Secrecy and Internet Security

DOP Shiuh-Jeng **WANG** /王旭正

- 中央警察大學 資訊管理系
- 中華民國資訊安全學會 (www.ccisa.org.tw, 理事 (2000-2012)
- 中華民國資訊安全學會 副理事長 (www.ccisa.org.tw, 2012-)
- Visiting Scholars at FSU and UF in USA, 2002, 2004, 2010.
- Academic tour for International Project Inspection at CMU in USA, 2007
- Columnists of Domestic Information-tech Magazines, http://www.netadmin.com.tw/
  網路通訊/iThome/網管人雜誌, 2002-2006, 2007-至今
- Director of ICCL, http://hera.im.cpu.edu.tw
  (Information Cryptology and Construction Lab.)
- sjwang@mail.cpu.edu.tw, http://www.wretch.cc/blog/icclsjwang

內容

- 鑑定技術的重要
- 密碼元件
- 使用者鑑定
- Cyber-security and Forensics
- 結論

鑑定技術

- 資料的鑑定

  沒有被竄改、偽造或重送

- 使用者的鑑定

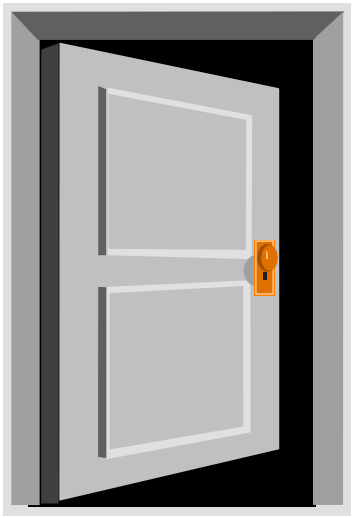
  沒有被冒充

鑑定技術的重要

- 政黨網頁抹黃案
- 金融業務單位駭客案
- 科技公司財務資料篡改案

密碼元件(一)

- 密碼器
- 數位簽章
- HASH函數
- ＩＣ卡



密碼學之假設

- 假設給破密者最大的知識
- 一密碼系統之安全性必須僅依賴其解密key

密碼(cryptology)

- 原意為隱藏
- 現泛指所有有關研究秘密通訊之學問
- 包括如何達到秘密通訊與破解秘密

密碼的領域

- 密碼學(cryptography)

  如何達到資訊的秘密性或鑑定性的科學(藝術)

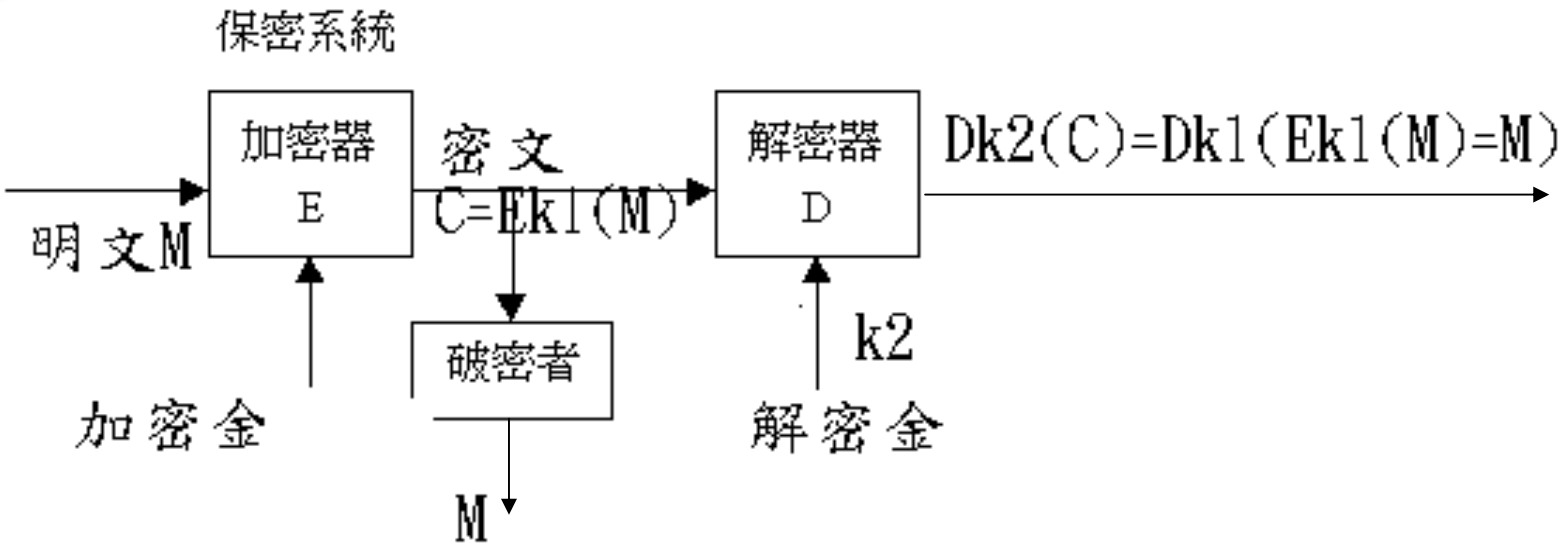
- 破密學(cryptanalysis)

  如何破解前人密碼系統或偽造系統使密碼系統誤以為真的科學(藝術)

密碼系統的功能

- 秘密性(secrecy or privacy)
- 鑑定性(authenticity)
- 完整性(integrity)
- 不可否認性(non-repudiation)

密碼技術



若已知k1即知k2,則稱為對稱式保密系統

- 若已知k1,但卻無法得知k2,則稱為非對稱式保密系統或公開金鑰保密系統,此時k1稱為公開金鑰,k2稱為私有金鑰

對稱式保密系統(一)

- 用途
  - 保護敏感資料
  - 確保資料之完整性
  - 加解密速度快

對稱式保密系統(二)

- 缺點
  - 收發雙方如何獲得k1及k2？
  - key數目太大
  - 無法達到存証(或不可否認性)之功能

非對稱式保密系統

- 1975年

  Diffie的思考

  - 從未見面的兩人是否可以從事秘密通訊？
  - 數位電子訊息是否可以向其他人證明確是發送自某人？

安全公開金鑰系統的功能

- 保護機密資訊
- 簡化key分配及管理的問題
- 可達到不可否認性的功能

金鑰管理：RSA與DES密碼系統的比較

	RSA	DES
提出年代	1977	1976
發明人	美國麻省理工學院教授 Rivest, Shamir, Adleman	IBM 及美國國家安全局 (未公開)
基本特徵	加密 KEY 異於解密 KEY	加密 KEY 就是解密 KEY
主要優點	加(解)密 KEY 可公開，而且可提供數位印鑑的功能	加解密速度快
主要缺點	解密速度慢、系統成本高、KEY 生成費時	不夠安全(KEY 不夠安全)而且 KEY 管理困難
應用	Apple's PowerTalk Novell's Netware 4.x Secure Telephone & Fax Link/Node Encryption CCIT X.509 電子現金	Sun's des MIT's Kerberos Norton Utilities diskreet CNS X5011(中華民國國家標準"數據保密(加/解密)運算法")

RSA加密技術及基本應用(一)

