資訊安全(Information Security)

淡江大學 資訊工程系
黃心嘉

大綱(OUTLINES)

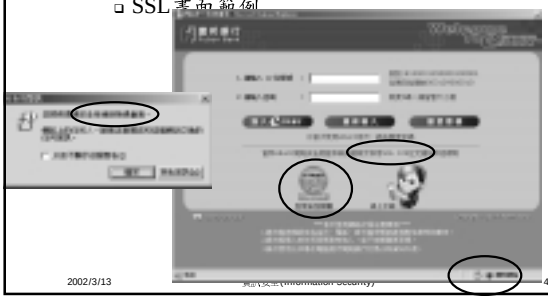
- 簡介：資訊安全的重要性
- 凱撒加密法
- 加解密系統與數位簽章
- 公開金匙基礎架構(PKI)
- 世界各國數位簽章法的近況
- 電子商務的安全(EC-Security)
- 防火牆(Firewalls) &侵入偵測系統
- 結論

簡介：資訊安全的重要性

- 日常生活中的資訊安全
  - 銀行提款機的密碼：身分辨識
    - 數位世界中，人的代號變成一組數字。
    - 還有哪些身分辨識的例子?
  - 網路報稅的公開金匙憑證
  - 網頁的安全傳輸機制：SSL
    - 網路銀行
    - 網路購物
  - 趨勢公司的GateLock
  - 防毒軟體

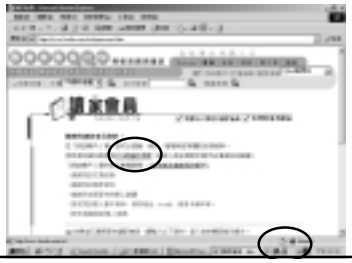
簡介：資訊安全的重要性

- SSL畫面範例



簡介：資訊安全的重要性

- SSL畫面範例

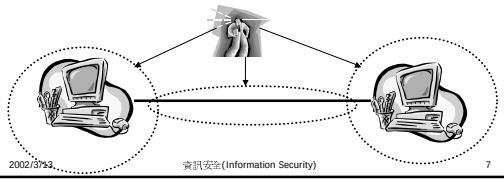


簡介：資訊安全的重要性

- 趨勢公司的GateLock畫面

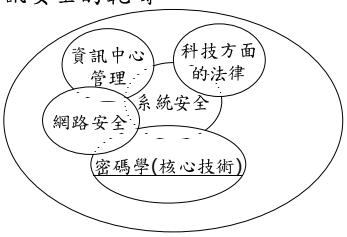
簡介：資訊安全的重要性

- 資訊安全：保護存放在*電腦*中與在*網路*上傳輸的資訊，以防止未經允許的*讀寫與更改動作*發生。



簡介：資訊安全的重要性

- 資訊安全的範疇



凱撒加密法

- 凱撒加密法(Caesar Cipher)
  - 已知最早的加密法，傳為凱撒大帝所提的。
  - 問題: 如何把英文字母變成數字?
  - 加密規則: C=E(P)= (P+3) mod 26.

```
plain:   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
cipher:  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
```

  - 範例:

```
plain:    meet me after the toga party
cipher:   PHHW PH DIWHU WKH WRJD SDUWB
```

  - Problem: 解密規則???

凱撒加密法

- 凱撒加密法加強版
  - 重要觀念:任何Objects在電腦中都是數字。
    - 凱撒加密法中英文字母變成數字。
  - 重要觀念
    - 秘密金匙k的概念。
    - 加解密雙方皆須事先知道秘密金匙k。
  - 加密規則: C= E(P)= P+k mod 26.
  - 解密規則: P=D(C)= C-k mod 26.
  - *Problem: 一共會有多少法種加密方式?*

凱撒加密法

- 破解凱撒加密法加強版
  - 暴力攻擊法(Brute-force attack): 把所有可能的秘密金匙全部試一次。
  - 已知明文攻擊法(Known-plaintext attack)
  - 重要觀念
    - Large key space: 所有可能秘密金匙的個數要夠多，至少不能被用電腦以暴力攻擊法所猜到。
    - Example: SSL採用128位元的秘密金匙。
    - Problem:採用128位元的SSL，其秘密金匙的個數多少個?

