基礎密碼學 (一)

- 密碼學基本概念
- 早期密碼系統
- 近代密碼系統

密碼學基本概念

- 什麼是資料***加密***?
  - 將資料以特定方式予以***重新排列***、***打亂***或***隱藏***於負載媒體中
- 資料為什麼要加密?
  - 網路傳遞機密資訊易被***竊聽***。因此，對機密資料存入磁碟、備援磁帶或傳遞網路前，先加密成***密文***，使未經授權人員不能得知其內容
- 密碼學是一種藝術
  - 加密 + 解密
  - 加密 ➔ 容易
  - 解密➔ 難如登天

密碼學基本概念 (Cont.)

- 密碼系統依應用可提供下列功能
  - ***秘密性***(Secrecy or Privacy)：防止未被授權者發現明文
  - ***鑑定性***(Authenticity)：確定資訊來源的合法性
  - ***完整性***(Integrity)：確定資訊沒有被有意或無意的更改
  - ***不可否認性***(Nonrepudiation)：發送方在事後不可否認其傳送過的資訊
- 保密技術的價值
  - 保密程度 → 越高越好
  - 金鑰大小 → 越小越好

密碼學基本概念 (Cont.)

- 加解密運算的複雜度 → 越簡單越好
- 明文擴充 → 越少越好

- 測試加密系統的方式
  - ***只知密文攻擊*** (Cipher-text-only attack)：僅知密文而還原成明文，現代密碼學下不易成功
  - ***已知明文攻擊*** (Known-plaintext attack)：知道加密前的明文及加密後的密文，藉此推算出加密金鑰

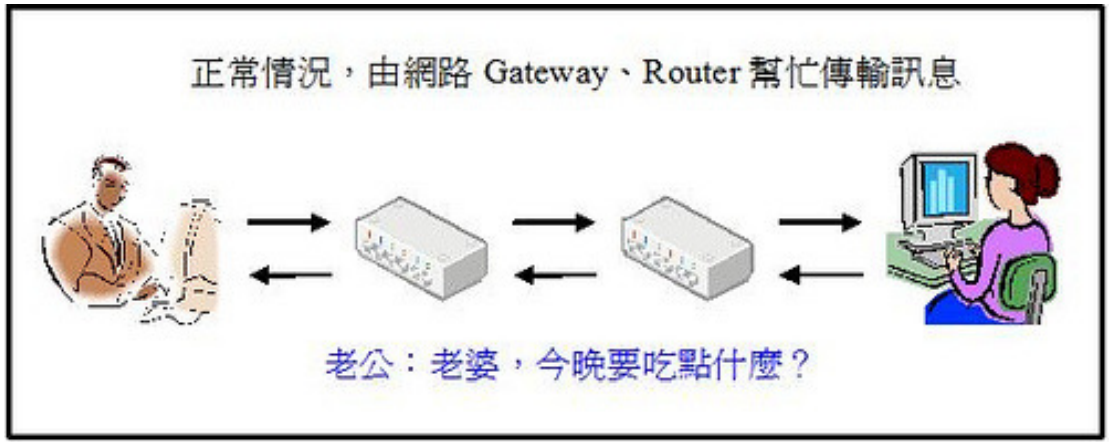
密碼學基本概念 (Cont.)

