國立成功大學
National Cheng Kung University

古典密碼學
Classical Cryptography

計網中心 網路與資訊安全組

李南逸

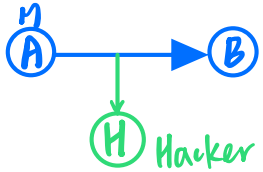
National Cheng Kung University

資訊安全之定義與範圍

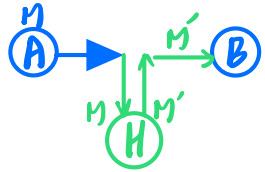
- 安全：一種放心，沒有危險的感覺
- 資訊安全：保護資料於儲存、處理、傳送、存取時，免於遭受竊取、破壞、偽造等攻擊
- 資訊安全包含的範圍：
  - 機密文件的存取權限
  - 員工的資訊安全知識訓練
  - 機器放置地點有否考量天然災害
  - 檔案是否定期備份
  - https://haveibeenpwned.com 密碼安全
  - 等等

○ 安全攻擊分類

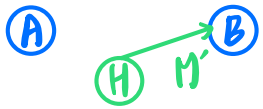
1. 竊聽



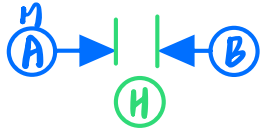
2. 修改



3. 偽裝



4. 阻斷式服務 DoS

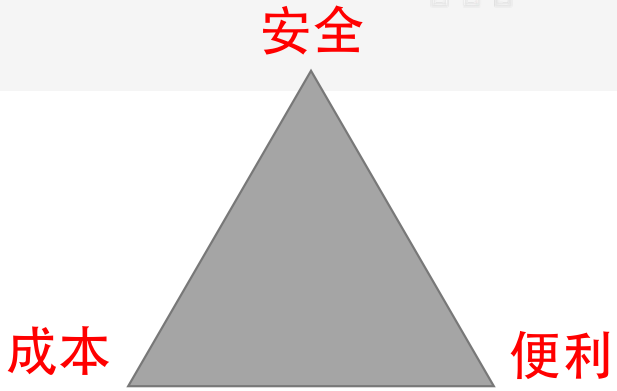


① Passive attack 被動：1

② Active attack 主動：2、3、4

資訊安全之建議

- 國際密碼學大師Shamir對商業安全有十項建議：
  1. 不要追求完美無缺的安全性
  2. 不要誤以為問題解決了，但根本的問題仍然存在
  3. 不要使用由下而上的策略解決問題
  4. 不要過分的使用密碼技術，反而造成使用者的不方便
  5. 不要使用太複雜的方法 複雜≠安全
  6. 不要使用太昂貴的設備
  7. 不要使用單一防線策略
  8. 不要忽略了可能發生的“神秘攻擊法” 未知、Zero day
  9. 不要太過於仰賴系統操作
  10. 不要太過於仰賴人員忠實



資訊安全之技術

- 密碼術(Cryptology)：為保護資訊安全之最重要且最常用的技術與基礎
- 緣起：希臘文*kryptós*（隱藏）及 *gráphein*（訊息）
- 西元1949年Shannon提出第一篇討論密碼系統通訊理論之論文
- 實例：
  - 西方，凱撒大帝使用凱撒加密法傳送軍事情報
  - 東方，清朝紀曉嵐題詩，鳳遊禾蔭鳥飛去 馬走蘆邊草不生

