投稿類別：數學類

篇名：
你想知道的密碼學！

作者：
邱詠智。大園國際高中。高二 14 班
蘇育賢。大園國際高中。高二 14 班

指導老師：
邱國輝 老師

壹●前言

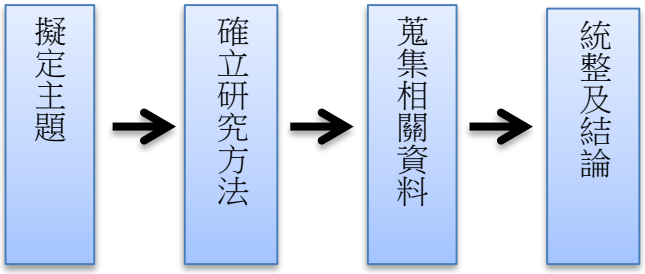
一、研究動機

從古至今在政治、經濟、軍事及科技方面都有防止重要機密洩漏的安全管制，在當今資訊爆炸的時代，各式各樣的訊息在網路中傳遞，若沒有經過任何保密措施，這些資訊就等同於直接提供給所有人，因此如何保護重要資訊成為了重要的課題。

二、研究目的

探討關於加密的模式，並對一些普遍方法進行分析和安全性比較，希望找出更好保密資訊的策略。

三、研究流程



貳●正文

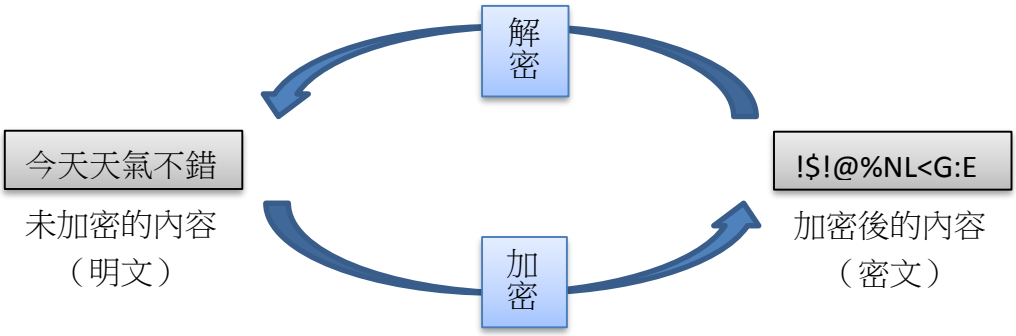
一、密碼學

為了保護軍事、商業、個人機密資訊而衍生出了密碼學，所謂密碼學是利用各種方法對資訊加密的學問。

（一）相關用語

明文 P（Plain text）：未加密的資料
密文 C（Cipher）：已加密的資料
加密金鑰（Encryption Key）：將明文密碼化的演算法
解密金鑰（Decryption Key）：解開密文的演算法

（二）流程圖



三、共通金鑰加密

又稱對稱金鑰加密，是密碼學中最古老且最有名的。加密和解密都是用相同的鑰匙。運算速度快，經常被用來加密大量資料。

（一）替代式密碼

將原本的文字以相對應的文字替換。範例:I have to think an example

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

這種方法最大的缺點就是一對一的對應關係，如果密文短的話可以用窮舉證法破解，長的話用頻率分析破解。

改良方向：字母 A~Z 對應 1~26，每個字母向右平移 3 格，這就是最早被使用的替換式密碼的一種，在上面加點變化。例如：第 2n 個字母向右平移 6 格，第 2n+1 個字母向左平移 2 格。

相同的 p 對應到不同的字母，如此一來就可以解決一對一的問題了。

（二）移位密碼

將原本的文字重新排列。例如：倒過來寫 It is a simple→elpmisasitI

但上述例子易被破解，所以移位式密碼也有相應的演變，縱欄式移項密碼，是其中一個例子。

使用方法：

取一個關鍵字，關鍵字的英文字母對應相對的字母順序，再將原文寫在關鍵字下，以由左而右，由上至下，以關鍵字為寬度續寫下去。關鍵字序號由小至大的縱排依序由上至下寫下即完成加密。

範例：關鍵字:Handsome，原文: It is not the true you are ugly

H	a	n	d	s	o	m	e
(8)	(1)	(14)	(4)	(19)	(15)	(13)	(5)
I	t	i	s	n	o	t	t
h	e	t	r	u	e	y	o
u	a	r	e	u	g	l	y

