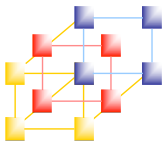
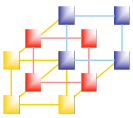


Unit 2
Cryptography

1



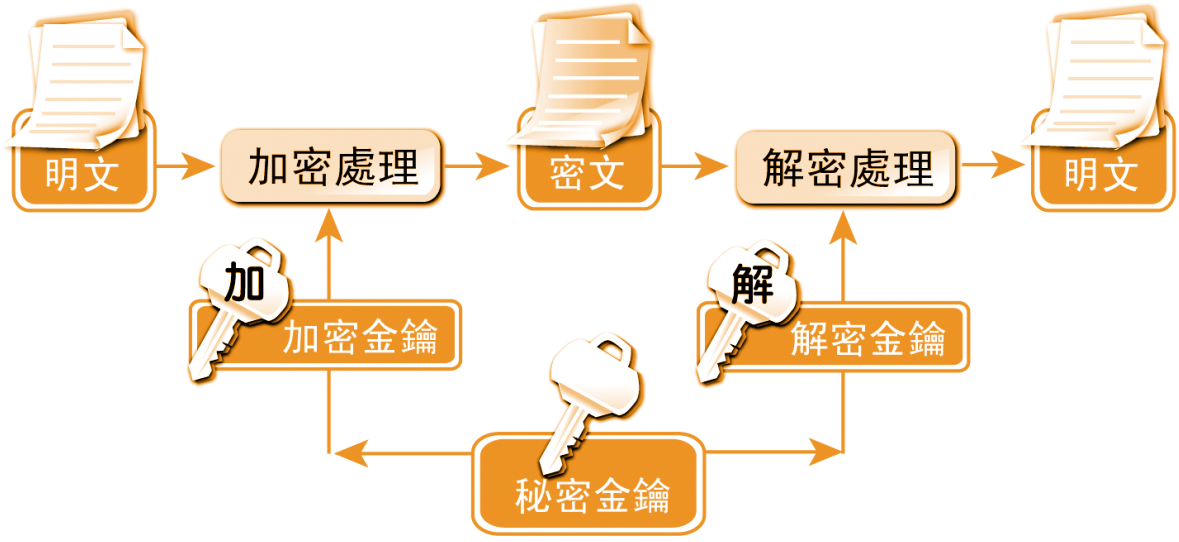
Outline

- 加密的基本概念
- 對稱式加解密法
- 非對稱式加解密法
- 雜湊函數
- 數位簽章

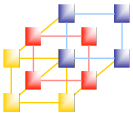
加密的基本概念

- 加密
  - 將資訊 (Information) 打散、避免無權檢視資訊內容的人看到資訊的內容的一種方式，而獲得授權的人，可看到資訊的內容。
  - 所謂『獲得授權的人』是指擁有解密金鑰（key）的人。
- 透過網路來傳遞機密資訊，很容易就被竊聽。因此，對於機密資料存入於磁碟、備援磁帶、或經由網路傳遞前，應先加密成密文，使一般未經授權人員不能得知其內容。

密碼學基本概念



基本的加解密系統



密碼學基本概念

E：加密演算法

D：解密演算法

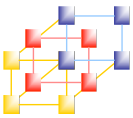
K：金鑰

C：密文

M：明文

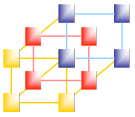
加密公式： $C = E_K(M)$

解密公式： $D_K(C) = D_K(E_K(M)) = M$



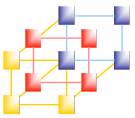
公開的加密方法或演算法

- 較不佔空間
  - 不需再儲存相關的加解密程式
- 即使為保密的加解密演算法也難保其安全
- 相容性的問題
  - 不需為每一對加解密的使用者準備一組加解密程式