禿 驢

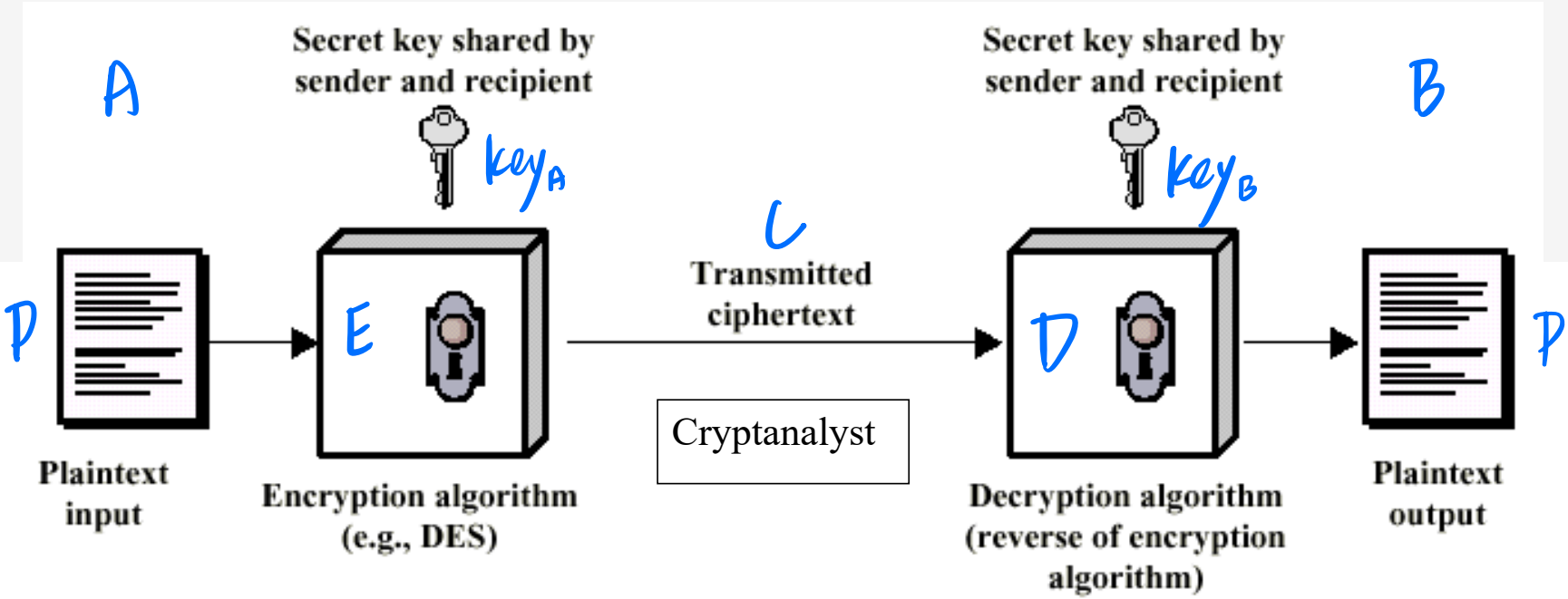
密碼術

- 密碼術(Cryptology)：包含2個領域
  - 密碼學(Cryptography)：指如何達到資訊的秘密性、鑑定性的科學或藝術
  - 破密學(Cryptanalysis)：指如何破解密碼系統，或偽造訊息使密碼系統誤以為真的科學或藝術

密碼學術語

- P 明文(Plaintext)：原始可辨識的訊息(message) 加密前
- C 密文(Ciphertext)：轉換過難以辨識的訊息 加密後
- K 金鑰(Key)：使用在加密器中相當重要且關鍵性的資訊，只有傳送方與接收方知道的資訊
- E 加密(Encipher, Encrypt, Encode)：使用加密器與金鑰去轉換明文成密文的程序
- D 解密(Decipher, Decrypt, Decode)：使用解密器與金鑰去轉換密文回明文的程序

