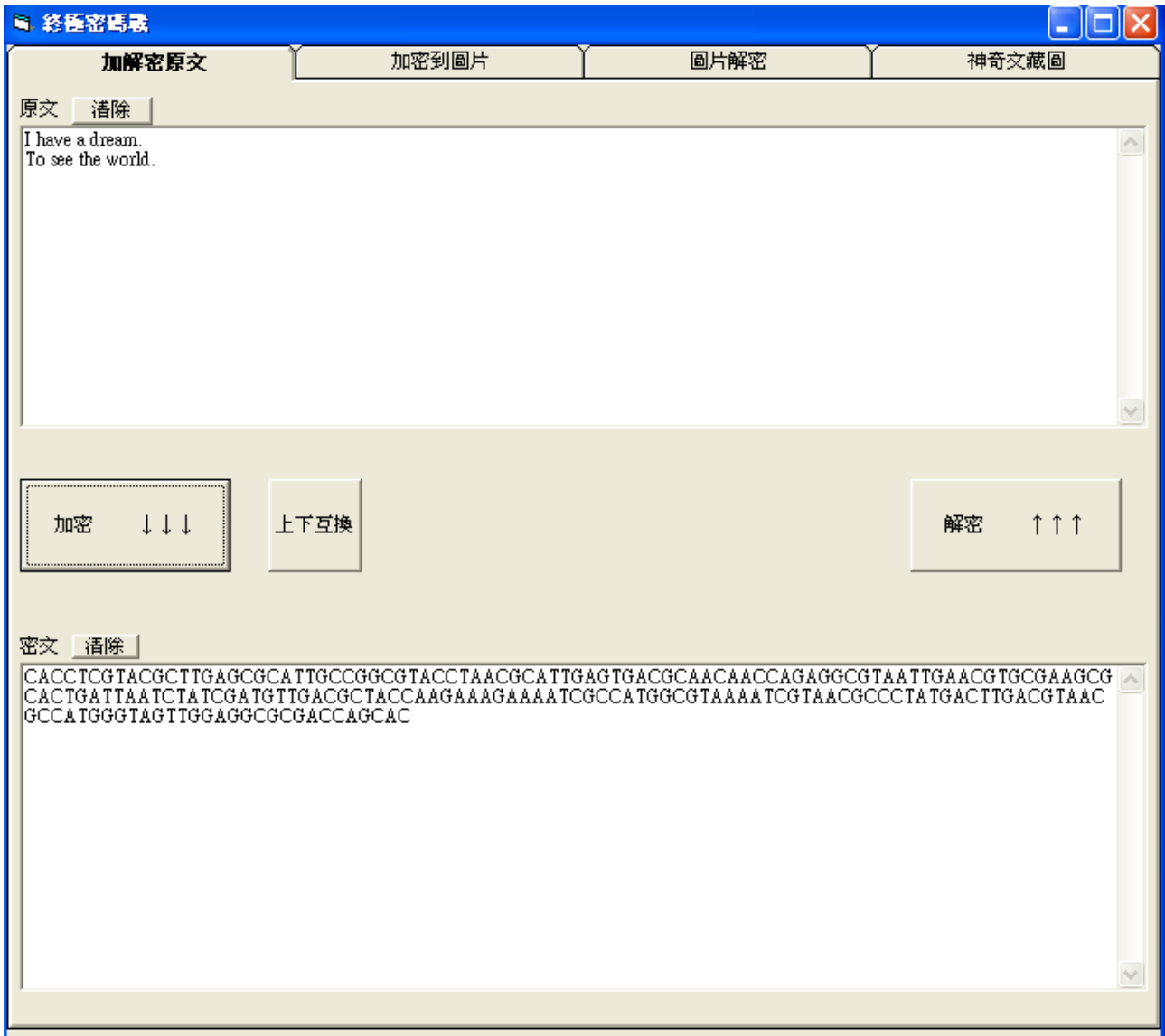
Next ‘i2 遞增

Text1.Text = wi ‘輸出原文字串

End Sub ‘文字解密副程式結束



操作介面 (附錄 3)



單色加密的密圖

I have a dream.

To see the world.

一般圖片加密的原圖



一般圖片加密的密圖



外表都一模一樣，一個卻隱藏了密文。

評語

030806 國中組生活與應用科學科 第二名

終極密碼戰

密碼系統一直是現今電腦充斥，實用於生活層面，為了資訊保護而需要的技術。本作品對各式密碼作一完整的整理分析並發展新的密碼系統，其中神奇文藏圖利用影像色差作加解密具有多項好處，有其創意。

密碼學也是一不容易的領域，本作品勇於挑戰此重要且困難的題目，值得鼓勵。