

密碼學



(圖片來源:CommuniLink 聯絡國際網路)

班級:213

座號:06

學號:811412

姓名:范心瑜

目錄

學習動機.....	3
內文	
1. 密碼學是什麼?	3
2. 為什麼需要密碼學?	3
3. 密碼學的目的.....	3
4. 密碼學史.....	4、5
5. 密碼學基本判讀與運算介紹.....	5、6
6. 密碼學常見詞彙介紹.....	7
7. 加密流程.....	7
8. 密碼學應用.....	8
9. 自製密碼盒成品展示.....	8
結論與心得.....	9
參考資料.....	9

學習動機：

之前上數學課時，我曾經聽到數學老師說密碼學與數學有密不可分的關係，這令我感到十分新奇、有趣，那陣子剛好又看到了一部與密碼學相關的電影——模仿遊戲，因此使我產生了興趣，想要一探究竟密碼學的奧秘。

內文：

密碼學是什麼？——

密碼學，是一門將信息進行加密處理與傳遞，以及 分析加密信息的學科。

密碼學分為古典密碼學與現代密碼學兩部分。古典密碼學以「置換法」與「替換法」為基礎，多應用於軍事與情報領域；現代密碼學則是建立在數學、計算機與通信科學的基礎上。

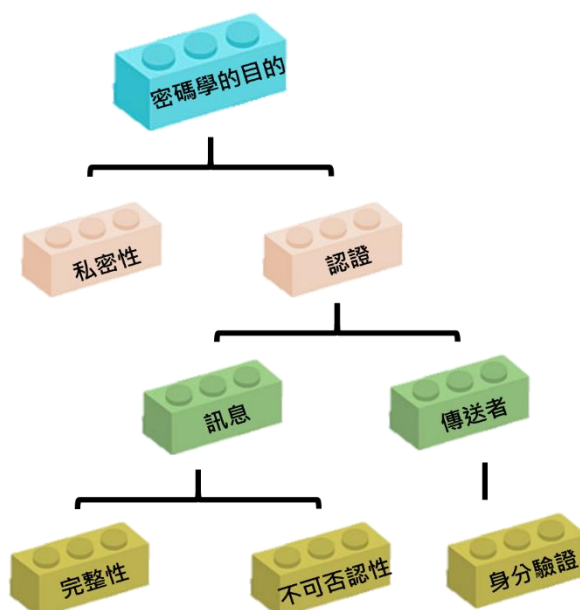
為什麼需要密碼學？——

- 【一】提供驗證識別
- 【二】確保資訊的私密性
- 【三】偵測資料是否被不當的竄改
- 【四】提供資訊傳送來源、接收目的或交易的證明



（圖片來源：集圖網）

密碼學的目的——



密碼學史——

【一】

公元前 1900 年左右的古埃及，已經出現過使用特殊字符和簡易替換式的密碼來保護信息。

【二】

美索不達米亞平原曾經出土過一個公元前 1500 年左右的泥板，其上記錄了加密描述的陶器上釉工藝配方。

【三】

古希臘時期（公元前 800~前 146 年）發明出通過物理手段來隱藏信息的“隱寫術”。

【四】

後來在古羅馬時期還出現了基於替換加密的凱撒密碼，據說凱撒曾使用過此方法和其他部下通信而得以命名。

【五】

現代密碼的研究是在第一次和第二次世界大戰中，軍事為使通信內容進行保護和破解而衍生出來的。

【六】

1901 年 12 月，意大利工程師奎里亞摩·馬可尼成功完成了跨越大西洋的無線電通信實驗，在全球範圍內造成轟動，也因此推動了無線電通信。無線電極大提高了遠距離通信的能力，但其中還存在著缺陷——它很難控制接收的對象，這也就意味著要想保護所傳遞信息的安全，必須採用可靠的加密技術。而對無線電信息進行加密以及破解的過程直接促進了近現代密碼學和計算機技術的出現。

