網路安全的認識與策略

陳金鈴 (Chin-Ling Chen) 博士
朝陽科技大學資訊工程系
Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung, Taiwan 41349, ROC.
E_mail: clc@mail.cyut.edu.tw

大綱

- 網路安全的認識
- The “PAIN” Model
- 使用者驗證議題
- 網路安全技術之解決方案
- 資訊安全防護鐵三角
- 個人資訊安全六大守則
- 結論

一、網路安全的認識

- 多用網路，少用馬路。
- 網路如虎口！
- 網際網路上的虛擬社會即為實體社會的縮影有好人，也有壞人！
- 再多硬體、軟體防護措施，還是需要有良好的網路使用習慣！
- 防人之心不可無，害人之心不可有！
- 節制上網，以免網路沈迷，甚至上癮。

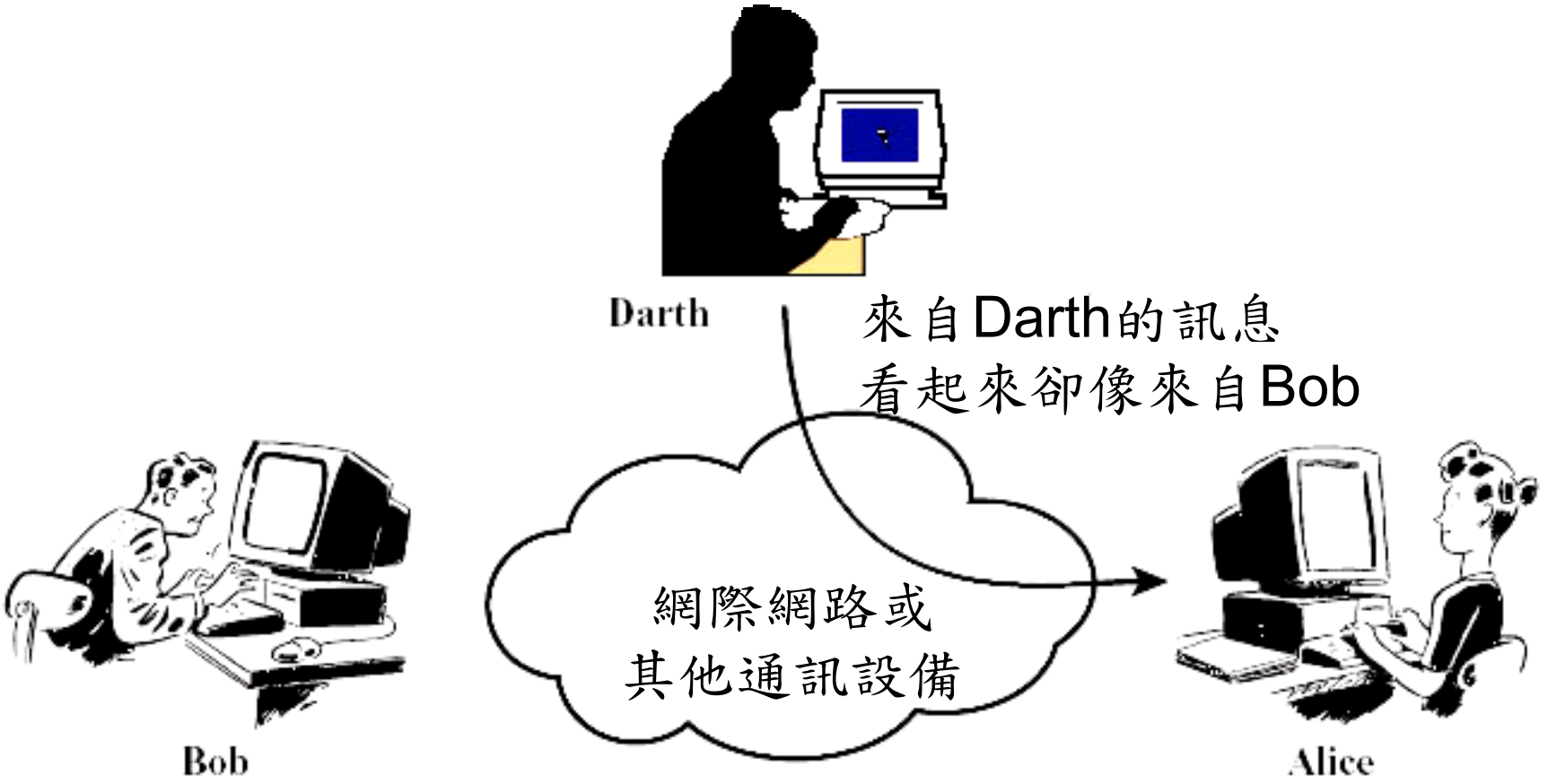
資訊安全的意義

- 資訊安全是保護資訊資產的一種概念、技術及管理方法，使資訊資產免受有意或無意的洩露、破壞、遺失、假造，及未經授權之獲取、使用和修改。
- 資訊資產包括：硬體、軟體、網路、通訊、資料、人員、服務、建築及保護設施等。

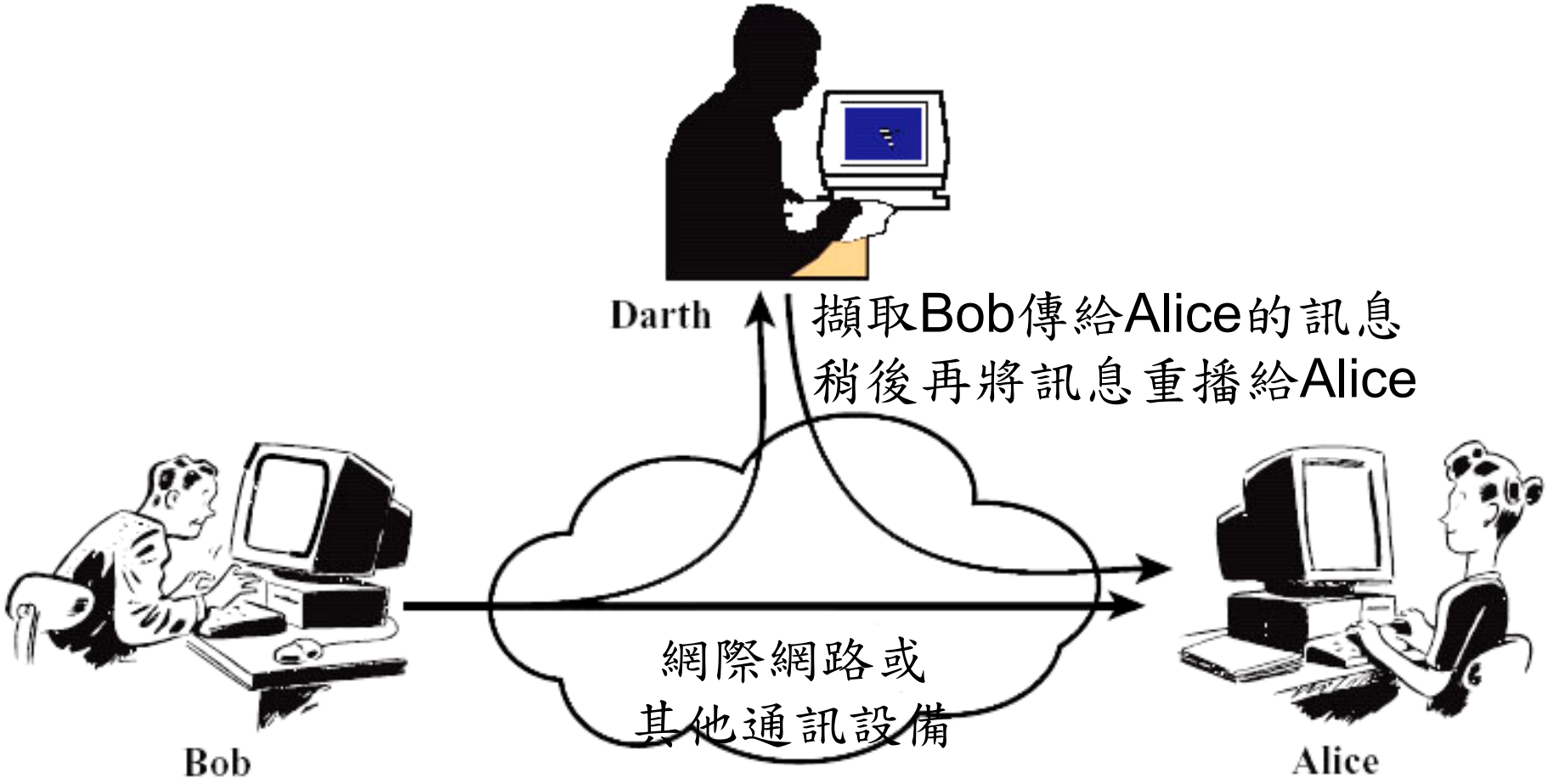
網路如虎口

- 危害資訊安全的網路攻擊方式
  - 被動式攻擊(Passive Attack)
    - 釋出的訊息內容。
    - 網路流量分析。
  - 主動式攻擊(Active Attack)
    - 偽裝、重送。
    - 修改訊息、阻絕服務。
- 駭客入侵與惡意程式騷擾破壞。