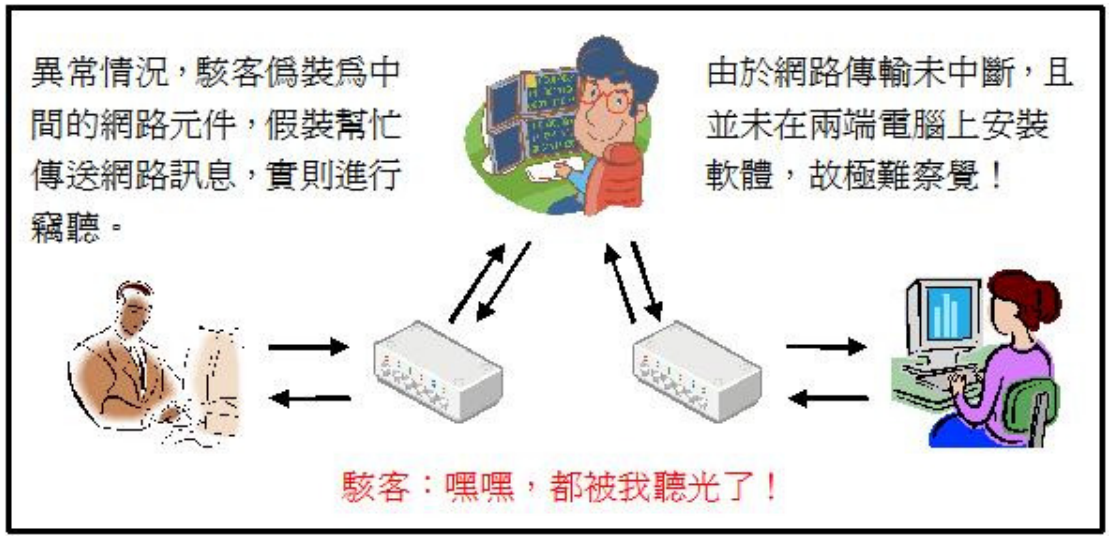
- ***選擇密文攻擊*** (Chosen-cipher-text attack)：藉由自選的密文及其相對應的明文以求得其他密文的明文
- ***選擇明文攻擊*** (Chosen-plain-text attack)：藉由自己的明文及其相對應的密文以求得其他密文的明文

- 密碼攻擊技巧
  - ***窮舉法攻擊*** (Brute-force attack)：依加密金鑰的長度進行所有排列組合嚐試
  - ***字典攻擊*** (Dictionary attack)：一般使用者設定密碼通常不夠亂，且長以易記憶的字串為主

密碼學基本概念 (Cont.)

