市立陽明高中107學年度科展作品說明書

作品名稱：密碼學

科別：數學科

關鍵字： 古典密碼學、近代密碼學

壹、摘要

密碼學可分為古典密碼學以及近代密碼學。而古典密碼學大多用於軍事上，因此主要是以訊息的保密書寫及傳遞為主，以及相對應的破解方法。如今，近代密碼學，不僅僅著重於資訊的保密問題，同時還著重於資訊的完整性驗證(例如：訊息驗證碼)、資訊的不可抵賴性(例如：數位簽章)，以及分散式計算中所產生來源於內部或外部攻擊的所有資訊安全問題。

密碼學是數學及電腦科學的分支，而密碼學的發展促使電腦科學日益發達，與此同時，它也已經應用在日常生活上，例如：自動櫃員機的晶片卡、電腦使用者存取密碼、電子商務等。

貳、研究動機

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，當今資訊網路的時代，各式各樣的訊息在網路中傳遞，若沒有經過任何加密措施，這些資訊就毫無保護的洩露給有意者，而密碼的重要性當然就或不可缺。但由於現今的科技發達，加密後的訊息是否真的不會被人破解，這還是存留著一個疑問。

參、研究目的

我們透過了解密碼學古至今的演變，來加以探討密碼的安全性，並對其做比較，使我們對於密碼這個虛擬的區塊有更深的了解。

肆、研究設備及器材

一．電腦

二．密碼棒之模型

伍、研究過程或方法

(一)利用石膏塊刻成木棒狀模擬密碼棒的樣子，再以長條狀的紙寫好明文，並纏繞於密碼棒上，纏繞後則會得到密文

(二)使用 DES 加密系統做出一個密碼，並嘗試破解

明文

Well begun is half done.

密文

U2FsdGVkX19g2ivxPoMyGVgx9L3eD2yR92rXvbhVSogckxEdCPzJLIZyvVAATMrC

(三)使用 RSA 加密系統做出一個密碼，並嘗試破解

明文

Well begun is half done.

密文

bpYJlmedqihOYFKdCTWx/35qCKahyVOms+uZ/vxeHYdxX6LsDxBuRzpYTagT+heqtExFD+qa6W657
OfWj7ZfpDe5+YC315sIevjIyTVE7vAM/c0qDKajI5EFDX4Q/RIVMejweEriVlYXLzSYfMpGhVncbH/d
XWiXdPzBJLZhi7g=

(四)最後再以這三種密碼加密系統作比較，並且設計出一個密碼

先由 Triple DES 加密，再將加密後的密文由 RSA 進行加密，之後在把加密後的密文由 AES 進行加密，加密完即為所要的密文

明文

Well begun is half done.

以 Triple DES 加密

U2FsdGVkX19TLURZ4DBRyCw7pQnohAoFKZVov2eEgYyKYghMJAsTUjihMrZLEAJu

再以 RSA 加密

P7Vt+CM12H475aYRI3ix/yjHC+VnVHZJEgC5/YcGmdiefudshoS3WUn+37kUacaaCAttu55
StLyuRSUDRb9ebtxI+RmvAC8E2urLdGGUrKbaT4J4kfbTVxLgqje+LDZWOKlo2bAiiyaM
VJVFWcZBHG9sn6iwqLycmkWtUbp4WKGXv8wQXJ0a64R95SU0jB0bcESGYus6Am6a1D
lnZp6AfykOyTD2GDKa5/U5JnRZMmd/IOwzEWSfixlZEeHZ4OzPP73yP9Pr174n2GnBw4Q
NSWq7CCbCwViMEDoVEHgCti9b1SAFrUU0A2VeFd9nF4Uls6vmGjL6/sWvMwK6HF4/Jg
==

再以 AES 加密

U2FsdGVkX1/dhSvZ5Bk8nCSuSVhwFMHWXlq5JOFZYzt5DNTuB8eV9nuIdOY3ner4
9Uxok/lLvu/y1J6E3pSy2lGMMsp5rxzzcYuc0B5Va9HoRgZimSfhDBtfHC7XXmqf
N+XqljvxLMbESz+m9LOWiz5/MH+Go5le8AqciOcfzp2yEaaJqimuIIdtQObxf9xJ
h8ySxU22Zmi1JUr1lV7rhgNnKgpZwCSg59jZOO6IZ6dPmeWyqYvUPLMZ2Dfj9mLU