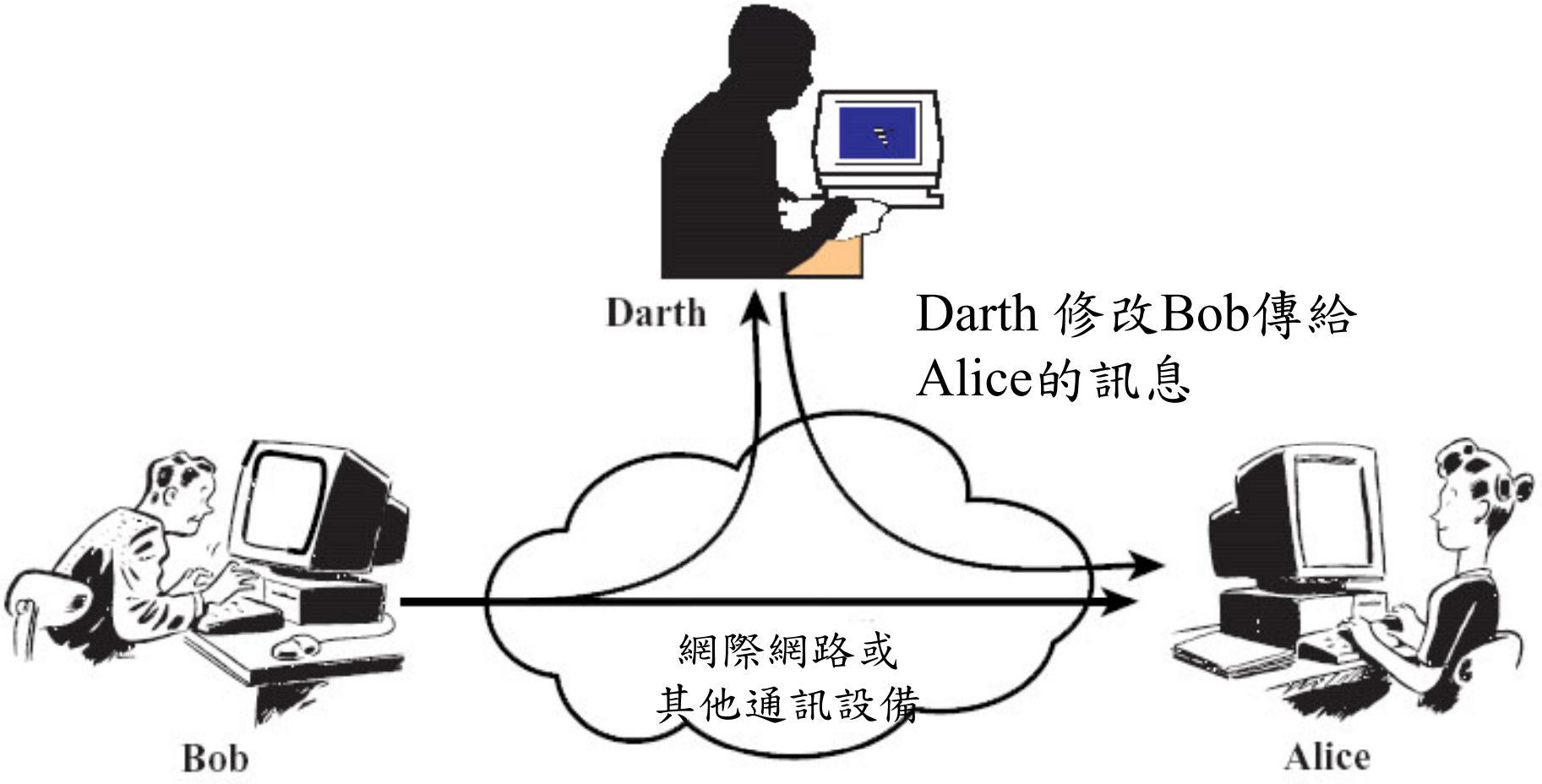
偽裝



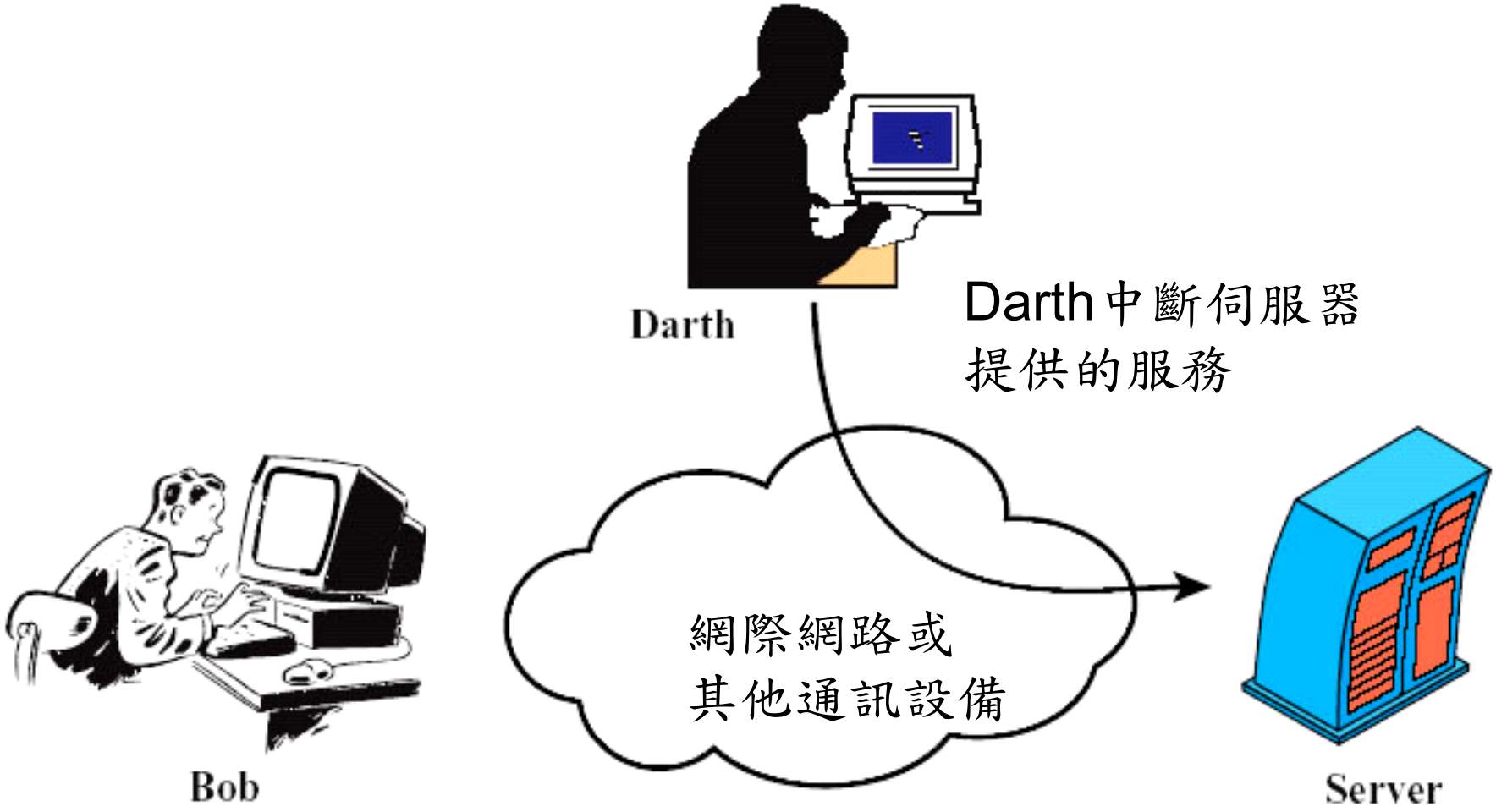
重送


Darth
擷取Bob傳給Alice的訊息
稍後再將訊息重播給Alice
網際網路或
其他通訊設備
Bob
Alice

修改訊息



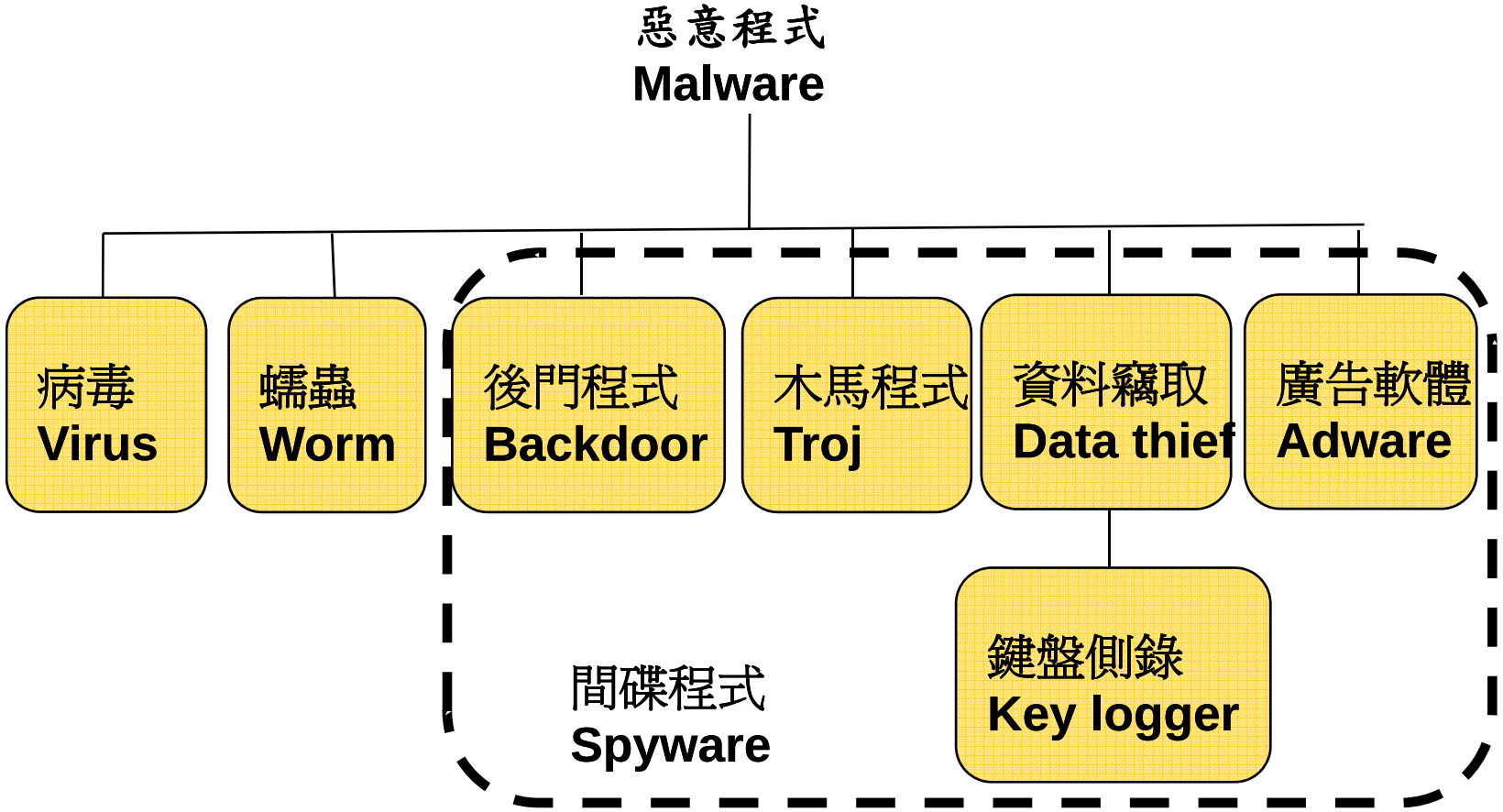
阻絕服務



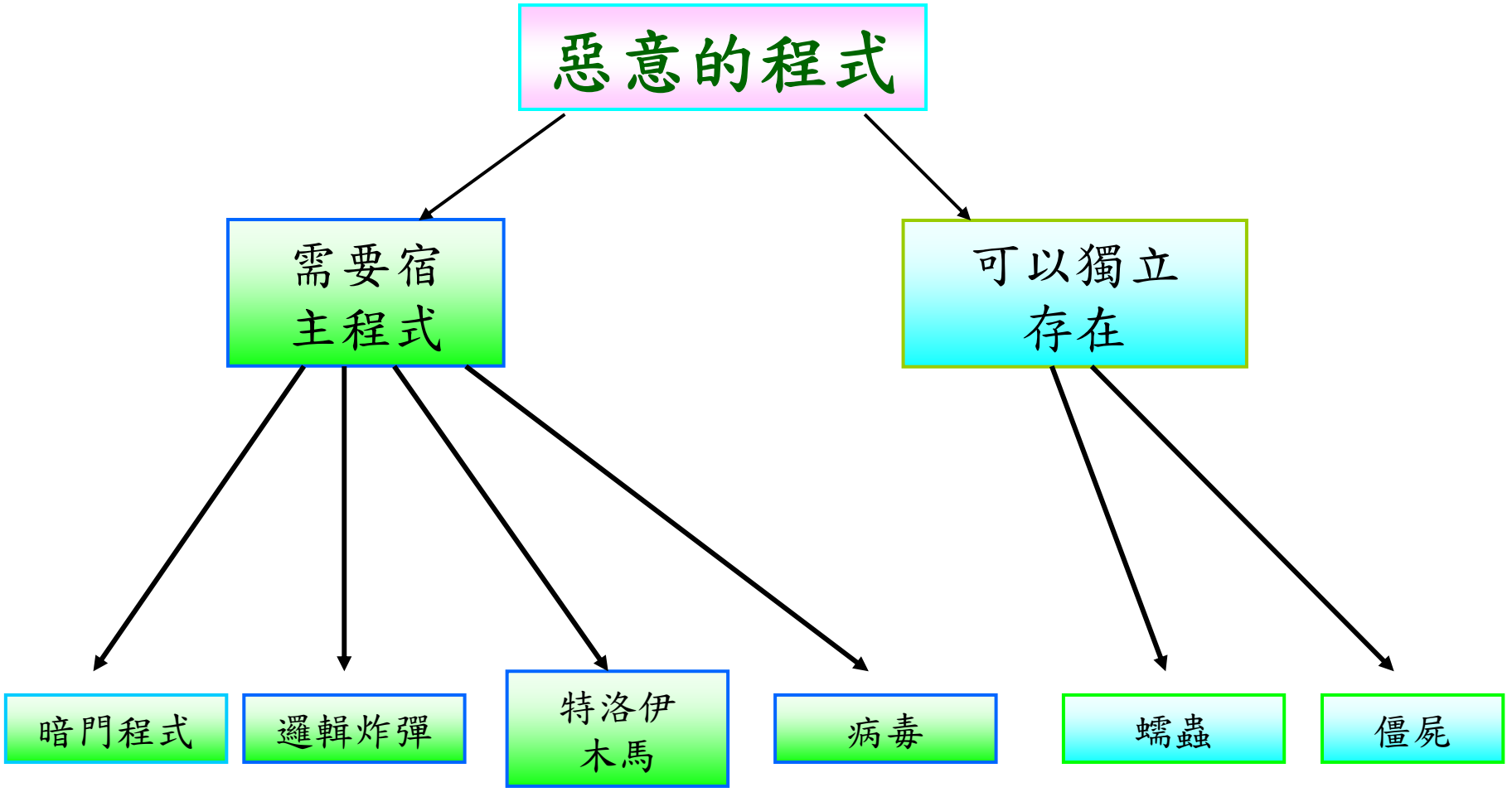
駭客任務- 如何破解密碼

- 嘗試系統給定的標準帳戶的預設密碼。
- 用窮舉法嘗試所有短密碼。
- 利用線上字典來猜密碼(這類清單會公開在駭客網站)。
- 蒐集使用者的資訊：姓名、嗜好等等。
- 嘗試使用者的電話號碼、身分證號、汽車牌照號碼。
- 竊聽、偷看使用者的密碼。

電腦病毒種類


惡意程式
Malware
病毒
Virus
蠕蟲
Worm
後門程式
Backdoor
木馬程式
Troj
資料竊取
Data thief
廣告軟體
Adware
鍵盤側錄
Key logger
間碟程式
Spyware

惡意的程式



資訊安全的重要性

- 隨著網際網路時代來臨，人們對電腦及網路的依賴日深。
- 網際網路的特色：
  - 急速成長。
  - 任何人都可由任何連線機器接觸任何連線機器。
  - 好人與壞人都連接在一起。
  - 開放架構。
  - 天涯若比鄰。
- 各色人等混雜其中，入侵網站、散佈病毒、竄改網頁、竊取機密、癱瘓系統、盜刷信用卡、製造及散佈謠言…等不良行徑，已成揮之不去的網路夢魘。唯有在做好資訊安全防護措施下，我們才能放心享受資訊的便利。

資訊安全的種類及潛在威脅

- 硬體安全：遭遇天災人禍，例如：硬體毀損、遭竊、遭破壞、停電、水災、風災、地震、炸彈等。
- 軟體安全：病毒感染、軟體缺陷等。
- 網路及通訊安全：內部網路故障、對外線路故障 、資料（含帳號及密碼）在傳輸時外洩等。
- 服務安全：網站遭阻絕服務攻擊。
- 資料安全：書面資料遺留於桌面上、字紙簍、影印機上、遺留板書、於公共場所交談、電話交談太大聲、資料在機器中被竊取或傳輸時被攔截。
- 個人安全：人身安全受威脅、個人隱私權受侵犯等。
- 資訊安全最大的威脅是人員作業疏失及故意行為。

組織面臨的風險

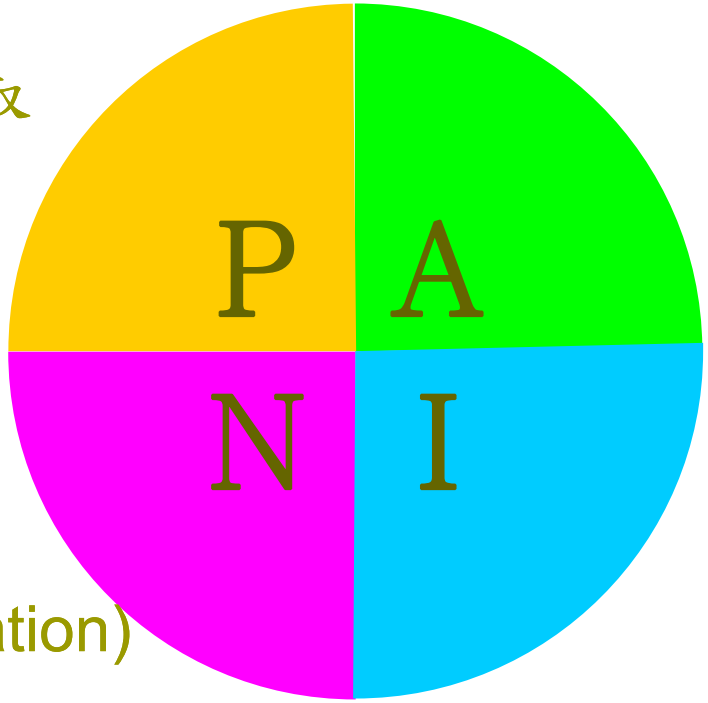
- 弱點 (Vulnerability)
  - 設計上缺陷，例如：SQL Injection、Buffer Overflow 、 Cross-Site Scripting (XSS) 等。
  - 使用上壞習慣，例如：密碼設定。
  - 該關沒關、該防未防，例如：通訊埠 (port) 。
- 威脅 (Threat)：威脅是任何可能對系統或網路引起潛在危害的情況或事件。
  - 組織內部威脅：人為、實體故障。
  - 組織外部威脅：滲透、入侵。

這麼不安全! 怎麼辦??

二、The “PAIN” Model

內容不被竊取
(Privacy)

身分驗證
(Authentication)



不可否認
(Non-repudiation)

不被竄改
(Integrity)

The "PAIN" Model

- 依據 ISO/IEC 7498-2 的定義，資訊安全的基本五大需求為：隱密性 (privacy) 、鑑別性(authentication) 、資料完整性 (integrity)、不可否認性 (non-repudiation) 與存取控制(access control)。
- 隱密性 (privacy)：
  - 確保資料訊息於傳輸時不會被他人偷窺或竊取，以保護資料傳輸的隱密性，一般可透過資料加密 (data encryption) 來達到此項需求。

The "PAIN" Model

- 鑑別性 (authentication)
  - 根據 ISO/IEC 10181-2，確認資料傳輸訊息之來源者正確——「個體鑑別 (entity authentication)」及訊息內容正確 (message authentication)，以避免資料傳輸訊息被偽造或發送來源者身份遭冒用。
  - 一般透過數位簽章 (digital signature) 或資料加密(data encryption) 等方式達到訊息鑑別；而個體鑑別一般均使用帳號、密碼或憑證 (Certification)。

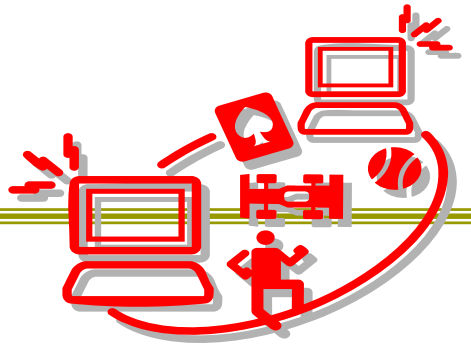
The "PAIN" Model

- 完整性 (integrity)
  - 依據 ISO/IEC 9797的定義，完整性係指資料未經非授權的修改或資料未毀損；ISO/IEC 10181-6 指出資料保持完整性必須不會有非經授權的資料修改、刪除、創造、增加及重複利用，故完整性應同時具有資料正確與資料為真的概念。
  - 一般使用數位指紋 (digital fingerprint)、數位簽章(digital signature)、數位封條(digital seal)、時戳(time stamp)、序號、亂數技術…等以維持完整性。

The "PAIN" Model

- 不可否認性 (non-repudiation)
  - 根據ISO/IEC 10181-4的定義，不可否認性分為兩部份，包含傳送端的不可否認性及接收端的不可否認性，亦即交易的雙方不可否認交易的存在。一般應用ITU-T X.509 的公鑰 (public key) 憑證證明身分並以私鑰 (private key) 附加電子簽章達成不可否認性。
- 存取權限控制 (access authority control)
  - 以資源面觀之，依不同資源之特性規範其被存取方式；而以使用者面觀之，需確保身份進行存取資料控管機制正常化，「存取權限控制」規範存取資源者與被分享資源間存取關係的正常化。

資訊應用安全



- 資訊安全考量點
  - 讓機關團體資訊資產或個人隱私資訊不受到有意或無意地洩漏、破壞、假造，以及未經授權的獲取、使用、修改。
  - 無論是企業或機關團體的整體資訊安全，或個人使用安全顧慮，通常都是在使用過程中所產生的，因此了解資訊安全弱點，並培養良好的使用習慣是很重要的。

三、使用者驗證議題 (User Authentication)

交易身份識別 (Identification) 的重要

- 人力成本不斷的提高，越來越多的服務經由「非臨櫃」的方式提供予顧客。
- 迄2004年6月止，台灣地區金融機構裝設自動櫃員機 (ATM) 之數量已超過二萬台。
- 隨著生活型態多樣化及為了提昇顧客更高的服務品質，金融機構亦開始提供電話銀行(Telebank)及網路銀行(e-Bank)的服務。
- 通信網路 (電話網路、數據網路) 交易具有「匿名」特性。

