資訊安全簡介

Public Key Infrastructure

世新大學資訊傳播學系余顯強 副教授

資訊工業安全

- 威脅與機會
  - 我們所需的資訊安全，不僅要能夠保護我們的資產，還要能借助其優勢創造出新的商機
  - 我們需要在電子世界裡，能夠具備如同紙本世界般的的真確性和信賴度

資訊安全危機

- 病毒肆虐
  - 防毒保全
- 非法盜取、盜用資料
  - 資訊安全
- 駭客入侵
  - 資訊防護

是否值得信賴?

- 當我們進入電子世界裡，我們如何能確認、信賴那些我們無法看到、聽到的對方？
- 我們如何在沒有加簽的信封或隱密的電話之中，確保交易的安全?
- 我們如何讓對方接收到明確的訊息，並同意彼此的交易?

紙本世界的信賴

- 在紙本世界所採行的方式:
  - 寫封信並寄出
  - 或許有位證人來驗證我們的簽章真偽
  - 將信件放入信封並將之密封
  - 透過正規的管道郵寄出去
- 應具備信賴的要素:
  - 內容並沒有被其他人閱讀過
  - 信封的內容原封不動
  - 信封是來自於宣稱寄送出來的那個人
  - 宣稱寄送給他的人無法否認送出這封信

資訊安全基本目的

- 能確認發送者確實是本人
- 防止對資料進行未經授權的讀取
- 防止對資料進行未經授權的修改
- 防止對資料進行未經授權的重複傳送
- 發送者事後無法否認
- 有公正的機構能仲裁

電子世界安全的基礎

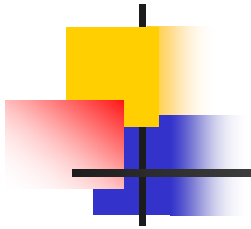
名詞說明

- 鑑別(authentication)
  - 對於網路上所傳遞的訊息，檢驗並證明訊息來源與其所宣稱者是否相符
- 真確(Integrity)
  - 訊息的接收者應該能夠驗證訊息是否在傳遞的過程遭到修改
  - 入侵者無法擅自以偽造的訊息取代原本的訊息

安全威脅的本質及對策

安全威脅	安全對策
非法侵入系統存取資料	存取控制
訊息遭中途截聽因而洩露	資料保密
冒名交易或傳送資料	鑑別資料來源確認
訊息遭竄改、重送、刪除或遲滯	資料完整性
發送者或接收者否認已收送的資料	不可否認性

以密碼學為基礎的網路認證制度



PKI

- 公鑰基礎建設
  - Public Key Infrastructure (PKI)
  - 提供了電子世界安全性的解決方案

何謂PKI

- 提供在電腦網路運作的個人資料、商務與商業能夠如同信封簽章與封印般的技術

- **簽章(Signature)提供鑑別**
- **封印(Seal)提供真確與機密性**

密碼(Cryptography)

- 「密碼 」透過使用一個加密金鑰配合演算法，將訊息加密以確保機密性
- 接收者能夠將訊息加密所產生的「亂碼」，使用原先的金鑰還原
- 使用的金鑰能夠讓雙方共享，但能對其它人保密

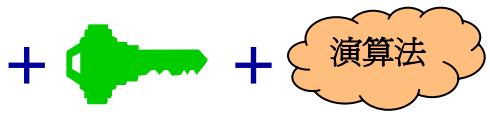
共同金鑰加密步驟

雙方分享共同的金鑰(secret key)

加密:

To: 李四
From: 張三
Date: 民國 91 年 5 月 18 日

請幫我從
帳號1234567
轉出100萬到
帳號7654321



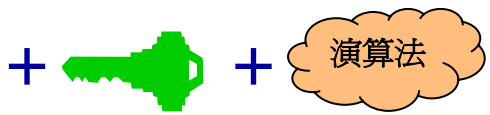
*> *ql3*UY
#~00873/JDI
c4(DH: IWB(883

th=S9is=Uiwriting=29byas
Shien=9e-Chiang=ea
Yu=sdofijhas9djerhp7goe.>
(*Y23k^wbvlqkwcyw83
zqw-_89237xGyjdc

解密:

*> *ql3*UY
#~00873/JDI
c4(DH: IWB(883

th=S9is=Uiwriting=29byas
Shien=9e-Chiang=ea
Yu=sdofijhas9djerhp7goe.>
(*Y23k^wbvlqkwcyw83
zqw-_89237xGyjdc