ESzIUIsVNFUgffbrygySPyjYqQE5GyDwvqYI+E3hWc9gwqn76O0qHwNz3WlAHkW8

dMUdQvPO3zTUp9xlquVclOTbdm2kkD6SAaQl4otxRJos0M8atU3cV/nbGPUzUp8d

aa4mJK/NRRcVEeQV2h5Cg2ZGBcGZzZwEAol0c7Iixqm5lWVkmbY4inHwZPSKF5Jt

TSCWf9ZknN7V3NbHZOvMgpogx214W4IIV2iCJVfDFws=

陸、研究結果

- 古典密碼

1、摩斯密碼

是一種訊號程式碼，通過不同的排列順序來表達不同的英文字母、數字及文字符號

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 _ _ . .	1 . _ _ _ _	2 . . _ _ _	3 . . . _ _	4 . . . . _
5	6 _	7 _ _ . . .	8 _ _ _ . .	9 _ _ _ _ .
0 _ _ _ _ _	• ._._._	，_ _ . . _ _	： _ _ _ . . .	？ . . _ _ . .
- _ . . . _	/ _ . . _ .	= _ . . . _	() _ . _ _ . _	

2、凱薩密碼

將明文使用的英文字母，固定位移一定的字數，進行加密

Ex: 密鑰為位移兩個字母

明文 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 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 b

3、Vigenère 密碼

為凱薩密碼的延伸，是由一系列交織的凱薩密碼文本，利用關鍵字，是一種多字母替代形式

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

4、阿特巴希密碼

出現在聖經中，由希伯來字母使用的簡易替換字母。密碼學上的示沙克之謎出現在<<耶利米書>>中，而示沙克其實是加密後的巴別(巴比倫)