凱撒加密法

Table 2.2 Average Time Required for Exhaustive Key Search

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

加解密系統與數位簽章

- 資訊安全的四大基本需求
  - 機密性(Confidentiality)—加解密系統
    - e.g.交易內容保密
  - 完整性(Integrity)—數位簽章
    - e.g.交易內容非授權者不可更改
  - 確認性(Authentication) —數位簽章
    - e.g.交易確認是誰提出
  - 不可否認性(Non-reputation)—數位簽章
    - e.g.交易內容不可否認

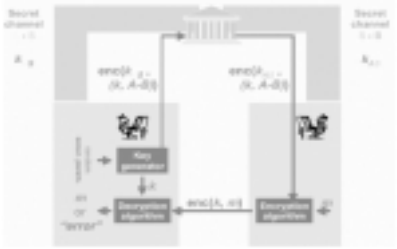
加解密系統與數位簽章

- 傳統加解密系統
  - 又稱單金匙加解密系統

  - 有名的傳統加解密系統:凱撒加密法, DES, AES
  - 金匙分配問題:雙方必須事先共同擁有秘密金匙 k

加解密系統與數位簽章

- 金匙分配的解法一



加解密系統與數位簽章

- 公開金匙加解密系統(Public key cryptosystems)
  - 又稱雙金匙加解密系統

  - 著名的系統: RSA public key cryptosystem
    - Key size: ~512-2048 bits

加解密系統與數位簽章

- 問題：
  - 執行速度約為傳統加解密系統的1/10。
  - 公開金匙的認證問題。
- 混合式加解密系統=公開金匙加解密系統+傳統加解密系統
  - 用傳統加解密系統加密+臨時的秘密金匙k
  - 用公開金匙加解密系統對臨時的秘密金匙k加密

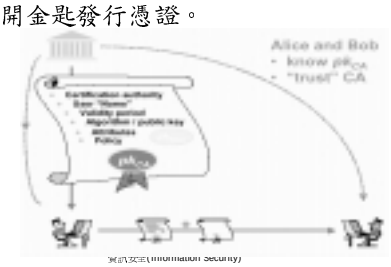
加解密系統與數位簽章

- 數位簽章：手寫簽章的數位版

  - 著名的數位簽章法: RSA, DSA, …

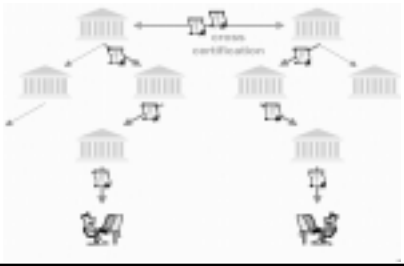
公開金鑰基礎架構(PKI)

- 公開金匙的認證:由公信單位為每個人的公開金匙發行憑證。



公開金匙基礎架構(PKI)

- CA的階層式架構

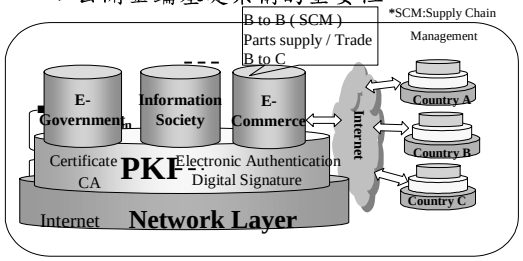


公開金匙基礎架構(PKI)

- 公開金鑰基礎架構(PKI)
  - PKI的三種成員
    - 憑證中心 (Certificate Authorities CA),
    - 登錄中心 (Registration Authorities RA)
    - 管理機制 (The repository and the management consoles).

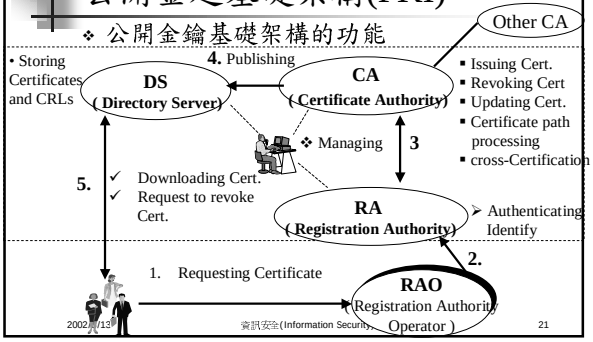
公開金匙基礎架構(PKI)

- 公開金鑰基礎架構的重要性



公開金匙基礎架構(PKI)