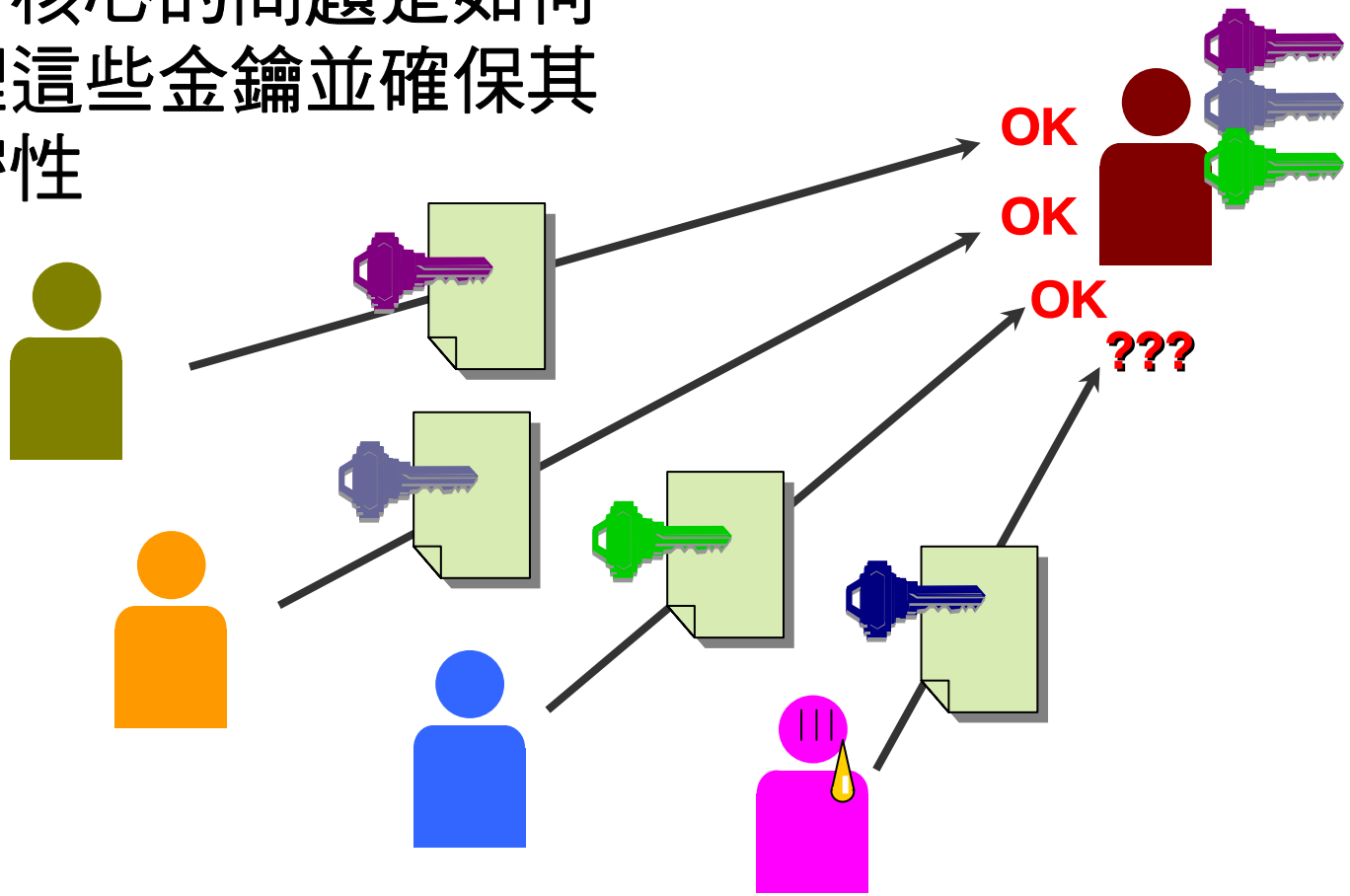


To: 李四
From: 張三
Date: 民國 91 年 5 月 18 日

請幫我從
帳號1234567
轉出100萬到
帳號7654321

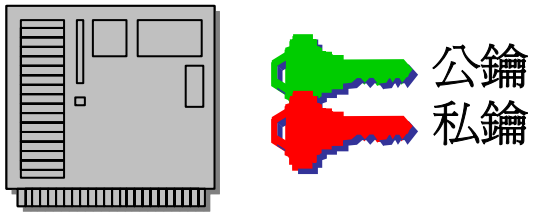
使用共同金鑰的問題

- 對大多數的應用程式而言，核心的問題是如何管理這些金鑰並確保其私密性



公開金鑰加密

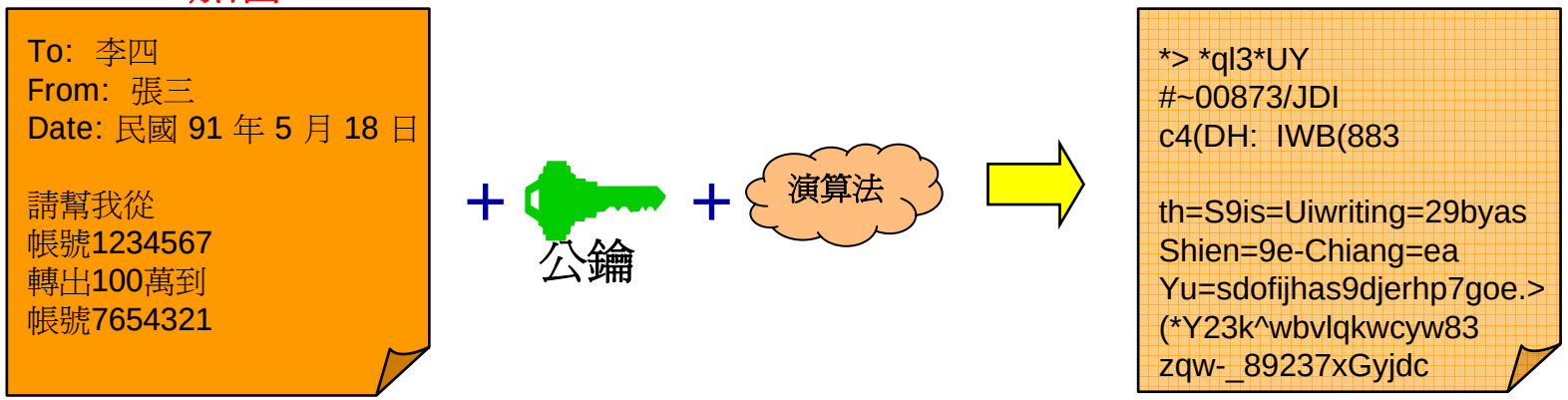
- 公開金鑰加密(又稱非對稱性加密)
  - 藉由一組私用與公用的金鑰，取代共同金鑰
  - 傳送的訊息使用公鑰加密，接收端則必須使用相對應的私鑰方能解密
  - 所有使用者的公鑰均可自由散佈
  - 依據密碼原理，公鑰和私鑰可以用來產生和驗證數位簽章(digital signatures)
    - 確認訊息的真確性與鑑別發送者