A	B	G	D	H	V	Z	Ch	T	Y	K
Th	Sh	R	Q	Tz	P	O	S	N	M	L

5、凱薩完全平方密碼盒

為凱薩大帝慣用的一種利用『完全平方』的密碼宮格編碼方式

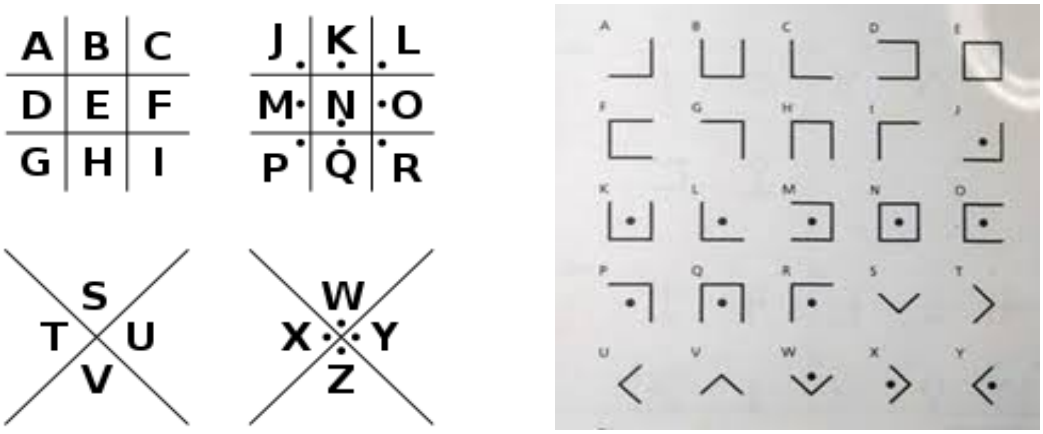
Ex： 明文： I DONT KNOW

I	D	O
N	T	K
N	O	W

密文： INNDTOOKW

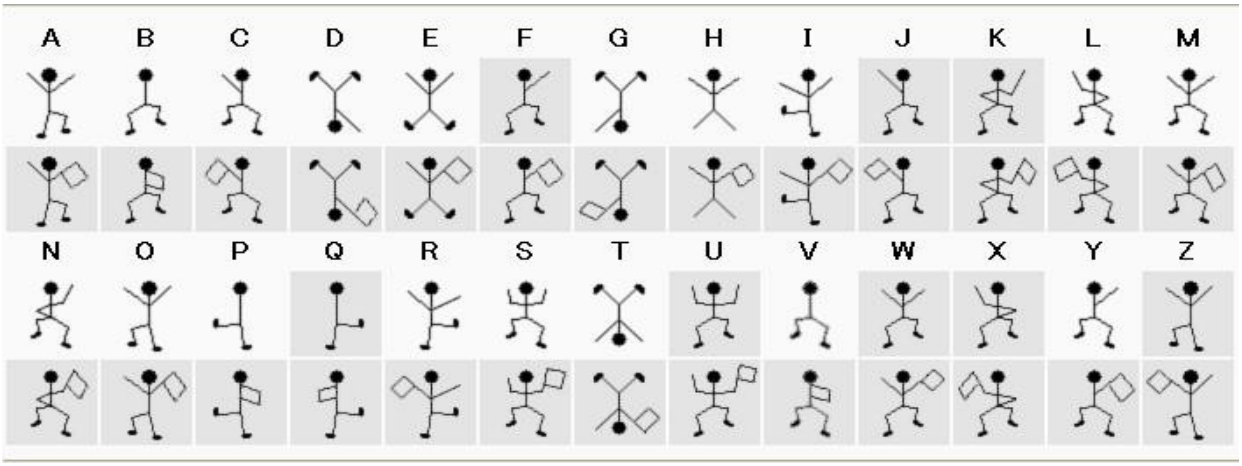
6、豬圈密碼(共濟會密碼)

是一種以格子為基礎的替代式密碼，即使使用符號，也不會影響到密碼分析



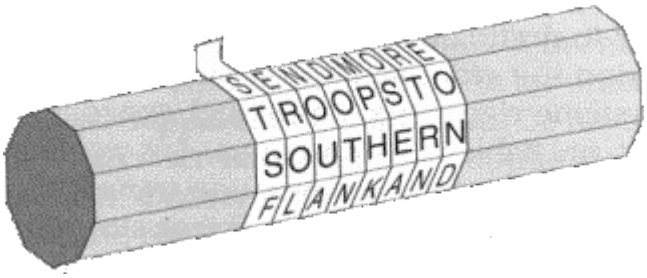
7、福爾摩斯-跳舞的小人

出自於柯南・道爾的小說<福爾摩斯>一書，其中的小舞人探案



8、密碼棒(scytale)

是個可使傳遞訊息字母順序改變的工具，由一條加工過、且有夾帶訊息的皮革繞在一個木棒所組成



- **近代密碼**

1.對稱密鑰加密（Symmetric-key algorithm）

又稱為對稱加密、私鑰加密、共用密鑰加密，是密碼學中的一類加密演算法。

這類演算法在加密和解密時使用相同的密鑰，或是使用兩個可以簡單地相互推算的密鑰。常見的對稱加密演算法有 DES、3DES、AES、Blowfish、IDEA、RC5、RC6。

2.區塊加密(Block cipher)

	名稱	優點	缺點	備註
ECB模式	Electric CodeBook 電子密碼書模式	・簡單 ・快速 ・可同步處理(加密、解密)	・明文中的重覆部分會反應在密文上 ・可利用刪除或調動密文區塊來操控明文 ・出現位元錯誤的密文，經過解密之後，對應的區塊就會出現錯誤 ・可能遭受到重送攻擊	・不建議使用 ・機密性最低的一種模式
CBC模式	Cipher Block Chaining 密碼區塊鏈結模式	・明文中的重覆部分不會反應在密文上 ・可同步處理(僅限解密) ・可解密任意密文區塊	・出現位元錯誤的密文解密之後，整個區塊及下個區塊對應的位元會出現錯誤 ・加密時無法進行同步處理	・CRYPTREC建議使用 ・Practical Cryptography建議使用
CFB模式	Cipher-FeedBack 密碼回饋模式	・不需要執行填補處理 ・可同步處理(僅限解密) ・可解密任意密文區塊	・加密時無法進行同步處理 ・出現位元錯誤的密文，經過解密之後，整個區塊及下個區塊對應的位元會出現錯誤 ・可能遭受到重送攻擊	・CRYPTREC建議使用
OFB	Output-FeedBack 輸出回饋模式	・不需要執行填補處理 ・可以進行加密、	・無法進行同步處理 ・主動式攻擊者	・CRYPTREC建議使用