密碼系統之安全性程度

- 無條件安全(Unconditionally Secure)
  - 非法使用者不管截獲多少個密文，用盡各種方法還是沒有足夠資訊可以導出明文機密資料。
  - Ex: 一次性密碼系統 (One-Time Pad)
- 計算安全(Computationally Secure)
  - 目前或未來預測之科技、以合理之資源設備下，要破解密碼系統需要一段相當長的時間（例如數百年）。



無條件安全密碼系統

One-time Pad 加密方法

$$c = k \oplus m$$

$$m = k \oplus c$$

加密 $c = k \oplus m$

$= 0011111000111000 \oplus 1001101101010011$

$= 1010010101101011$

解密 $m = k \oplus c$

$= 0011111000111000 \oplus 1010010101101011$

$= 1001101101010011$

1. 加解密金鑰使用一次即丟
2. 需擁有一份與明文長度相同或更長的金鑰

密碼系統的分類

- 對稱性密碼系統(Symmetric Cryptosystems)或秘密金鑰密碼系統(Secret-Key Cryptosystems) 或單金鑰密碼系統(One-Key Cryptosystems)

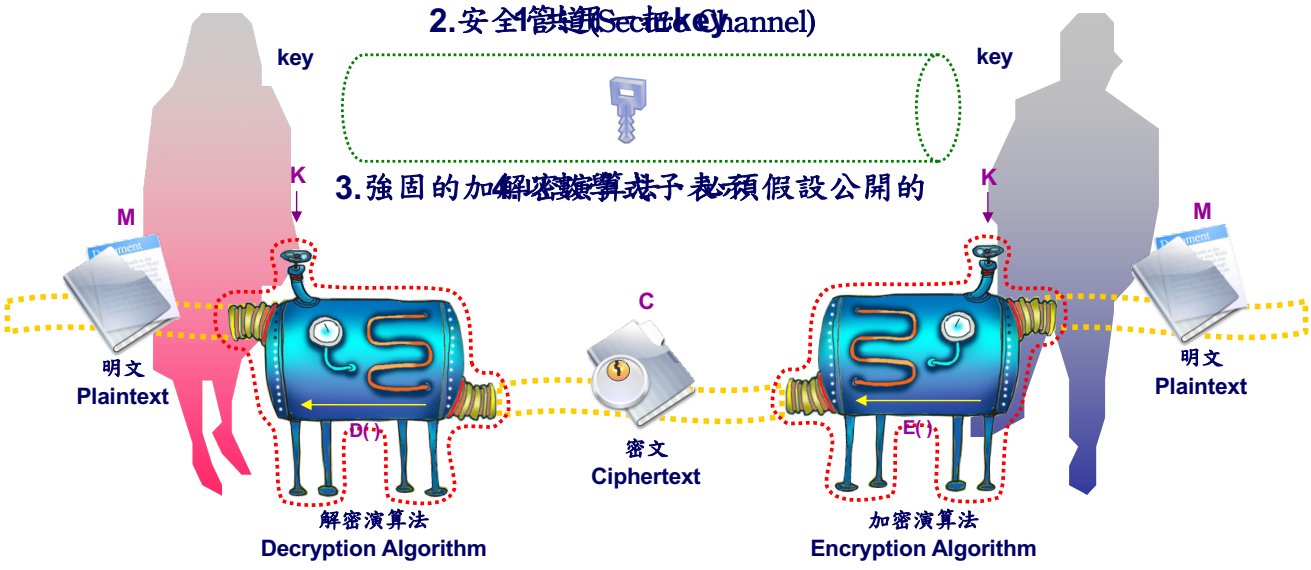
  加密金鑰及解密金鑰為同一把

- 非對稱性密碼系統(Asymmetric Cryptosystems)或公開金鑰密碼系統(Public-Key Cryptosystems) 或雙金鑰密碼系統(Two-Key Cryptosystems)

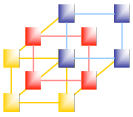
  加密與解密金鑰為不相同的二把金鑰

對稱式加密(Symmetric Encryption)