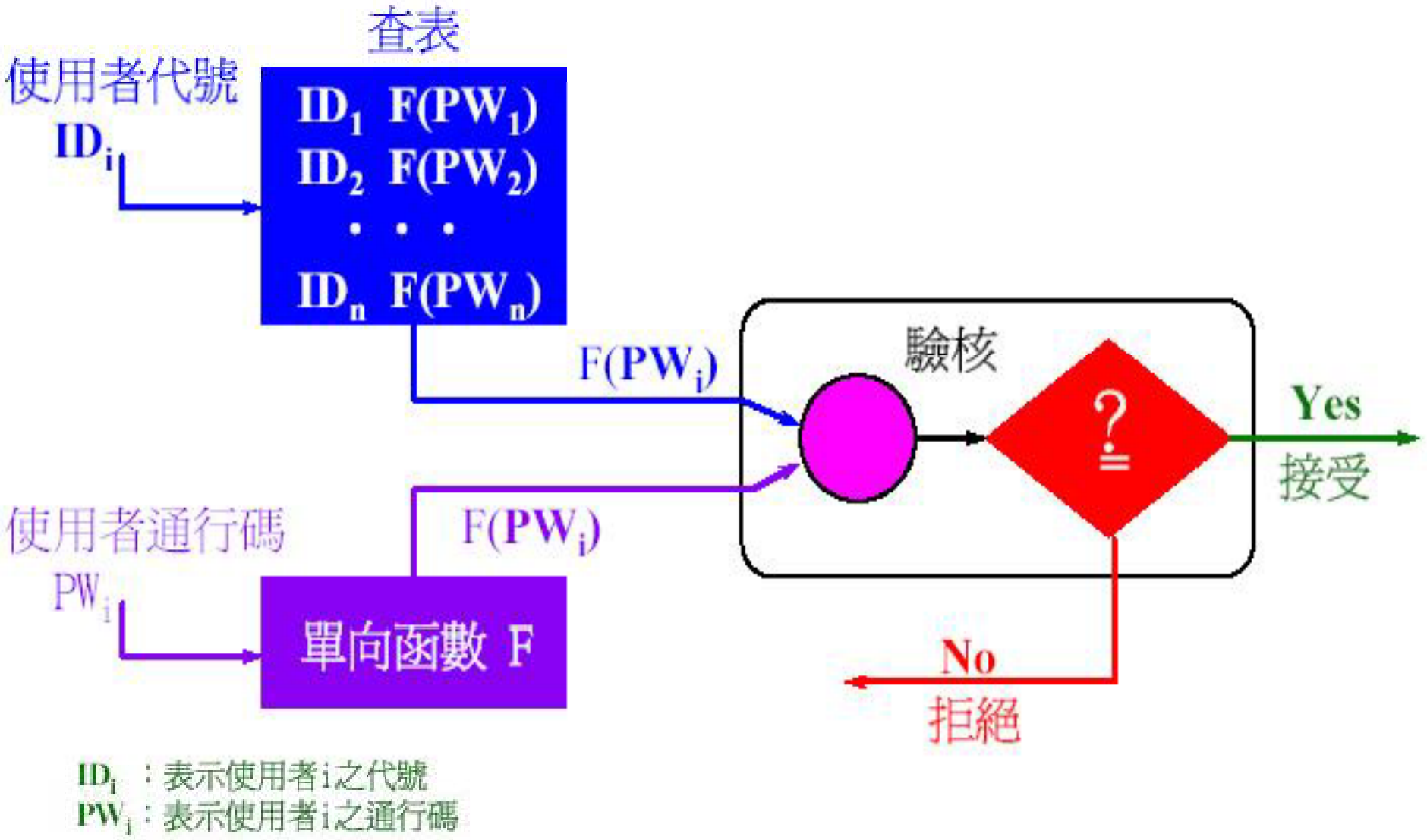
使用者辨識

- 證明一個人或物是符合他所自稱的，通常欲達成此功能，需和下列事物配合：
  - 使用者知道事物【通行碼】。
  - 使用者使用地點【控制台 (Console)】。
  - 使用者攜帶【背章、鑰 (Key)】 。
  - 使用者本身自有的【指紋、簽章】 。

通行碼

- 事先設定之特別資料，以辨認使用者之身份(User Authentication)。
- 資料儲存方式：
  - 直接儲存原文。
  - 先經加密後儲存密文。
  - 先經單向函數處理後儲存其函數值。
- 在電腦通常以(使用者代號，通行碼)成雙儲存。

通行碼處理示意圖


查表
使用者代號
ID_i
ID_1 $F(PW_1)$
ID_2 $F(PW_2)$
ID_n $F(PW_n)$
$F(PW_i)$
驗核
?
Yes
接受
使用者通行碼
PW_i
$F(PW_i)$
單向函數 F
No
拒絕
ID_i ：表示使用者i之代號
PW_i：表示使用者i之通行碼

通行碼設定

- 使用者自選：
  - 較友善 (Friendly) 。
  - 若於申請時使用者即需告知，則有暗語洩漏，保管等問題。
- 解決方法：
  - 核准時，均為特定之預設值 (例如：User) 。
  - 在第一次使用時，強迫使用者自己直接輸入通行碼。
  - 若用於卡片上，需考慮硬體設備 (更新磁條) 。
- 由系統直接設定：
  - 較不友善使用者不易接受。
  - 需制定處理如何告訴使用者之安全程序。

通行碼設定應注重事項

- 1979年 Bell Lab 曾研究有86% 之通行碼是可破解。
- 為了易於記憶，通行碼資料常和個人資料有關 (例如：生日，電話號碼，身份證字號等)。
- 為了使用方便，通行碼資料均很短，或因通行碼資料太長，將其記載於易於查看的地方。
- 使用環境不良，在公共場所使用通行碼易被窺視。

通行碼設定原則

- 絕對避免的通行碼：
  - 不設通行碼。
  - 與帳號相同。
  - 與主機名稱相同。
  - 生日、身分證字號、英文姓名等個人資料，以及公司，部門等公司資訊。
  - 使用1111、1234、123456、2000、aaaa、abcdef此類簡單的組合。
  - 通行碼別留在紙上或是文字檔中。

通行碼使用須知

- 通行碼需經常變更。
- 一通行碼使用的時間愈長風險愈高。
- 使用【好的】通行碼。
- 不要使用和個人屬性資料作為通行碼，如生日、地點、電話、身份字號等。
- 不可洩漏你的通行碼。
- 須視通行碼為有價事物而嚴加保護。

通行碼使用須知

- 時時檢查你的資料。
- 如果懷疑，有人入侵你的檔案，應立刻向安全小組報告。
- 不要離開使用中的電腦。
- 在離開電腦前一定先登出系統或上鎖。
- 懷疑電腦濫用應向安全小組報告。
- 無論是否直接影響到你，電腦資源的濫用或誤用將會阻礙公司的作業完成的時間和品質。

資料在網路上傳輸安全嗎？

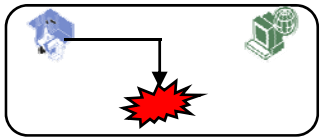
SECURITY ATTACKS

Normal Flow

Intruder

➢你的資料可安全送達嗎?

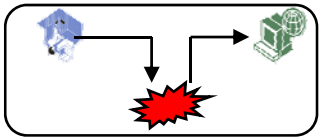
攔截 (Interruption)



Availability ?

➢你送達的資料完整嗎?

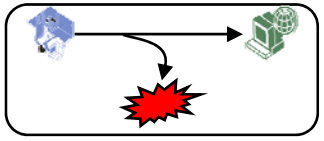
竄改 (Modification)



Integrity ?

➢你的資料具有機密性嗎?

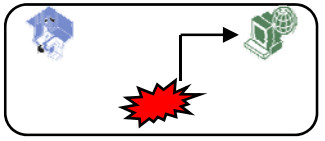
竊取 (Interception)



Confidentiality ?

➢是否會有人偽冒你傳送資料?

偽冒 (Fabrication)



Authenticity ?

你知道嗎？

大部分資訊犯罪行為的發生…
都是來自於企業內部！

89%

電子交易之基本考量

和誰交易?	**Authentication**
是否真如他所說的?	**Validation**
他被允許去做及觀看的事項有哪些?	**Authorisation**
如何確保交易的機密性?	**Confidentiality**
如何確認確實執行這項交易?	**Non-Repudiation**
何時進行交易?	**Time stamp**

四、網路安全技術之解決方案

	鑑別性	機密性	完整性	不可否認性
防毒			✓	
防火牆	✓	✓		
存取控制	✓	✓		
加密		✓		
公開金鑰基礎建設PKI	✓	✓	✓	✓

傳統密碼法

密碼法(cryptography)與隱匿法(steganography)兩者合併可強化安全性.

現今之研究著重前者.

傳統密碼法本身又可分成兩類:

移位法(transposition) 與 替代法(substitution).

傳統密碼法

(1) 換位法是將訊息裡的字母調動順序.

S	T	R	I	K	E
W	H	I	L	E	T
H	E	I	R	O	N
I	S	H	O	T	E

此法不適用於短的訊息;因為排列組合數少.
若訊息是n個相異字母,則有 n! 種排列.若n=10,
10! = 3,628,800
歷史上最早用此法於軍事上是紀元前五世紀之
斯巴達密碼棒(scytale).

紀元前五世紀之斯巴達密碼棒(scytale)

圖2：從發信人的密碼棒解下來時，這皮帶上的字母猶如隨意胡寫的；S、T、S、F……。唯有把這皮帶纏繞在一根直徑正確的密碼棒上，訊息才會重現。

三種換位加密法：

一、鐵軌法(Railroad Method)

首先，它要求明文的長度必須為 4 的倍數，若明文不符合此項條件則可在明文末梢加上一些字母以符合加密的條件。例如“STRIKE WHILE THE IRON IS HOT”這段明文便不滿足此條件(空白不計)，故我們可在尾端加上字母 “E” 使得明文的長度變成4的倍數。接著我們將明文寫成如下型式。

表 鐵軌法明文

S	R	K	W	I	E	H	I	O	I	H	T
T	I	E	H	L	T	E	R	N	S	O	E

根據上表，依序由左而右再由上而下地寫出字母即為密文，表示如下：

SRKWIEHIOIHTTIEHLTERNSOE

為了方便起見，我們可將密文每4個字母一數，其間以空白隔開：

SRKW IEHI OIHT TIEH LTER NSOE。

當接收方收到此密文之後，他可將密文以一直線從中分為兩個部份，如下所示：

SRKW IEHI OIHT ｜ TIEH LTER NSOE。

然後左右兩半依序輪流讀出字母便可還原成原來的明文了。

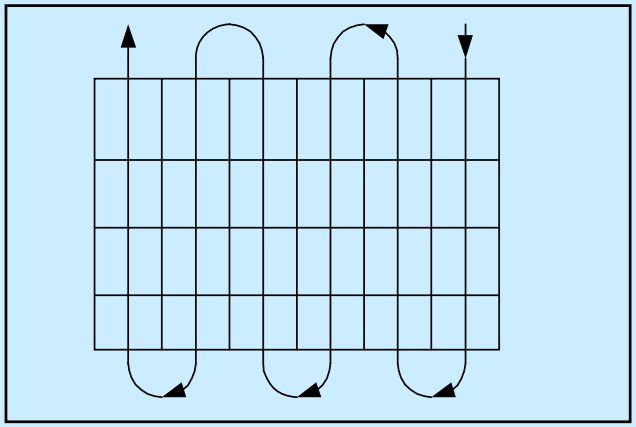
二、路遊法

這個方法可說是一種鐵軌法的推廣。

同樣地，此法也須將明文的長度調整為4的倍數。之後便將調整過的明文依由左而右由上而下的順序(此順序我們稱之為排列路徑)填入方格矩陣中。依前例，我們可以得到以下矩陣。

S	T	R	I	K	E
W	H	I	L	E	T
H	E	I	R	O	N
I	S	H	O	T	E

有了此矩陣後，我們便可依照某一事先訂定的路徑(稱為遊走路徑)來遊走矩陣並輸出所經過的字母，此即為密文。



遊走路徑圖

如果我們以圖之遊走路徑來走，則我們可以得到如下的密文

ETNETOEKILROHIIRTHESIHWS。

這個方法的安全性主要是取決於排列路徑與遊走路徑的設計，讀者可以自行設計不同的路徑來體會一下此法的精神，但必須注意的是排列路徑與遊走路經絕不可以相同，否則便無法加密了。

三、金匙法

此法最大的好處就是將加密者與解密者雙方所持有的加解密訊息具體化。金匙法大致來說與路遊法相似，首先也是將明文填入一個矩陣，舉例如下：

明文矩陣

S	T	R	I	K	E
W	H	I	L	E	T
H	E	I	R	O	N
I	S	H	O	T	E

接著，任意挑選一個金匙，譬如以 "PREDICT" 這個英文單字為加解密雙方所協議的共同金匙。有了加密金匙以後，我們便可將此金匙書寫於矩陣上方，如下表。

P	R	E	D	I	C	T
S	T	R	I	K	E	
W	H	I	L	E	T	
H	E	I	R	O	N	
I	S	H	O	T	E	

接著，我們依加密金匙字母的順序分別依序讀出其相對應的行便可得到密文

ETNEILRORIIHKEOTSWHITHES。

當收方收到此密文時，可依事先與送方約定好的金匙重新自密文中還原回明文。請注意此金匙不宜太短；若短於矩陣之行數則可重複幾回直到大於矩陣之行數為止。如果遇到字母重複時，可由加解密雙方事先約定一個優先順序，譬如 "左" 優先於 "右" 即可解決此種衝突。

傳統密碼法

替代法: 不改變字母之間的順序而以別的字母或符號取代每一字母.

ABCDEFGHIJKLMNOPQRSTUVWXYZ

↓

DEFGHIJKLMNOPQRSTUVWXYZABC

若字母數是n， 則其最大組合數為 n!

表面上看上述二者好像一樣! 不， 若移位法之訊息長度大, 則比替代法之字母集之組合數多 .

傳統密碼法

替代法:

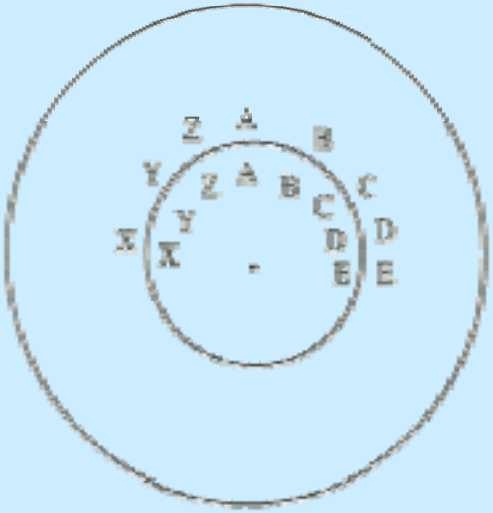


圖2.1

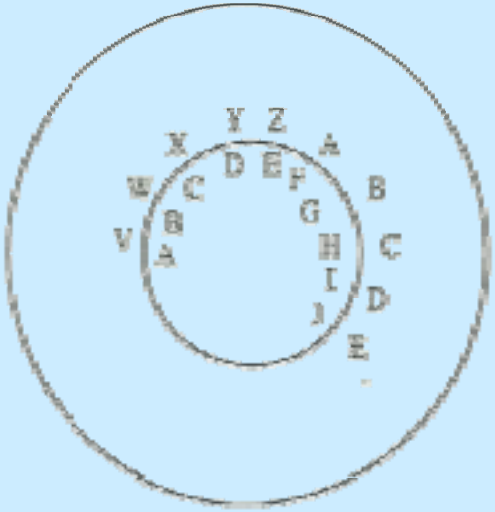


圖2.2

傳統密碼系統之破解法

- **窮舉法(Exhaustive 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為止。
- **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。

傳統密碼系統

傳統數據保密技術並不能保證系統的安全，而且應用上也受到相當大之限制，比如中文系統就很難用換位法以達到保密效果，試想將〞今天我不回家〞之明文換位置成〞回不天家我今〞之密文，該密文一看就可重組成明文而不需藉其它工具來破解，所以我們需要使用一些以“位元”為處理單位的加密系統。

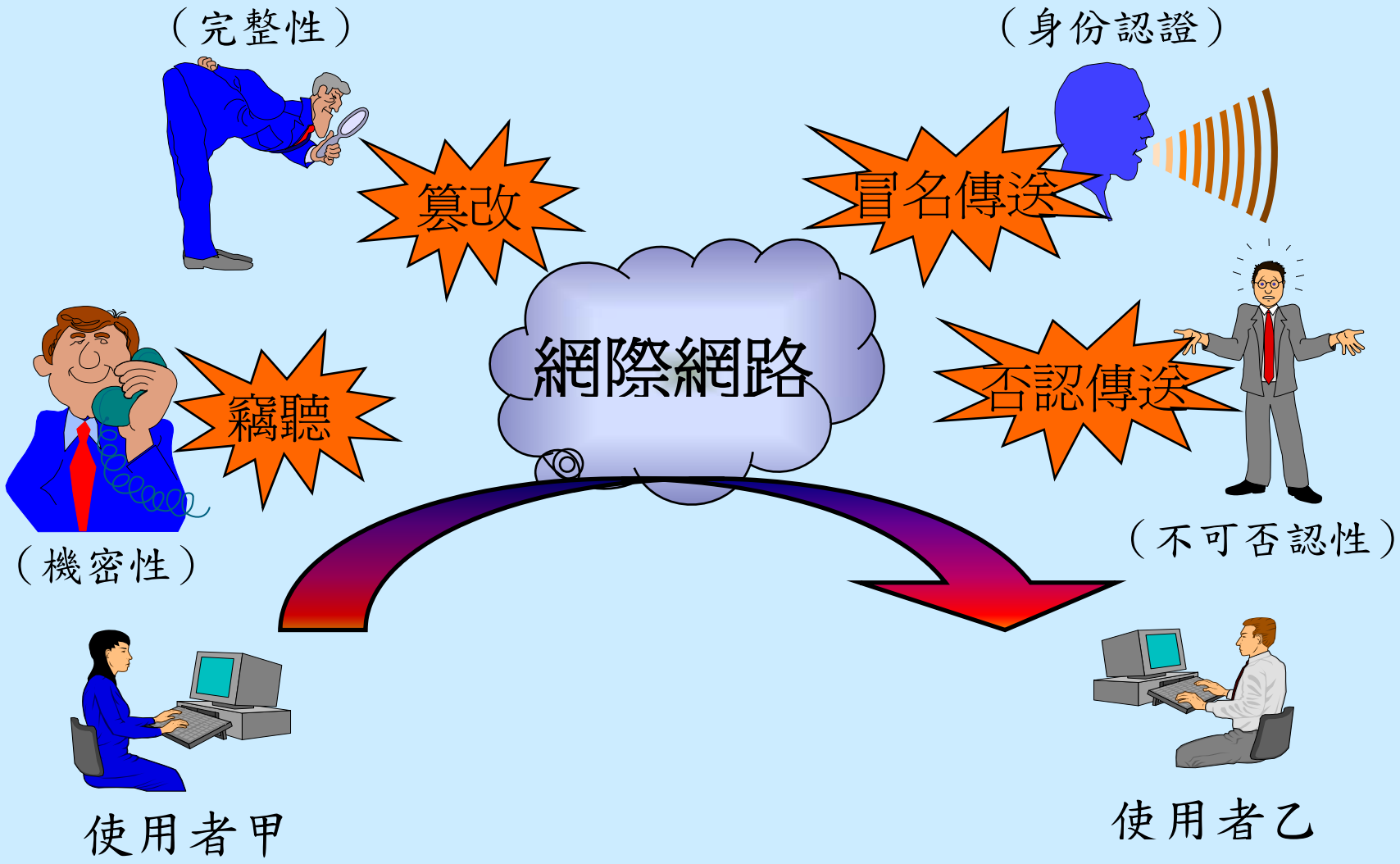
傳統密碼系統的濫殤

- 傳統密碼系統或稱單金鑰密碼系統(Single Key Cryptosystem)，就是結合了加密演算法E、解密演算法D、所有可能明文所成集合P、所有可能密文所成集合C與所有可能秘密金鑰值所成集合K，由這五項要件所構成的一套密碼系統，並且對於秘密金鑰k與明文p而言，加密演算法E(k, •)與解密演算法D(k, •)，必須滿足D(k, E(k, p))= p。由於是單金鑰密碼系統，收送密文的雙方必須事先約定好共同秘密金鑰k，藉以執行加解密函數。傳統密碼系統的優點就是加解密速度快，同時也可以提供身份驗證(Authentication)的功能，也就是說在密文收到時，收方可以確認送方身份，就是共同擁有秘密金鑰k的另一人。但是使用傳統密碼系統，必須先解決秘密金鑰分配與管理問題。