- PUBLIC KEY：
  n=p x q (p,q are 2 primes and must remain secret)
  e = is relatively prime to (p-1)x(q-1)
- PRIVATE KEY：
  $d=e^{-1} \pmod{(p-1) * (q-1)}$,
  i.e. e * d mod (p-1)(q-1) =1
- ENCRYPTING ：
  $C=M^e \pmod{n}$
- DECRYPTING ：
  $M=C^d \pmod{n}$

RSA加密技術及基本應用(二)

p=47,q=71

n=p*q=3337

(p-1) x (q-1)=46 x 70=3220

Let e*d mod (p-1)(q-1) =1

e=79 (is a prime, and chosen randomly)

$d=79^{-1} \pmod{3220}=1019$ (d is an inverse of e)

$M=688 \quad C=688^{79} \pmod{n}=1570$

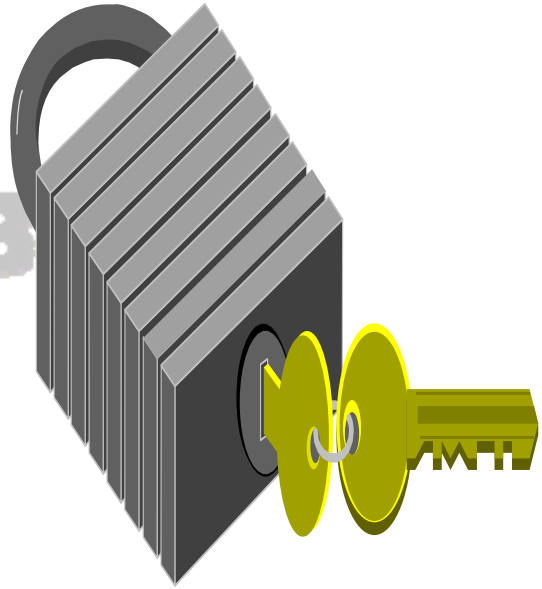
$M'=C^{d} \pmod{n}=1570^{1019} \pmod{n}=688$

破密者的攻擊方式

- 密文攻擊法
- 明文攻擊法
- 選擇攻擊法
- 選擇密文攻擊法
- 選擇明文攻擊法

加密器的設計原則

- 安全性
- 簡易性
- 迷惑性
- 擴散性
- 規律性
- 相同性



理論安全與實際安全(一)

若明文M有n位元,則直接猜對明文之機率為 2^{-n}

- 理論安全:一保密系統若其解密金鑰之長度為k,且對於n位元的明文加密後,使得破解此系統而得到明文之機率等於直接猜對明文之機率,則稱此系統為理論安全

  達理論安全之必要條件為k≧n

理論安全與實際安全(二)

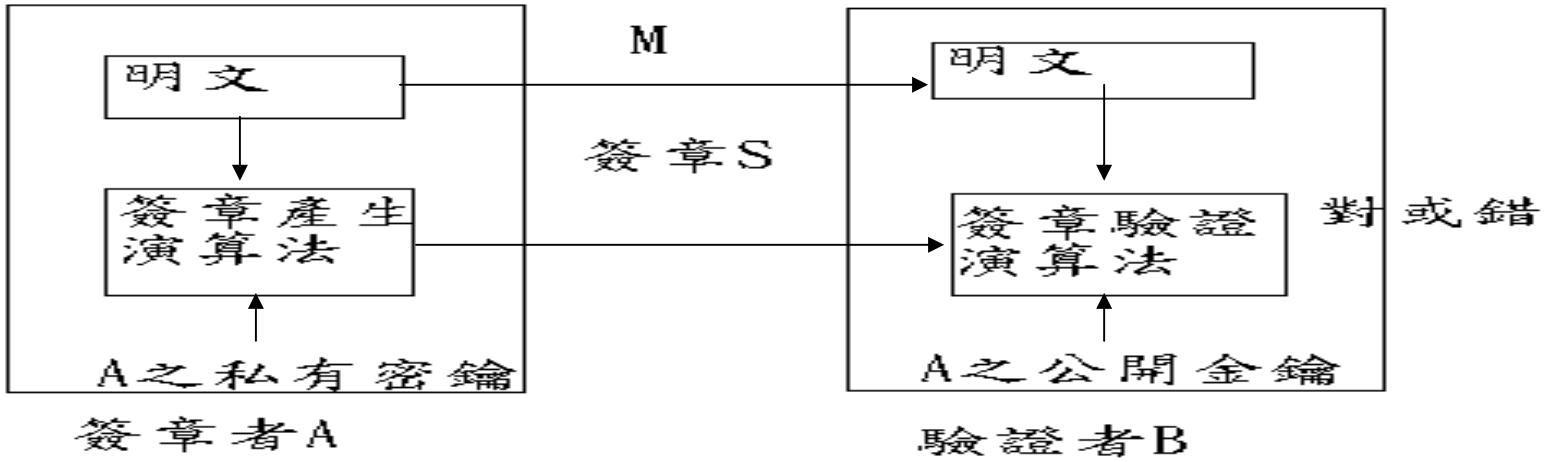
- 實際安全:一保密系統雖無法達到理論安全但卻能使破解此系統所需之計算能力與時間無法在合理的範圍內達成,則稱此系統為實際安全
- 理論工作函數:破解此保密系統理論上所需之最少代價

理論安全與實際安全(三)

- 歷史工作函數:破解此保密系統現在已知之最少代價
- 現稱一保密系統為安全,係指其歷史工作函數無法在合理範圍內達成,換句話說,現稱一保密系統為安全並不保証未來仍為安全

電子簽章

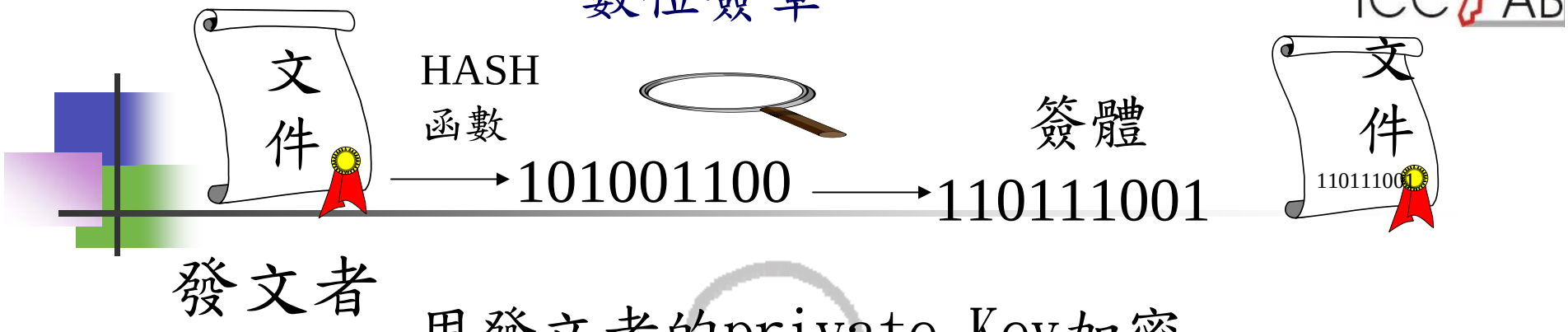
- 只有A能產生明文M之簽章S
- 任何人均可驗証A對M之簽章S是否正確
- 若A與B對簽章有爭議,第三者可加以公正之判決

