附件 1

國立竹南高中彈性學習時間－學生自主學習申請表

108 學年度第二 學期

申請學生資料	班級座號	學號	姓名（請親自簽名）
	11410	811401	李昀蓉
執行學期	108-2	共學同學	（無則免填）
申請週數	從 4 週至 16 週	計畫名稱	RSA 加密系統之專題研究
學習主題	☑專題探究 ☐藝文創作 ☐自我閱讀 ☐其他：		
主題屬性	☐國語文 ☐英語文 ☑數學 ☐社會 ☐自然 ☐化工 ☐藝能		

自主學習規劃內容	節數	日期	實施內容與進度	設備（手機使用次數以 6 節為限）	場地
	1.2	3/17	與指導教師討論自主學習規劃，完成本學期自主學習實施內容與進度。	☐手機 ☐電腦 ☐其他	☑教室 ☐圖書館 ☐其他
	3.4	3/24	參閱相關書籍〈世界第一簡單密碼學〉，並大致了解密碼學的常見詞彙，以初步認識此領域。	☐手機 ☐電腦 ☐其他	☑教室 ☐圖書館 ☐其他
	5.6	4/14	找尋古典密碼學的種類及歷史，並利用時間學習「同餘問題」。	☐手機 ☐電腦 ☐其他	☑教室 ☐圖書館 ☐其他
	7.8	4/21	了解密碼學的運作模式及生活中的相關應用，並試著寫出一個屬於自己的密碼系統。	☐手機 ☐電腦 ☐其他	☑教室 ☐圖書館 ☐其他
	9.10	4/28	上網學習數論中的「歐拉定理」並找找尋相關題目練習，再結合前幾週的成果大致了解 RSA 加密系統之背景。	☑手機 ☐電腦 ☐其他	☑教室 ☐圖書館 ☐其他

	11.12	5/5	結合前面所學，再進一步學習RSA加密系統的運作流程，以達到最終之學習目的。	☐手機 ☐電腦 ☐其他	☑教室 ☐圖書館 ☐其他
	13.14	5/12	整理所有的資料並思考這段時間之學習歷程，再構思及撰寫出小論文各部分的草稿。	☐手機 ☐電腦 ☐其他	☑教室 ☐圖書館 ☐其他
	15.16	6/2	整理前一次之結果，以電腦打成Word檔形式。	☐手機 ☑電腦 ☐其他	☑教室 ☐圖書館 ☐其他
	17.18	6/9	進入最後步驟一修正有誤部分，及編輯排板。 完成後上傳發表作品。	☐手機 ☑電腦 ☐其他	☑教室 ☐圖書館 ☐其他

學習目標與預期效果	（請具體寫出預期產出的作品） 學習目標：了解現代密碼學之「RSA加密系統的運作模式」。 預期效果：整理自己在這期間所學到的知識，寫出一篇小論文並上傳發表作品。

父母或監護人簽名	陳乙果	指導老師簽名	陳書誼	導師簽名	陳書誼

申請受理情形（此部分，申請同學免填）				
初審		☑通過 ☐修正 ☐不通過	複審	☐修正通過 ☐不通過
受理日期	編號	科代表	教學組長簽章	教務主任簽章
3/11		教師兼圖書館主任 鄒永灝	教師兼教學組長 陳錦萍	教師兼教務主任 陳廷宇

※本計畫請於○○前完成內容及簽章後，以班級為單位交由導師轉教務處教學組。

附件 2

國立竹南高中彈性學習時間－自主學習成果紀錄表

108 學年度 2 學期

申請學生資料	班級	學號	姓名（請親自簽名）
	114	811401	李昀蓉
執行學期	108-2	共學同學	（無則免填）
申請週數	從 4 週至 16 週	計畫名稱	RSA加密系統之專題研究