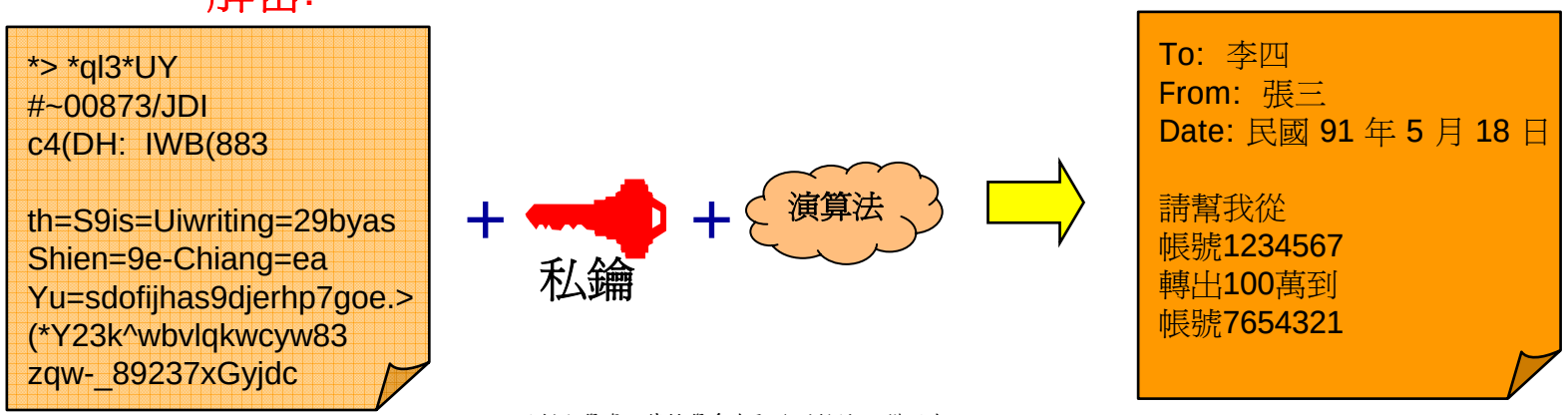
公開金鑰加密步驟

同時產生一對鍵值：一個公鑰一個私鑰

加密:



解密:



加密方式比較

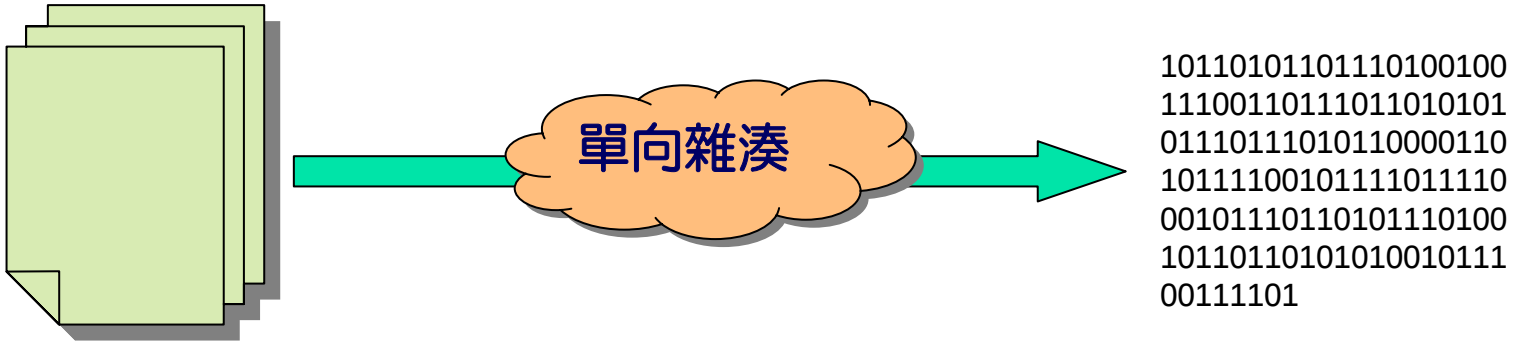
	共同金鑰	公開金鑰
金鑰數量	單一key	一對 keys
型態	Key必須保持隱密	一個是公開的key，一個是私用的key
管理	簡單但不容易管理	需要數位憑證和信賴第三者
加密速度	非常快	較慢
應用	用於大量資料的加密處理	用於特定需求的應用程式，處理小量資料的加密或簽章

單向雜湊(One Way Hash)