傳統密碼系統的濫殤

- 秘密金鑰分配問題就是如何讓收送雙方可以安全地共同擁有秘密金鑰k；而秘密金鑰管理問題，就是因爲任兩人間的秘密通訊都需要一把秘密金鑰，所以當一個人要與n個人要秘密通訊，就需要n把秘密金鑰，因此有管理這些秘密金鑰的需求。此外傳統密碼系統雖然利於提供機密性的保護，但不利於提供不可否認性的功能。

網路的安全問題



電子認證技術之資訊安全服務

資訊安全服務項目	抵抗威脅	可採用防護技術
資料機密性服務 (Confidentiality)	● 竊聽 ● 非法取得資料 ● 資料洩露	加密系統 數位信封
資料完整性服務 (Integrity)	● 篡改 ● 重送 ● 損壞	訊息認證碼（MAC） 安全雜湊函數或數位簽章 序碼（Serial）或時戳（Time）
資料來源認證服務 (Authentication)	● 冒名傳送假資料	訊息認證碼（MAC） 數位簽章
不可否認服務 (Non-repudiation)	● 否認已收資料 ● 否認已送資料	數位簽章
存取控制服務 (Access Control)	● 非法存取資料	可信賴作業環境 防火牆系統、身份卡

密碼學基本技術

對稱與非對稱密碼系統(私密金鑰 vs.公開金鑰)

雜湊函數（Hash function）

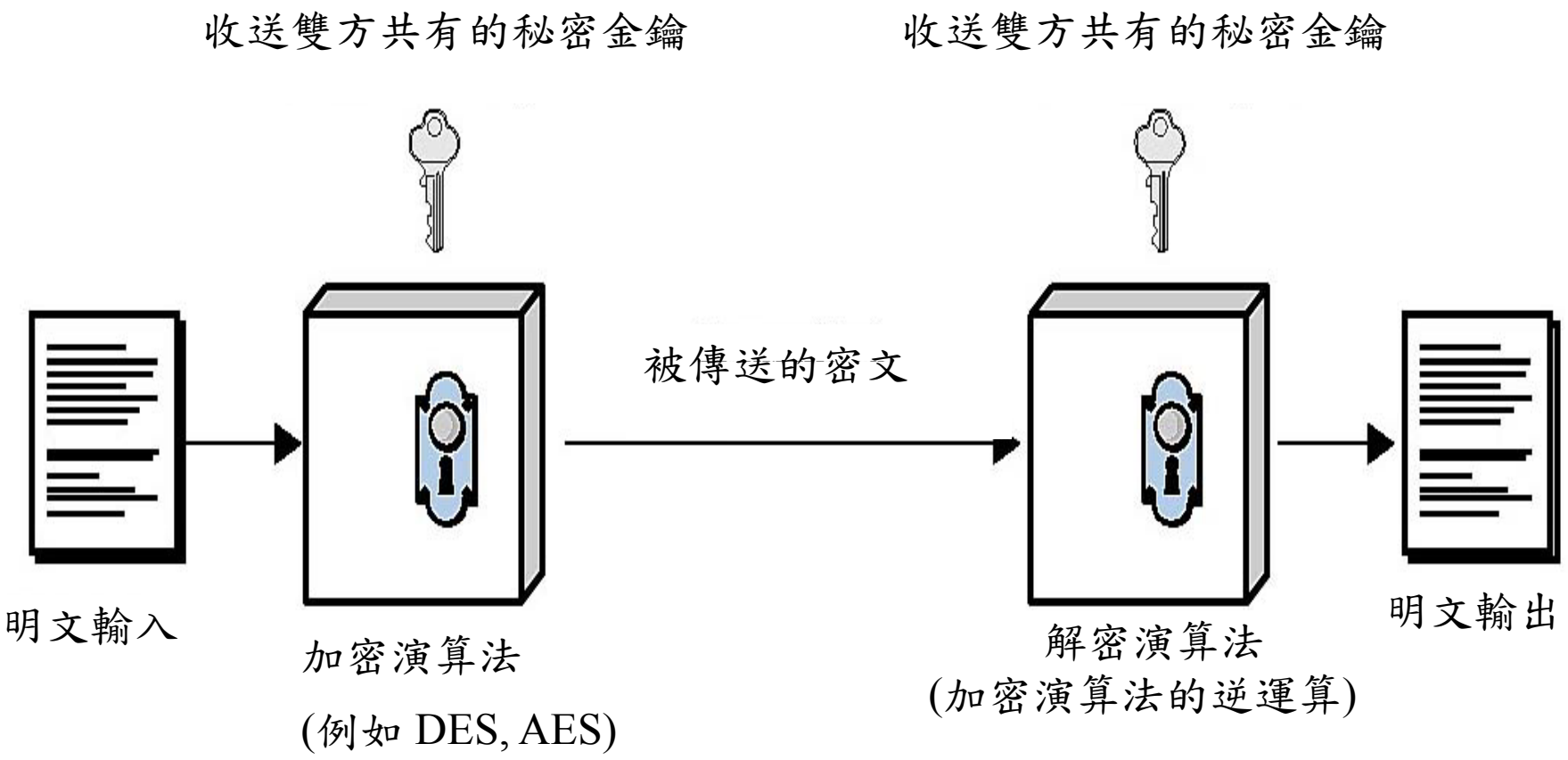
數位簽章（Digital signature）

數位信封（Digital envelope）

憑證作業（Certificate）

維護資料機密性—加密

對稱式加密法(傳統加密法)



對稱式金鑰加密方式

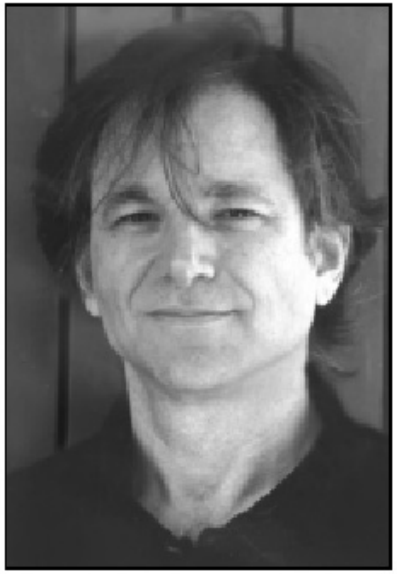
資料的加密及解密是採相同的金鑰

RSA-重要的公開金鑰演算法

- Rivest, Shamir, and Adleman 三位教授榮獲 2002 年Turing Award.
- Turing Award被稱為 “計算機的諾貝爾獎"

Ronald L. Rivest

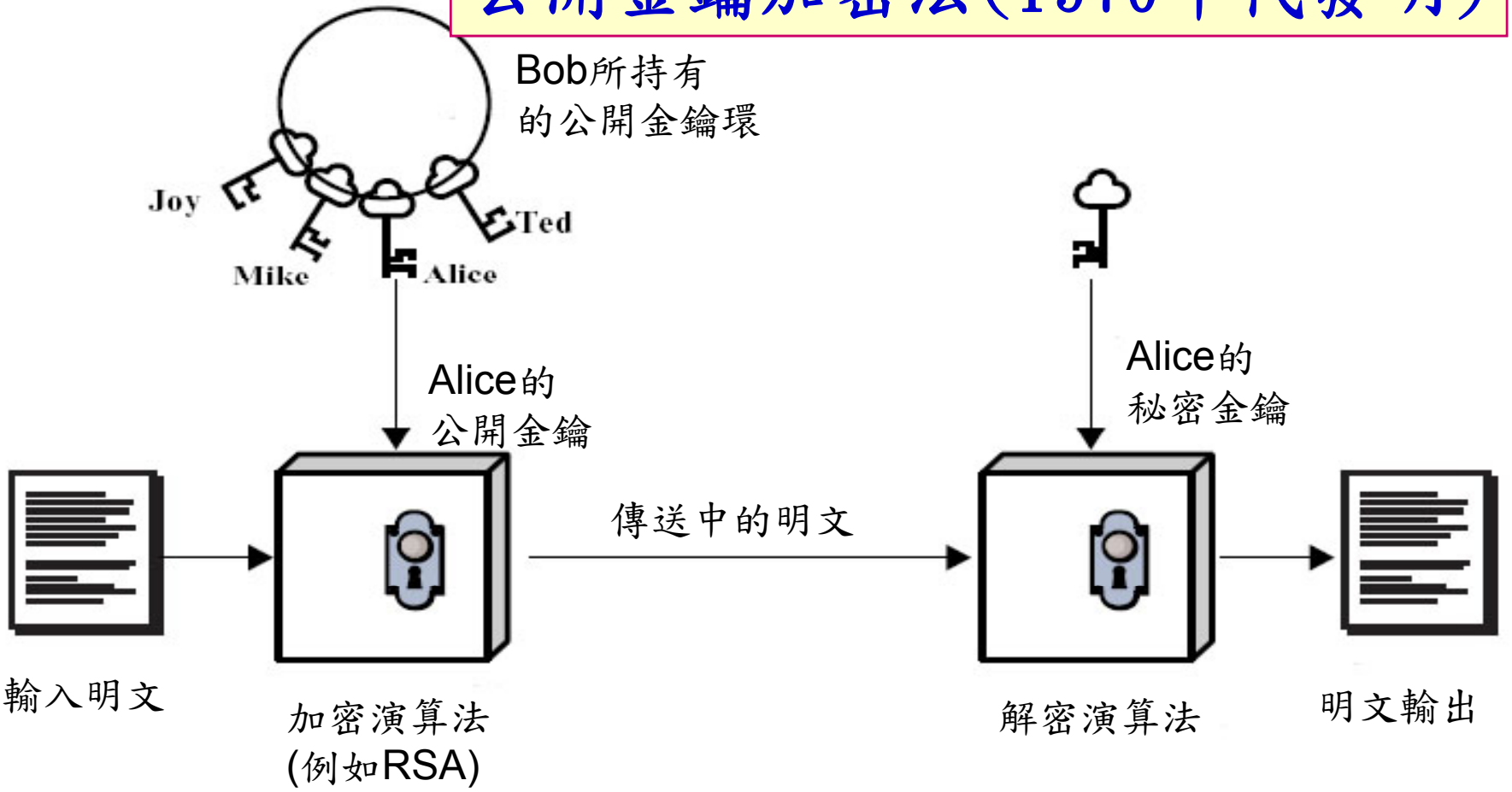
Adi Shamir



Leonard M. Adleman

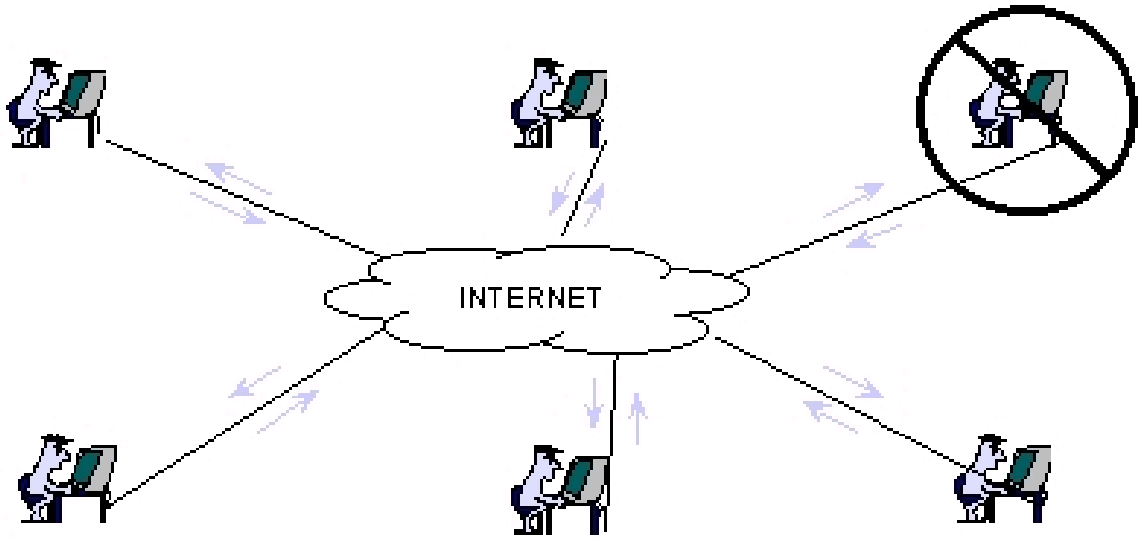
維護資料機密性—加密

公開金鑰加密法(1970年代發明)



