



你有秘密嗎？

揭開密碼學的幕後



姓名：范心瑜
班級：2年13班
座號：06
學號：811412



目錄

01

前情提要
遊戲探索

02

密碼相關電影
電影介紹

03

密碼學的基本
判讀與計算

密碼對照方法
與質因數計算解密

04

密碼學介紹
密碼學是甚麼？

05

密碼學的應用
密碼學生活中
哪裡可以看到？

06

密碼學史
密碼設計學
的演變

01

前情提要
遊戲探索

遊戲探索

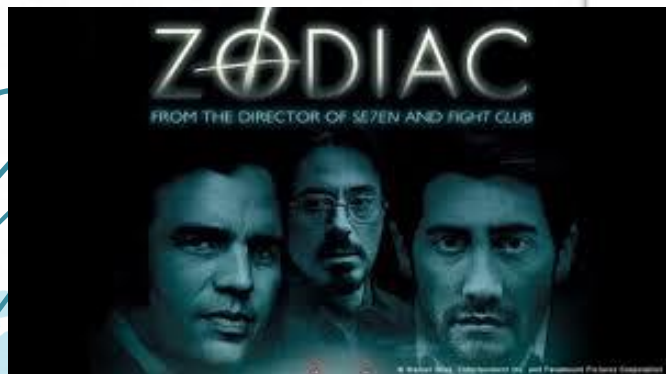
問題1:

VW DU



遊戲探索

問題2:



【落日殺神】馬克盧法洛 【斷背山】傑克葛倫霍 【心機掃描】小勞勃道尼

當密碼殺人魔橫肆加州，只有一個人看透所有玄機

【火線追緝令】【門陣俱樂部】導演 最新力作

ZODIAC

索命黃道帶

根據真實案改編

5月18日(週五)晚場起

www.zodiacmovie.com.tw

SEARCHING FOR THE ZODIAC
THE TRUE STORY OF AN AMERICAN HORROR

Produced & Directed by David Twohy Screenplay by Scott Chisum & Michael Crichton

02

密碼相關電影
電影介紹

模仿 遊戲



M4 ENIGMA



03

密碼學的基本

判讀與計算

密碼對照方法

與質因數計算解密

古典密碼學

質因數

$$213 = ? \times ?$$

古典密碼學

質因數

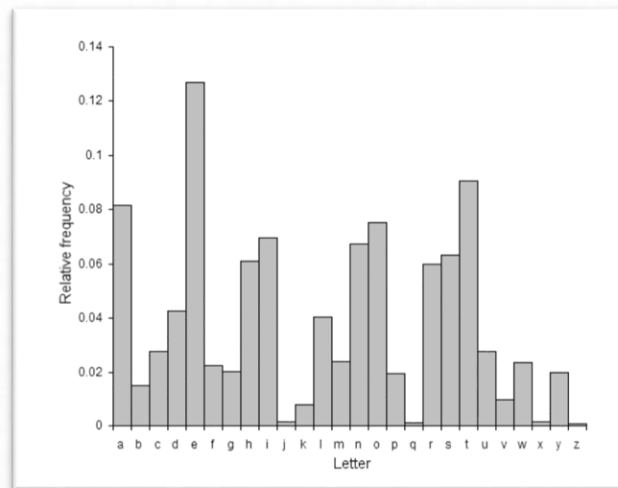
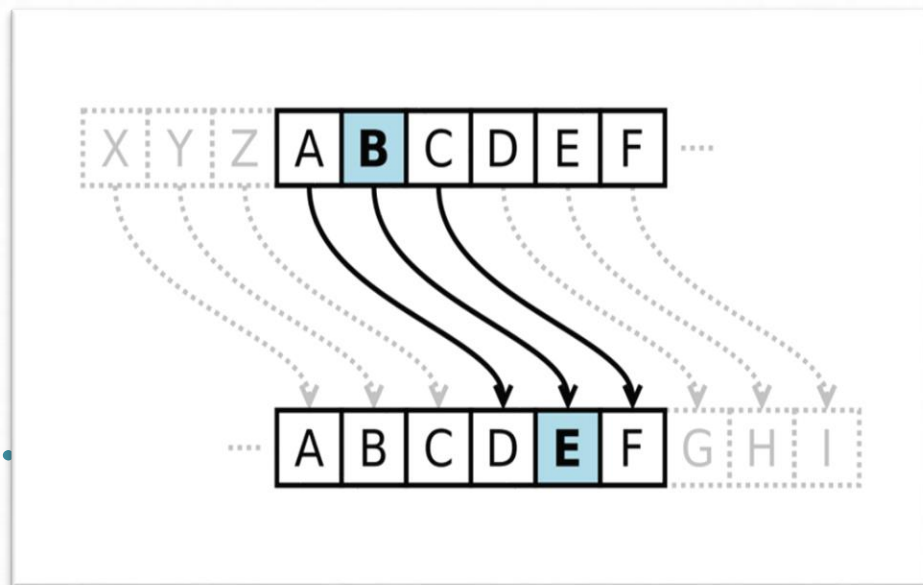
$$14910 = ? \times ? \times \dots$$