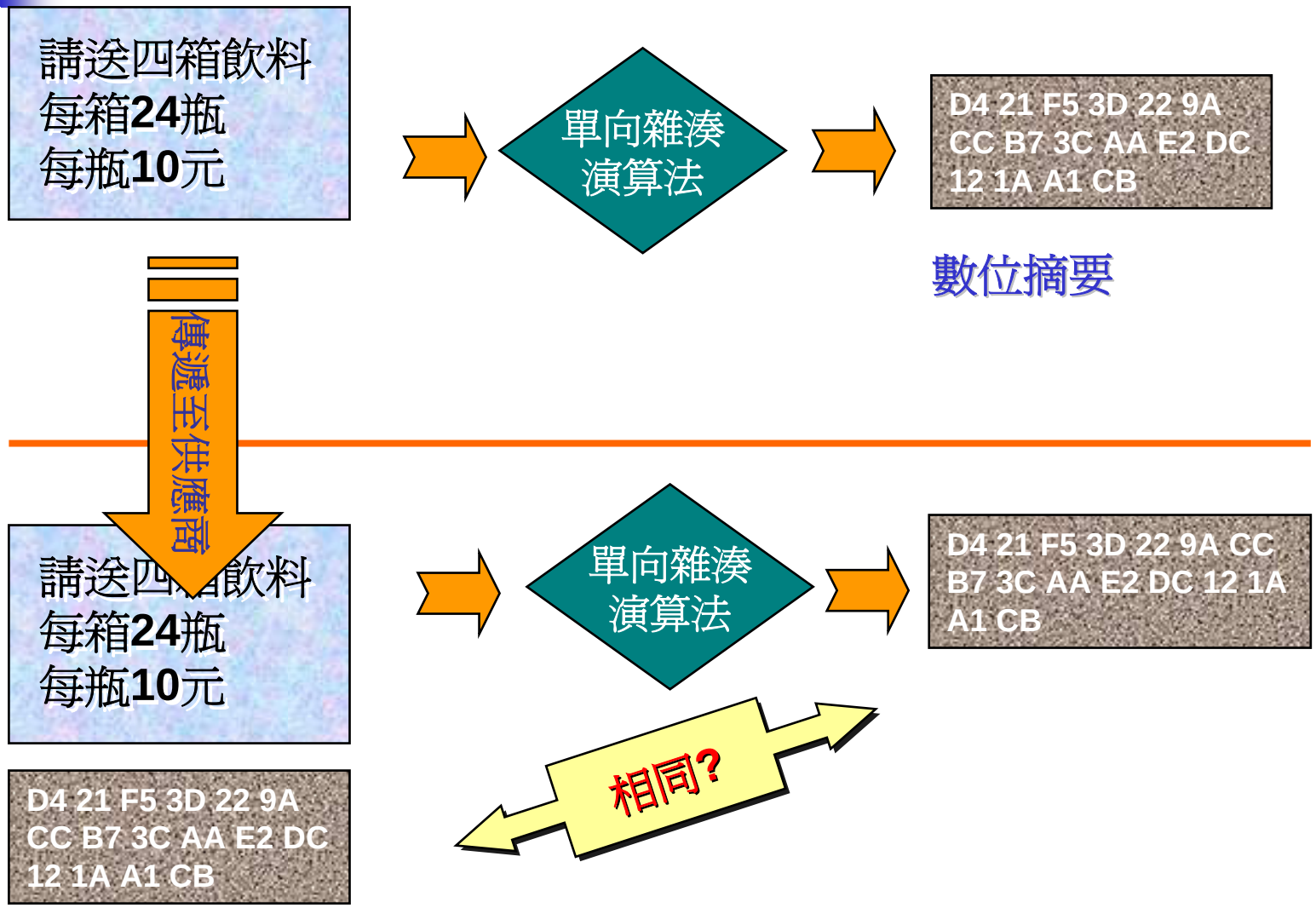
- 用來辨識資料是否被竄改
- 將文件透過雜湊演算法產生輸出結果
- 產生的結果為固定長度的 **“fingerprint”** 資料，通常為**128**或**160** 位元**(bits)**
  - 不同輸入長度，相同輸出長度
  - 數位摘要
- 類似電腦的位元檢查**(CRC)**，但更為複雜
- 不可能編造出一個能產生相同摘要的文件
- 資料中任何一個字元被更改均會導致不同的摘要