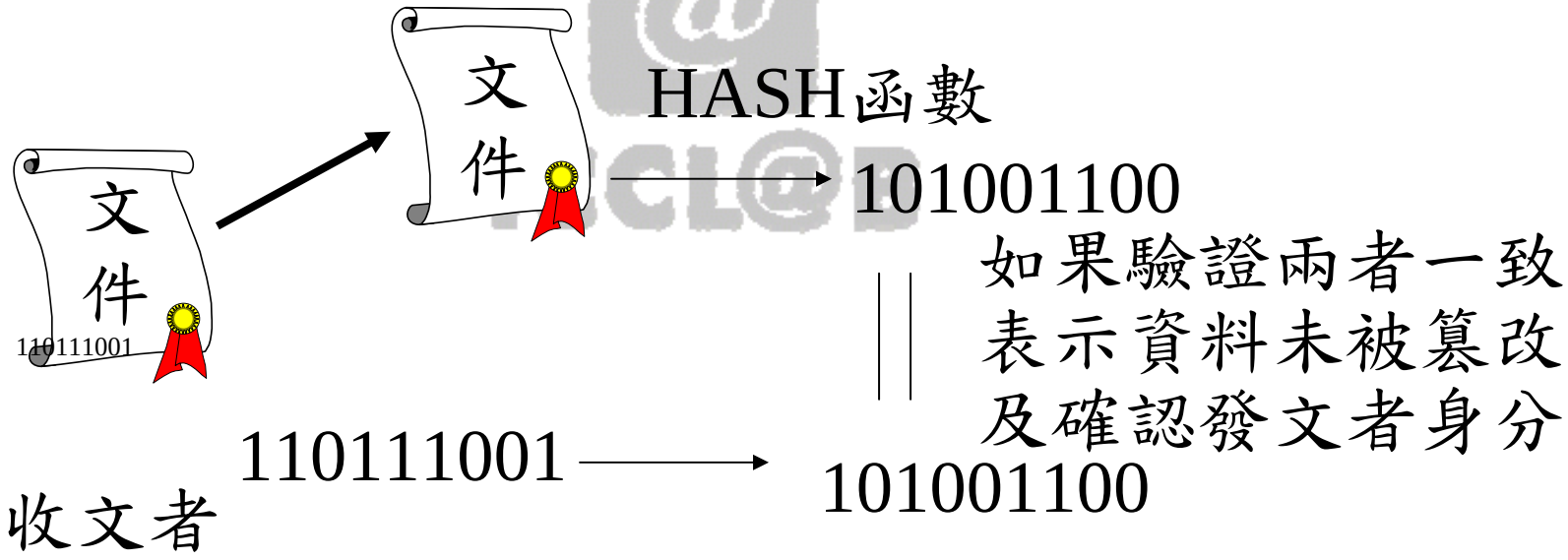


電子簽章之用途

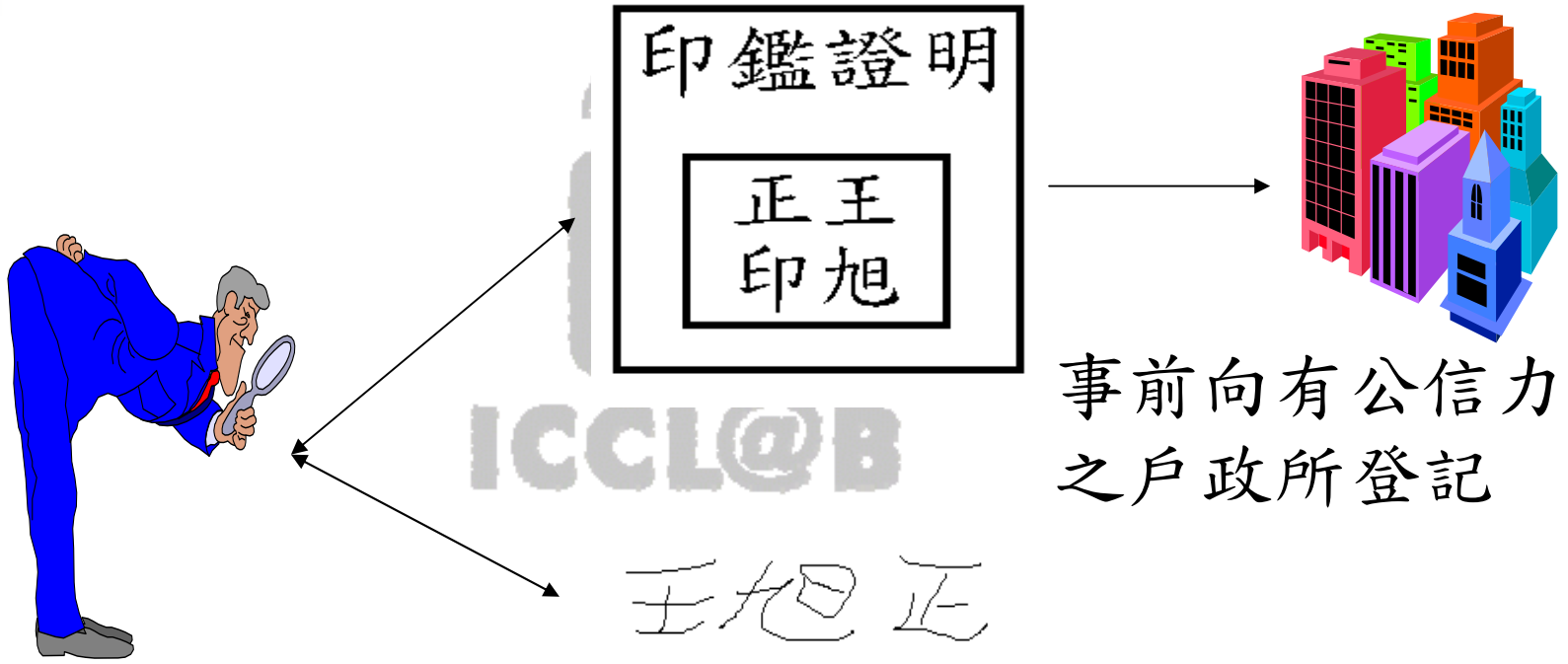
- 對明文M之資料完整性
- 對A身份之認証
- 存證(A不可否認曾送過明文M)
- 缺點:無法達到秘密通訊

數位簽章


文件
HASH
函數
101001100
簽體
110111001
文件
110111001
發文者
用發文者的private Key加密


文件
110111001
文件
HASH函數
101001100
如果驗證兩者一致
表示資料未被篡改
及確認發文者身分
110111001
101001100
收文者
用發文者的public Key解密