【七】

一戰時期德國外交部長阿瑟·齊默爾曼拉攏墨西哥構成抗美軍事同盟的電報（1917 年 1 月 16 日）被英國情報機構——40 號辦公室破譯，直接導致了美國的參戰；二戰時期德國使用的恩尼格瑪密碼機被盟軍成功破譯（1939 年到 1941 年），造成了大西洋戰役德國失敗。

【八】

1945 年 9 月 1 日，克勞德·艾爾伍德·香農完成了劃時代的內部報告《A Mathematical Theory of Cryptography》，1949 年 10 月，該報告以《Communication Theory of Secrecy Systems》為題在貝爾系統技術期刊上正式發表。這篇論文首次將密碼學和信息論聯繫到一起，並且對密碼技術提供了數學基礎。這也表示著近現代密碼學的正式建立。

註：《A Mathematical Theory of Cryptography》（密碼術的一個數學理論）

《Communication Theory of Secrecy Systems》（保密系統的通信理論）

【九】

1976 年 11 月，Whitfield Diffie 和 Martin E. Hellman 在 IEEE Transactions on Information Theory 上發表了論文《New Directions in Cryptography》，探討了無需傳輸密鑰的保密通信和簽名認證體系問題，正式開創了現代公鑰密碼學體系的研究。

註：《New Directions in Cryptography》（密碼學的新方向）

密碼學基本判讀與運算介紹——

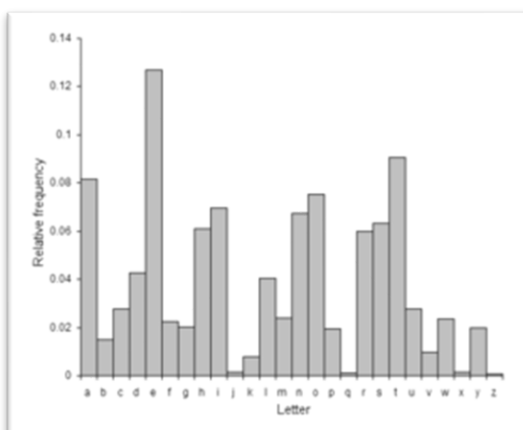
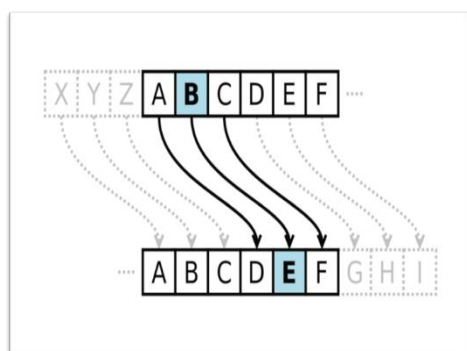
【一】密碼學基本判讀（古典密碼學）

（一）凱薩密碼

用替換加密方式加密。

凱薩密碼解密方法：

將英文字母往後移 3 位，然後重新讀取即可。



（二）維吉尼亞密碼

維吉尼亞密碼由一些偏移量不同的凱撒密碼所組成，屬於多表密碼的一種簡單形式，為了生成密碼，需要使用表格法。這一表格包括了 26 行字母表，每一行都由前一行向左偏移一位得到。具體使用哪一行字母表進行編譯是基於密鑰進行的，在過程中會不斷地變換。