對稱式金鑰加密方式

- 假使一把金鑰遭洩漏就必須更換所有金鑰
- 在交易上不具實用性及價值

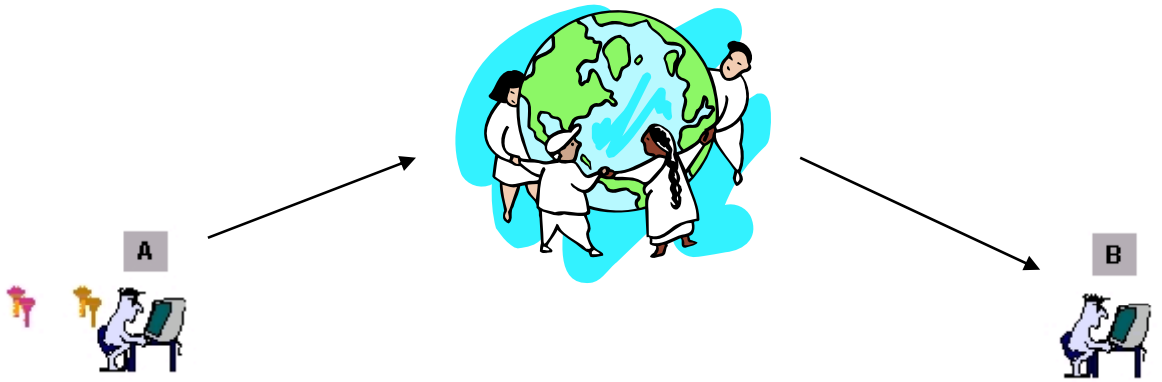


公開金鑰加密方式

- 公開金鑰加密是使用數學模式的加密架構, 採用不同的金鑰。
- 每個使用者有一對金鑰（公鑰及私鑰）。
- 經過公鑰加密的資料只能被成對的私鑰解密。

公開金鑰加密方式

- 公鑰是用作加密資料，以成對之私鑰解密。
- 私鑰是用作對資料簽章，以成對之公鑰驗證。

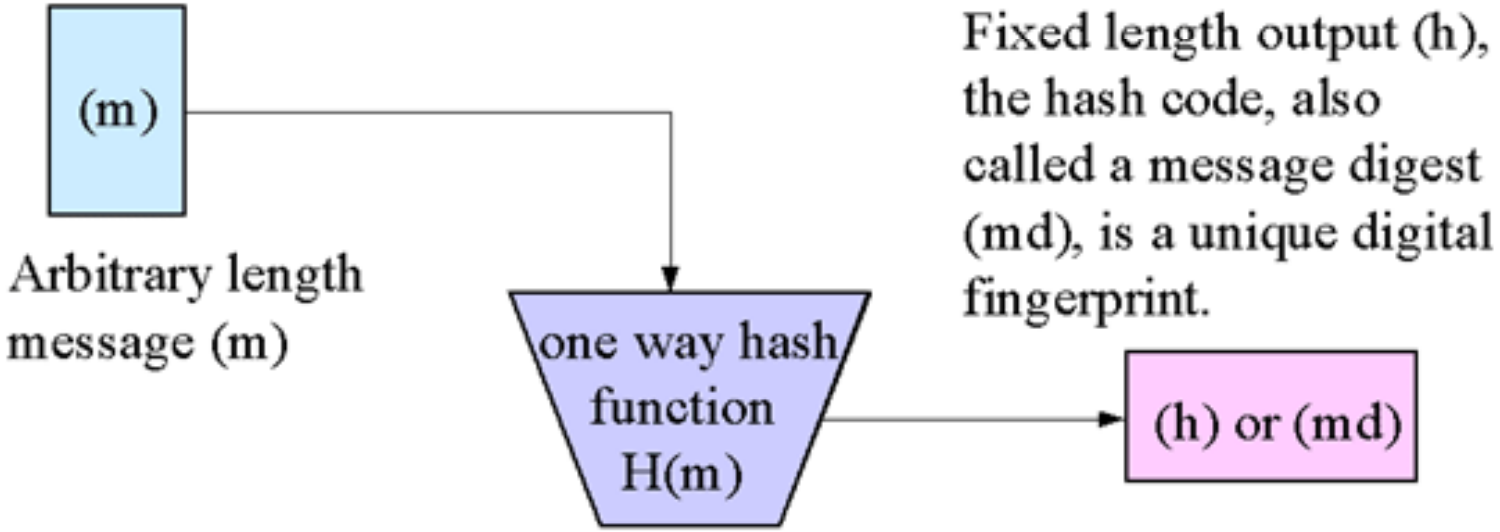


- A將公鑰送給B
- A使用私鑰來解開加密資料

- B利用A的公鑰加密
- B將加密的資料送給A

HASH function 加密方式

- Hash function 又稱為 Digital digest。
- 單向加密方式, 為不可逆反應。
- 提供資料的 fingerprint。

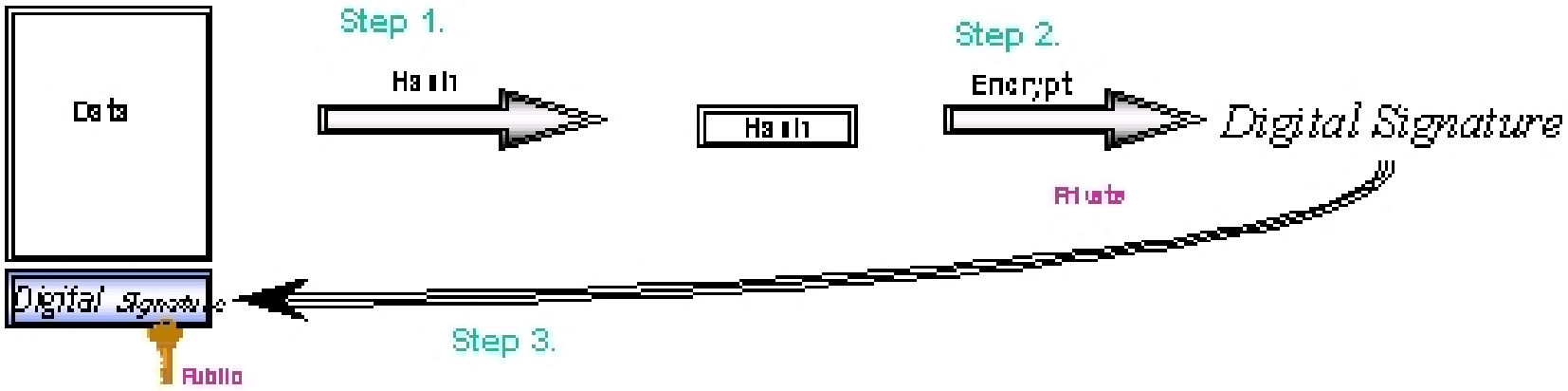


何謂數位簽章？

- 數位簽章是一個電子戳記伴隨資訊一同傳送。
- 數位簽章是對要交換的資料經過雜湊及加密的結果。
- 雜湊是一數學演算過程將資料簡化成一固定的長度的方法。
- 對一份文件經過相同的雜錯演算會得到唯一的值。
- 數位簽章類似封包彌封，避免接到竄改過之資料。
- 簽章過程與加密過程相反，主要是用私鑰來作加密，公鑰來驗證簽章。
- 數位簽章可以用作所有電子通訊，包括 Web, Mail及電子商務。

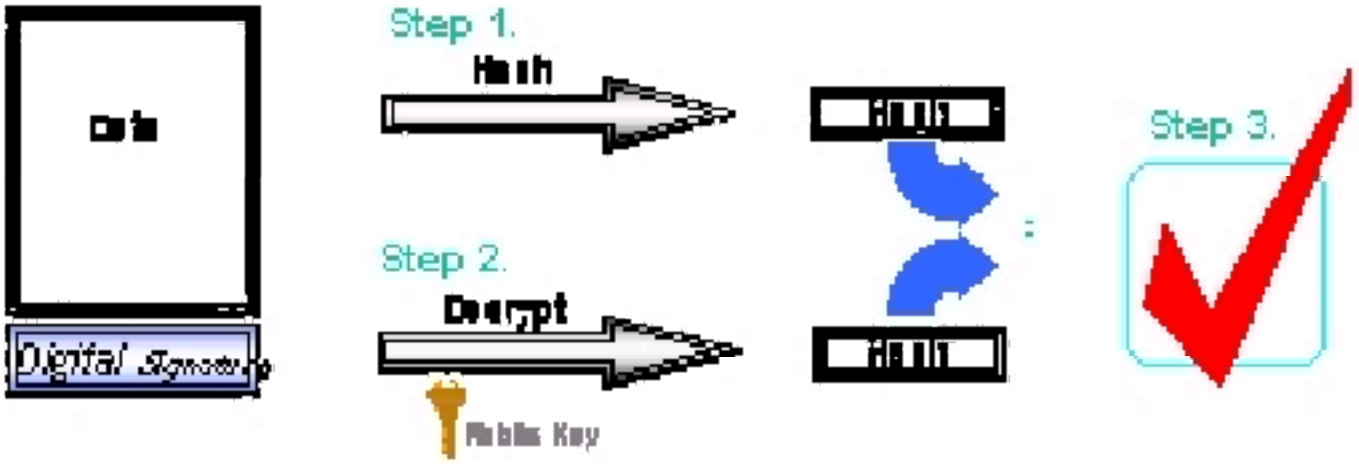
數位簽章的程序

- 第一步 ： 利用雜湊演算法將資料重新組合, 雜湊演算法有 MD2, MD5 或是 SHA-1 。
- 第二步 ： 利用傳送者的私鑰將雜湊資料加密,形成數位簽章。
- 第三步 ： 將數位簽章及公鑰附加到文件中一起傳送。

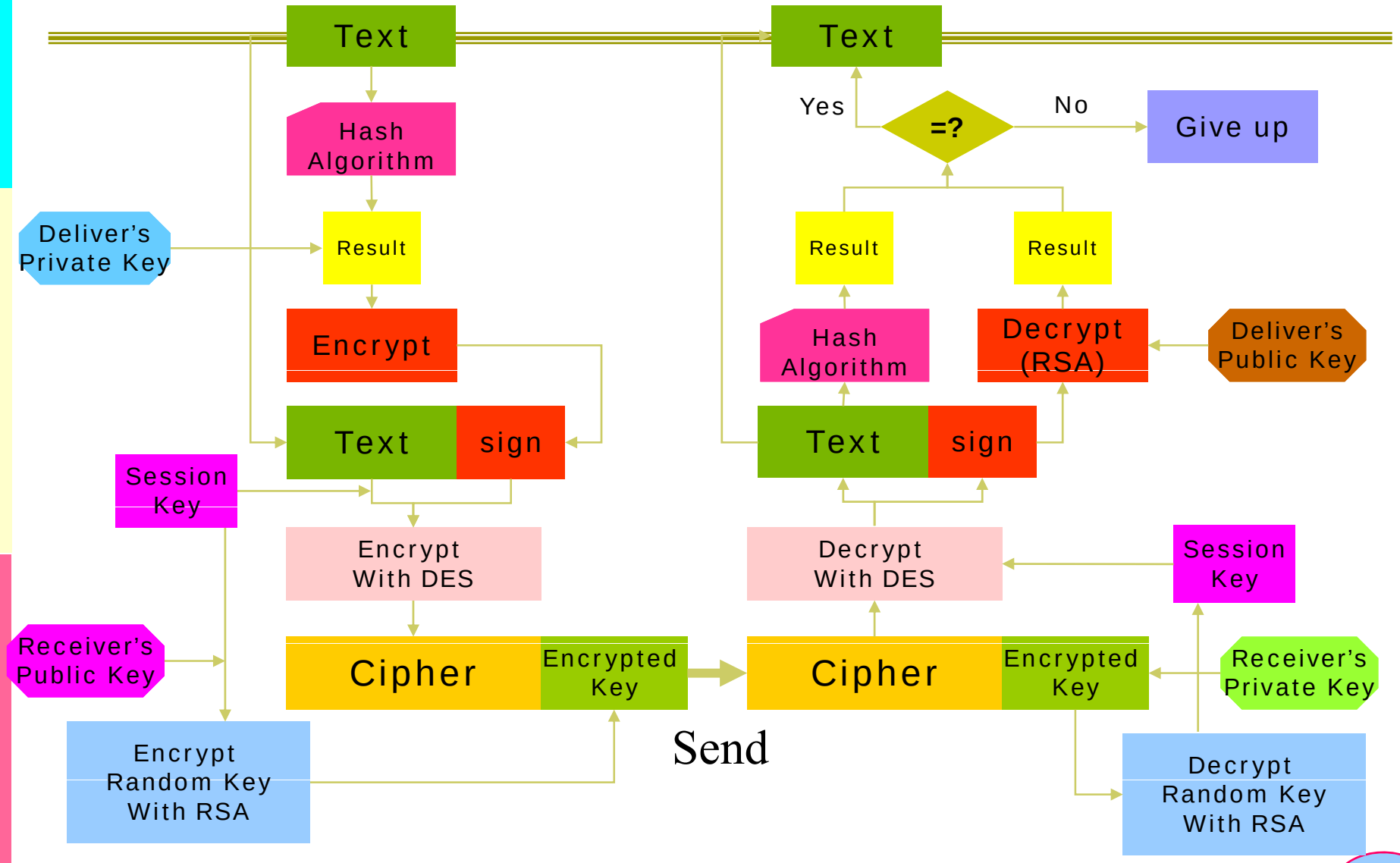


簽章驗證的過程

- 第一步 ： 用相同的雜湊演算法來對文件作處理。
- 第二步 ： 利用傳送者之公鑰來對數位簽章解密，所有數位簽章包含傳送者的公鑰。
- 第三步 ： 比較加密及解密後文件之雜湊值，假使核對無誤表示簽章經過驗證，假使雜湊值不相同，表示資料或是簽章在傳送時經過竄改。

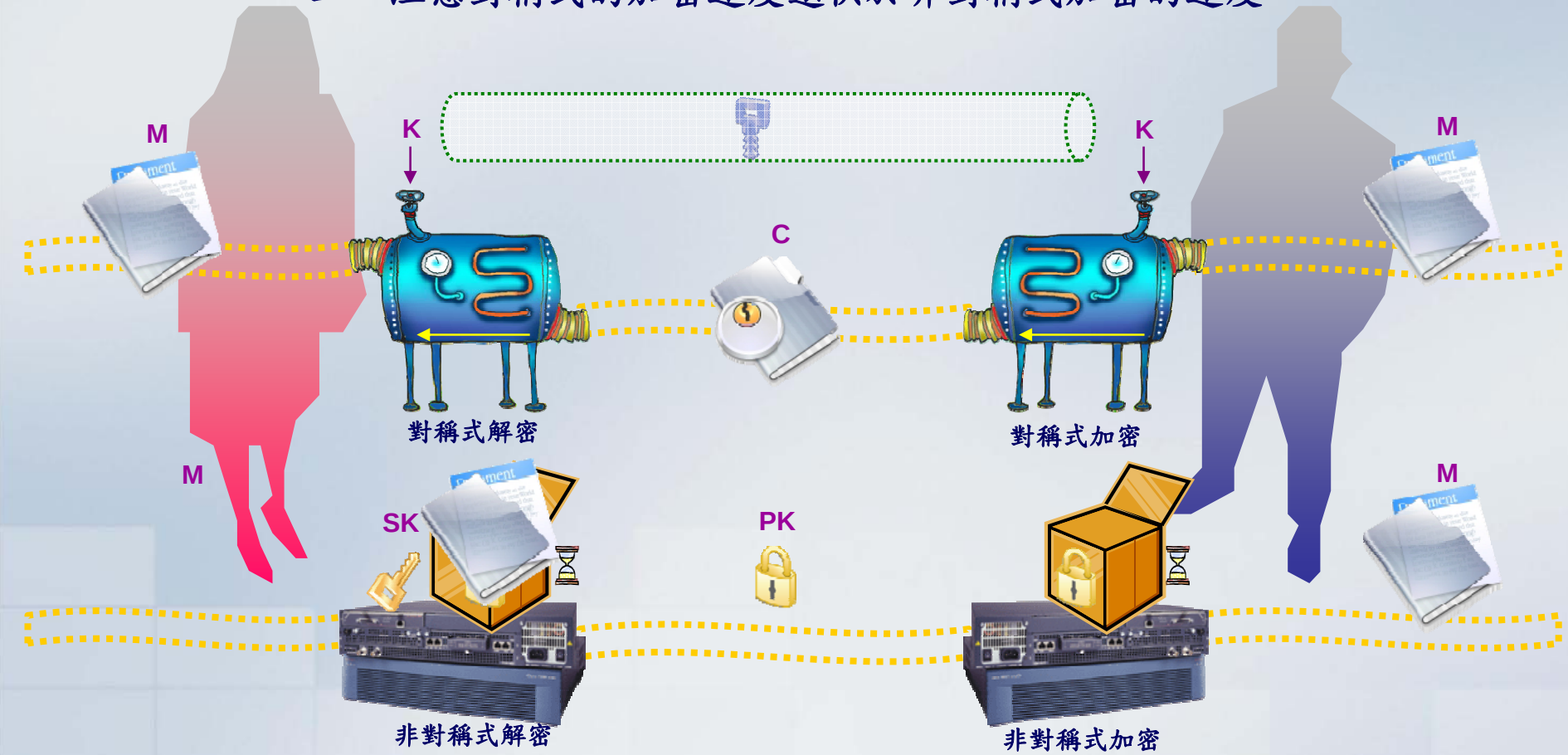


數位簽章之流程


Text
Hash Algorithm
Deliver's Private Key
Result
Encrypt
Text
sign
Session Key
Encrypt With DES
Receiver's Public Key
Cipher
Encrypted Key
Encrypt Random Key With RSA
Send
Text
Yes
=?
No
Give up
Result
Result
Hash Algorithm
Decrypt (RSA)
Deliver's Public Key
Text
sign
Decrypt With DES
Session Key
Cipher
Encrypted Key
Receiver's Private Key
Decrypt Random Key With RSA