模式		解密的事前準備工作 ・加密與解密的結構相同 ・出現位元錯誤的密文解密之後，只有明文對應的位元會出現錯誤	若反轉密文區塊的位元，對應的明文區塊也會出現位元反轉	
CTR模式	CounTeR 計數器模式	・不需要執行填補處理 ・可以進行加密、解密的事前準備工作 ・加密與解密的結構相同 ・出現位元錯誤的密文解密之後，只有明文對應的位元會出現錯誤 ・可同步處理(加密、解密)	・主動式攻擊者若反轉密文區塊的位元，對應的明文區塊也會出現位元反轉	・CRYPTREC建議使用 ・Cryptography建議使用

3.非對稱加密 （asymmetric cryptography）

又稱公開金鑰加密（Public-key cryptography），是密碼學的一種演算法，它需要兩個金鑰，一個是公開密鑰，另一個是私有密鑰；一個用作加密的時候，另一個則用作解密。使用其中一個金鑰把明文加密後所得的密文，只能用相對應的另一個金鑰才能解密得到原本的明文；甚至連最初用來加密的密鑰也不能用作解密。雖然兩個密鑰在數學上相關，但如果知道了其中一個，並不能憑此計算出另外一個；因此其中一個可以公開，稱為公鑰，任意向外發布；不公開的金鑰為私鑰，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，也不會透露給要通訊的另一方。

名稱	對稱加密	非對稱加密
別名	秘密金鑰加密	公開金鑰加密
金鑰	加密與解密使用相同金鑰	加密與解密使用不同金鑰
金鑰保存	秘密金鑰不可公開	私密金鑰不可公開 公開金鑰必須公開
金鑰數目	與多人交換資料則必須保管多把秘密金鑰	無論與多少人交換資料只需保管私密金鑰

加密速度	演算法較簡單 速度較快	演算法較複雜 速度較慢
應用	用來加密較長的資料 例如:電子郵件	用來加密較短的資料 例如:數位簽章

柒、討論

明文在加密過後形成密文，要以什麼方式破解密碼，並且能達到最快速度破解出來，而古今中外擁有不可勝數且各式各樣的密碼，要如何選擇才是最安全的。科技的發達是否會使密碼更容易出現破綻導致密碼的安全性下降，然而，自製密碼是否就真的安全。這些問題都是我們要去探討的。

捌、結論

雖說密碼與時俱進，但同時破解密碼的手法也如此。至今，線性分析法為最快數破解密碼的一種方式，比早期的暴力破解法還快上許多，但仍有一些密碼至今尚未破解，不過我們也極少採用。而我們現在最常使用的莫過於公鑰密碼，擁有兩把不同金鑰，不必擔心私密金鑰被知道、密文被破解。但始終科技帶給我們便利，同時也會帶來一些威脅，密碼的安全性必然會降低，而使用脆弱的密碼比不使用密碼來的危險，也不要使用不公開的密碼，倘若是重大機密，使用這樣的加密系統，一旦被破壞，後果不堪設想，我們應該要使用公開且強大的加密系統，即使使用多重加密系統加密，一樣會出現破綻。

玖、參考資料及其他

網址

https://zh.wikipedia.org/wiki/%E5%AF%86%E7%A0%81%E5%AD%A6#%E7%8F%BE%E4%BB%A3%E5%AF%86%E7%A2%BC%E5%AD%B8_2

https://zh.wikipedia.org/wiki/%E5%85%AC%E5%BC%80%E5%AF%86%E9%92%A5%E5%8A%A0%E5%AF%86

https://zh.wikipedia.org/wiki/%E5%B0%8D%E7%A8%B1%E5%AF%86%E9%91%B0%E5%8A%A0%E5%AF%86

書籍:近代密碼學與其應用 鍾慶豐 著

書籍:密碼學與比特幣原理 結城浩 著