自主學習成果記錄

節次/週次	實施內容與進度	自我檢核	指導教師確認
3/17 1	與指導教師討論自主學習規劃，完成本學期自主學習實施內容與進度	□優良 □尚可 □待努力	◎
2	查閱密碼學相關資訊	□優良 ☑尚可 □待努力	陳書誼
3/24 3	閱讀〈世界第一簡單的密碼學〉之常見詞彙介紹、說明	☑優良 □尚可 □待努力	
4	結合上週與上節課之所學，大致統整與延伸	□優良 ☑尚可 □待努力	
4/14 5	找尋古典密碼學的種類及歷史，閱讀科學人雜誌之「來上一堂質數課」	□優良 ☑尚可 □待努力	
6	學習同餘問題及其相關應用	☑優良 □尚可 □待努力	
7	了解並統整密碼學的運作模式及生活中的相關應用	☑優良 □尚可 □待努力	
4/21 8	參考既有的密碼種類，寫出一個屬於自己的密碼系統，並統整歸納	☑優良 □尚可 □待努力	
4/28 9	利用所找資料學習費馬小定理之概念、	□優良 ☑尚可 □待努力	陳書誼
10	利用所找資料學習歐拉定理(函數)之概念及參考相關證明	□優良 ☑尚可 □待努力	
5/5 11	尋找密碼學的相關補充以彌補前面不足之處	☑優良 □尚可 □待努力	
12	利用所找資料及前面所了解的先備知識學習RSA加密系統之運作流程	☑優良 □尚可 □待努力	
5/12 13	複習前面所學之內容	□優良 ☑尚可 □待努力	陳書誼
14	整理前面所學內容並用word打好小論文的架構	☑優良 □尚可 □待努力	
15	撰寫小論文	□優良 ☑尚可 □待努力	

6/2 ~ 6/9	16	撰寫小論文	☐優良 ☑尚可 ☐待努力	許
	17	修正小論文有誤之處	☑優良 ☐尚可 ☐待努力	陳書誼
	18	編輯小論文排板	☑優良 ☐尚可 ☐待努力	
自主學習成果說明	為了解RSA加密系統的運作模式，先從密碼學最基礎的部分開始認識，再學習其所需之數論原理與運算流程，最後將所有學習內容結合並應用於RSA加密系統，並產出一篇小論文。			
自主學習歷程省思	和RSA加密系統有關的數論原理需要花很多時間了解、練習計算，然而，礙於時間的限制，未能很徹底地學習相關證明，若有機會，定會進行更深入的研究。			
指導教師簽章建議	RSA加密系統是密碼學裡基本的加密法，對於高一生較難理解，時參加認真將RSA所需工具一一整理並理解，再試著撰寫一份小論文，內容淺顯易懂，對於想了解密碼學的高中生是很好的文章之一。 陳書誼			

投稿類別：數學類

篇名： 淡談 RSA 加密系統

作者：
李昀蓉。國立竹南高級中學。一年十四班

指導老師：陳書誼 老師

淡談 RSA 加密系統

壹、前言

一、研究動機

國中有一堂課，老師讓我們欣賞一部電影 -《模仿遊戲》，自從那時，我便對密碼學深深著迷，艾倫圖靈在二次世界大戰期間主要負責破譯德國人的 Enigma 密碼系統，破解密碼時，需要大量的計算，於是他便發明出「圖靈機」，這台計算機的發明加快了二戰的結束。

以往都是使用對稱加密算法，而圖靈突破了這一點，它使用的為非對稱式密碼算法，在老師的介紹下，我知道了目前非對稱式加密運用最廣泛的-RSA 加密系統，於是我便朝著這方面進行研究。

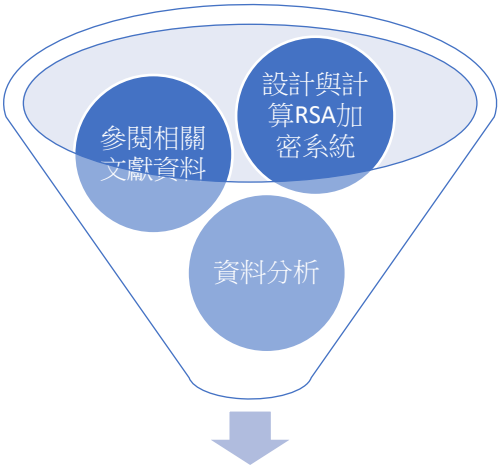
二、研究目的

（一）了解 RSA 加密系統之加密解密概念
（二）了解 RSA 加密系統之運算流程
（三）了解 RSA 加密系統在生活中的相關應用
（四）實際設計與操作 RSA 加密系統