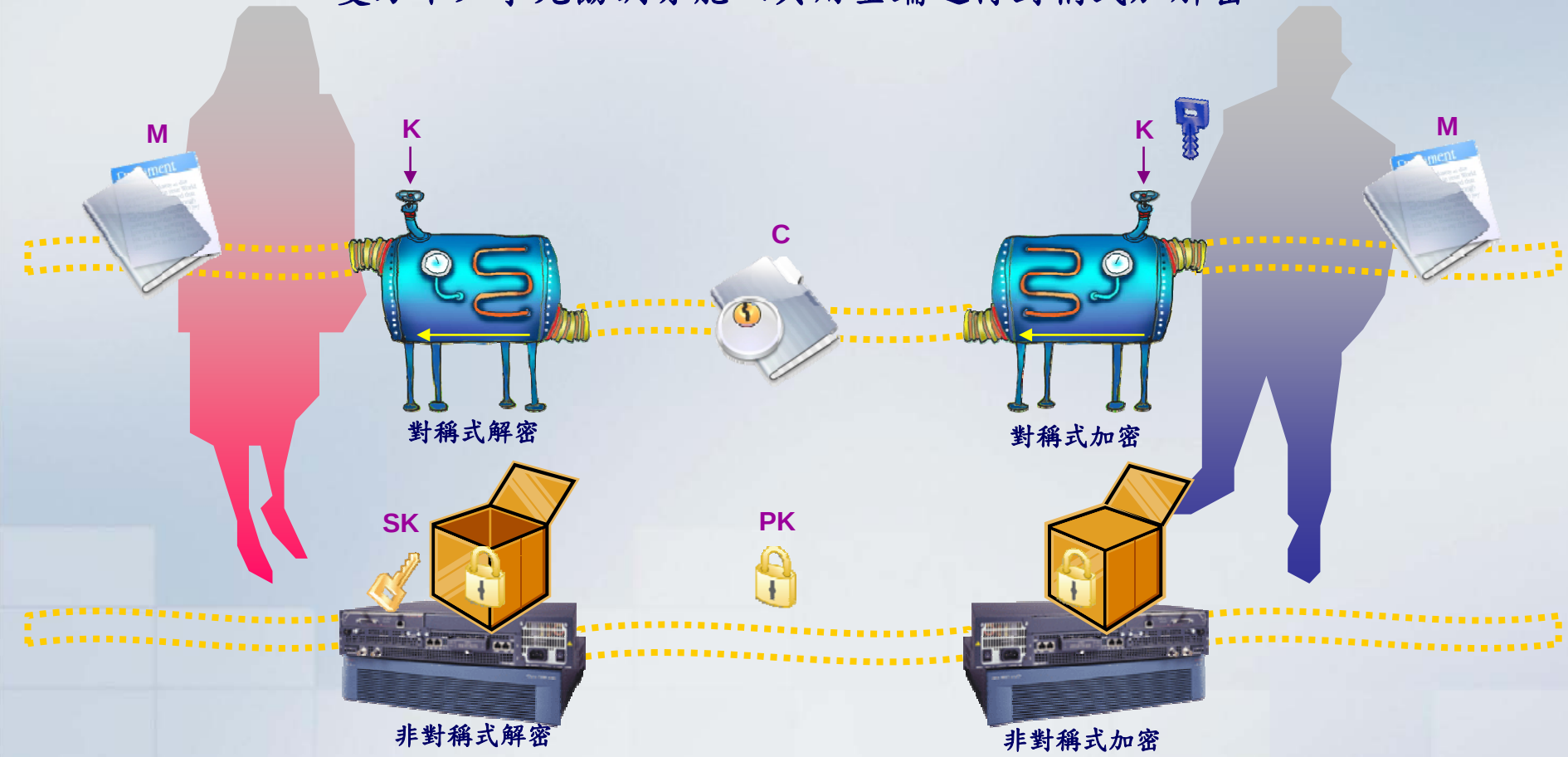
對稱式加密 v.s. 非對稱式加密

一、注意對稱式金鑰(K)與非對稱式金鑰(PK, SK)的差異
二、注意對稱式的加密速度遠快於非對稱式加密的速度



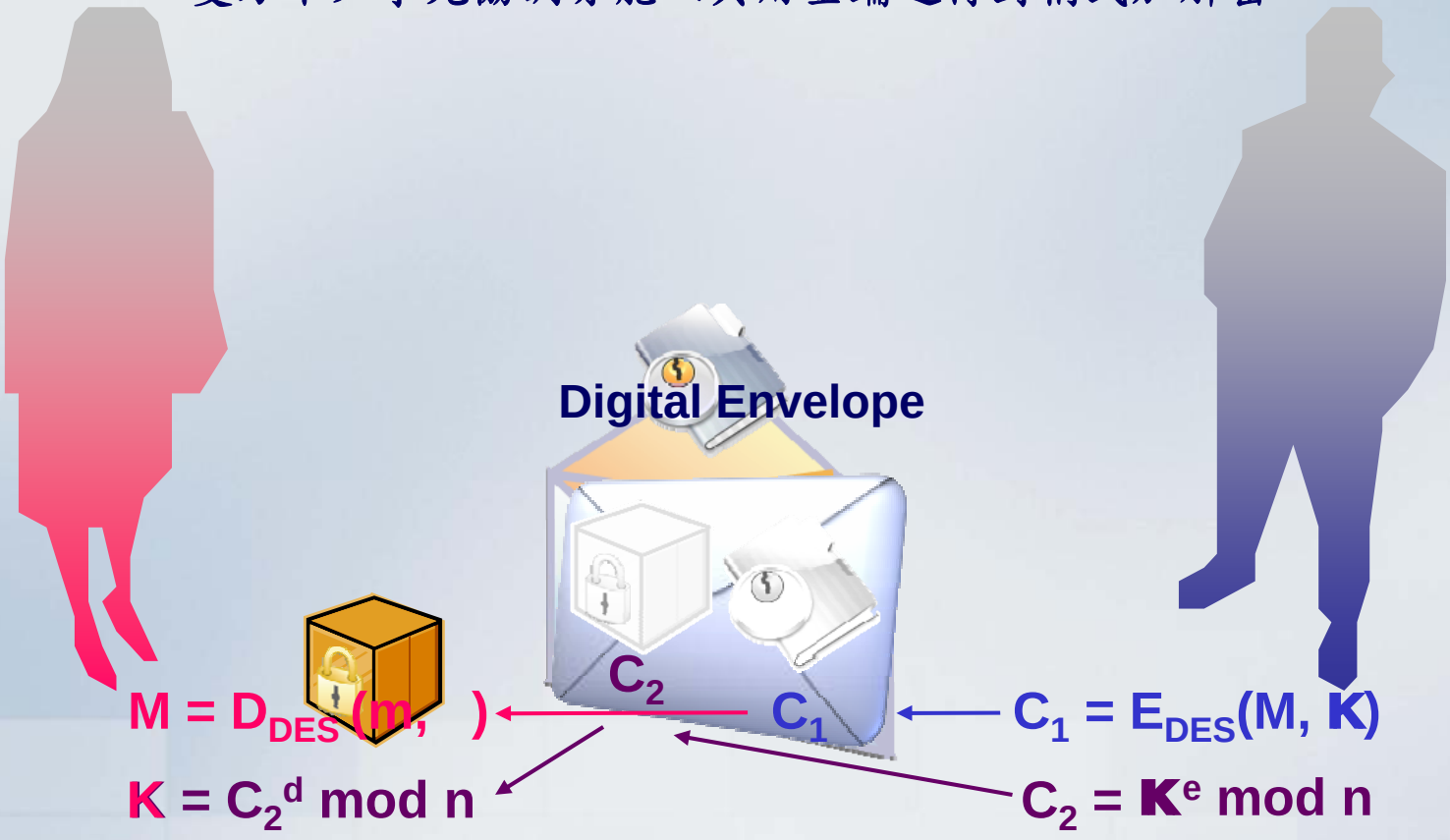
對稱式加密＋非對稱式加密 → 數位信封

對稱式加密的共用金鑰(K)若用非對稱式加密傳送之
雙方不必事先協調亦能以共用金鑰進行對稱式加解密

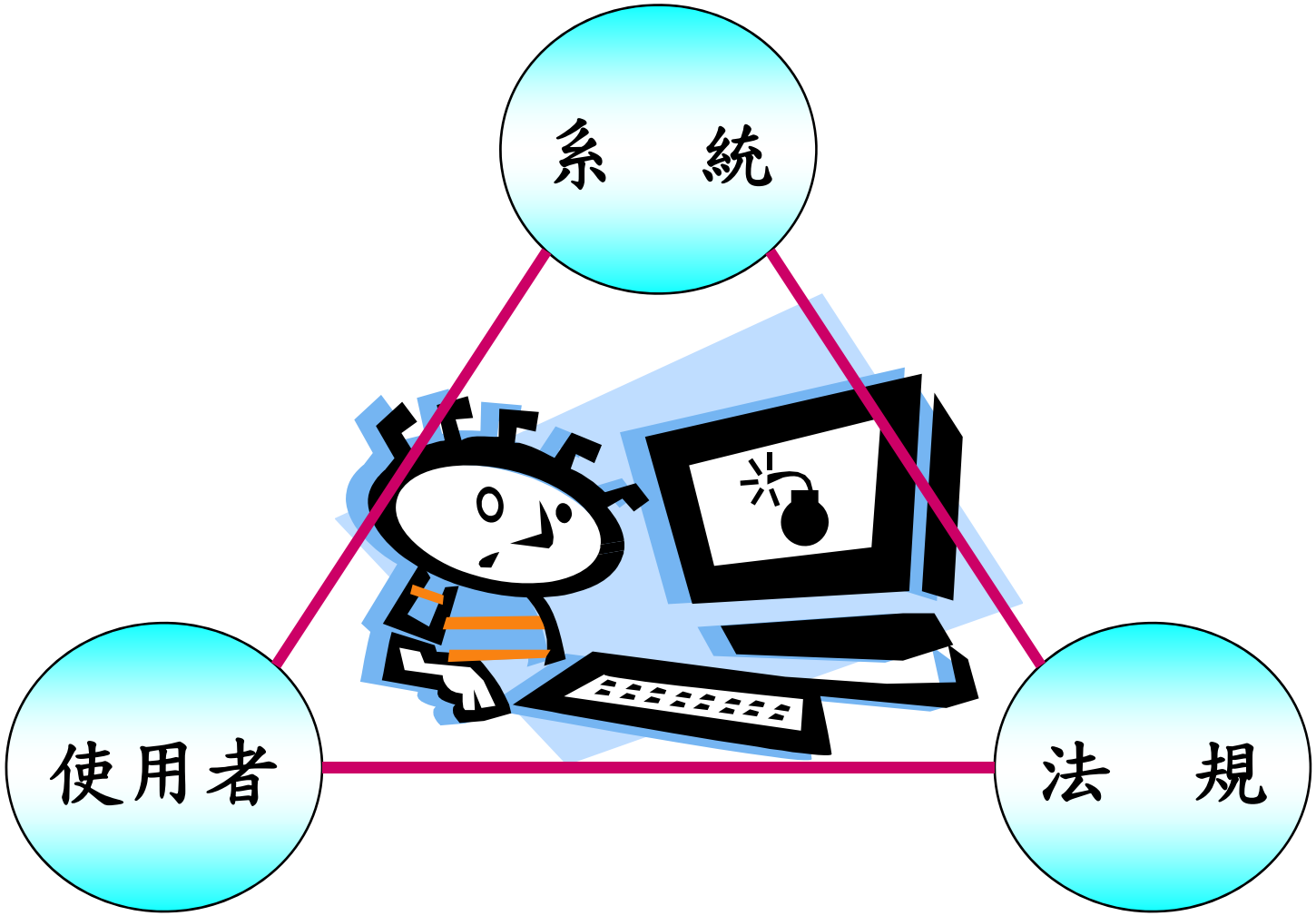


對稱式加密＋非對稱式加密 → 數位信封

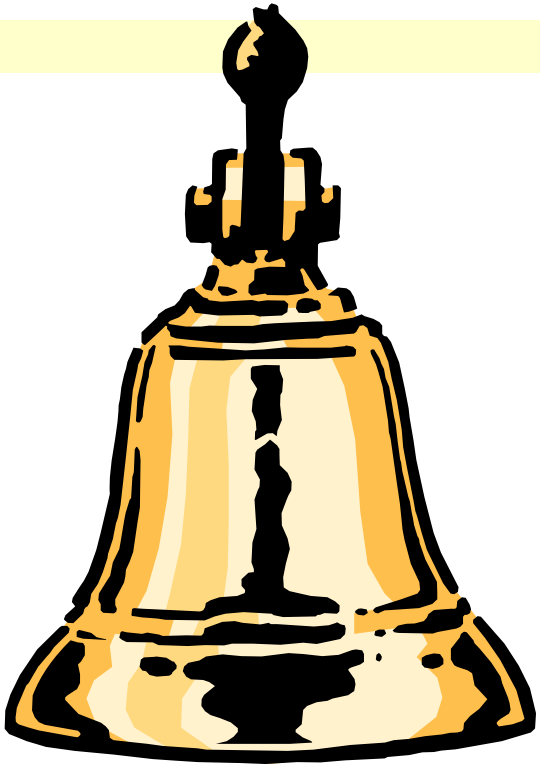
對稱式加密的共用金鑰(K)若用非對稱式加密傳送之
雙方不必事先協調亦能以共用金鑰進行對稱式加解密



五、資訊安全防護鐵三角

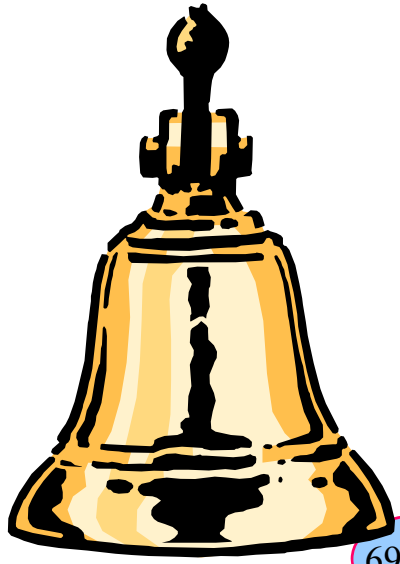


1.系統金鐘罩



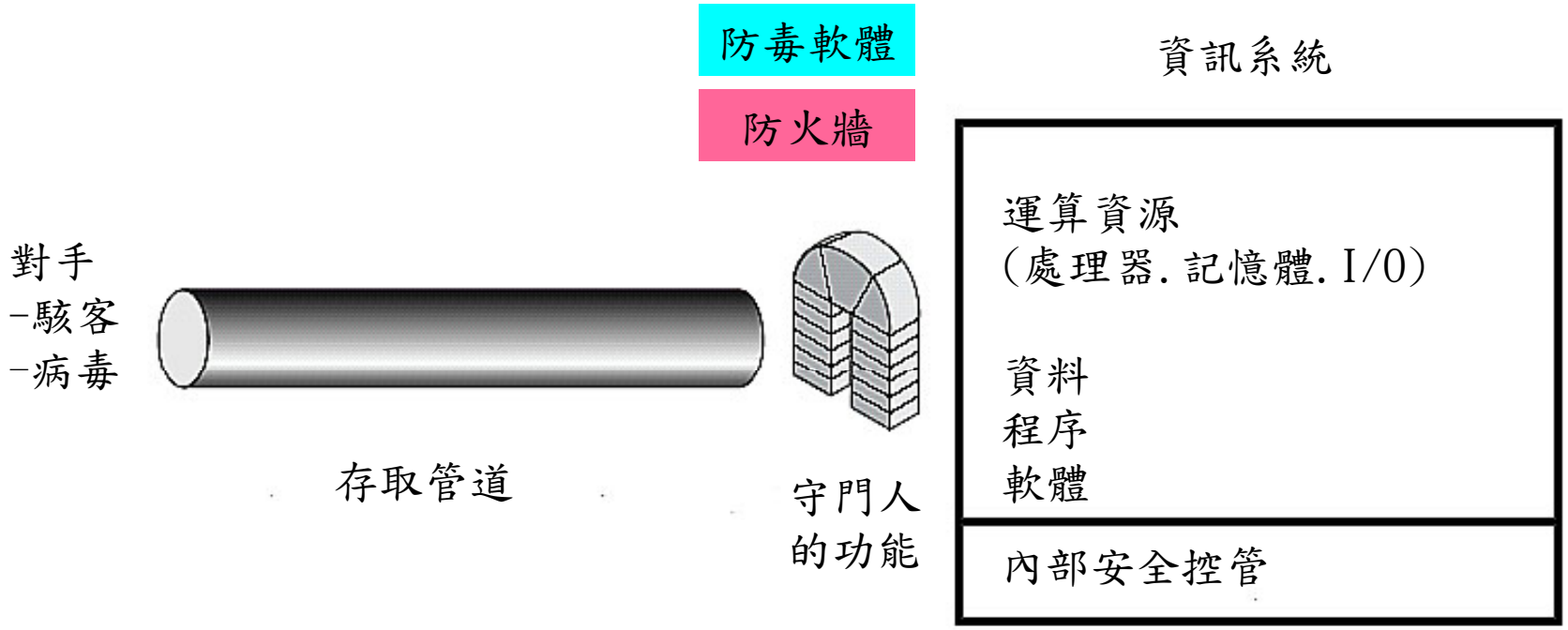
系統金鐘罩

- 系統應該要提供安全服務
  - 安全存取控制 (Access Control)
  - 安全認證 (Authentication)四要素
    - 資料機密性 (Data Confidentiality)
    - 資料完整性 (Data Integrity)
    - 不可否認性 (Non-repudiation)
    - 可用性 (Availability Service)
- 安全網站認證（信賴標章）
- SSL與SET安全電子交易