密碼系統(Cryptographic System)簡圖



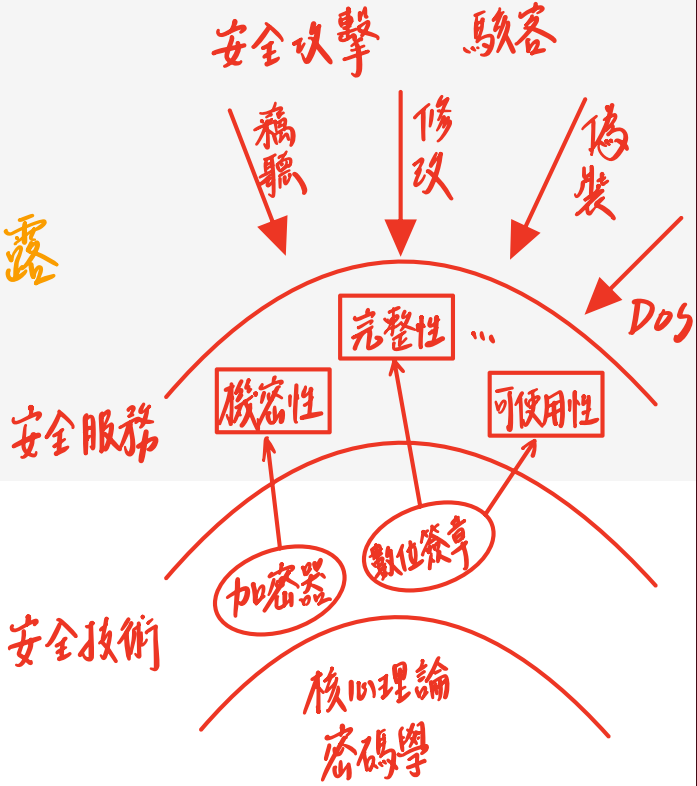
if $key_A = key_B$, 對稱式加密器

else, 非對稱式加密器

密碼系統可提供的安全服務種類

- 機密性(Confidentiality) 避免機密訊息內容洩露
- 確認性(Authentication) 中訊息回身分
- 完整性(Integrity) 避免訊息被修改
- 不可否認性(Non-repudiation) 避免否認簽名
- 存取控制(Access Control)
- 可使用性(Availability) Server的服務不被中斷

w CIA



密碼系統之安全性

密碼學的假設

- 密碼系統之安全性需僅依賴其秘密金鑰，而非其密碼演算法之隱藏(Kerckhoff's principle)
- 破密者依在密碼系統中所收集的資訊，依層次有下列五種可能的破密方式：

1. 密文攻擊法(Ciphertext-Only Attack)
2. 已知明文攻擊法(Known-Plaintext Attack)
3. 選擇明文攻擊法(Chosen-Plaintext Attack)
4. 選擇密文攻擊法(Chosen-Ciphertext Attack)
5. 選擇文攻擊法(Chosen-Text Attack)

不可選擇破解的密文C

攻擊強度

1. $P \rightarrow E_K \rightarrow C$
攻擊者知道的資訊：
① 加密演算法E
② 欲破解的密文C
⇒ 擬解出P or K
(如果攻擊者能解出P or K 則代表其利用密文攻擊法破解了此加密器)

2. $P \rightarrow E_K \rightarrow C$
攻擊者知道的資訊：
① 加密演算法E
② 欲破解的密文C
③ 過去的明文密文對
(如果攻擊者能解出P or K 則代表其利用已知明文攻擊法破解了此加密器)

- 一般密碼系統必須至少禁得起「已知明文攻擊法」，而公開金鑰密碼系統需禁得起「選擇明文攻擊法」

3. 攻擊者知道的資訊：
① 加密演算法E ② 可任意選擇明文得到對應密文
② 欲破解的密文C

4. 攻擊者知道的資訊：
① 加密演算法E ② 可任意選擇密文得到對應明文
② 欲破解的密文C

5. 攻擊者知道的資訊：
① 加密演算法E ② 可任意選擇密文or明文得到對應明文or密文
② 欲破解的密文C

安全密碼系統之定義

- 無條件安全(unconditionally secure)：不管破密者有多少強大的計算能力或時間皆無法解出明文，只有one-time pad system可達成，又稱Vernam Cipher，但並無真正one-time pad system存在

絕對安全

Key無限長,由亂數產生 ⇒ L會一直改變
純亂數 pure random：① 週期無限長 ② 不可預測性
虛擬亂數 Pseudo random：由演算法產生

- 計算安全(Computationally Secure)：若達到以下兩種標準其中一種則稱之

1. 破解密碼系統的代價超出破解得到的好處
2. 破解密碼系統所需的時間超出明文可利用的時間

利用金鑰搜尋窮舉法(暴力攻擊法)破解系統所需時間表

Brute force attack

Key Size (bits)	Number of Alternative Keys	Time required at 1 encryption/μs	Time required at 10^6 encryptions/μs
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} years	5.4×10^{18} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} μs = 6.4×10^{12} years	6.4×10^6 years

DES

AES

PC

超級電腦

金鑰搜尋窮舉法破解系統範例

- 可利用Office軟體或WinZip密碼加密保護檔案的方法建立密文檔，再利用軟體Advanced Office 2000 Password Recovery或Advanced ZIP Password Recovery(Shareware, 30days)採用金鑰搜尋窮舉法破解密文檔得到明文及金鑰
- 網站：http://www.elcomsoft.com/prs.html