單向雜湊的應用

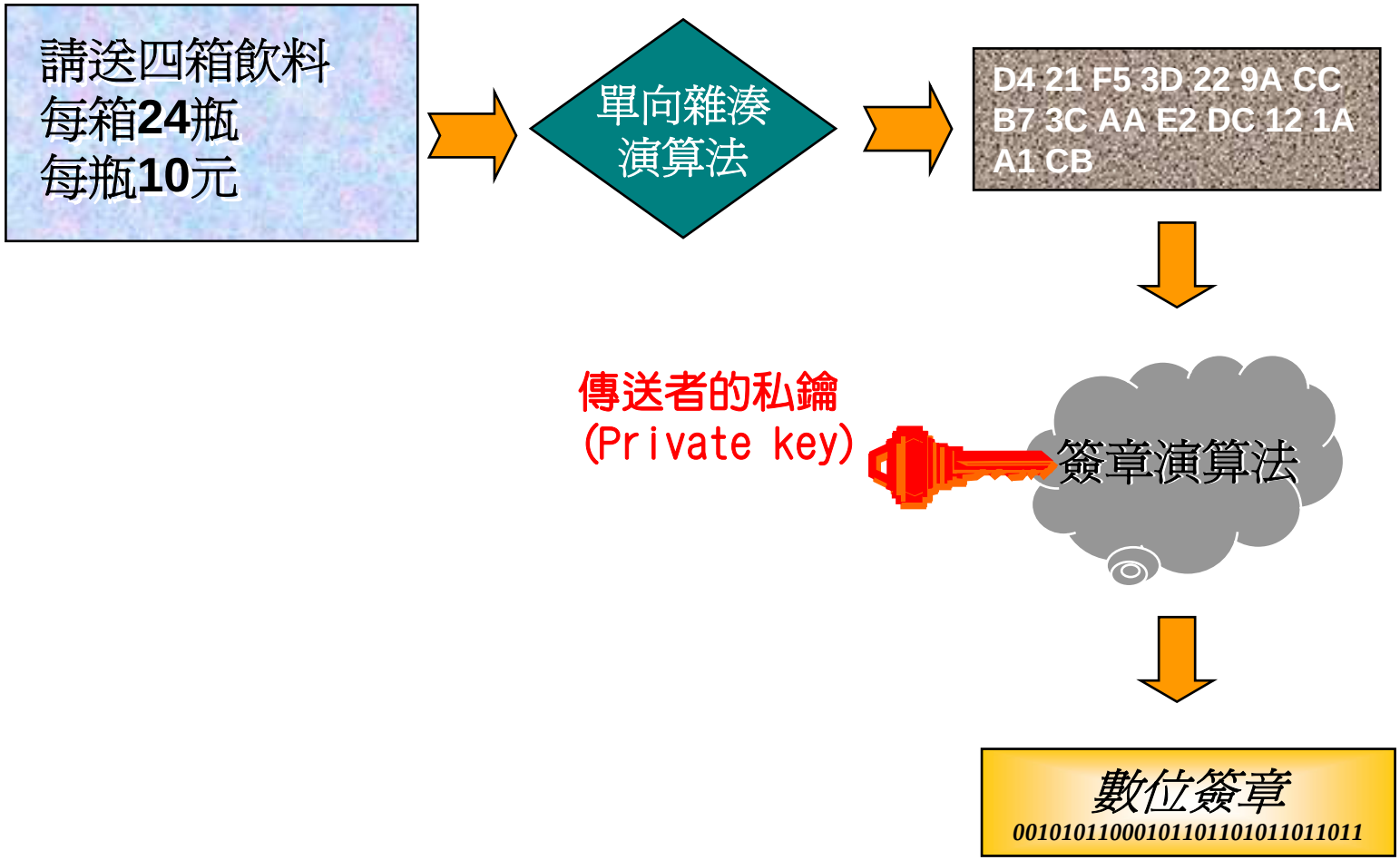
- 使用公開金鑰加密方式執行雜湊運算產生摘要 **(digests)**
  - 用來檢查資料的完整性
  - 用來產生數位簽章



單向雜湊作用



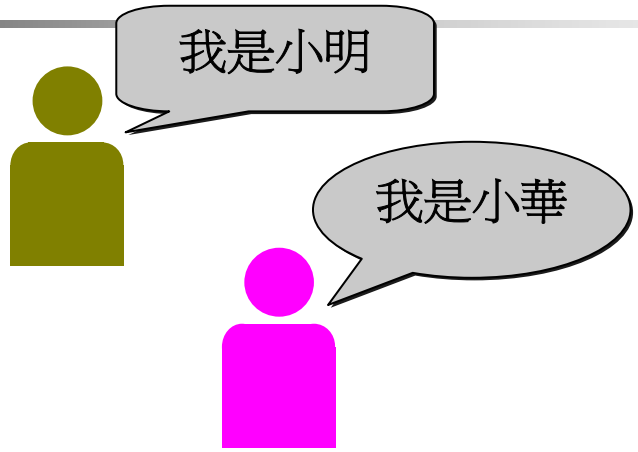
數位簽章(Digital signature)