三、研究方法

本研究採文獻分析法進行研究，確定研究主題及目的後，先閱讀參考書目和網路資訊以及相關研究，再將資料分析後統整分類。

四、研究流程



貳、正文

一、密碼學相關名詞簡介

（一）加密

明文信息轉變為密文內容，使之不可讀的過程。（Encrypt）

（二）解密

密文內容轉變為明文信息的程序。（Decrypt）

（三）明文

加密前的訊息。（Plaintext）

（四）密文

加密後的訊息。（Cipertext）

（五）演算法

解決複雜問題的程序。（Algorithm）

（六）密碼學演算法

做與密碼學相關程序的演算法。（例：加密、解密、數位簽章）

（七）公開金鑰

1. 用作加密。
2. 可公開（可向外公布）。

（八）私密金鑰

1. 用作解密。
2. 不公開，意謂必須由用戶自行嚴格秘密保管，絕不透過任何途徑向任何人提供，也不會透露給被信任要通訊的另一方。

（九）密鑰（又稱為金鑰）

1. 指某個用來完成加密、解密、完整性驗證等密碼學應用的秘密信息。
2. 加密金鑰：密碼化的鑰匙。
3. 解密金鑰：解開密碼的鑰匙。

（十）共同金鑰密碼

1. 為了不讓別人知道金鑰，必須特別注意配送和保管。
2. 由於加密和解密計算量少且快速，因此適用於大量資料的連繫。
3. 需要多數的金鑰及管理，因此不適用於和不特定多數對象間的連繫。

二、RSA 密碼必備數學知識簡介

（一）素數

又稱「質數」，在大於 1 的自然數中，除了 1 和該數自然數外，無法被其他自然數整除的數。

（二）互質數

若 N 個整數的最大公因數為 1，則這 N 個整數互質。

（三）輾轉相除法的原理

又稱歐幾里德算法，是求最大公因數的算法。若 a、b 為整數，滿足 a = bq + r，則 a、b 的最大公因數等於 b、r 的最大公因數。

（四）質數無窮多定理

古希臘數學家歐幾里德運用反證法證明，一個大於 1 的正整數，若質數只有有限個，標記 N_1、N_2、則 $P + (N_1*N_2*\cdots*N_K) +1$ 皆無法被前列質數整除，故 P 為質數，與假設不符。

（五）同餘定理

$a \equiv b \pmod N$

這是一般同餘式的表示方式，也可稱為模數運算。又可讀作以 *N* 為模數，a 和 b 為同餘數。即在模數 N 之下，a 和 b 具有相同的意思，如 5 除以 7 餘數為 5，12 除以 7 餘數亦為 5，可形成 $12 \equiv 5 \pmod 7$

（六）費馬小定理

設 P 為質數且整數 a 與 P 互質，則下列算式成立:

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

換句話說，a 的 p-1 次方除以 p 會餘 1。

（七）歐拉函數

記為 $\varphi(n)$，1 至 n 的自然數中和 n 互質的整數個數。

（八）歐拉公式

若 p、q 為質數，則 $\varphi(pq)=\varphi(p)*\varphi(q)$。

例如: $\varphi(15)=8$，$\varphi(3)=2$，$\varphi(5)=4$，則 $\varphi(15)=\varphi(3)*\varphi(5)$