	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

維吉尼亞密碼解法：

維吉尼亞密碼必須先有一个密鑰(由字母组成)，然後根據已知的密文與密鑰進行回推，即可得到其明文。

舉例：

	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

假設密文為 H

密鑰為 S

明文為 L

【二】密碼學基本運算

(一) 質因數

有些密碼會藉由極大數進行質因數分解創造出密碼來

Ex: RSA……

密碼學常見詞彙介紹——

【一】加密

將明文資訊改為難以讀取的密文內容。

【二】解密

給經過加密的信息去除密碼，使其還原成加密前的狀態，以便獲取信息。

【三】明文

未經過加密的訊息。

【四】密文

對明文加密後的訊息。

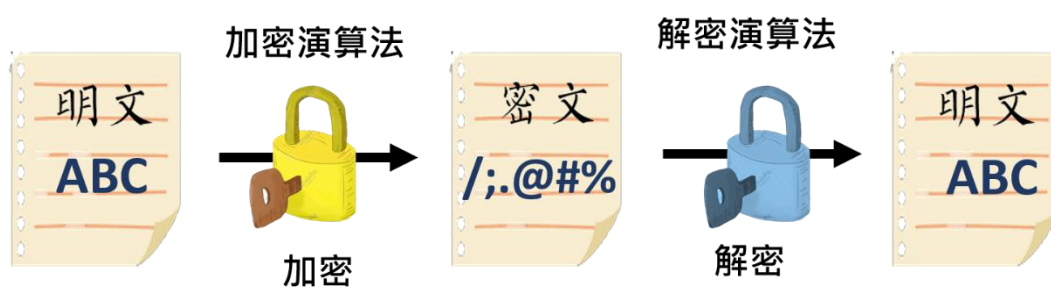
【五】金鑰/密鑰

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。

【六】密碼學演算法

做與密碼學相關程序(如加密、解密、簽章……)的演算法。

加密流程——



密碼學應用——

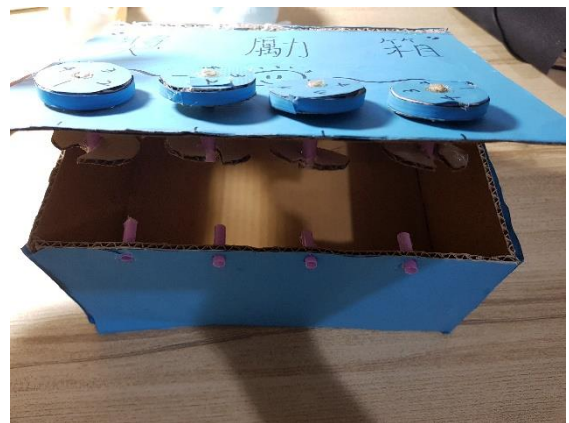
【一】涉及密碼學的相關職業

- (一) 軟體設計工程師
- (二) 軟體設計工程師
- (三) Internet 程式設計師
- (四) 演算法開發工程師
- (五) 韌體設計工程師
- (六) 網路安全分析師……

【二】與密碼學相關的生活常見事物

- (一) 信用卡
- (二) 電腦密碼
- (三) 一維條碼
- (四) 二維條碼(QR code)……

自製密碼盒成品展示——



密碼盒開關影片：<https://www.youtube.com/watch?v=X4VZwn3vQHE>

結論與心得：

藉由這次的自主學習，我不但了解到密碼對我們的重要性，還得知了整個密碼學的演變史，再踏進這門知識之前，我都從未了解到訊息在傳遞之前其實已經發生過加密了，這使我們的訊息可以安全的傳送到接收方，不會使自己的隱私曝露出來。

也因為探索密碼學讓我對自己有了新的認知，我發現我十分喜歡解謎和設計謎題，雖然這次學到的數學比較少，但我卻收穫了新的想法，我忽然覺得數學的應用不在是我想的那樣無趣，反而是既新奇又新穎。這讓我對數學有了更多的學習動力。

參考資料：

1. 鏈聞 CHAINNEWS

<https://www.chainnews.com/zh-hant/articles/577594859080.htm>

2. 區塊鏈技術指南-繁中

<https://poweichen.gitbook.io/blockchain-guide-zh/crypto/history>

3. 數學小魔女(書)

4. C8_ppt. PDF

<http://avp.toko.edu.tw/docs/class/3/%E5%AF%86%E7%A2%BC%E5%ADB8%E5%8E%9F%E7%90%86%E8%88%87%E6%8A%80%E8%A1%93.pdf>

5. 一分鐘講不完的密碼(影片)

<https://www.bilibili.com/video/av71024212/>

6. POLLY PENG

<https://yellowgirl3614.medium.com/%E5%AF%86%E7%A2%BC%E5%ADB8-%E4%B8%80-%E5%8F%A4%E5%85%B8%E5%AF%86%E7%A2%BC%E5%ADB8-455e43038241>

7. d1_s2_r4. pdf

https://hitcon.org/2018/CMT/slide-files/d1_s2_r4.pdf