現代有電腦可以快速運算嘗試所有的可能，所以這種密碼非常不安全。

改良方向：不單獨使用，而是跟其他方法進行連用。

例如：和替代式密碼連用。

這樣的話就可以避免被窮舉法破解，同時增加了安全性。

（三）弗納姆密碼

又稱一次性密碼本。用一組隨機產生、不可重複的字母當作加密金鑰，而最需要注意的是，用過一次的金鑰不能用於其他的訊息。

使用方法：

1.將每一個字母代換成數字(A=1.B=2.C=3.....)。

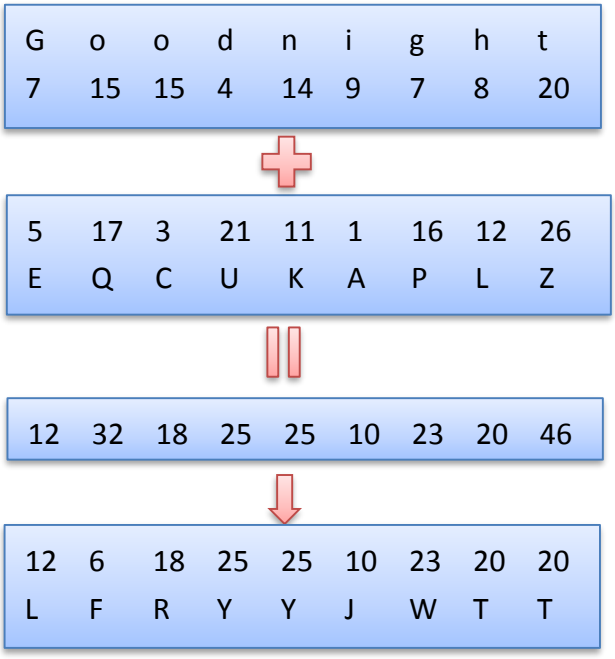
2.生產一組和明文等長且隨機的字母。

3.把明文對應的數字和金鑰對應的數字相加。

4.若相加起來大於 26，則減去 26。

5.將數字對應回字母，得到的就是密文。
6.若要解密只要把密文減去金鑰，若數字小於 0，則加 26

範例：對“Good night” 加密



弗納姆密碼最大的優點是沒有金鑰的情況下絕對安全，唯一的缺點是金鑰必定和明文等長。

改良方向：我認為在保留絕對安全的優勢前提下，這個缺點無法被修正。要縮短金鑰就必須讓隨機產生的字母產生替代規則，就會失去絕對安全這個最大的優點。

四、公開金鑰加密

利用單向函數特性（在知道x的情況下計算$f(x)$沒有問題，但逆算非常地困難，例如：$f(x)=x^{17}$）的加密方法。

用法：使用者要有一組加密金鑰和解密金鑰，加密金鑰廣泛公開，解密金鑰必須嚴格保密。想傳訊息的人使用公開的金鑰對訊息加密，然後傳給對方，讓對方使用保密的金鑰解密。

和共通金鑰最大的不同點：每個人都知道如何加密，除了有解密金鑰的人外，沒有人能在短時間內解密，從加密金鑰算出解密金鑰的時間是以數十年為單位，即使破解了也已經失去了價值。

（一）RSA 加密

根據歐拉定理（對任意正整數a .n 如果$(a,n)=1$ *則* $a^{\varphi(n)}\equiv 1(\mathrm{mod}\, n)$）和質因數分解的困難度所創造的加密方法。

使用方法：

1.找任兩相異質數a,b（通常會找幾百位數的質數）

2.$a\times b=n$

3.計算$\varphi(n)=(a-1)(b-1)$（比 n 小且和 n 互質的正整數個數）

4.隨機選出與$\varphi(n)$互質的一正整數e

5.找出一正整數d，使$ed\equiv 1(\mathrm{mod}\ \varphi(n))$

6.生成

加密金鑰：$C\equiv P^e mod\ n$ （$P<n$）

解密金鑰：$P\equiv C^d mod\ n$

7.公開(n,e)和$C\equiv P^e mod\ n$

範例：

選質數

$a=53, b=11$

$n=53\times 11=583$

$\varphi(n)=520$

令$e=17$ 則 $d=153$

假設$P=17$

$C\equiv P^e mod\ n$ （$P<n$）

$C\equiv 17^{17} mod\ 583$

$C=272$

RSA 加密的運算量過大，不適合加密過長的訊息。所以 RSA 加密經常用在保密共通金鑰的方面，是目前全世界最重要的加密法之一。隨著科技的進步 RSA 演算法也岌岌可危，全新的量子演算法很有可能會破解他，如果量子計算機發展完全的話，RSA 演算法將會走入歷史。