密碼系統之類別

- 密碼系統可用以下三種規則來分類：
  1. 依轉換明文成密文的動作分類 ①代換 ②換位
  2. 依金鑰的數目分類 ① 1把key (對稱式) ② 2把key以上
  3. 依加密明文的長度分類 ① 串流 (1bit/1byte) ② 多bit
- 一般常以第二種規則來分類密碼系統

密碼系統之分類（以第二種規則）

- **秘密金鑰密碼系統** (Private Key Cryptosystem)：又稱**私密金鑰密碼系統**，或**對稱式金鑰密碼系統**(Symmetric Key Cryptosystem) 或**單一金鑰密碼系統** (One-Key Cryptosystem) 或**傳統密碼系統** (Conventional Cryptosystem)
  1. 古典技術 (Classical Techniques)
  2. 現代技術 (Modern Techniques)
- **公開金鑰密碼系統** (Public Key Cryptosystem)：又稱**非對稱式金鑰密碼系統** (Asymmetric Key Cryptosystem) 或**雙金鑰密碼系統** (Two-Key Cryptosystem)

秘密金鑰密碼系統之古典技術

不用計算機 or 電腦

- 使用兩種基本元件
  1. 代換法(Substitution)
     - 原字母用其他字母來取代
     - 如：凱撒加密法
  2. 換位法(Transposition)
     - 原字母用不同順序排列
     - 如：籬笆加密法

秘密金鑰密碼系統之古典技術(Cont.)

- 代換法(Substitution)
- 凱撒加密法：25種可能的金鑰 (k=1~25)
  - Plaintext :
  - Ciphertext :

0	1	2																						25
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
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

  - C=E(P)=(P+3) mod (26)
  - P=D(C)=(C-3) mod (26)
- plaintext : meet me after the toga party（成年禮宴）
- ciphertext : PHHW PH DIWHU WKH WRJD SDUWB

加密

秘密金鑰密碼系統之古典技術(Cont.)

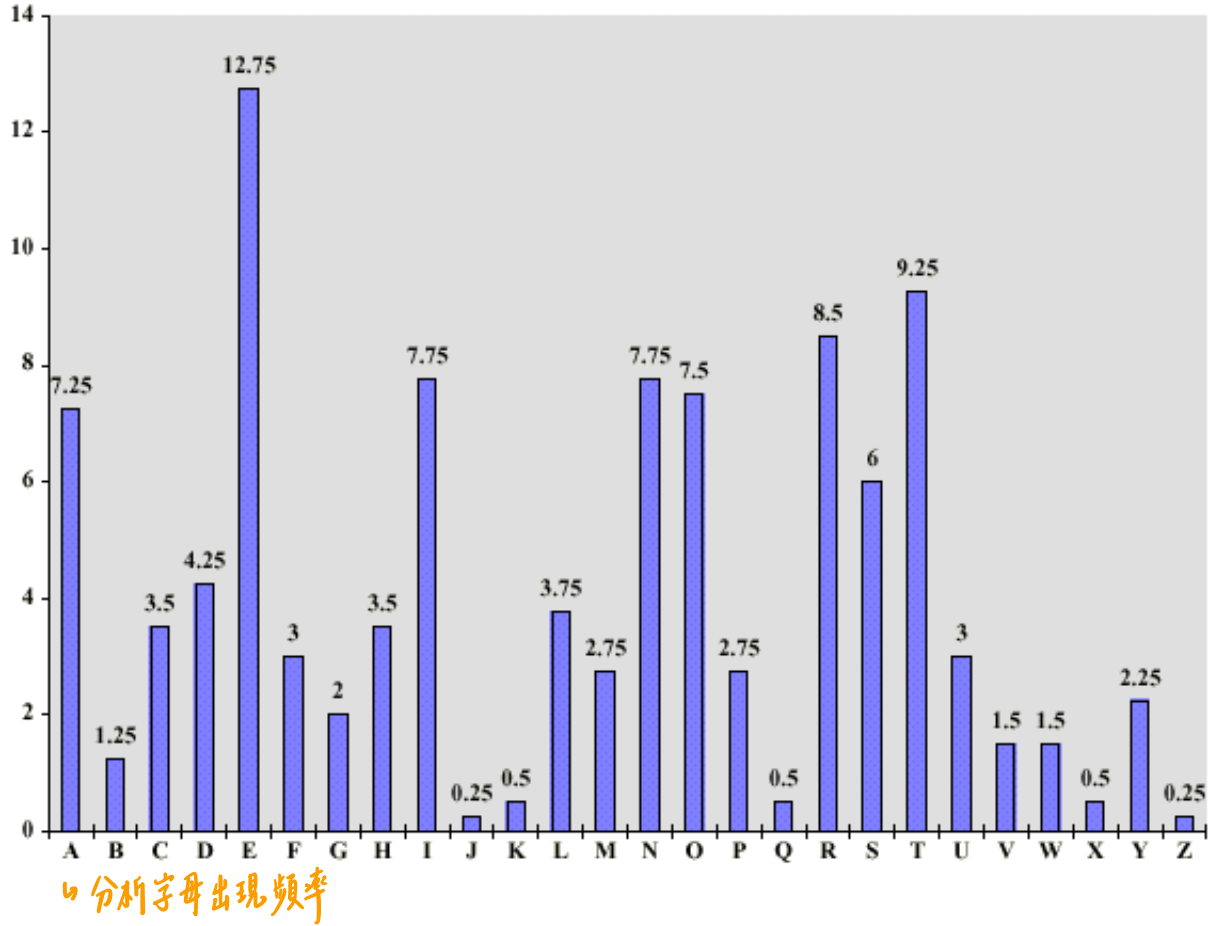
- 代換法(Substitution) ⇒ 1對1
- 單一字母加密法(Mono-alphabetic Cipher) : 26!種可能的金鑰
  - Plaintext :
  - Ciphertext :