- 中間人攻擊 (Man in the meddle attack



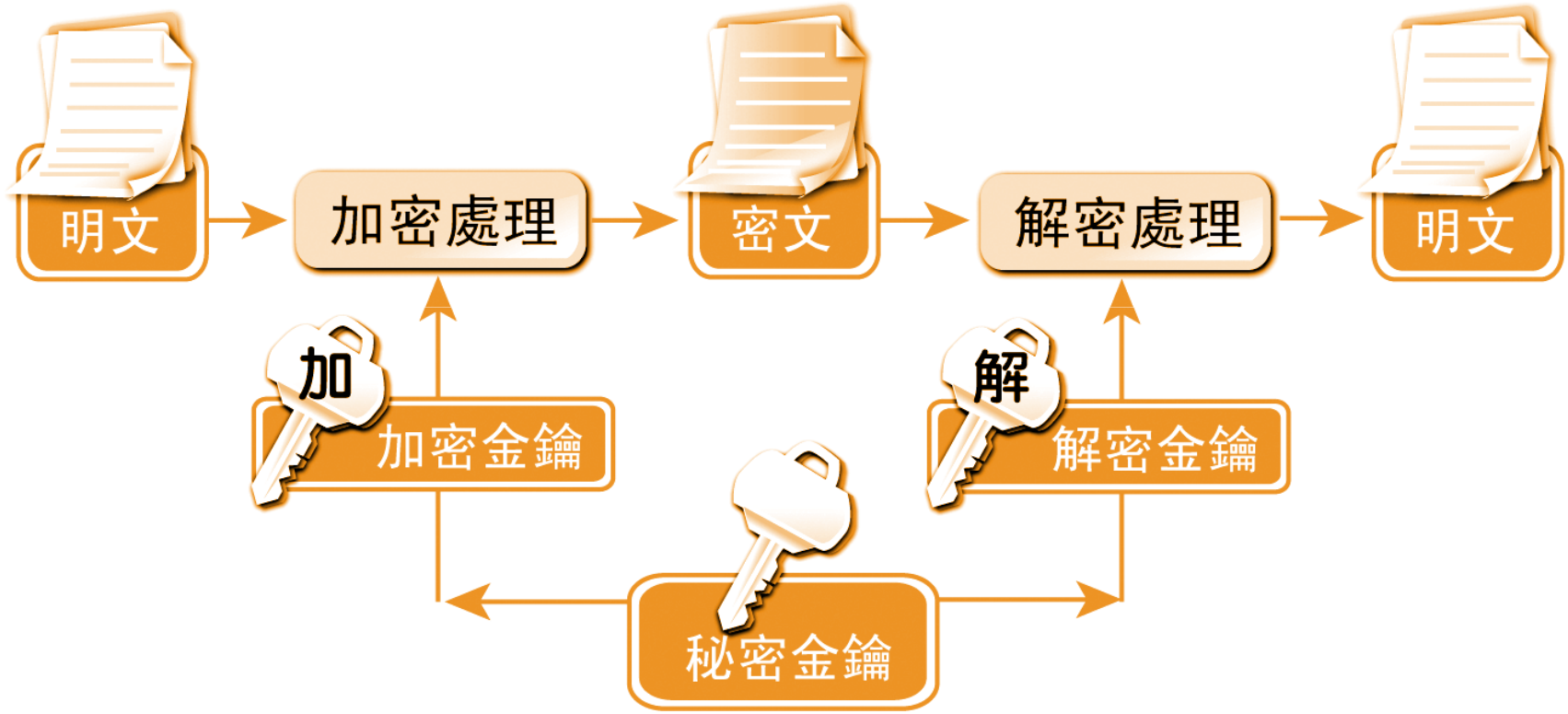


資料來源：http://mmdays.com/2008/11/10/mitm/

密碼學基本概念 (Cont.)

- 解密
  - 將加密後的訊息反打亂變成可閱讀的訊息
- 加解密系統
  - 收送雙方須先溝通好加解密方式
  - 使用者即使知道加密協定，在其不知道金鑰的情況下在有限時間內無法解得正確訊息

密碼學基本概念 (Cont.)



密碼學基本概念 (Cont.)

E：加密演算法

D：解密演算法

K：金鑰

M：明文

加密公式：

$$C = E_K(M)$$

解密公式：

$$D_K(C) = D_K(E_K(M)) = M$$

密碼學基本概念 (Cont.)

- 為什麼加密方法或演算法必須公開
  - 較不佔空間
  - 未公開的加解密演算法也難保其安全
  - 相容性的問題
- 密碼系統的安全性程度
  - ***無條件安全***(Unconditionally Secure)
    - 未被授權使用者不管截獲多少個密文，用盡各種方法還是沒有足夠資訊可以導出明文之機密資料
  - ***計算安全***(Computationally Secure)
    - 目前或未來預測之科技、在合理之資源設備下，要破解密碼系統需要一段相當長的時間（例如數百年）

無條件安全密碼系統

- 二進制的基本運算
  - AND
    $$\begin{array}{r} 1101 \\ 1001 \\ \hline 1001 \end{array}$$
  - OR
    $$\begin{array}{r} 1101 \\ 1001 \\ \hline 1101 \end{array}$$
  - XOR
    $$\begin{array}{r} 1101 \\ 1001 \\ \hline 0100 \end{array}$$
- 這三種運算的差別在哪?

無條件安全密碼系統 (Cont.)

- 以XOR加密
  - 將明文轉換成ASCII碼
    - A DOG ==> 065 032 068 079 071
  - 將ASCII碼轉成二進制
    - 0100 0001, 0100 0100, 0100 1111, 0100 0111

A D O G

  - 以加密金鑰(1111 0111)進行XOR 加密運算

01000001	01000100	01001111	01000111
11110111	11110111	11110111	11110111
10110110	10110011	10111000	10110000

無條件安全密碼系統 (Cont.)