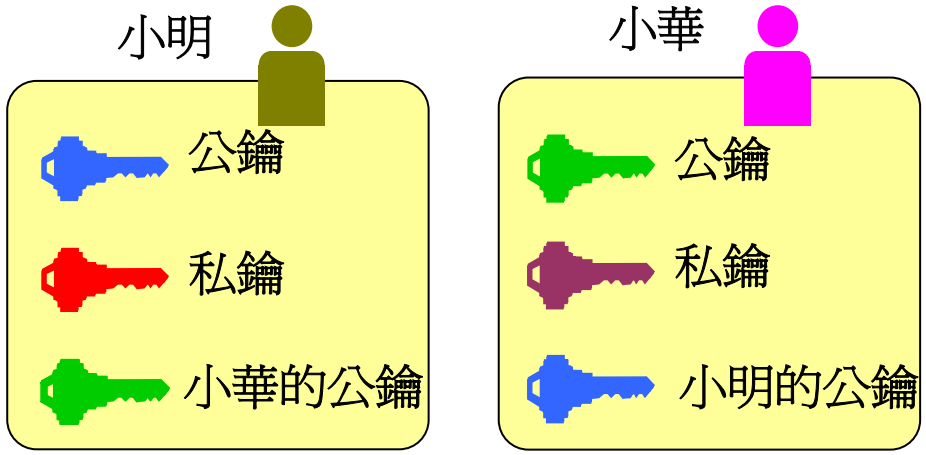


資訊安全的完整步驟

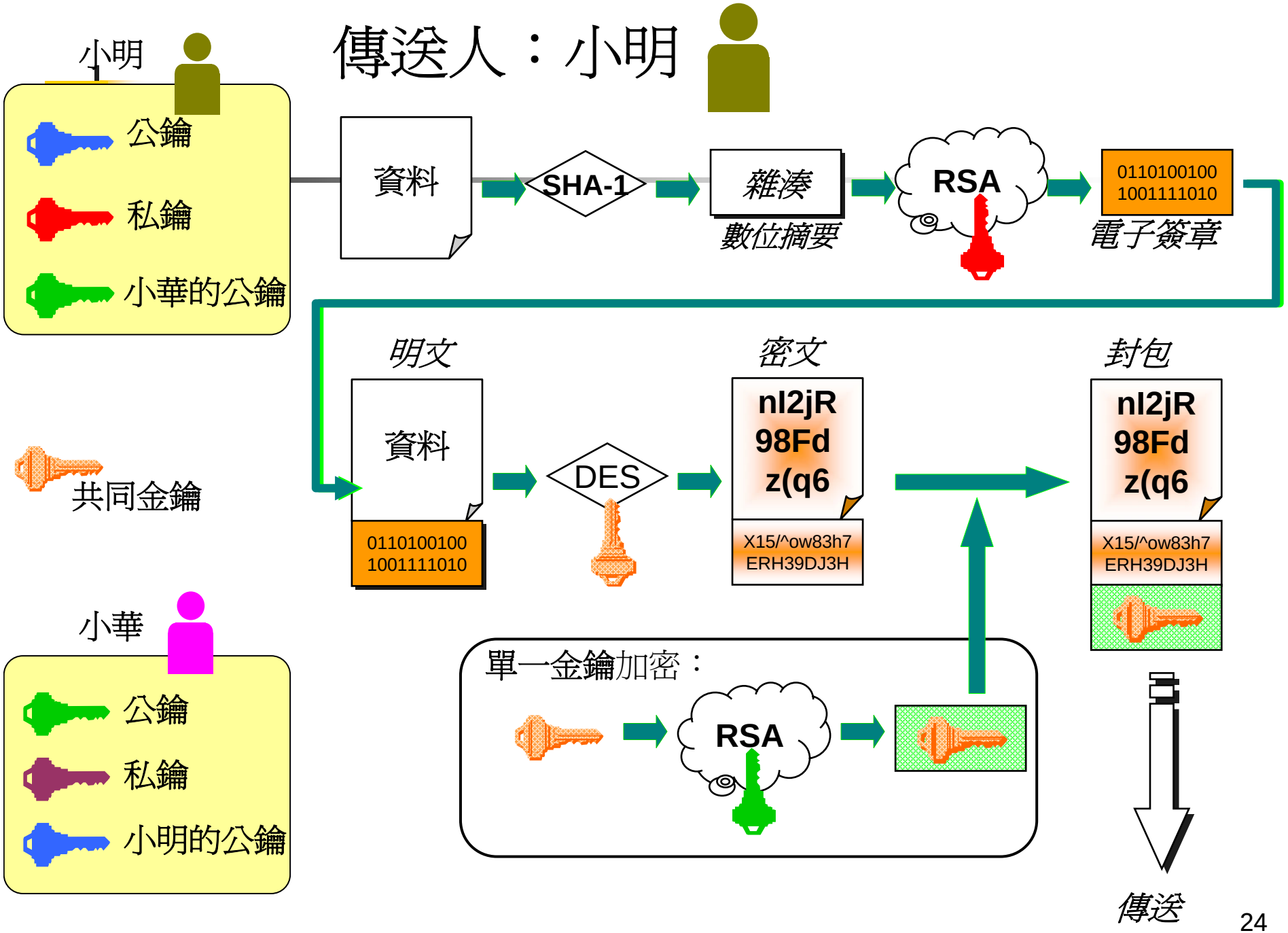
場景

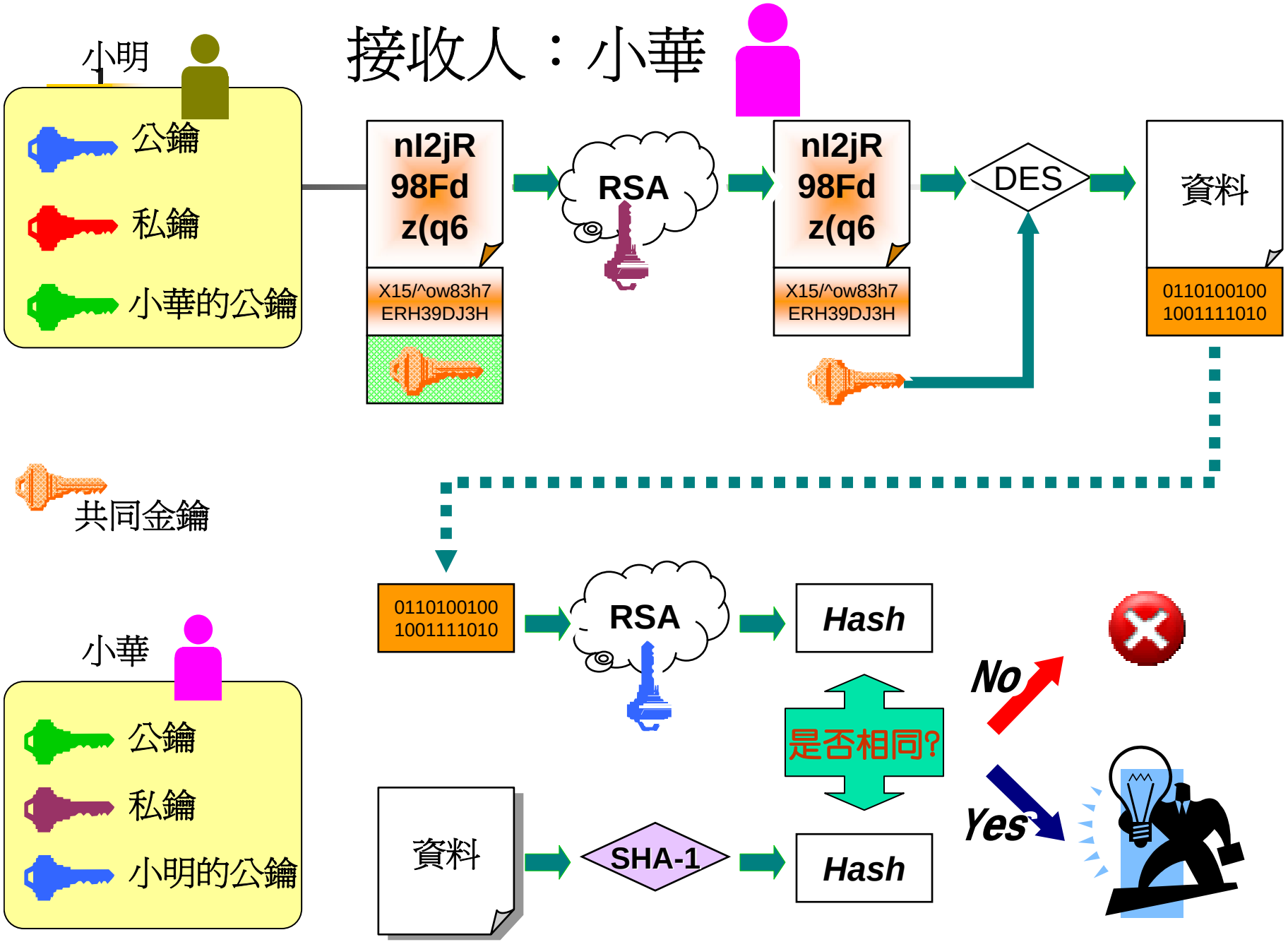
- 人物：
  - 小明
  - 小華
- 事件
  - 小明寫信給小華
- 金鑰種類





隨機產生之
共同金鑰





公開金鑰加密機制是否足夠

- 如果要在電子世界裡重新創造如同傳統紙本方式的商務，光有公開金鑰加密機制仍嫌不足。
- 我們還需要：
  - 資訊安全政策—定義密碼機制如何運作的遊戲規則
  - 有效處理Key 的產生、儲存與管理的運作規範
  - Key和數位證書如何產生、公佈與使用的處理原則

PKI所能達成的目標

- **PKI**提供了包括廣泛多樣的元件、應用程式、政策和實作等核心框架，可以用來組合並達成商業交易的四個安全要求：

1. 機密性
   - 保持資訊隱密
2. 真確性
   - 證明資訊並未遭受竄改
3. 驗證性
   - 證明個人或應用程式的標識
4. 不可否認性
   - 確保發送者不能否定訊息與其關係