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

↳隨便填

- plaintext : meet me after the toga party
- ciphertext : RCCI RC SJICU ITC IZWS DSUIV

秘密金鑰密碼系統之古典技術(Cont.)



- 分析字母出現頻率

秘密金鑰密碼系統之古典技術(Cont.)

- 代換法(Substitution)
- 多種字母加密法(Poly-alphabetic Cipher) ⇒ 1對多，避免被用頻率分析
  ↳不能多對1

- Key: d e c e p t i v e d e c e p t i v e d....
- plaintext: w e a r e d i s c o v e r e d s a v e....
- ciphertext: z i c v t w q n g r z g v t w a v z h....

$C = (P+K) \% 26$

秘密金鑰密碼系統之古典技術(Cont.) 查表

Plaintext

Key

	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

秘密金鑰密碼系統之古典技術(Cont.)

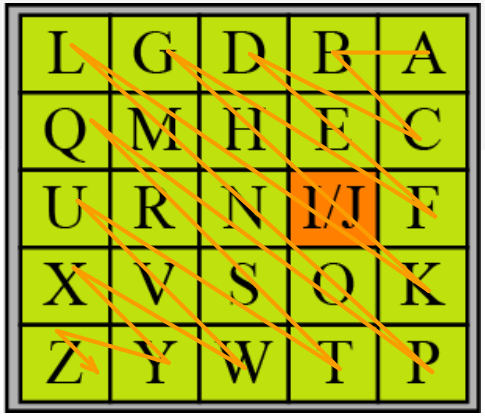
- 換位法(Transposition)
- 籬笆加密法(Rail Fence Technique)
- 軌道長度為2 key=2
- Plaintext : meet me after the toga party
- m e m a t r h t g p r y
- e t e f e t e o a a t

明文拆成2行

- Ciphertext : MEMATRHTGPRYETEFETEOAAT

秘密金鑰密碼系統之古典技術(Cont.)

- 換位法(Transposition)
- Playfair Cipher



- Key: (亦可設定)
  - 先由左上-左下填key
  - 再把剩下的字母填表
- Plaintext : hello
  - lx lo
- Ciphertext : EC QZ BX

ex: informationx
⇒FIIT VRBPOTUS

- 規則

a) 兩個字母出現在同一直排，轉換為下面一格的字母。

b) 兩個字母出現在同一橫列，轉換為右邊一個的字母。

c) 其他情形，找出另外兩格使該四個字母形成一個矩形。

d) 如果兩個字母一樣、或最後只剩一個字，則插入字母X
  - 填充字元

國立成功大學
National Cheng Kung University

Thank you !

National Cheng Kung University