傳統識別個人身分之方法

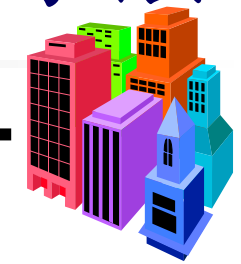


網路時代識別個人身分之方法

電子印鑑

流水號,數位簽章運算基碼ID,發證者名稱,有效日期,持有人姓名,持有人公開金鑰資訊,發證者特殊識別碼

CA簽章



事前向有公信力的第三者--CA註冊登記,由其簽發電子印鑑

王旭正

Private Key

數位簽章

Public Key

個人持有

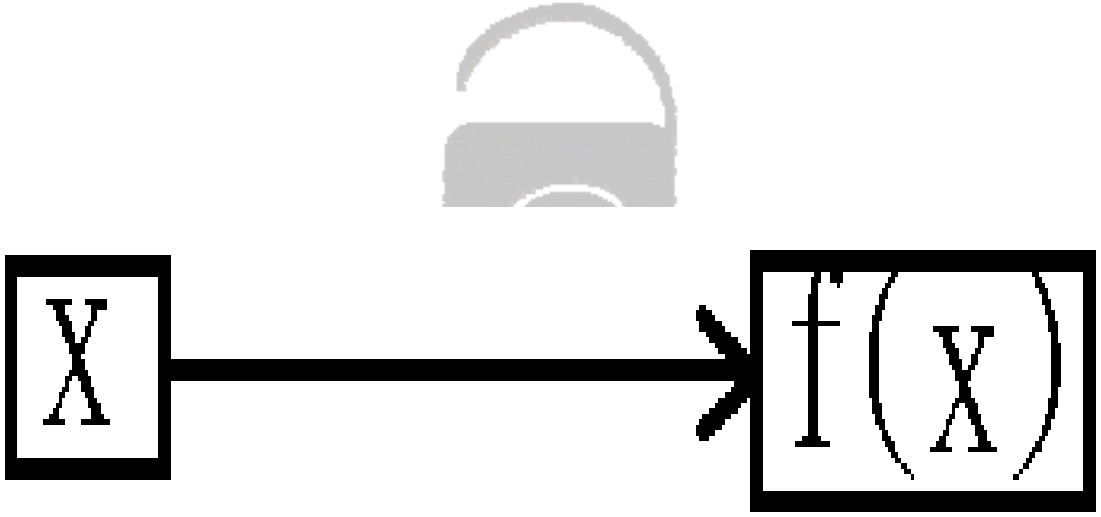
公開供各界用來與持有者通信之用,並由CA公證

由數學函數產品一對公開金鑰及私密金鑰,私密金鑰不能由公開金鑰反推

單向函數及單向暗門函數(一)

- 單向函數:一函數f若滿足下列二條件,則稱f為單向函數
- 對於所有屬於f之域的任一x,可以很容易算出f(x)=y
- 對於幾乎所有屬於f之範圍的任一y,則在計算上不可能求出x使得y=f(x)

單向函數 f由x求f(x)很容易 由f(x)求x很難



單向函數及單向暗門函數(二)

- 單向暗門函數:一"可逆"函數F若滿足下列二條件,則稱F為單向暗門函數
- 對於所有屬於F之域的任一x, 可以很容易算出F(x)=y
- 對於幾乎所有屬於F之範圍的任一y, 則在計算上除非獲得暗門否則不可能求出x使得$x=F^{-1}(y)$, F^{-1}為F之逆函數。但若有一額外資料z(稱為暗門)則可以很容易求出
- $x=F^{-1}(y)$ 。

單向函數之例子(一)

- 例一:令f為一n階多項式且

  $y=f(x)=x^n+a_{n-1}x^{-1}+\ldots+a_1x+a_0 \bmod p$

- 例二:解離散對數問題(Discrete Logarithm Problem, DLP)

  令質數p滿足p-1含有另一大質因數q(即q整除p-1)及一整數g, 1<g<p-1。已給一整數x, 欲求$y=g^x \bmod p$很快。但若已給p, q及y欲求x, 此問題稱為解離散對數問題, 現今已知最快的方法需要

  $DLP(p)=\exp\{(\ln p \ln(\ln p))^{1/2}\}$

  當p=512位元時, DLP(p)約為$2^{256} \fallingdotseq 10^{77}$

單向函數之例子(二)

- 例三:分解因數問題

  已知一大的奇數p, 欲判斷其是否為質數, 現已有許多有效的方法。大抵上, 需要$[\log_2 p]^4$運算即可判斷是否為質數。但若已知n, 欲分解n求得確實的p及q, 稱為分解因數問題, 這也是幾千年來數學界無法突破的問題, 現今已知最快的方法需要$\exp\{C(\ln n \ \ln(\ln n))^{1/2}\}$次運算, 其中C為小於1之正整數。

單向函數之例子(三)

- 例四:迷袋問題(Knapsack problem)

  已給有限個自然數序列集合, B=(b1, b2, ..., bn)及二進位序列 x=(x1, x2, ..., xn), xi∈{0, 1}, 欲求出 $s=\sum_{i=1}^{n} xibi$ 最多祇需要n-1次加法, 但若已給B及S, 欲求出x則非常困難。

HASH函數(一)

- HASH函數之性質:
  - F必為滿足任意位元長的輸入
  - F輸出必為固定位元長
  - 給予F和x,即可容易求得輸出值F(x)
  - 給予F(x)和F,即在"高成本計算量"下求得x
    (意指:欲解得x是很困難的)

HASH函數(二)

- 一般HASH函數F (或H)是一個無暗門(Trapdoor)的HASH函數
- 所謂有暗門的HASH函數係指在輸入x值時,需利用一秘密金鑰k,以求得輸出值F(x)或H(x)
- 無暗門的HASH函數係指在求F(x)或H(x)值時,不需任何秘密金鑰,亦即給予x,任何人均可求得F(x)或H(x)
- 資訊安全領域的HASH函數可以喻為一種可壓縮資料,但不可解壓的函數

IC卡簡介

- IC卡:塑膠卡片上崁入IC以達到記憶、識別及加解密等功能者
- IC卡種類:
  - IC記憶卡:祇具記憶IC,多用於資料保存與身份識別,如電話IC卡
  - IC智慧卡:具CPU及記憶能力,多用於財務金融、身份識別等,如金融IC卡、健保IC卡及身份IC卡
  - 超級智慧卡:具智慧卡功能並有獨立電源、營幕、鍵盤等,可直接在卡上認證持有人

磁卡、IC卡與光卡之比較

類別/項目	磁卡	IC 卡	光卡
特徵	成本低廉 廣泛使用	內有 CPU 具高保密性 通用性高	記憶容量大
記憶媒體	磁性條	IC 記憶體	光感材料
記憶容量	ISO 1.2 Kbits JIS 0.5 Kbits	8 Kbyte-16 Kbyte	2 Mbyte- 4 Mbyte
存取	容易(磁性)	CPU 控制	容易(光學)
運算功能	無	有	無
記錄方式	磁性	連接器/磁性/靜電	光學系統
安全性	容易讀取記憶內容	不容易讀取記憶內容(須經授權)	可設計改良具有安全性
資料之保存性	會受到外部磁場之影響,破壞記憶內容	用 IC 記憶體能永久保存不受外部磁場之影響	易受油漬、括痕影響
使用優點單價	價格低廉 使用方便 廣泛普及	防止犯罪及保密功能可作多目的之利用	容量大、價格低、可塑性大
每片價格	US$ 0.35-0.7 元	US$ 14-50 元	US$ 1-10 元