- 公開金鑰基礎架構的功能

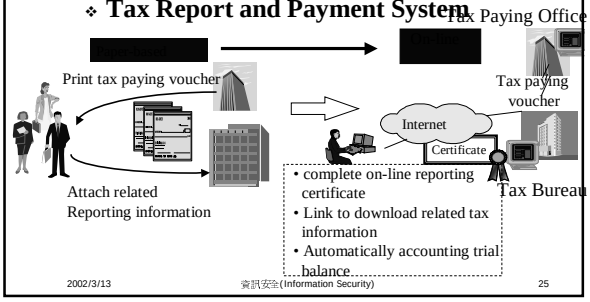


公開金匙基礎架構(PKI)

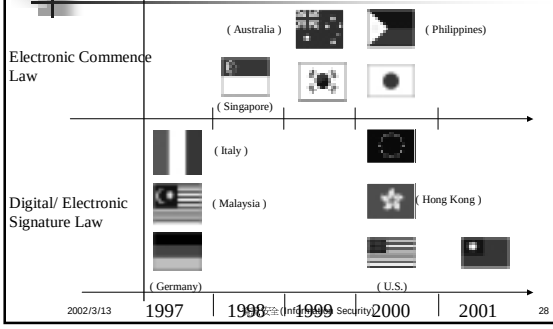
- 中華民國的PKI大事記
  - According to the mid-milestone of Electronic Government (from 1998 to 2000): Internet electronic verification mechanism, the Research and Development Commission of Exective Yuan has delegated the *Chunghwa Telecom Co. LTD* to establish the first stage of the *Government Certification Authority (GCA).*
  - In 1998, the GCA started to work and supported a field trial on two applications- *electronic tax report* and *electronic Mobile Vehicle and driver information system* in the first stage.
  - Until now, the GCA has supported 16 applications on the government service network

公開金匙基礎架構(PKI)

- **Tax Report and Payment System**

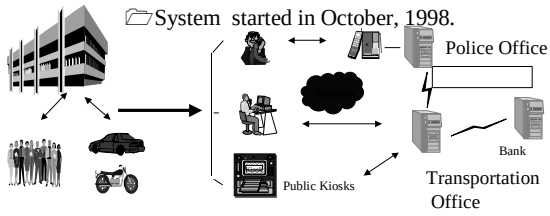


世界各國數位簽章法的近況



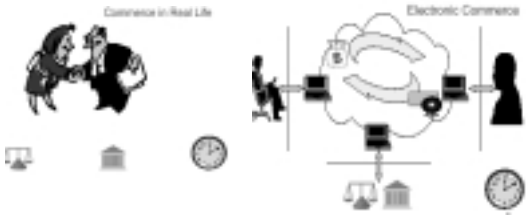
公開金匙基礎架構(PKI)

- **Electronic Motor Vehicle Inspection System**



電子商務的安全(EC-Security)

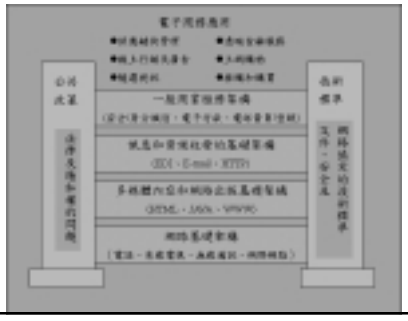
- 電子商務(Electronic Commerce)



公開金匙基礎架構(PKI)

- 中華民國GCA所使用的技術
  - Encryption algorithm : Triple DES CBC up to 112 bits
  - Digital Signature : RSA with SHA-1 up to 1024 bits
  - Certificate Distribution : X.500 (1993)
  - The format:
    - Digital Signature and Digital envelope: PKCS #7
    - Secret key storage : PKCS #5
  - The data format: Certificate : X.509 (v3 , 1993) & CRL : X.509 (v2, 1993)
  - Communication protocol: LDAP (RFC 1777) , TCP/IP , HTTP and OCSP (On-line Certificate Status Protocol)

電子商務的安全(EC-Security)

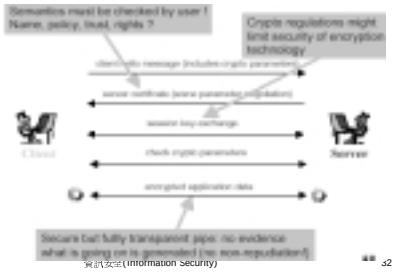


電子商務的安全(EC-Security)