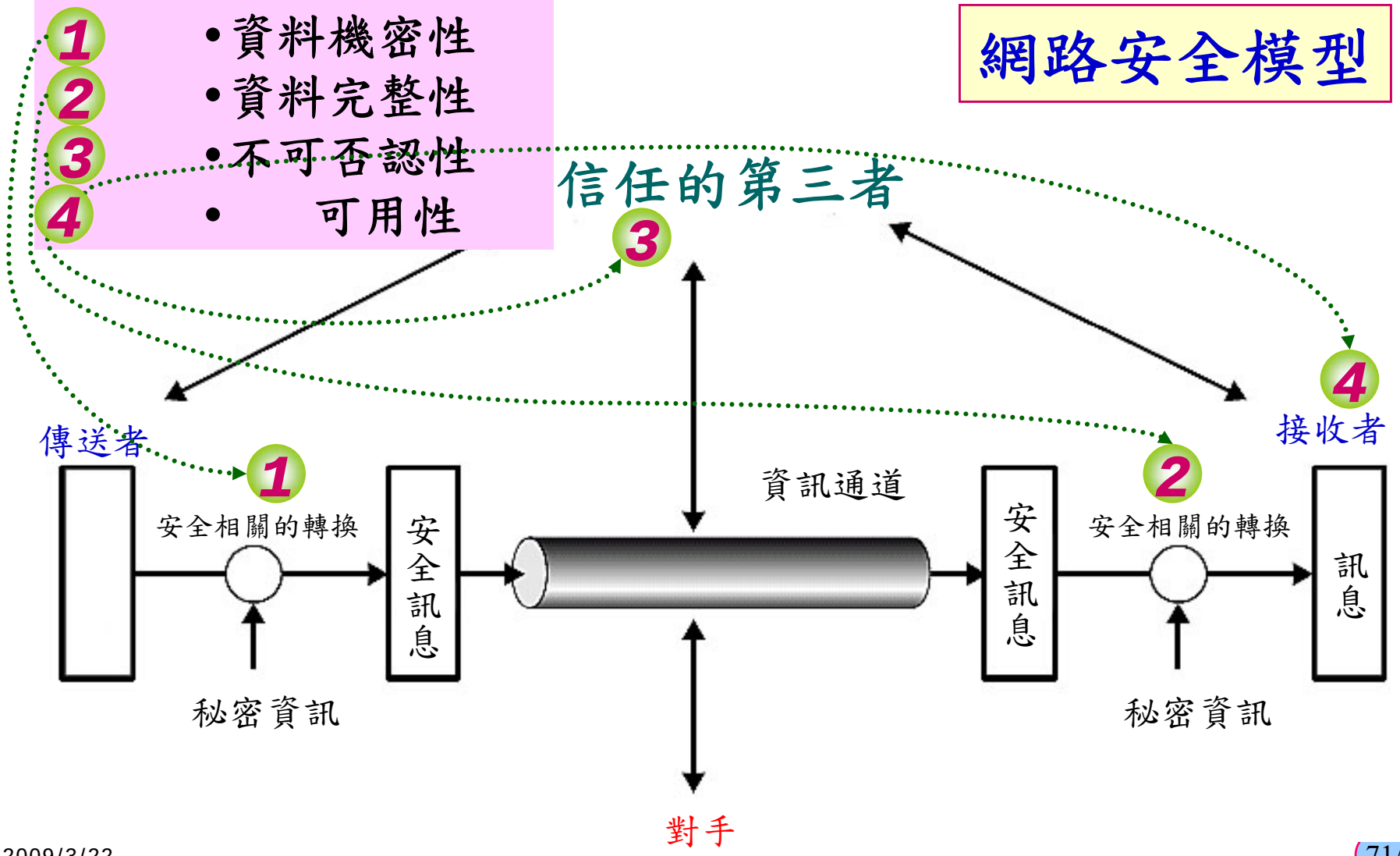
安全存取控制

網路存取安全模型



安全的認證（觀念）

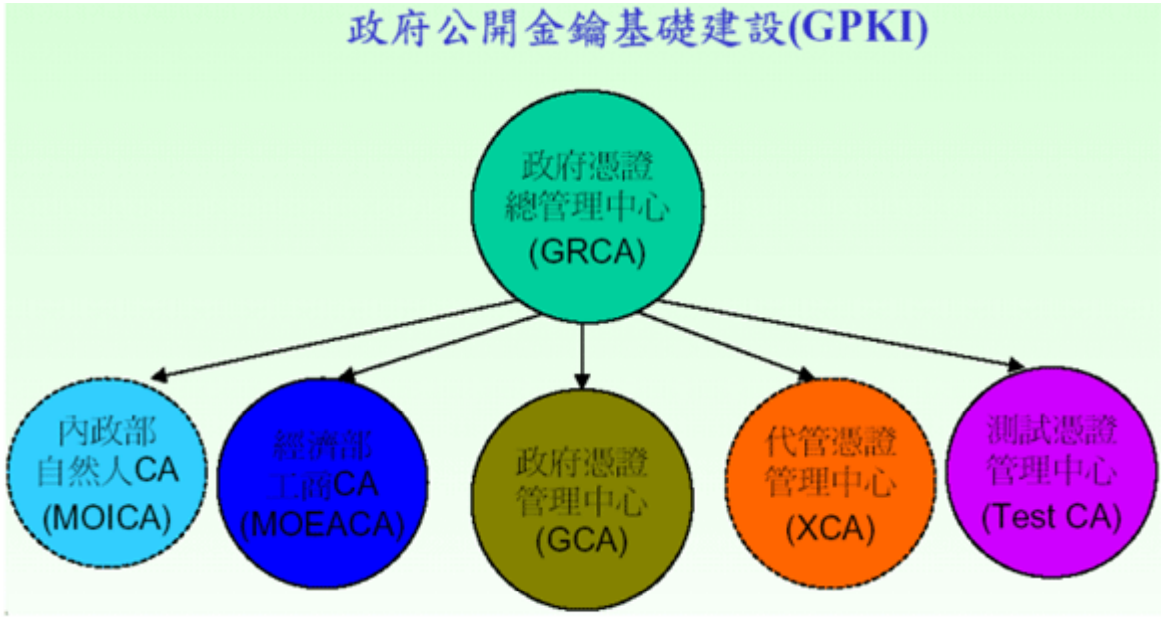
1. 資料機密性
2. 資料完整性
3. 不可否認性
4. 可用性



SSL網路安全傳輸機制

- SSL (Secure Socket Layer)
  - 一種Internet Commerce國際標準的網路安全協定，目的是保障網路交易的安全性。作法是透過資料加密的技術，傳輸的資料經過重新編碼，因此即使被攔截，攔截者沒有所謂的金鑰進行開啟(即無法進行資料的解密)，無法閱讀資料。
  - 但還是有要注意的地方：SSL在傳輸上面是安全的，不過它並不能辨識交易的對象，所以您在購物網站上的帳號和密碼，如金融卡的密碼，自己可要好好保密，以免遭人盜用。
- 如何得知網站有SSL加密？
  - 進入資料保護頁面時，網站位置(URL)前的協定名稱會由http變成https 。
  - 網站右下方顯示列中看到一個金鑰匙。

政府公開金鑰基礎建設(GPKI)



CA(Certificate Authority)
係一公正、公開的代理組織，負責核發、管理電子證書，並且存證。為指定的安全認證中心。

- 階層式的憑證管理架構。
- 政府憑證總管理中心(Government Root CA，GRCA)，做為整個GPKI的信賴基點。
- GRCA將簽發CA憑證給GPKI的下層CA 。

自然人憑證(公開金鑰憑證)

- 內政部憑證管理中心，負責簽發我國滿18歲以上國民之IC卡及公鑰憑證。
- 自然人憑證就是「電子身分證IC卡」，也就是「網路上的身分證」。
- 有「電子簽章」的功能，身分就可以確認，無法假冒。 有「電子密碼」的功能，傳送的資料都被密碼鎖住了，根本就解不開。
- 在家上網就可以經由網際網路享受政府E化服務。

網站認證

POSTSERV.PRSB.GOV.TW
是HiTRUST/VeriSign全球安全認證網站

身份鑑別	安全鑑別
• 中華郵政股份有限公司 確實擁有對 POSTSERV.PRSB.GOV.TW之網址使用權	此網站使用 Digital ID Class 3 - Affiliate Global Server Renewal 之安全加密等級。
• 經審查其所提供之文件，並查核政府資料庫之結果，確認其係一合法公司(機構)	您無須昇級您的瀏覽器，即可達到 128 位元的 SSL 高加密強度

憑證資料

申請網址

POSTSERV.PRSB.GOV.TW

效期

自Mar.09,2005至Mar.23,2006

憑證主旨(Subject)

Country = TW
State = Taiwan
Locality = Taipei
Organization = Postal Remittances and Savings Banks
Organizational Unit = PDPC
Organizational Unit = Terms of use at www.hitrust.com.tw/rpa (c) 04
Organizational Unit = Authenticated by HiTRUST Inc.
Organizational Unit = Member, VeriSign Trust Network
Common Name = postserv.prsb.gov.tw

網際網路

用滑鼠按一下

小圖示顯示SSL已經啟動

經濟部信賴電子商店

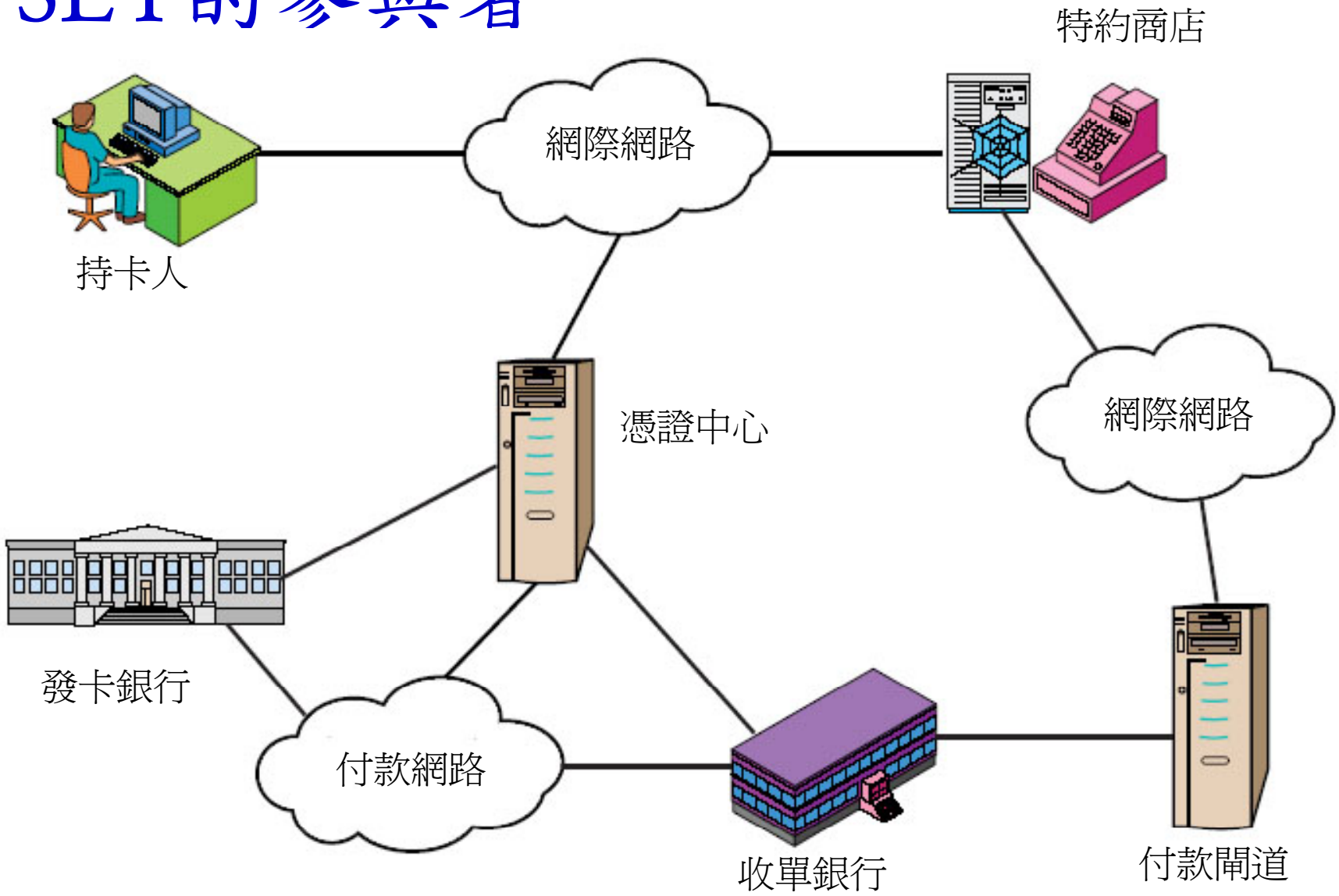
用滑鼠按一下

經濟部信賴電子商店

安全的電子交易 SET

- SET(Secure Electronic Transaction)
  - 一種在網際網路進行付款交易的安全機制，其規格採用**RSA**非對稱式運算法則（即利用公鑰及私鑰分別加密與解密）結合**DES**對稱式運算法則(加、解密為相同之基碼)為安全方案，用以保護網路付款交易之安全及隱密性。
- SET提供三種服務：
  - 為參與交易的節點提供一個安全通訊管道。
  - 能夠放心地使用數位憑證。
  - 在適當的時機與地點保障通訊雙方隱私權。

SET的參與者



2. 法規鐵布衫

台灣資訊安全相關法令規定

- 電子簽章法(制定/修正日期:2001年10月31日)(公布/施行日期:2001年11月14日)
- 電子簽章法施行細則
- 電信業電腦處理個人資料管理辦法
- 通訊保障及監察法
- 通訊保障及監察法施行細則
- 電腦處理個人資料保護法(制定/修正日期:1995年7月12日)(公布/施行日期:1995年8月11日)
- 電腦處理個人資料保護法施行細則
- 執行電腦處理個人資料保護事項協調連繫辦法
- 醫院電腦處理個人資料登記管理辦法
- 徵信業電腦處理個人資料辦法
- 不動產仲介經紀業電腦處理個人資料管理辦法
- 私立學校及學術研究機構電腦處理個人資料管理辦法

台灣資訊安全相關法令規定

- 私立就業服務機構電腦處理個人資料管理辦法
- 行政院環境保護署電腦處理個人資料管理辦法
- 金融業個人資料檔案安全維護計畫標準
- 保險業個人資料檔案安全維護計畫標準
- 證券業暨期貨業個人資料檔案安全維護計畫標準
- 行政院及所屬各機關資訊安全管理要點
- 電信法
- **中華民國刑法（第三十六 章 妨害電腦使用罪）**
- 商業使用電子計算機處理會計資料辦法
- 建立證券商/期貨商資通安全檢查機制
- **著作權法**
- 國家機密保護法
- **刑法防駭條款**
- 參考網站：http://www.i-security.tw/law/law.asp

法規鐵布衫

- 保障隱私權
  - 電腦處理個人資料保護法
  - 刑法第28章「妨害秘密罪」
  - 電信法
- 保障網路交易安全
  - 消費者保護法
  - 電子簽章法

隱私權

- 定義
  - 一種保有個人獨居不受干擾，避免暴露於公眾的權力，是一種免於刺探的權力。
- 憲法保障人權
  - §10人民有居住及遷徙之自由。
  - §12人民有秘密通訊之自由。
  - §22：凡人民之其他自由及權利，不妨害社會秩序公共利益者，均受憲法之保障。

個人資料保護法

- 電腦處理個人資料保護法（84年施行）
  - 法案名稱改為「個人資料保護法」，擴大保護的客體，不再以電腦處理個人資料為限，同時刪除非公務機關行業別的限制，明定除個人或家庭活動之目的外，任何自然人、法人或其他團體蒐集、處理或利用個人資料，皆適用本法之規定。
  - 擴大個人資料之定義與保護範圍，新增醫療、基因、性生活、健康檢查及犯罪前科等五類特種資料，若非符合法定要件，不得蒐集、處理或利用。
  - 提高相關罰責，若為圖利而非法使用他人資料，最高可處五年以下有期徒刑，並得併科五百萬元以下罰金。

個資法運用規範

- 商業利用之特定目的與符合§18所列各款：
  - 經當事人書面同意者。
  - 與當事人有特別約定而對權益無侵害的危險者。
  - 已公開的資料且無害於當事人的重大利益者。
  - 為學術研究且無害於當事人的重大利益者。
- 賦予網路用戶的權利
  - 1.查詢及請求閱覽。　　2.請求製給複製本。
  - 3.請求補充或更正。　　4.請求刪除。
  - 5.請求停止電腦處理及利用。

刑法第28章「妨害秘密罪」

- §315妨害書信秘密罪 告
- §315-1窺視、竊聽、竊錄罪 告
  - 窺視、竊聽，竊錄他人非公開之活動、言論或談話或身體隱私部位者。
- §315-2加重窺視、竊聽，竊錄罪 非
  - 圖利便利他人妨害秘密（幫助犯)。
  - 意圖散佈、播送、販賣而竊錄。
  - 製造、散佈、播送、販賣竊錄內容。

電信法

- §6 保障通信秘密
  - 電信事業及專用電信處理之通信，他人不得盜接、盜錄或以其他非法之方法侵犯其秘密。電信事業應採適當並必要之措施，以保障其處理通信之秘密。
- §7 從業及退職人員嚴守秘密
  - 電信事業或其服務人員對於電信之有無及其內容，應嚴守秘密，退職人員，亦同。
- §56-1 侵害通信秘密罪
  - 違反第六條第一項規定侵犯他人通信秘密者，處五年以下有期徒刑，得併科新臺幣一百五十萬元以下罰金。
  - 電信事業之負責人或其服務人員利用業務上之機會，犯前項之罪者，處六月以上五年以下有期徒刑，得併科新臺幣二百萬元以下罰金。
  - 前二項之未遂犯罰之。犯第一項之罪者，須告訴乃論。