卡片的用途

- 儲存工具
- 識別工具->認證工具
- 運算工具
- 支付工具->遠端支付

鑑別機制所需的密碼技術

- 個體鑑別(EA)
- 金鑰交換(KE)
- 訊息鑑別(MA)
- 訊息加密/解密(ME)
  - ---對稱演算法
  - ---非對稱演算法
- PIN認證(PV)
- 交易憑證(TC)

使用者鑑別(一)

- 你有什麼？
  - 生理的：指紋、聲紋及視網膜等

優點：與生俱來、不怕遺失、很難偽造及不會被代用

缺點：使用者不習慣、無法適用於遠端鑑別、價錢昂貴、速度緩慢及精確度問題

  - 非生理的：身份證、磁卡、票券及IC卡等

優點：便宜、快速及方便

缺點：容易遺失或被代用

使用者鑑別(二)

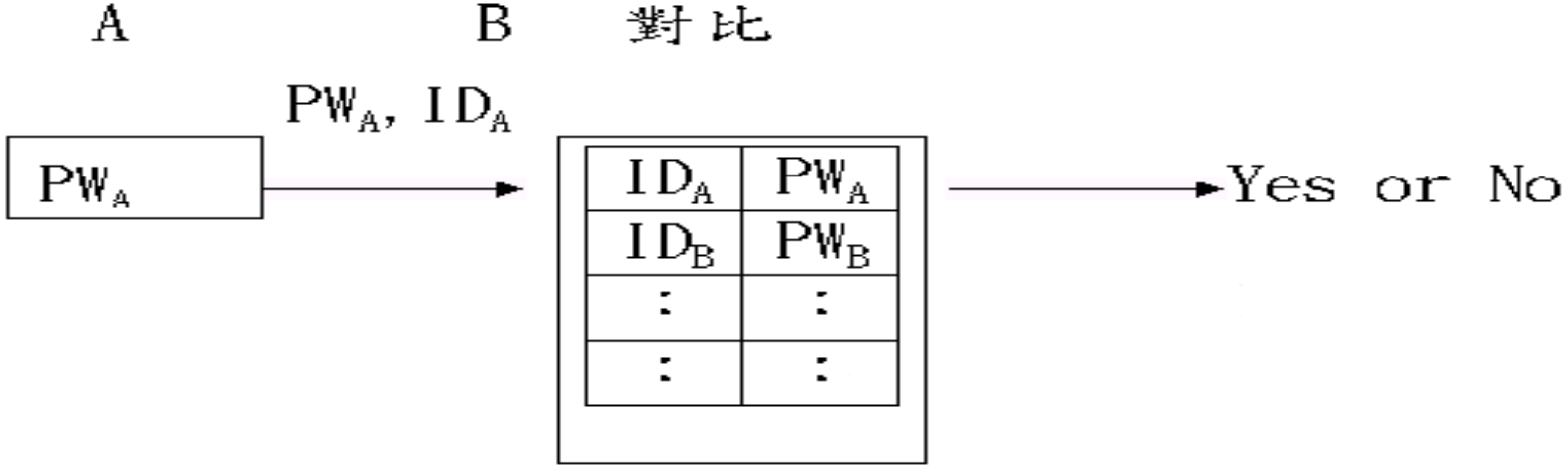
- 你知道什麼(秘密)?

優點：最便宜、簡單方便及不會遺失

缺點：會忘記、安全性不高

- 單向的：如通行碼

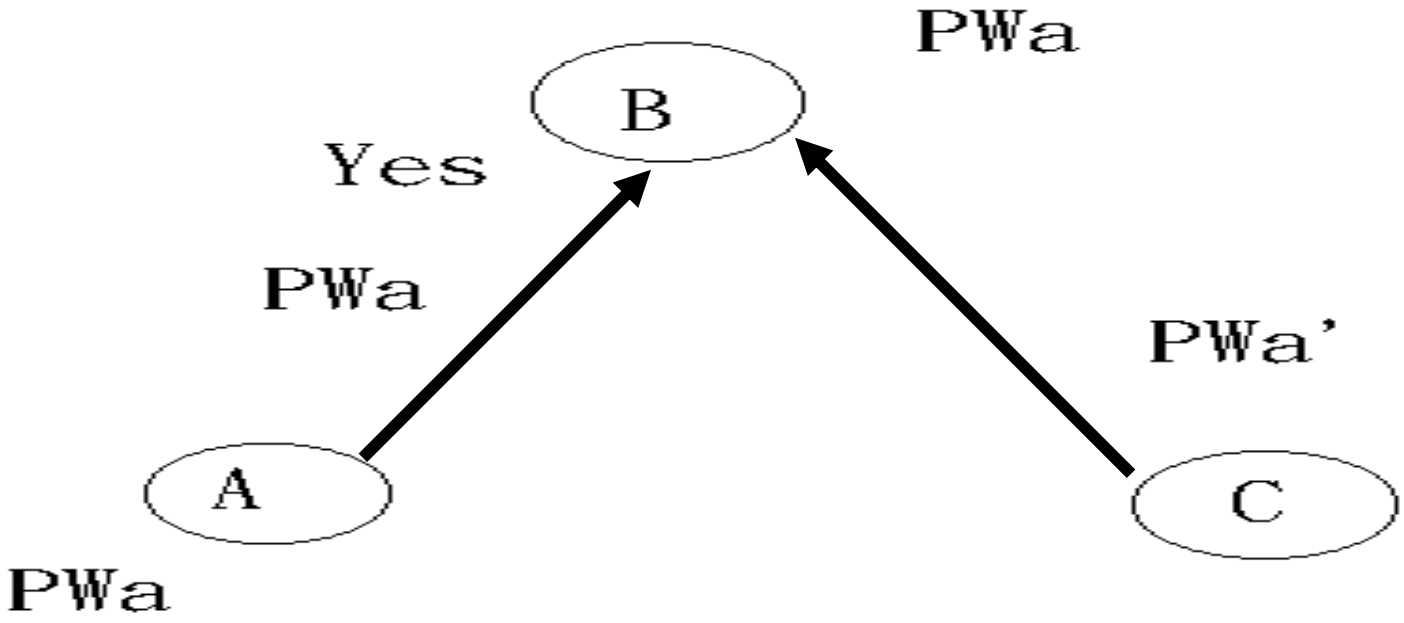
必須為亂數、不可與他人分享、不能夠在任意時間內改變、使用者用完後必須logout



鑑別的層次(一)