三、RSA 密碼的加密與解密概念

（一）加密

設明文為 M，密文為 C，則加密可表示如下。

$C=M^e \pmod N$

即 M（明文）的 e（公開金鑰之一）次方後所得之值，除以 N（另一個公開金鑰）後的餘數為 C（密文），便得以加密。

（二）解密

解密可表示如下

$M=C^d \pmod N$

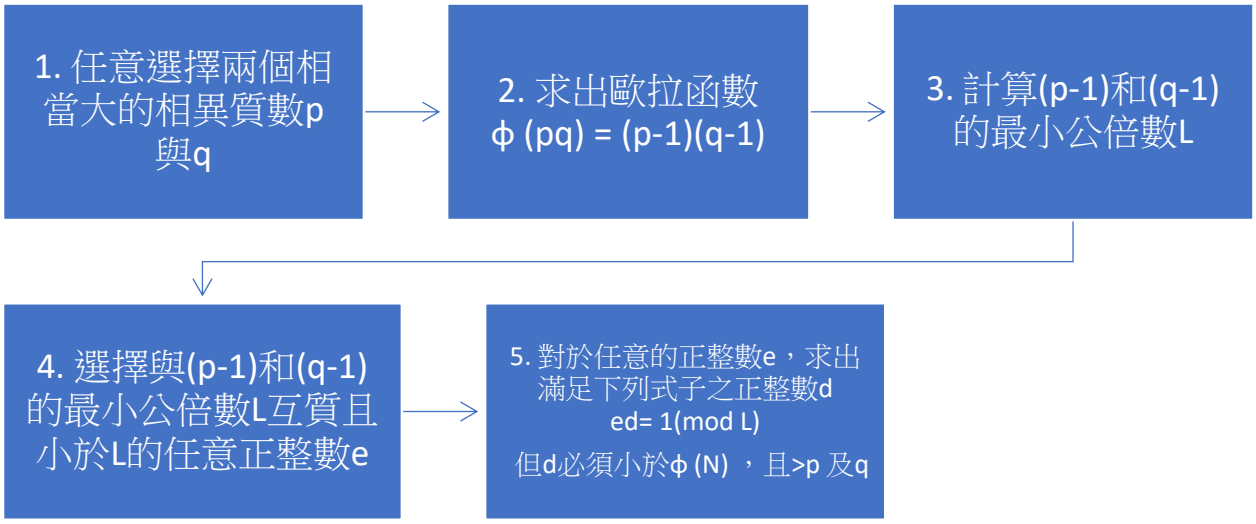
即 C（密文）的 d（秘密金鑰）次方後所得的值，除以 N（公開金鑰）後的餘數 M（明文），便得以解密。

（三）備註

此處的 N 為 2 個很大的相異質數相乘的結果。

四、RSA 密碼之金鑰生成方法

(一)流程圖



(二)備註

1. p*q 為 N，即為公開金鑰之一。
2. 第三步驟是為了產生公開金鑰之另一個準備作業，p 與 q 可於求出歐拉函數後，在不讓他人得知的狀況下銷毀，因求出歐拉函數後則不再需要 p、q 了。

五、公開金鑰與秘密金鑰之探討

(一) 由棄九法所得，利用同餘的加法性與傳遞性，我們可以進行四則運算的檢驗，而減法與除法運算之檢驗分別為加法與乘法運算的逆運算關係，從上可知，模數 L 中，d 相當於 e 的乘法逆運算數。即為**求出與加密金鑰 e 成對的解密金鑰 d 所必要的數。**

(二) 由歐拉定理所知 1 至 (n-1) 的所有整數 a，均會成立下列式子

a 的 k φ (n)+1 次方= a(mod n)

根據上式，對於 1 至(n -1)的所有整數，可得

a^{kL+1}= a(mod n*)*

由上可知，對於 1 至(n-1)的所有自然數 M(相當於明文)，會成立下式

$M^{ed}=M^{kL+1}=M(\text{mod } n)$

(三) 試求出與加密金鑰 e 成對的解密金鑰 d

因為 ed=1(mod *L*)，所以 ed-1=0(mod *L*)，即 ed-1 為 *L* 的倍數，因此 ed-1=*kL*(k 為非負整數)，且 ed=kL+1 成立(k 為非負整數)。由(二)所得之結論，會成立下式

$M^{ed}=M^{kL+1}=M(\text{mod } n)$

由上述可知，密文 C(=M^e)的 d 次方 M 的 ed 次方被解密為明文 M

結論:秘密金鑰 d 與公開金鑰 e 是成對的。

六、RSA 加密系統實際操作

（一）產生公開金鑰與私密金鑰

1. 假設兩大質數 p 和 q，為了方便計算，所以取較小質數 p=7，q=11，則 n=p*q=7*11=77
2. 計算歐拉函數 φ（n）= (p-1)(q-1)。

φ（n）=（7-1）(11-1）

= 6*10

= 60

3. 計算兩整數值 e 和 d，是其滿足數學關係式—
   e*d mod φ（n）= 1
   e*d = t* φ（n）+ 1
   d = (t* φ（n）+ 1) / e
   若 e = 23，d = (t*60 +1) / 23
   則當 t = 18，d = 47 時即為所求。