消費者保護法與電子商務

- 網路交易列為郵購買賣
  - §18 書面告知義務（買賣條件，經營場所…）。
  - §18 商品送達前之解約權。
  - §19 無條件退貨解約權（七日內）。
- 網路廣告
  - §22 (真實廣告之義務)確保廣告內容真實，對消費者所負義務不得低於廣告內容。
  - §23-1 (不實廣告之損害賠償)明知或可知託播廣告不實，需負連帶責任，且不得預先約定限制或拋棄。

電子簽章法

- 數位簽章：
  - 指將電子文件以數學演算法或其他方式運算為一定長度之數位資料，以簽署人之私密金鑰對其加密，形成**電子簽章**，並得以公開金鑰加以驗證者。
- 數位簽章可提供四種重要的安全保證:
  - **資料完整性**：文件接收者透過數位簽章之核對可確保此文件的完整性，避免被篡改、重送、遺失。
  - **資料來源辨識**：文件接收者可確認此文件之發送者的身分，避免被冒名傳送假資料。
  - **資料隱密性**：文件可以利用金鑰來加密、解密，以達到保密的安全保證。
  - **不可否認性**：因為只有文件發送者知道自己的私密金鑰，而且文件具有發送者之數位簽章，使其無法否認發送此文件的事實。

3.使用者好習慣

- 防駭入侵與密碼選擇策略。
- 預防惡意程式的入侵。
- 不要對陌生網友洩漏個人隱私資料。
- 不要任意註冊來路不明的網路服務。
  - 尤其不要拿身份證ID或是生日作為註冊帳號。
- 不要太有好奇心，網路是非多，小心為上。

密碼選擇策略與保護措施

- 系統管理者
  - 定期檢查密碼檔。
  - 由電腦產生密碼。
  - 事先審核密碼。
  - 系統將密碼檔加密。
  - 密碼檔存取控制。
- 一般使用者
  - 不要將密碼抄在電腦旁。
  - 不要用個人資料或簡單的數字作為密碼。

密碼設定的安全性

- 密碼遭破解之統計數據

密碼長度	26 英文字母	26 英文字母 +10 數字	52大小寫 英文字母	96 可印出字元
4	0	0	1 分鐘	13分鐘
5	0	10分鐘	1 小時	22 小時
6	50分鐘	6 小時	2.2 天	3 個月
7	22 小時	9 天	4 個月	[illegible]
8	24 天	10.5個月		
9	21 個月	32.6 年		
10	45 年	1159 年		2100萬年

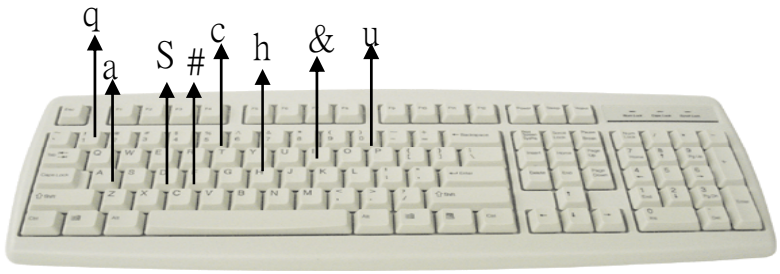
密碼設定要穩固
加強密碼的強度
密碼應定期更換

密碼設定小技巧

1. 以注音輸入法按鍵來當成密碼
   你好嗎 → Su#cla#8&

2. 以英文字或數字穿插
   good + 5829 → g5o8o2d9

3. 將英文字母往前位移,如Birthday往前位移1個字母Ahqsgczx



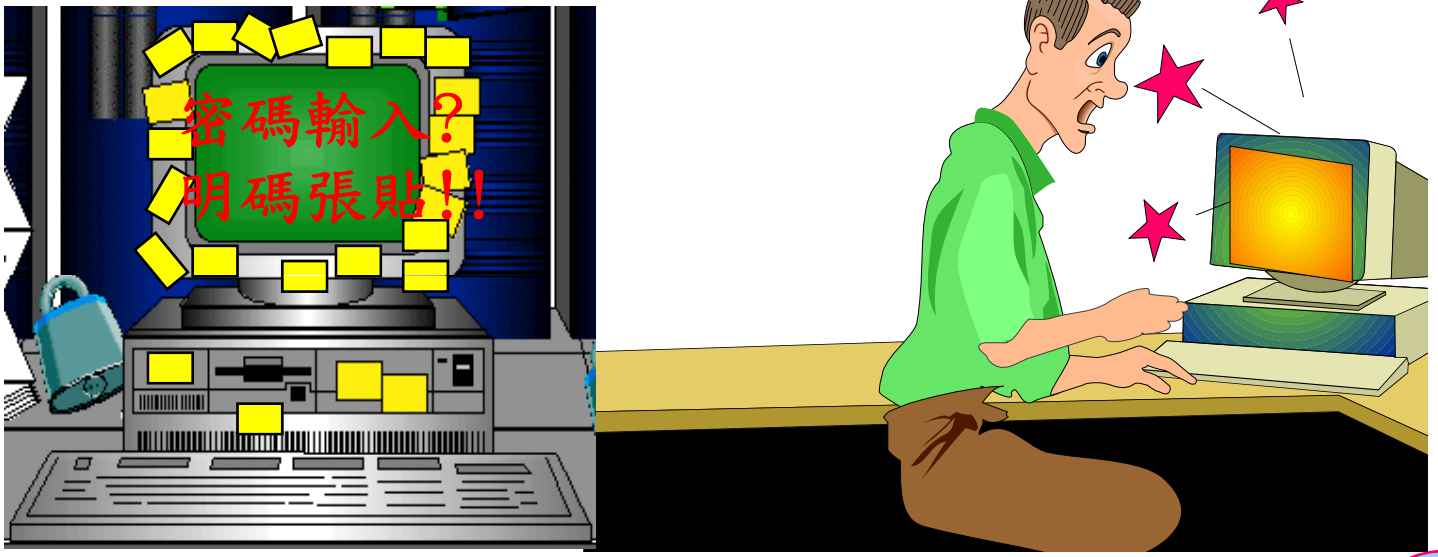
4. 以英文的一句諺語或一段歌詞取每個英文字字首當成密碼
   Best wishes for a happy New Year. →BwfahNY

如何保護密碼？

- 第一招：好密碼
- 嚴禁不設密碼。
- 與帳號相同、與主機相同 。
- 設定原則:
  - >= 8 個文數字。
  - 不是有意義的字。
  - 字母大小寫混合。
- 好的密碼:
  - **SSd5tion**
- 不好的密碼
  - **abcd**

如何保護密碼？

- 第二招：帳號密碼不外漏
  - 不將帳號密碼寫下來。
  - 不要將密碼貼在螢幕、鍵盤、桌面或隔板上。

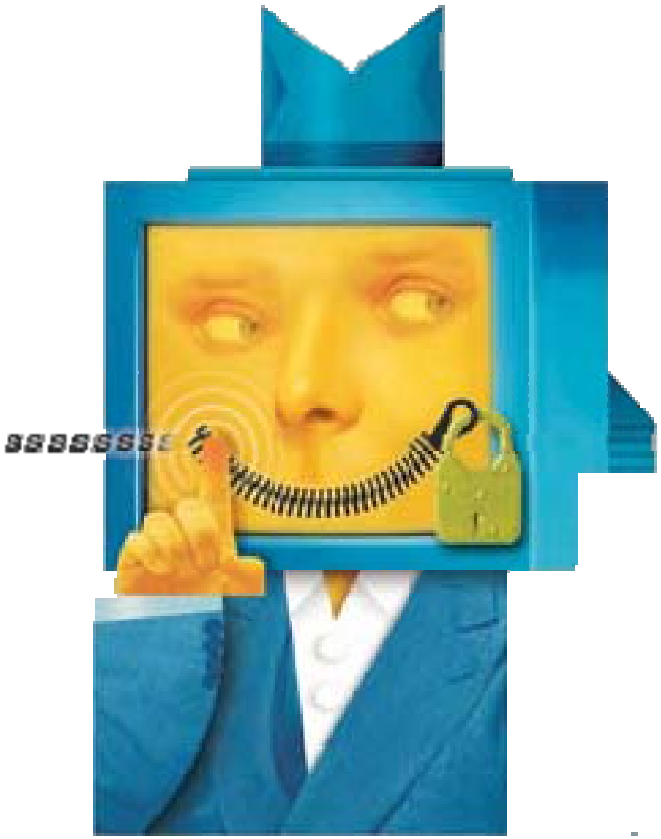


如何保護密碼？

- 第三招：螢幕保護
  - 設定密碼保護。
  - 設定幾分鐘後自動啟動螢幕保護。
  - 定期更換密碼。

如何保護密碼？

- 第四招：立即登出
  - 登出 (log off) 。
  - 簽出 (log out) 。



如何保護密碼？

- 第五招：公司與家不用相同密碼
  - 家中電腦保護程度較差。
  - 被入侵或截取可能危及公司的安全。

如何保護密碼？

- 第六招：不用自動儲存密碼
  - 瀏覽器大多有自動儲存帳號與密碼功能。
  - 萬一有人使用就可以自動登入系統。

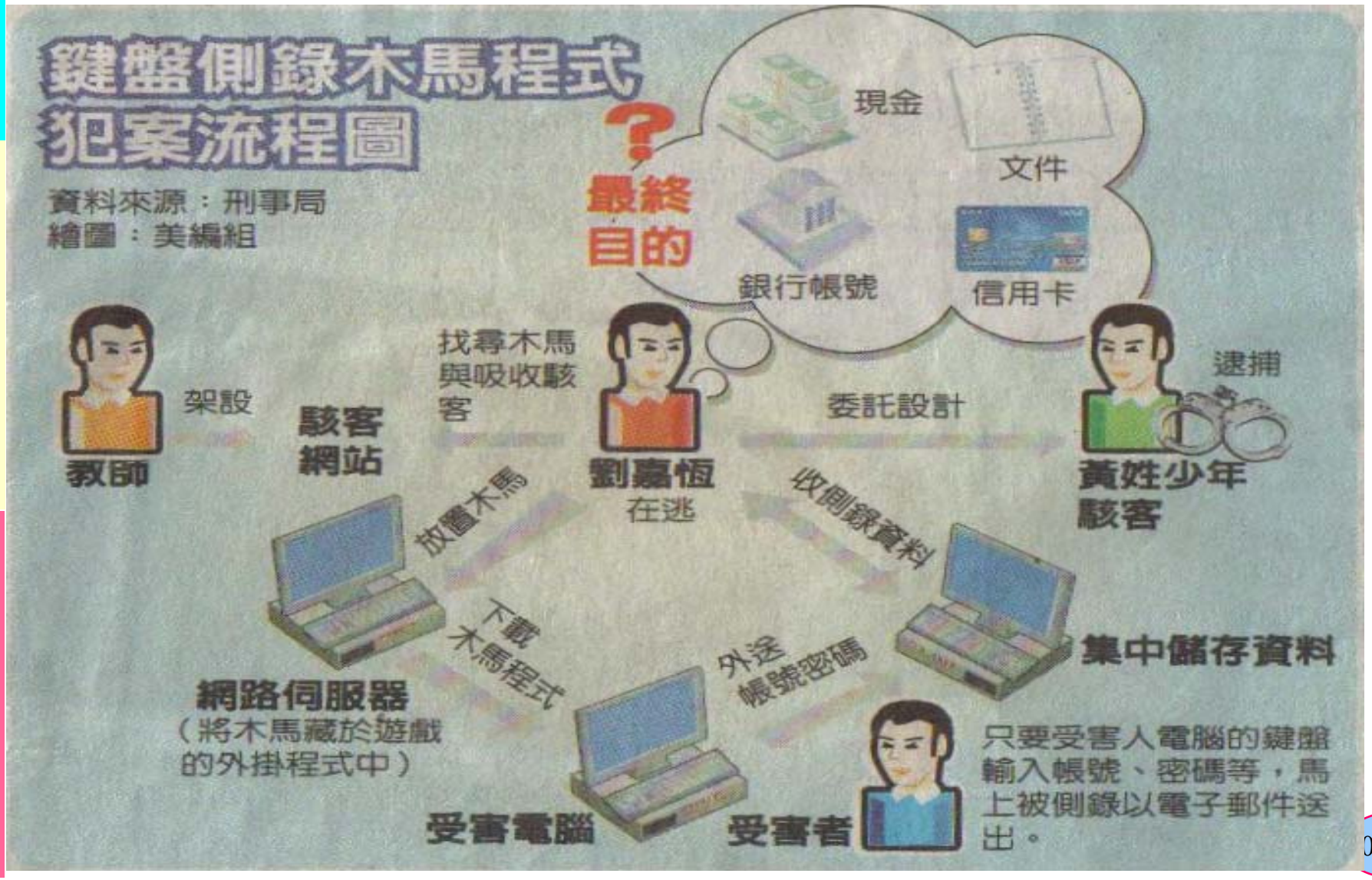
如何保護密碼？

- 最後一招：向誰求助
  - 異常時先將網路線拔除。
  - 求助資訊人員處理。

預防惡意程式的入侵

- 不隨便上網亂抓資料，有跳出視窗問你是否安裝時，不要隨意就按下YES 。
- 不輕易開啟或執行來源不明 E-Mail 中的附加檔案。
- 選擇一套值得信賴的防毒軟體，並設定自動定期更新病毒碼及引擎。
- 設定自動更新作業系統的修復工具或更新版，以修補系統漏洞。

個案：少年為駭網路 資料來源：2005/02/26自由時報



個人資訊安全守則 1

- 不要任意使用來路不明的程式：
  - 不使用來路不明之程式。
  - Email內之exe之附件。
  - 不明網站之程式。
  - 以免讓自己的電腦淪為駭客入侵電腦系統的後門。

資訊安全守則 2

- 使用穩當的密碼
  - 設定密碼可加入符號。
    - 「!@#$%^&*?」
  - 定期更改密碼。
  - 設定穩當的密碼。
    - 使用每個字的第一個字母："I went to Taipei " 可以翻譯成：IwtTpe
    - 微軟密碼強度測試網站 (http://www.microsoft.com/taiwan/athome/security/privacy/password_checker.mspx)

個人資訊安全守則 3

- 作業系統安全更新程式
  - 定期安裝Windows Update
    - 說明：
      - 請定期安裝Windows Update以保持windows作業系統安全
    - 執行步驟：
      - (1)網址是 http://v4.windowsupdate.microsoft.com/zhtw/default.asp
      - 或可從　開啟IE瀏覽器=>工具=>點選"Windows Update"
- 使用反間諜軟體 (20.2MB)

  http://www.download.com/Ad-Aware-2007-Free/3000-8022_4-10045910.html?part=dl-ad-aware&subj=dl&tag=top5
- 系統安全掃描工具

  http://onecare.live.com/site/zh-tw/default.htm

個人資訊安全守則 4

- Windows Live OneCare 家長監護系統—掌握小孩的線上活動 https://fss.live.com/Default.aspx
- 使用防毒軟體及定期更新病毒碼
  - 防毒程式
    - 賽門鐵克(http://www.symantec.com.tw)
    - 趨勢科技 (http://www.trendmicro.com/tw/home/enterprise.htm)
    - 卡巴斯基 (卡巴斯基實驗室) (http://www.kaspersky.com.tw/)
    - AntiVir Personal Edition (德國的免費防毒軟體) (http://toget.pchome.com.tw/intro/utility_antivirus/utility_antivirus_program/23441.html)
    - Panda (歐洲有名的線上掃毒服務) (http://toget.pchome.com.tw/intro/utility_antivirus/utility_antivirus_program/22886.html)
    - ✓McAfee AVERT Stinger (NAI 所提供的免費掃毒工具) (http://toget.pchome.com.tw/intro/utility_antivirus/utility_antivirus_program/21818.html)
    - 史萊姆的第一個家➔軟體下載➔防毒軟體 http://www.slime.com.tw/
  - 定期更新病毒碼

個人資訊安全守則 5

- 個人防火牆
  - XP內建防火牆
  - 免費的個人防火牆軟體
    - ZoneAlarm 個人防火牆(可參考)
      (http://net.mc.ntu.edu.tw/net_tutor/ZoneAlarm.htm)
    - ✓Outpost Personal Firewall (可參考)
      (http://toget.pchome.com.tw/intro/network_tool/network_tool_security/20568.html)
    - Sygate Personal Firewall (可參考)
      (http://toget.pchome.com.tw/intro/network_tool/network_tool_security/12837.html)
    - 天網防火牆(可參考)
      (http://www.hkworkshop.com/soft/sort.asp?zhuid=40&typeid=406)

個人資訊安全守則 6

- 系統備份
  - 系統設定 驅動程式
  - Ghost檔案(參考)(下載)(http://toget.pchome.com.tw/intro/utility_backup/22470.html)
- 資料備份
  - 「公務」 「教學」 「個人」 「 E-mail 」檔案
  - 壓縮檔案
- 備份方式
  - 燒錄
  - 異地備份
- 備份時機
  - 定時

結論(維護資訊安全的體認)

- 攻擊的發生是無所不在與無法預測。
  - 內部才是攻擊的主力---家賊難防。
    - 正面
      - 教育訓練
      - 觀念灌輸
      - 獎勵措施
    - 負面控制
      - 系統控制
      - 稽核
- 網路的安全是必須靠網路上的每一份子來共同維護。

Questions ?

謝謝聆聽

敬請指教