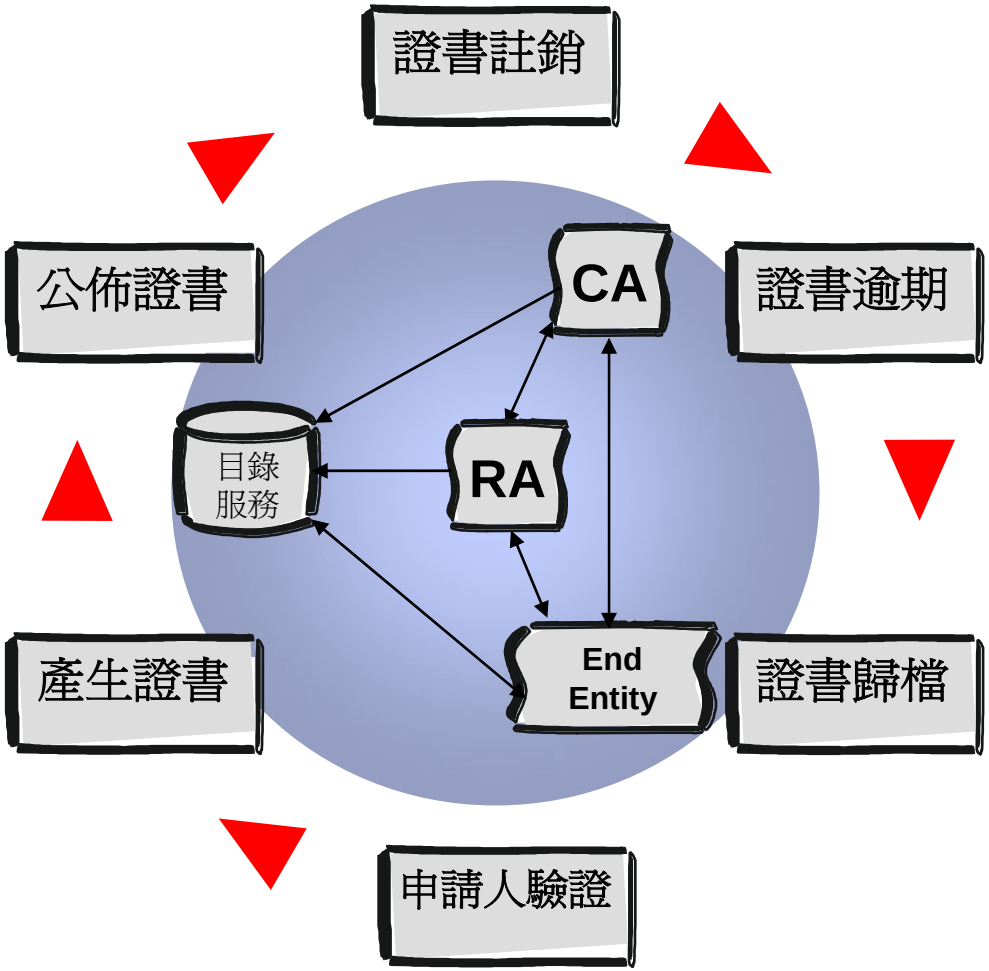
PKI 的組成元件

- **PKI**是由硬體、軟體產品、政策和執行程序等元件所組成
- **PKI**提供了電子商務基本的安全需求
  - 提供使用者能在彼此不認識、散佈世界各地之下能夠透過信任的連結達成安全的商務
- **PKI** 得運作主要即是基於「數位證書 」
  - 作用如同結合使用者公鑰與數位簽章的「電子通行證」

PKI應包含的模組

- 資訊安全政策
- 註冊管理中心(Registration Authority，RA)
- 憑證管理中心(Certificate Authority，CA)
- 憑證公佈系統(Directory Service)
- PKI應用程式

生命週期



資訊安全政策

- 資訊安全政策定義了一個組織的資訊安全最高發展方向，以及密碼學使用的處理方式與原則
- 基本上包含了組織如何管理**key**和機密資料的指導方針，使能夠將控制的層級符合風險的層級

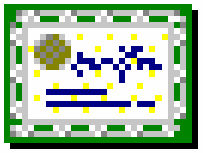
憑證實作準則

- 大部分**PKI**系統屬於商業化的憑證管理中心，因此需要憑證實作準則**(Certification Practice Statement, CPS)**
- **CPS**是一個包含「安全政策需要如何支援與實作」運作程序的詳細文件
- 基本上包括
  - 定義CA如何建構與運作
  - 證書如何發行、取得和收回
  - 金鑰如何產生、註冊、檢定、儲存
  - 如何讓使用者能夠運用

憑證管理 (Certificate Authority)

- **CA 系統是PKI信賴與管理的基礎**
- **對於數位憑證的生命週期，CA包括:**
  - 發行包含使用者個人識別或結合公鑰及數位簽章的憑證
  - 憑證的有效期限
  - 當需要時能夠依據憑證廢止清冊(Certificate Revocation Lists, CRLs)收回憑證

關於憑證



- 憑證內容包括：
  - 小明個人資料
  - 憑證管理中心的資料
  - 小明的公用金鑰
  - 有效日期
  - 由CA所簽發的憑證內容摘要
  - ……

憑證的發行

- 小明如何取得憑證

- 透過註冊管理中心(Registration Agent, RA)或前端應用程式、IC智慧卡產生公鑰與私鑰
- 小明或RA傳送一個包含公鑰的「憑證需求」給CA (RA必須驗證小明就是小明)
- CA將憑證發行給小明
- 小明的軟體或IC智慧卡將憑證儲存起來
- 小明(或CA)將小明的憑證公告週知

憑證的驗證

- 驗證小明的憑證是否有效(相對的其公鑰是否有效)

- 小華取得小明的憑證
- 小華的軟體執行下列步驟:
  - 取得簽發小明憑證的CA憑證
  - 使用憑證管理中心的公鑰計算小明的憑證摘要
  - 取出小明憑證的摘要
  - 比較這兩個摘要是否相同
  - 檢查小明的憑證是否過期

註冊管理中心

- **RA**是介於使用者和**CA**之間的溝通介面。它接收並鑑別使用者的識別資料，並向**CA**提出憑證需求
- 鑑別處理的品質決定了放置在憑證內的信賴層級

憑證公佈系統

- 憑證能夠在**PKI**架構下透過多種方式公佈
  - 例如使用者本身，或透過目錄服務

- 目錄服務可以是組織既有或是**PKI**解決方案的一部份

PKI應用程式

- 對於前端使用者而言，**PKI**的意義是透過**PKI**應用程式所提供的安全框架，讓使用者能夠信賴地安置

- **PKI**應用程式包括：
  - Web伺服器與瀏覽器之間的通訊
  - E-mail
  - 電子資料交換(Electronic Data Interchange, EDI)
  - 網路上的信用卡交易
  - 網路報稅
  - 虛擬私人網路(Virtual Private Networks, VPN)

PKI成功的基石

1. 彈性
2. 容易使用
3. 政策支持
4. 延展性大
5. 互通性
6. 具備足夠的安全性