- 以XOR解密
  - 以解密金鑰(1111 0111)進行XOR 解密運算

10110110	10110011	10111000	10110000
11110111	11110111	11110111	11110111
01000001	01000100	01001111	01000111

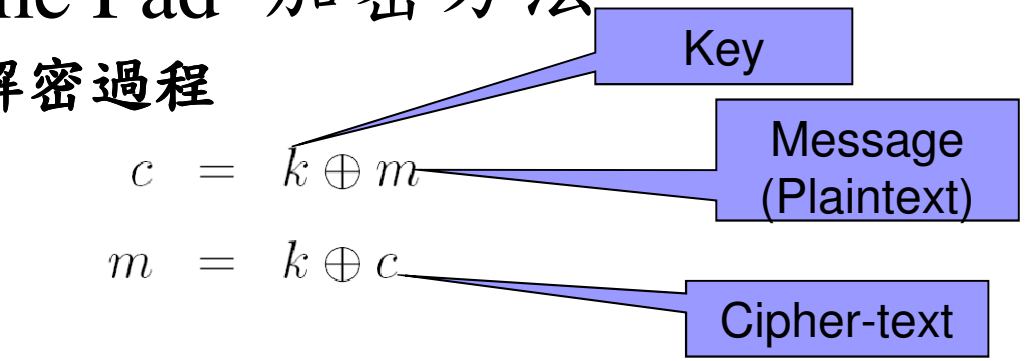
- 將二進制轉成ASCII碼
  - 0100 0001, 0100 0100, 0100 1111, 0100 0111

A D O G

無條件安全密碼系統 (Cont.)

One-time Pad 加密方法

加解密過程



$$c = k \oplus m$$

$$m = k \oplus c$$

加密

$$\begin{aligned} c &= k \oplus m \\ &= 00111000 \oplus 01010011 \\ &= 01101011 \end{aligned}$$