Authentication

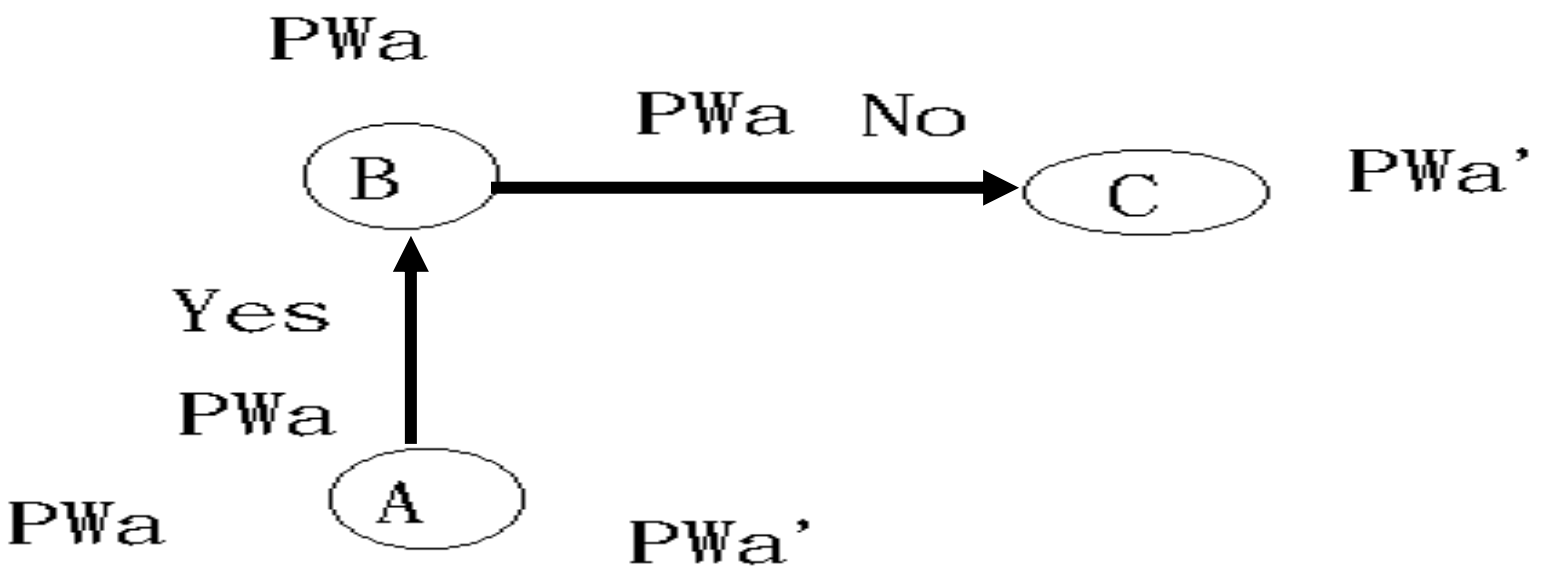
A能向B證明他是A,任何其他人無法向B證明他是A



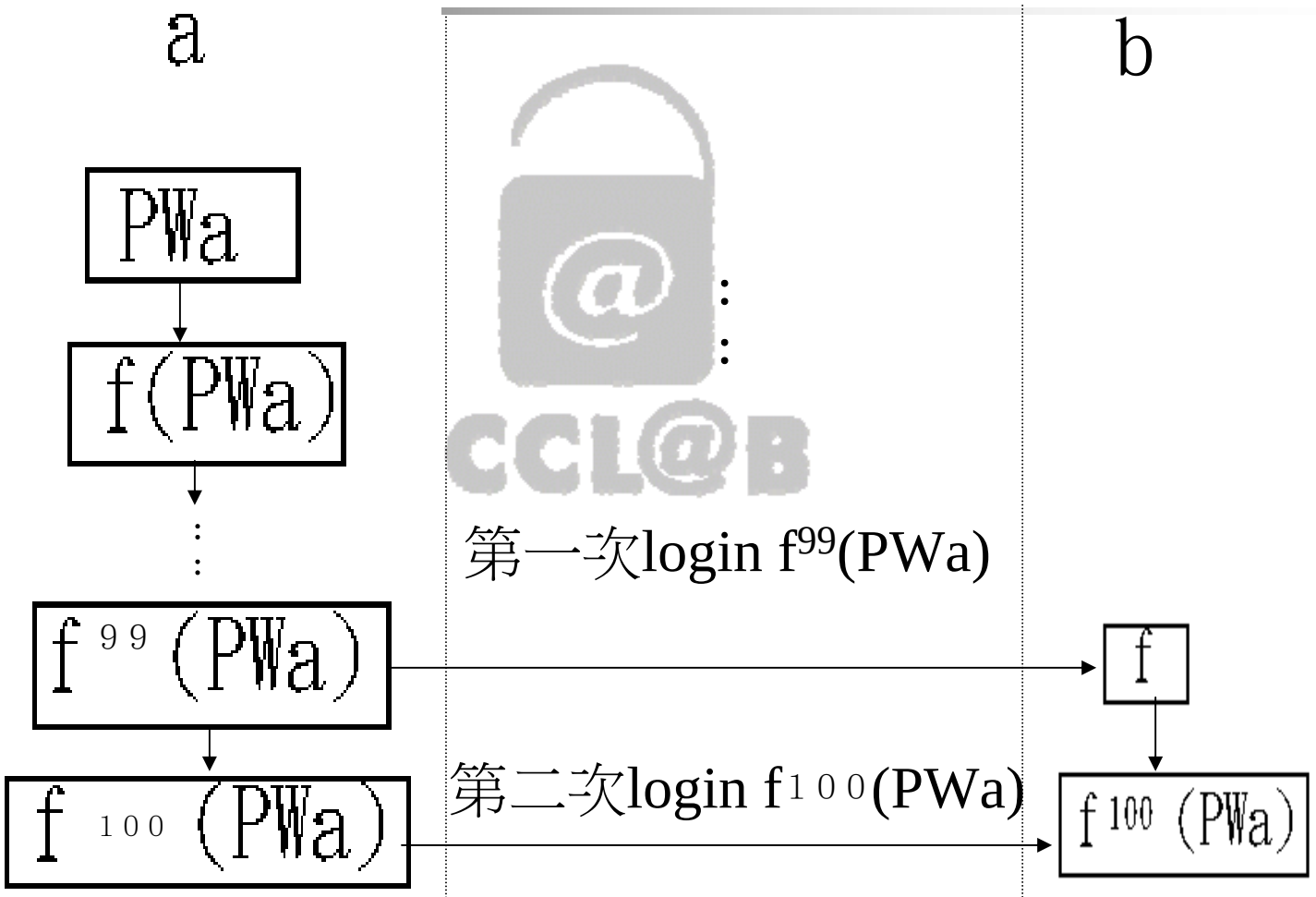
鑑別的層次(二)