4. 一般而言，為了密碼系統之安全性，即 e 不等於 d，所以我們選擇**公開金鑰（n , e）= (77,23)，私密金鑰 d = 47**。

（二）加密

1. 先設定一串明文：「FIGHTING」。
2. 參考表一，將明文依照 ASCII 碼轉換為整數，轉換後的整數如表二所示。

明文	A	B	C	D	E	F	G	H	I	J
對照碼	65	66	67	68	69	70	71	72	73	74
明文	K	L	M	N	O	P	Q	R	S	T
對照碼	75	76	77	78	79	80	81	82	83	84
明文	U	V	W	X	Y	Z				
對照碼	85	86	87	88	89	90				

表一： 明文數字對照（依照 http://ascii.911cha.com 繪製）

F	I	G	H	T	I	N	G
70	73	71	72	84	73	78	71

表二：明文轉換後的整數對照

3. 將表二轉換為二進位，如同下表(表三)所示。

明文	F	I	G	H	T	I	N	G
轉換後整數	70	73	71	72	84	73	78	71
二進位	1000110	1001001	1000111	1001000	1010100	1001001	1001110	1000111

表三：明文轉換後的整數對照（依照 http://ascii.911cha.com 繪製）

4. 將此二進位資料由左至右改以 k 位元為一區塊，其中 2^k-1 小於 n-1。如此例，二進位資料原以 7 位元為一區塊，改以 6 位元為一區塊，可表示之最大值為 63 (= 2^6-1)小於 77-1 = 76。若不足 6 位元時再由右至左補 0，如下表(表四)所示。

100011 010010 011000 111100 100010 101001 001001 100111 010001 110000									
以 6 位元為一區塊									
100011	010010	011000	111100	100010	101001	001001	100111	010001	110000

表四：將二進位整數以 6 位元分為一區塊，其中最後不足故補四個 0。

5. 將表四各區塊位元轉換為十進位，如下表（表五）所示。

二進位	100011	010010	011000	111100	100010	101001	001001	100111	010001	110000
十進位	35	18	24	60	34	41	9	12	17	48

表五：二進位整數轉換為十進位整數之結果

6. 利用加密金鑰（n = 77, e = 23）以及表五得到之結果代入公式—
   C = M 的 e 次方 mod n 進行各區塊的加密，即可得到下列結果：
   C = 35^{23} mod 77，C = 18^{23} mod 77，
   C = 24^{23} mod 77，C = 60^{23} mod 77，
   C = 34^{23} mod 77，C = 41^{23} mod 77，
   C = 9^{23} mod 77 ，C = 12^{23} mod 77，
   C = 17^{23} mod 77，C = 48^{23} mod 77。

7. 以下以 C = 35^{23} mod 77 為例，進行計算如下所示：
   C = 35^{23} mod 77
   = $(35^2)^{11}$*35 mod 77
   = 70^{11}*35 mod 77
   = $(70^2)^5$*70*35 mod 77
   = 49^5*70*35 mod 77
   = $(49^2)^2$*49*70*35 mod 77
   = 49^2*49*70*35 mod 77
   = 14^2 *49*70*35 mod 77
   = 42*49*70*35 mod 77
   =63

8. 其餘區塊以上述計算方式之計算結果如下所示：
   18^{23} mod 77 = 2 ， 24^{23} mod 77 = 19，
   60^{23} mod 77 = 37， 34^{23} mod 77 =34，
   41^{23} mod 77 = 6 ， 9^{23} mod 77 =71，
   12^{23} mod 77 = 34， 17^{23} mod 77 = 40，
   48^{23} mod 77 = 3。