- SSL: 安全傳輸方式

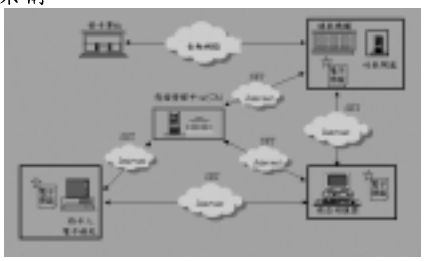
電子商務的安全(EC-Security)

- SSL: 安全傳輸方式[限制]



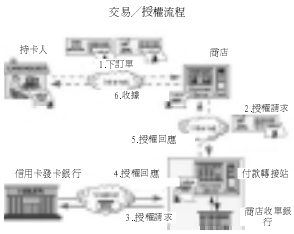
電子商務的安全(EC-Security)

- 架構



電子商務的安全(EC-Security)

- 安全的交易流程圖



電子商務的安全(EC-Security)

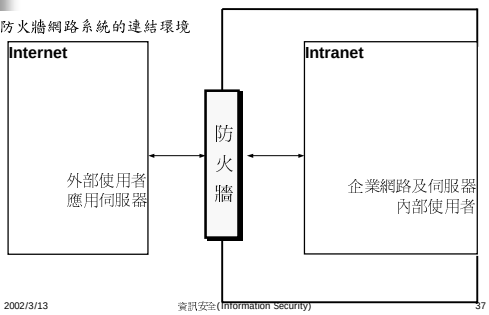
- SET: 網際網路信用卡付款機制
  - 由Visa、MasterCard、IBM、Netscape、Microsoft等公司於1996年共同制定與支援
  - 五種參與角色
    - 憑證管理中心：會同收單銀行與發卡銀行，負責核發特約商店或持卡人電子憑證。
    - 收單銀行：負責幫特約商店辦理認證與註冊的各項業務。透過付款轉接站 (Payment Gateway) 把線上交易資料轉換成現行銀行使用的信用卡交易訊息。
    - 特約商店：支援SET付款標準的電子商場。
    - 發卡單位：建立持卡人身分認證以及授予證書的各項業務。
    - 持卡人：持信用卡上網消費的顧客。

防火牆(Firewalls) &侵入偵測系統

- 防火牆
  - 一種軟體或硬體系統，可管制外部使用者對企業網路及網站的連結及存取作業，並可執行使用稽核。防火牆透過對使用者名稱、密碼、網路位址(IP address)或網域名稱(Domain name)等的檢驗，過濾外來使用者，只允許經授權的使用者連線使用。
  - 主要類別
    - 封包濾過器型防火牆(Packet filter firewalls)
    - 代理人型防火牆(Proxy firewalls)

防火牆(Firewall) ….

圖3-2 防火牆網路系統的連結環境



防火牆(Firewall)….

- 侵入偵測系統
  - 功能:偵查不當的侵入並發警訊及執行斷線措施。
  - 主要類別:
    - 反常偵測(Anomaly detection)系統：透過正常使用者及系統行為檔案的建立，採用統計方法以分析系統作業及異動記錄，查出違背正常操作行為的舉動，並向系統管理者發出反常警報
    - 誤用偵測(Misuse detection)系統：透過對已知攻擊行類型的建立，採用專家系統(Expert System)方法分析比對網路交通及系統使用類型，以檢測出含有已知攻擊行為類型的舉動。

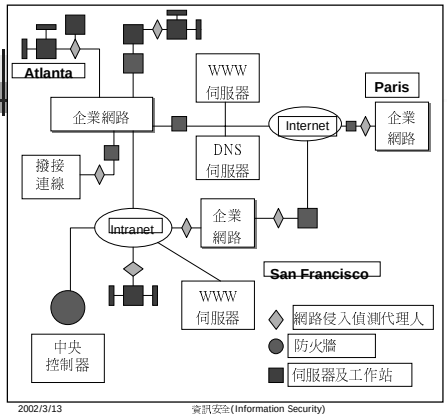


圖3-3 RealSecure網路侵入偵測系統的分散式環境[13]

結論

- 資訊化的社會除了資訊化的便利外，更需要資訊安全。
- 資訊安全的人員
  - 具國際化特性的人員
  - 具區域化特性的必需人才
    - 高薪
    - 不怕失業
    - 但是很辛苦的工作