- Identification

A能向B證明他是A, 但B無法向其他人證明他是A



利用多重單向函數之鑑別方法

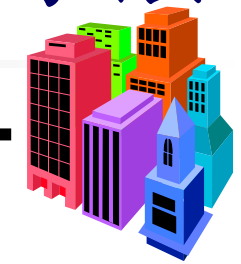


網路時代識別個人身分之方法

電子印鑑

流水號,數位簽章運算基碼ID,發證者名稱,有效日期,持有人姓名,持有人公開金鑰資訊,發證者特殊識別碼

CA簽章



事前向有公信力的第三者--CA註冊登記,由其簽發電子印鑑

王旭正

Private Key

數位簽章

Public Key

個人持有

公開供各界用來與持有者通信之用,並由CA公證

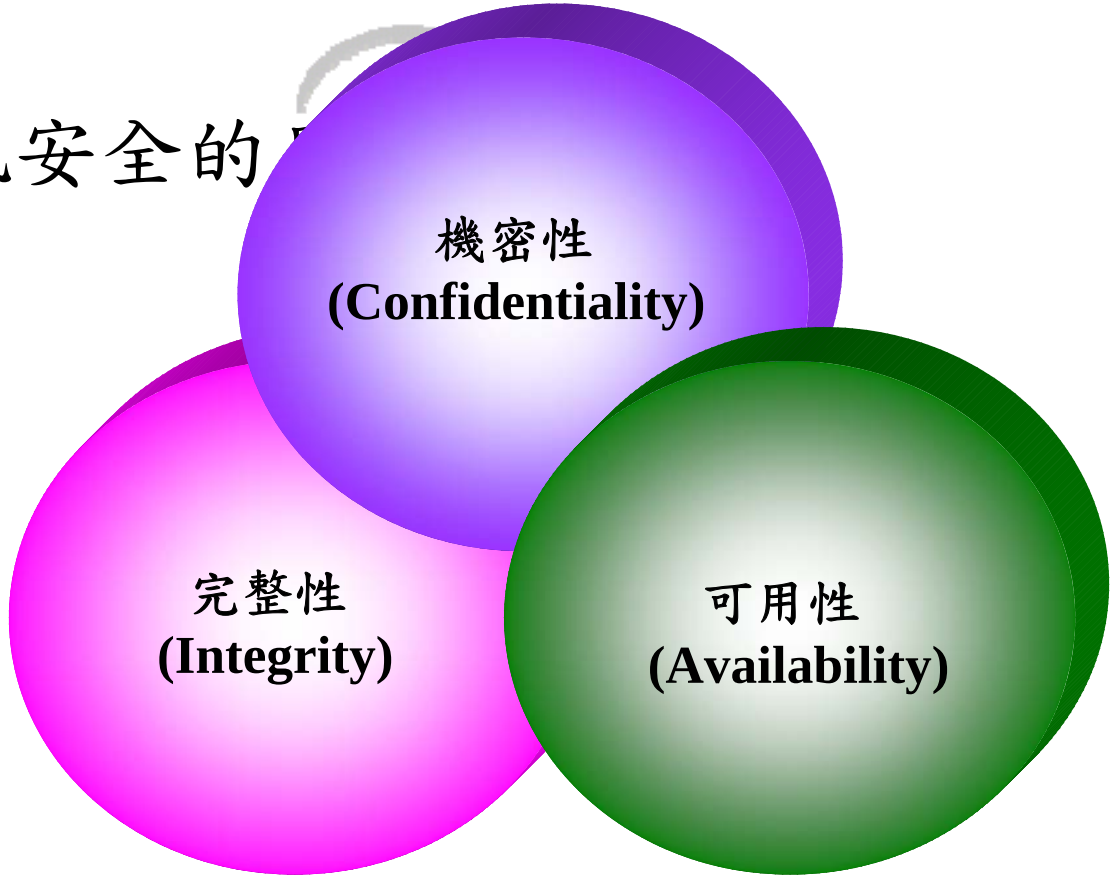
由數學函數產品一對公開金鑰及私密金鑰,私密金鑰不能由公開金鑰反推

C’est La Via

- HAKUNA MATATA
- Information/Network Security
- Authentication and Forensics
- Computer/Network Forensics

C.I.A.

- 資訊安全的



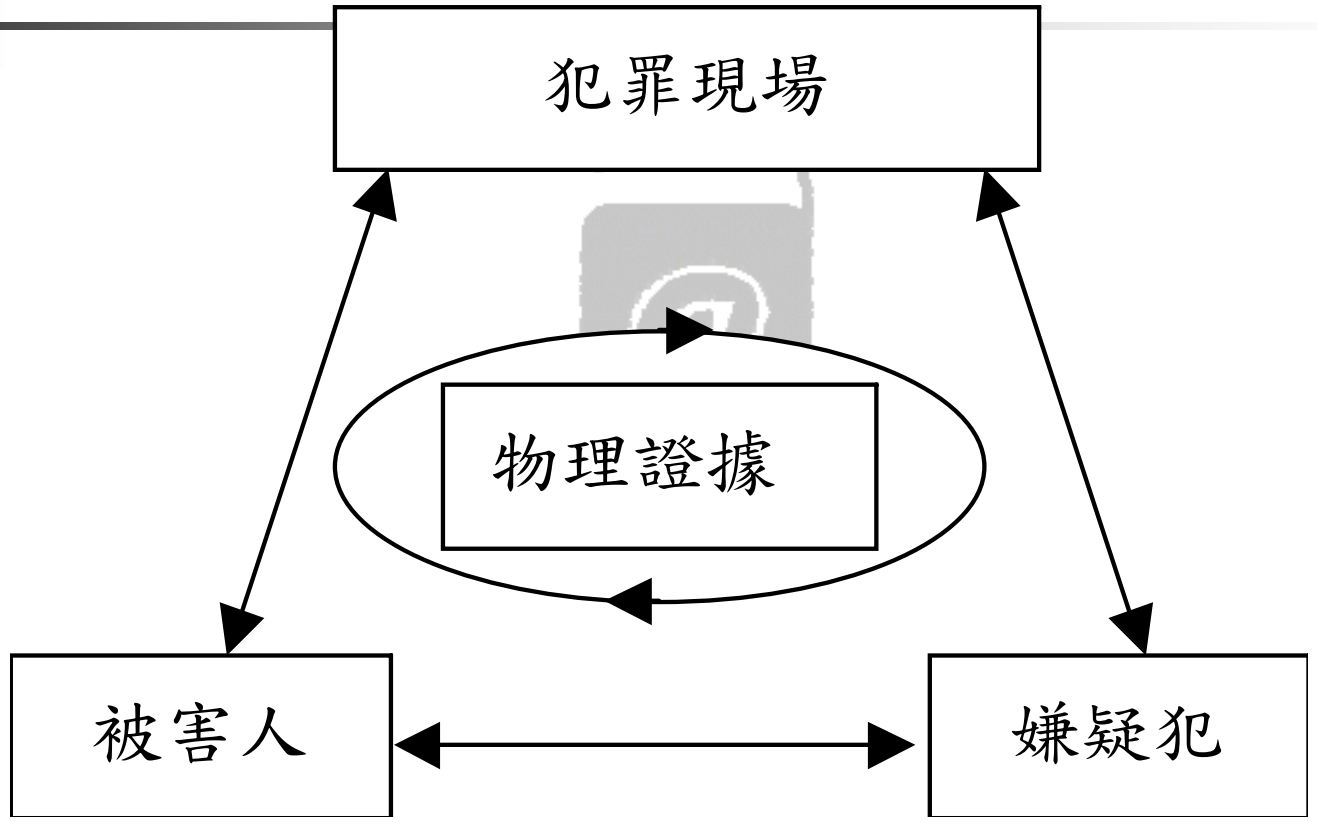
Cyber Crime

- 電腦犯罪日漸嚴重(調查報告)
  - 調查報告美國在西元兩千年因電腦犯罪所產生的財產損失即增加43%，由 $US265 million 增加為 $US378 million (FBI案件統計)
  - 美國85% 的企業及政府機構曾偵測到計算機系統遭到入侵
- 資料來源:http://www.smh.com.au/icon/0105/02/news4.html.