改良方向：如果把質數增加到 3 個的話 $\begin{cases} C\equiv P^e mod\ n \\ P\equiv C^d mod\ n \end{cases}$ 是否還會成立？

證明：$P\equiv P^{ed} mod\ n$

a,b,c為相異質數

$a\times b\times c=n$

$\varphi(n)=\varphi(a)\varphi(b)\varphi(c)=(a-1)(b-1)\ (c-1)$

$ed\equiv 1(\mathrm{mod}\ \varphi(n))\ \rightarrow\ ed=k\varphi(n)+1$

若$(P,n)=1$ 根據歐拉定理 $P^{\varphi(n)} \equiv 1 \ \ mod \ \ n$ 同乘k次方和P $P^{k\varphi(n)+1} \equiv 1^k \times P \ \ mod \ \ n$ $P^{ed} \equiv P \ \ mod \ \ n$	若$(P,n) \neq 1$ 令$P = ha$ 因$(a, b \times c) = 1$ 根據歐拉定理 $ha^{\varphi(b\times c)} \equiv 1 \ \ mod(b \times c)$ 同乘$k\varphi(a)$次方和ha $ha^{k\varphi(a)\varphi(b)\varphi(c)+1} \equiv 1^{k\varphi(a)\varphi(b)\varphi(c)} \times ha \quad mod(b \times c)$ $ha^{ed} \equiv ha \ \ mod \ \ b \times c$ $ha^{ed} = t(b \times c) + \ \ ha = t'(a \times b \times c) + \ \ ha$ (ha^{ed}可被a整除 → $t(b \times c) + \ \ ha$也可被整除) $ha^{ed} \equiv ha \ \ mod \ \ n$ $P^{ed} \equiv P \ \ mod \ \ n$

得證。

假如n的位數為三百位，n為 2 個 150 位的質數積的時候，和n為 3 個 100 位數的質數積的時候，哪一個分解的時間會比較久？403723 和 417779 做比較，$403723 = 829 \times 487$,$417779 = 97 \times 73 \times 59$，用目前效率較低的試除法來測試的話，2 個質數的比較久，所以增加質數的個數沒有太大的意義，雖然是目前分解幾百位數最有效率的方法，但那些方法分解 3 個質因數比 2 個質因數還慢的話，應該很早就有人提出並舉證了。

如何增加運算速度是所有密碼學家正在突破的地方，隨著科技的發展或許可以解決這個問題，也許未來會誕生量子演算法的密碼來取代它。

五、比較

	共通金鑰加密	公開金鑰加密
優點	1. 計算速度快 2. 金鑰夠複雜將難以破解	1. 沒有運送金鑰的問題
缺點	1. 運送金鑰問題 2. 多人互傳訊息，金鑰數量會大增	1. 計算速度慢

	替代式密碼	移位密碼	弗納姆密碼	RSA 加密
優點	金鑰製作簡單		絕對安全	適合短訊息加密
缺點	密文越長，破解機率越大		金鑰和明文一樣長	運算速度慢
破解法	頻率分析	窮舉證法	沒有金鑰無法破解	量子演算法

改良方向	破壞一對一對應關係	和其他方法連用	不犧牲優點 缺點無法修正	提高運算速度

叁●結論

所有的加密法都有各自的優點和缺點，有時這些方法搭配使用可能達到更好的安全性，就像用公開金鑰的優點去彌補共通金鑰的缺點。現在的密碼學有電腦幫忙，運算量可以越來越大，運算速度也越來越快，未來運算量極大的密碼遲早會被破解，就像 RSA 演算法一樣，我認為密碼學朝向針對計算機運算上的缺失而進行加密的方向發展，是大有可為的！

肆●引註資料

註一：莎拉 • 夫蘭納里、大衛 • 夫蘭納里（2001）。**數學小魔女**。天下文化。

註二：三谷政昭、佐藤伸一（2009）。**世界第一簡單密碼學**。世茂出版。

註三：中國科技大學教學資源平台。李文立（2011），第一單元：密碼學。2015 年 11 月 8 日，取自：
http://192.192.161.79/LinkClick.aspx?fileticket=mdmVkvF%2BjmM%3D&tabid=549&language=zh-TW