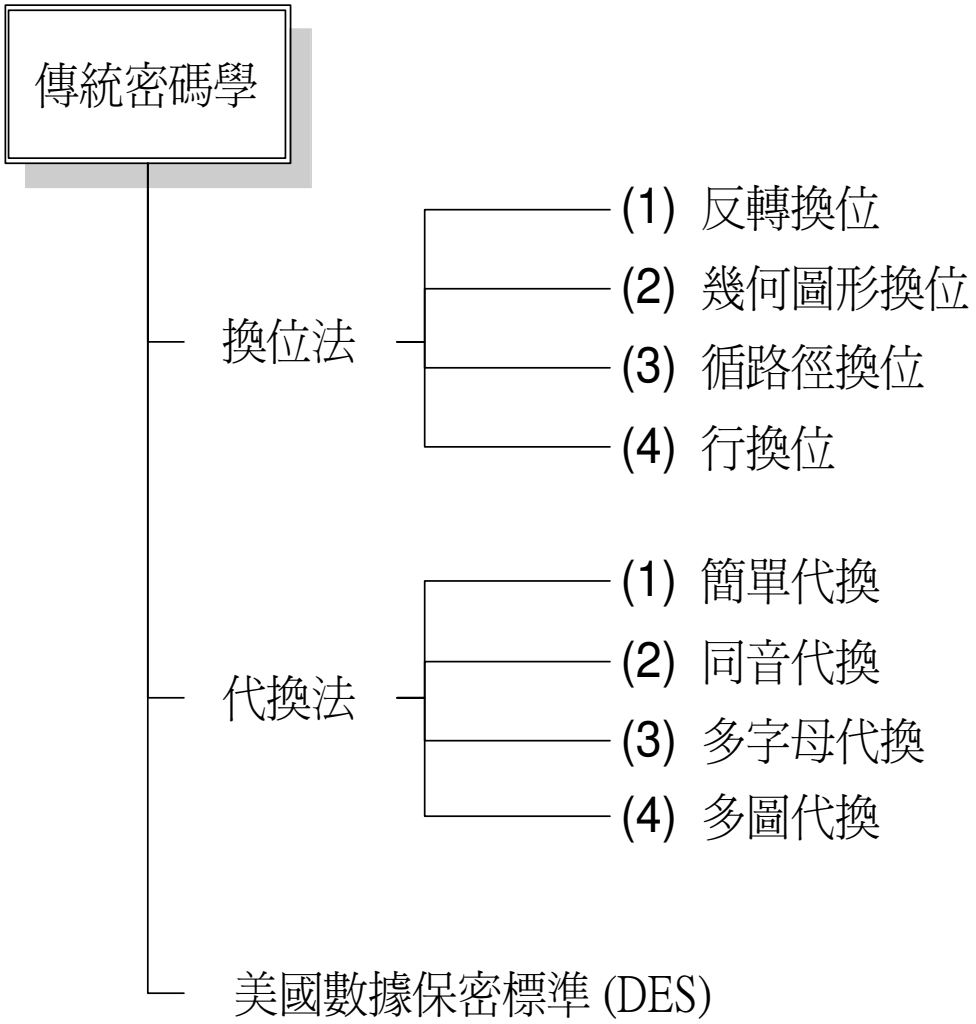
解密

$$\begin{aligned} m &= k \oplus c \\ &= 00111000 \oplus 01101011 \\ &= 01010011 \end{aligned}$$

密碼系統的分類

- 對稱性密碼系統(Symmetric Cryptosystems)或祕密金鑰密碼系統(Secret-Key Cryptosystems)或單金鑰密碼系統(One-Key Cryptosystems)
  - ***加密金鑰及解密金鑰為同一把***
- 非對稱性密碼系統(Asymmetric Cryptosystems)或公開金鑰密碼系統(Public-Key Cryptosystems) 或雙金鑰密碼系統(Two-Key Cryptosystems)
  - ***加密與解密金鑰為不相同的兩把金鑰***

傳統密碼學


傳統密碼學
換位法
(1) 反轉換位
(2) 幾何圖形換位
(3) 循路徑換位
(4) 行換位
代換法
(1) 簡單代換
(2) 同音代換
(3) 多字母代換
(4) 多圖代換
美國數據保密標準 (DES)

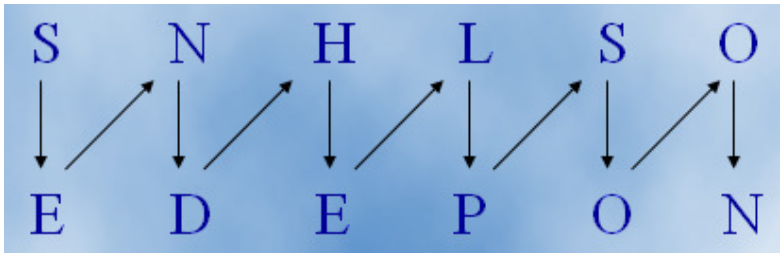
傳統密碼學 (Cont.)

- 反轉換位法
  - 明文：MEET ME MONDAY MORNING
  - 密文：GNINROM YADNOM EM TEEM
- 幾合圖形換位
  - 明文：CONCEAL ALL MESSAGES
  - 密文： CLOMNECSESAALGAELS