古典密碼學

凱薩密碼

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。



古典密碼學

維吉尼亞密碼

	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

維吉尼亞密碼解密方法:

維吉尼亞密碼必須先有一個密鑰(由字母組成)，然後根據已知的密文與密鑰進行回推，即可得到其明文。

假設密文為H

密鑰為S

明文為L

03

密碼學介紹
密碼學是甚麼？

密碼學介紹

古典密碼學

現代密碼學

很多數學

密碼

密碼學



密碼學介紹

常見詞彙解釋



加密

將明文經過某種
程序轉換成密文



密文

加密後的訊息



解密

將密文經過某種
程序轉換成明文



金鑰 / 密鑰 Key

加解密時所使用的
「鑰匙」



明文

加密前的訊息



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



男A



step1



男B



step2

step3



04

密碼學的應用

密碼學生活中

哪裡可以看到？

密碼學的應用



職業

- 軟體設計工程師
- Internet程式設計師
- 演算法開發工程師
- 韌體設計工程師
- 網路安全分析師.....



生活常見的事物

信用卡、
電腦密碼、
一維條碼、
二維條碼(QR code).....



05

密碼學史

密碼設計學的演變

密碼設計學史

公元前
1900
年

古埃及出現特殊字
符和簡易替換式的
密碼來保護信息

公元前
800-146
年

發明出隱藏信息
的“隱寫術”

第一二次
世界大戰

軍事為使通信內容進
行保護和破解而衍生
出來現代密碼學。

1945
年

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**》

1976
年

正式開創了現代
公鑰密碼學體系
的研究

1949
年

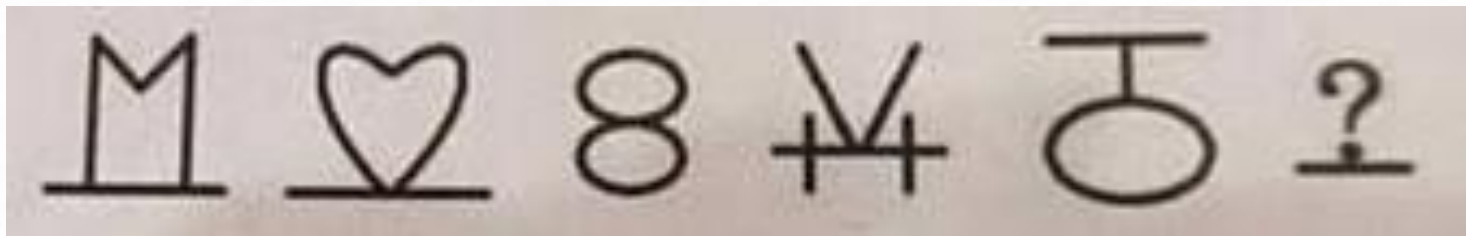
《**Communication Theory of
Secrecy Systems**》這篇論文首
次將密碼學和信息論聯繫到一起，並
且對密碼技術提供了數學基礎。



猜猜密碼大挑戰

(課後練習)

猜猜看最後一個圖形是什麼？



解答

06

猜猜密碼大挑戰

(課後練習)

1 8 88 101 ?

解答

111

參考網址

- <https://www.chainnews.com/zh-hant/articles/841515752915.htm>
- <https://djj.ee.ntu.edu.tw>
- <https://zh.wikipedia.org/wiki/%E5%AF%86%E7%A0%81%E5%AD%A6Current>
- https://hitcon.org/2018/CMT/slide-files/d1_s2_r4.pdf
- <https://medium.com/@yellowgirl3614/%E5%AF%86%E7%A2%BC%E5%AD%B8-%E4%B8%80-%E5%8F%A4%E5%85%B8%E5%AF%86%E7%A2%BC%E5%AD%B8-455e43038241>



THANKS