9. 將上述計算結果依 ASCII 碼轉換為字元，如表六所示：

明文	35	18	24	60	34	41	9	12	17	48
密文	63	2	19	37	34	6	71	34	40	3
字元	?			%	”		G	”	(	

表六：以 ASCII 碼轉換為字元（依照 http://ascii.911cha.com 繪製）

備註：表六部分有空白處是由於十進位制的 0 至 31、127 為控制字符，也算是個可顯示字符，其顯示為空白。

（三）解密

1. 當我們得到對方利用公開金鑰傳給我們的加密訊息時，配合使用相對應的解密金鑰即可進行解密，了解對方欲傳達給我們的訊息。我們已經知道密文訊息且將其轉換為十進位整數，再利用解密金鑰（d = 47），將密文還原為明文。
2. 加密公式為 M = C 的 d 次方 mod n，我們以密文 C = 63 為例，令解密金鑰 d = 47、n = 77 進行還原
3. $M = 63^{47} \bmod 77$
   $= (63^2)^{23} * 63 \bmod 77$
   $= 42^{23} * 63 \bmod 77$
   $= (42^2)^{11} * 42 * 63 \bmod 77$
   $= 70^{11} * 42 * 63 \bmod 77$
   $= (70^2)^5 * 70 * 42 * 63 \bmod 77$
   $= 49^5 * 70 * 42 * 63 \bmod 77$
   $= (49^2)^2 * 49 * 70 * 42 * 63 \bmod 77$
   $= 14^2 * 49 * 70 * 42 * 63 \bmod 77$
   $= 42 * 49 * 70 * 42 * 63 \bmod 77$
   $= 42^2 * 49 * 70 * 63 \bmod 77$
   $= 70 * 49 * 70 * 63 \bmod 77$
   $= 70^2 * 49 * 63 \bmod 77$

= 49*49*63 mod 77
= 49^2*63 mod 77
= 14*63 mod 77
= 35

4. 將其餘密文以上述之方法計算可得到下列結果：
   2^{47} mod 77 = 18 ， 19^{47}mod 77 = 24，
   37^{47}mod 77 = 60 ， 34^{47} mod 77 = 34，
   6^{47} mod 77 = 41 ， 71^{47} mod 77 = 9，
   34^{47} mod 77 = 12， 40^{47} mod 77 = 17，
   3^{47} mod 77 = 48。
5. 將上述結果（十進位）轉換為二進位，結果如下表（表七）所示：

十進位	35	18	24	60	34	41	9	12	17	48
二進位	100011	010010	011000	111100	100010	101001	001001	100111	010001	110000

表七：將十進位的明文轉換為二進位

6. 將表七轉換之結果（二進位整數）以 7 位元為一區塊並以 10 進位表示之

1000110 1001001 1000111 1001000 1010100 1001001 1001110 1000111								
以 7 位元為一區塊								
二進位	1000110	1001001	1000111	1001000	1010100	1001001	1001110	1000111
十進位	70	73	71	72	84	73	78	71

表八：將表七之二進位整數以 7 位元分為一區塊並以 10 進位表示之

7. 將表八轉換之十進位數值依 ASCII 表，還原為字元，可得到明文:「FIGHTING」。

密文	70	73	71	72	84	73	78	71
明文	F	I	G	H	T	I	N	G

表八：將十進位數值還原為字元（參考表一）

參、結論

RSA 加密系統須具備之背景知識涵蓋極廣，但深入探討後，其實也未必如同想像中那麼艱澀難懂。從加密到解密需要比一般簡單的加密擁有繁瑣的步驟，不過這也意味著，珍貴的資料不會輕易被盜用、外流。

由於非對稱式加密系統擁有兩把金鑰，一為公開金鑰，二為私密金鑰，如果無法持有私密金鑰進行解密，則需進行極大整數之質因數分解，故即使外人得到公開金鑰也無濟於事。

RSA 加密系統在現代在公開金鑰加密、電子商務中被廣泛應用，從簡單加密到數位簽章，都和我們的生活息息相關。

但假如有人可以找到很快進行質因數分解的方法，此加密系統的可靠性便會大幅降低，但這可能性是非常小的。

肆、參考資料

1. 三鼓政昭、佐藤伸一（2020 年 1 月 3 日）。**世界第一簡單的密碼學**。
2. 王旭正（2015 年 2 月 26 日）。**認識密碼學的第一本書**。
3. 曹亮吉（2010 年 6 月）。**科學人雜誌-來上一堂質數課**。
4. **每日頭條-數論算法編程之歐拉函數與歐拉定理的理論證明**（2019 年 2 月 1 日）2020 年 5 月 10 日取自 https://www.google.com.tw/amp/s/kknews.cc/code/r5nr88x.amp
5. **密碼學原理與技術(對稱式與非對稱式密碼技術)** 2020 年 5 月 10 日取自 http://avp.toko.edu.tw/docs/class/3/密碼學原理與技術.pdf
6. **Module 2: 密碼學基礎** 2020 年 5 月 17 日取自 http://163.25.97.1/~ansel/teaching/1002_NetworkSecurity/Module%2002-密碼學基礎.pdf