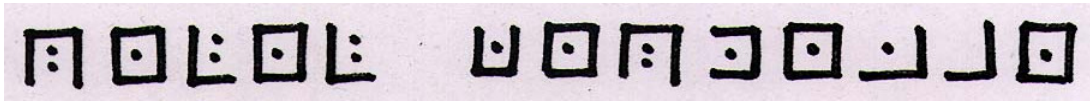
明文：CONCEAL ALL MESSAGES

CL	CON
OM	CEA
NE	LAL
CS	LME
ES	SSA
AA	GES
LG	
AE	
LS	

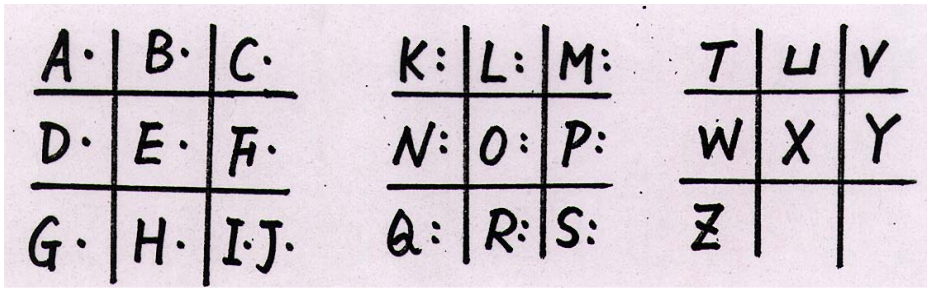
傳統密碼學 (Cont.)



- 循路徑換位法
  - 明文：SEND HELP SOON
  - 密文：SNHLSOEDEPON
- 代換法
  - 明文： M = RENAISSANCE
  - 密文：$E_K(M)$ = XKNAUGGANSK
- Affine 轉換
  - 密文：



依照右側取代法則取代而成

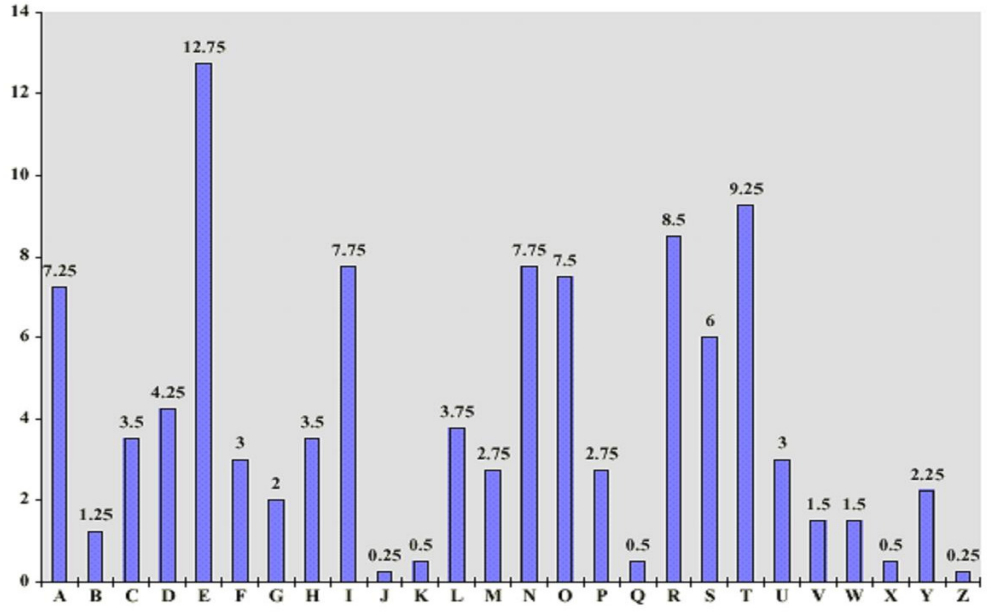


傳統密碼學 (Cont.)

- 凱撒加密法(Caesa Cipher)
  - 換位加密
    - 明文：A DOG
    - 位移1位➔B EPH
    - 位移2位➔C FQI
    - 位移 -1位➔ Z CNF
  - 容易被破解
    - 利用統計分析的技巧
    - 分析一般文章中最常出現的字母
    - 分析一份密文出現最多的字母
    - 比較兩者即有可能被破解

傳統密碼學 (Cont.)