鑑識科學(Forensic Science)

- 定義
  - 運用科學於執法
  - *科學*: 化學, 生物學, 物理學, 地理學, …
- 目標: 確定犯罪現場及相關證物之證據能力

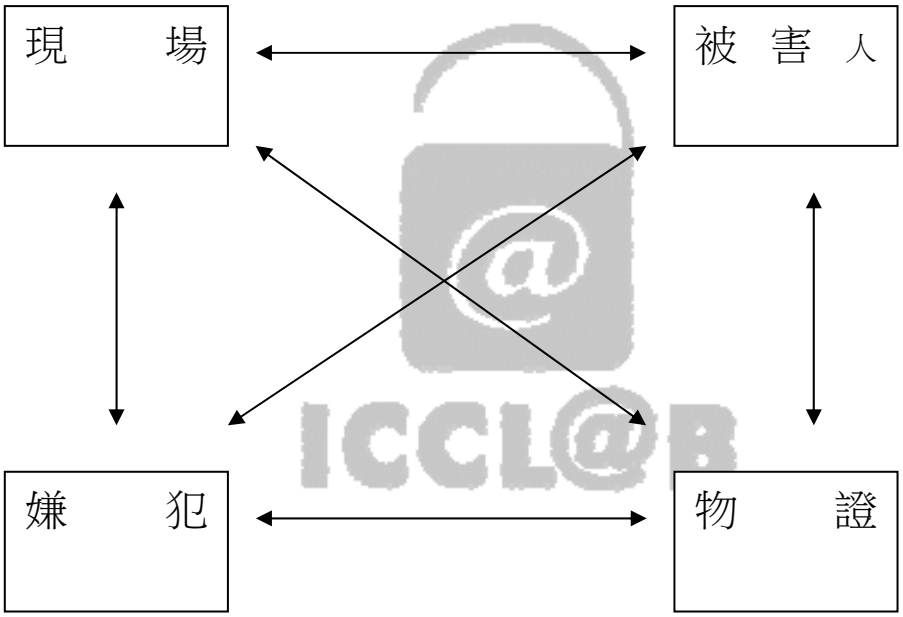
鑑識科學 (Locards's Exchange Principle)



Implications

- 多方面偵查，勿匆下結論:除數位證據之外，仍需訪問受害人、目擊證人、以及檢視相關之物理證據。
- 探討犯罪者之行為特質，可據以作為推論犯罪模式
  - 犯罪地點及型態
  - 接近及控制被害者之方式
  - 犯罪者之作為、不作為、及反應。
- 探討被害者之特質
  - 可藉以了解犯罪者，及其與被害者之關係。
  - 網路跡證與被害者之關係。
  - 可藉以推測受害者之類型並提出警告。
  - 犯罪者之冒險因素及被害者之危險因素。

犯罪現場的立即偵查



四相面間連接方式基本原則

Computer Forensics

(Warren, G. Kruse ii and Jay G. Heiser, 2002, *Computer Forensics – Incident Response Essentials*, Addison Wesley)

- 定義:
  - 以周延的方法及程序保存，識別，抽取，記載，及解讀電腦媒體證據與分析其成因之科學
- 方法與基本原則:
  - 在不改變或破壞證物的情況下取得原始證物
  - 證明所抽取的證物來自扣押的證物
  - 在不改變證物的情況下進行分析

證物之抽取

- 從電腦系統抽取證物
  - 是否即刻關機或斷絕網路連線需視情況而定
  - 從運行中的系統抽取證物
- 證物處理:
  - 證物鏈之管理
  - 採證
  - 證物之識別
  - 證物之運輸
  - 證物之保存
  - 偵查活動之記載

證物之分析

- 將原證物完整拷貝兩份
  - 包含正常檔案,刪除檔案, 及硬碟之其他部分
- 重複鑑定證物

Example to digital information

- 通連紀錄
- 交易紀錄(如提款、購物、轉帳等等)
- 電子郵件備份
- 網路連線紀錄
- BBS 備份
- 機密文件

數位證物鑑識之目的

- 確認嫌犯
- 起訴犯罪者
- 保護無辜
- 了解犯罪行為與動機

數位證據與物理證據之比較

- 為物理證據之一種
- 易於複製與修改
- 不易證實其來源及完整性
- 無法直接被人類所感知、理解的內容

數位證據與犯罪重建

- 重建被刪除、破壞、隱藏或加密之資料。
  - 利用特殊工具。
  - 利用公用程式。
  - 破解密碼(猜解密碼)。
- 推論犯罪事實 (5W1H)。
  - 何事(What)
  - 何人(Who)
  - 何時(When)
  - 何地(Where)
  - 如何(How)
  - 為何(Why)

檔案系統證物之蒐集

- 正常檔案: 搜尋, 文件分析, …
- 加密檔案: 密碼分析與破解,…
- 已刪除檔案
- 剩餘空間(slack space)之資料

討論

- 數位證據的偵防所必須遵遁的程序與原則，為因應泛網路犯罪的行為亦不斷的提出。
- 現行刑法中有明訂規範的賭博、詐欺等泛網路犯罪，司法與執法機關在追查泛網路犯罪行為上，已開始利用新興工具對數位證據進行分析
- 利用六何(5W1H)要件作為分析條件，以求獲取相關電腦網路證據，並以發生案例作說明，希冀能對未來的數位證據蒐證工作有所助益。
- 法律並非打擊犯罪的唯一手段，正確的網路倫理及使用方式才是抗泛網路犯罪的重要概觀。

- **Dr. Professor Shiuh-Jeng WANG**
- PhD. National Taiwan University, Taiwan, 1996
- Full Professor, Central Police University, Dept. of Information Management
- Director Information Crypto and Construction Lab
- Chair of ICCL-FROG (**F**orensic **R**esearch devel**O**pment task force **G**roup)
- Vice-President, Chinese Cryptography Information Security Association (**www.ccisa.org.tw**)

- Chairs of IEEE-CS/LNCS Proceedings, Internat'l confs.
  http://www.sersc.org/SH08/ http://www.ftrg.org/MPIS2009
  http://ncs2009.ntpu.edu.tw/CI/CI.htm http://www.ftrg.org/futuretech2010
  https://sites.google.com/site/uicuipm2012/ IEEE-sponsored,
  http://www.ftrai.org/music2012
- Editor-in-Chief AT JITAS (http://jitas.im.cpu.edu.tw)
- SCI-Journals, Guest-editors-,
  - IEEE J-SAC, http://www.comsoc.org/livepubs/sac/index.html
    http://hera.im.cpu.edu.tw/sjw_2006/meeting_report/IEEE-GUEST-EDITORIAL-0808-2011-.pdf
  - Journal of Internet Technology (JIT)
    http://jit.ndhu.edu.tw/callforpaper/April-2011-SI-JIT.pdf
  - The Computer Journal, http://comjnl.oxfordjournals.org/
  - Springer Telecommunication Systems
    http://www.springer.com/business/business+information+systems/journal/11235
  - The Journal of Supercomputing,
    http://www.springer.com/computer/swe/journal/11227 (Springer)
  - Peer-to-Peer Networking and Applications,
    http://www.editorialmanager.com/ppna/ (Springer)