	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



傳統密碼學 (Cont.)

- 簡單替代法
  - **M → C 為一對一之對應關係**
    - *M* = COMPUTER (明文)
    - *C* = DXIJSRAW (密文)

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

傳統密碼學 (Cont.)

- 編碼法

隨機編碼本範例

明文	號碼
電腦	0711
資訊	1232
安全	2243
管理	3661
系	4538

『資訊管理系』：

1232 3661 4538

編碼本範例

明文	頁	位置
電腦	12	31
資訊	14	02
安全	18	24
管理	26	63
系	45	28
中興大學	65	84

『資訊管理系』：

14 02 26 63 45 28

傳統密碼學 (Cont.)

- 同音異字替代法

將明文每個字母以一組數中的任意一個來替代

字母	同音異字
C	07,11,70,83
E	04,17,33,88,96
M	01,13,19,20
O	02,06,61,92,97
P	08,18,21,38
R	10,81
T	05,16,50,63
U	03,09,14,15,43,47

M **= COMPUTER (明文)**

(同音異字法加密)

C **= 11 61 19 08 14 16 17 81 (密文)**

傳統密碼學 (Cont.)

- 多字母替代法

將最常見的為 Vigenere加密法，以數學式子表示

$$E_K(M)=(M+K_i) \bmod n$$

M=COMPUTER (明文)

K=LOVELOVE

(多字母替代法加密)

$E_K(M)$ =NCHTFHZV (密文)

傳統密碼學 (Cont.)

■ 多圖替代法

多圖替代法其基本觀念是將一組字母加密，其基本精神是將每一對之明文之字母m_1,m_2一起加密成密文字母c_1,c_2，如Playfair密碼法其規則如下：

1). 若 m_1 和 m_2 在同一列，則 c_1 和 c_2 分別爲其右邊之字母，其中最後（右）一行之字母的右邊爲第一行之字母。

2). 若 m_1 和 m_2 在同一行，則 c_1 和 c_2 分別爲其下方字母，其中最下一列之字母的下方爲第一列之字母。

3). 若 m_1 和 m_2 不在同一行也不在同一列，則 c_1 和 c_2 爲與 m_1 和 m_2 相對應方形邊角位置的字母，其中 c_1 與 m_1 同一行，c_2 與 m_2 同一行。

4). 若 $m_1 = m_2$，則將一空字母（設爲 x）加在 m_1 及 m_2 之間，使不成爲連續相同字母。

5). 若明文之字串長度爲奇數，則在尾端加一空字串 x。

傳統密碼學 (Cont.)

- 多圖替代法 (Cont.)

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

Playfair 加密法金鑰表

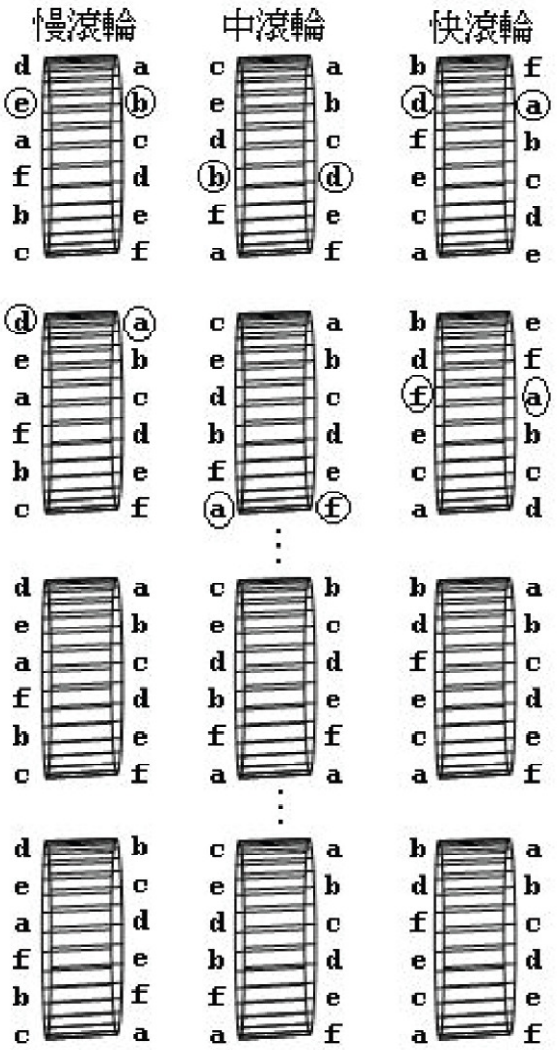
M=CO MP UT ER (明文)

(多圖替代法加密)

C=OD HT MU HG (密文)

傳統密碼學 (Cont.)

- 旋轉機
  - 由三個滾輪與一個反射滾輪組成使明文與密文產生一對多的對應關係增加安全性
  - 每做完一次加密動作，就會改變一次密碼字母集

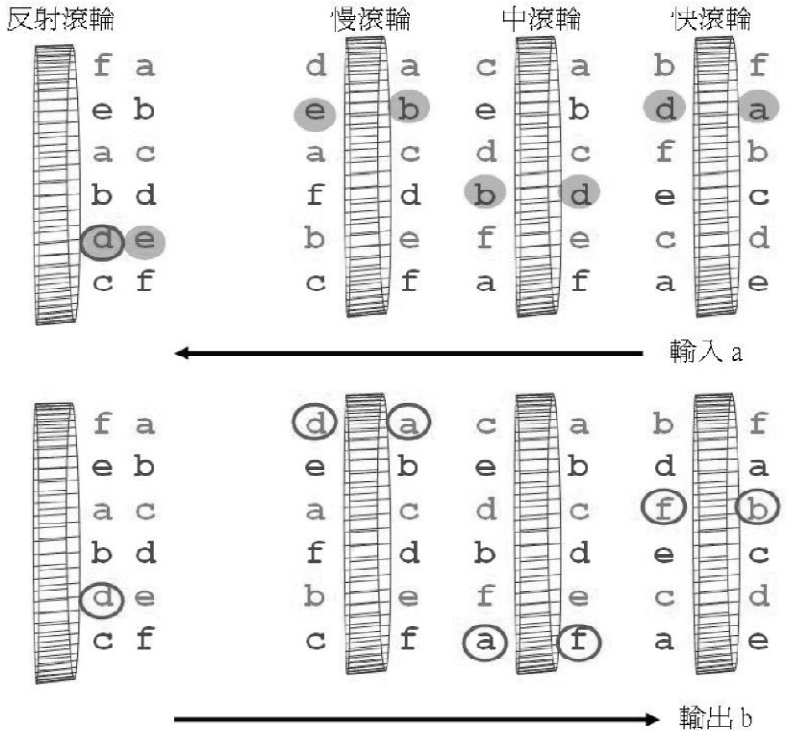


三個滾輪週期26x26x26=17576

滾輪間共有 3!=6種可能

每次按鍵所產生的輸出可能10546種(=17576x6)

傳統密碼學 (Cont.)



- 旋轉機 (Cont.)
  - 輸入a
  - a→d→b→e→d
  - d→a→f→b
  - 輸出b

此例中，

三個滾輪週期6×6×6=216

滾輪間共有 3!=6種可能

每次按鍵所產生的輸出可能 1296種(=216×6)

傳統密碼系統之破解法

- **窮舉法(Brute-Force Attack)**
  - 將所有可能的情況均嘗試一遍，直到找出正確的解密方式。
- **統計法(Statistics Attack)**
  - 利用一些統計資料來協助破解密碼，例如以字母出現的頻率。
  - EX. {A, E, I, O, U}出現頻率比{Q, X, Z}的出現頻率高出許多