又稱為Conventional / Private-key / Single-key Encryption

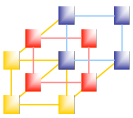


1.共用一把key　2.安全管道　3.強固加密演算法、必須假設是公開的　4.以數學公式表示之 $C=E_K(M)$, $M=D_K(C)$



對稱式加解密法

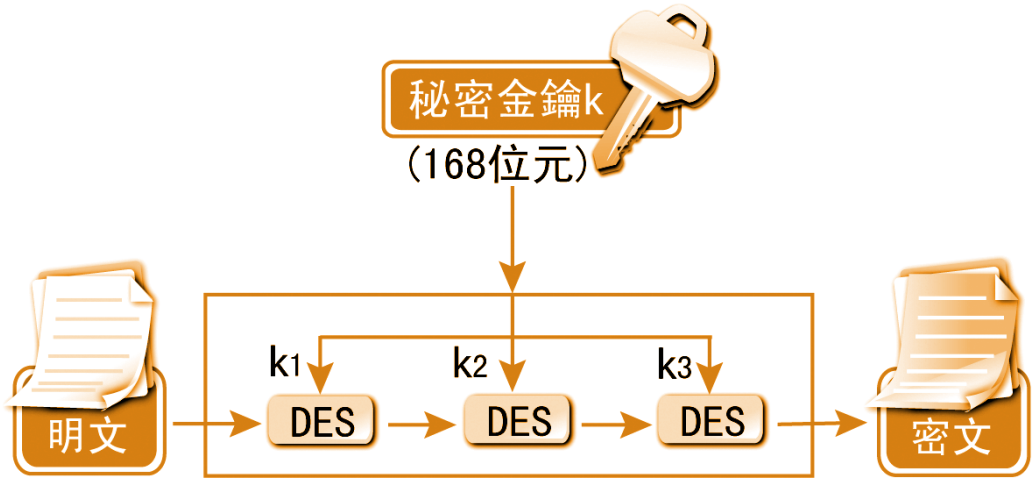
- DES (Data Encryption Standard)
- Triple DES
- AES (Advanced Encryption Standard)
- …



DES (Data Encryption Standard)

- 對稱式加密系統之代表
- 1970年代中期由IBM公司所發展
- 一種區塊加密法(Block Cipher)，由美國國家標準局公佈為資料加密標準
- DES 屬於區塊加密法，而區塊加密法就是對一定大小的明文或密文來做加密或解密動作
- 每次加密解密的區塊大小均為 64 位元(Bits)

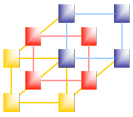
Triple DES



Triple DES 加密架構

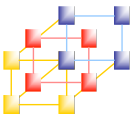
AES (Advanced Encryption Standard)

- 為了取代DES，NIST在1997年公布AES (Advanced Encryption Standard，高等加密標準)徵選活動。
- 在2000十月，NIST宣佈來自比利時的兩位密碼學家 — Joan Daemon-Vincent Rijmen，他們提出的Rijmen演算法贏得這項競賽。
- 並於2001年十一月完成評估，發佈為FIPS PUB 197標準。
- AES牢靠度高、適用於高速網路、可在硬體設備建置等因素，都是這個演算法獲選的原因。



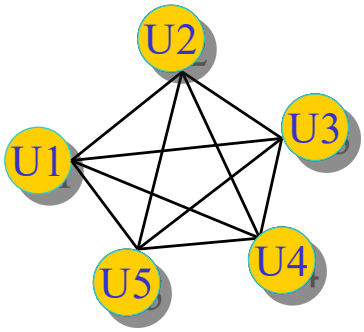
AES 的特色

- 採用私密金鑰的對稱式區段加密法。
- 資料區段為 128 位元, 金鑰為 128/192/256 位元。
- 運算速度比 Triple-DES 更強更快。
- 具有完備的規格與設計細節供參考。
- AES可採用 C 與 Java 來實作。



公開金鑰基本概念

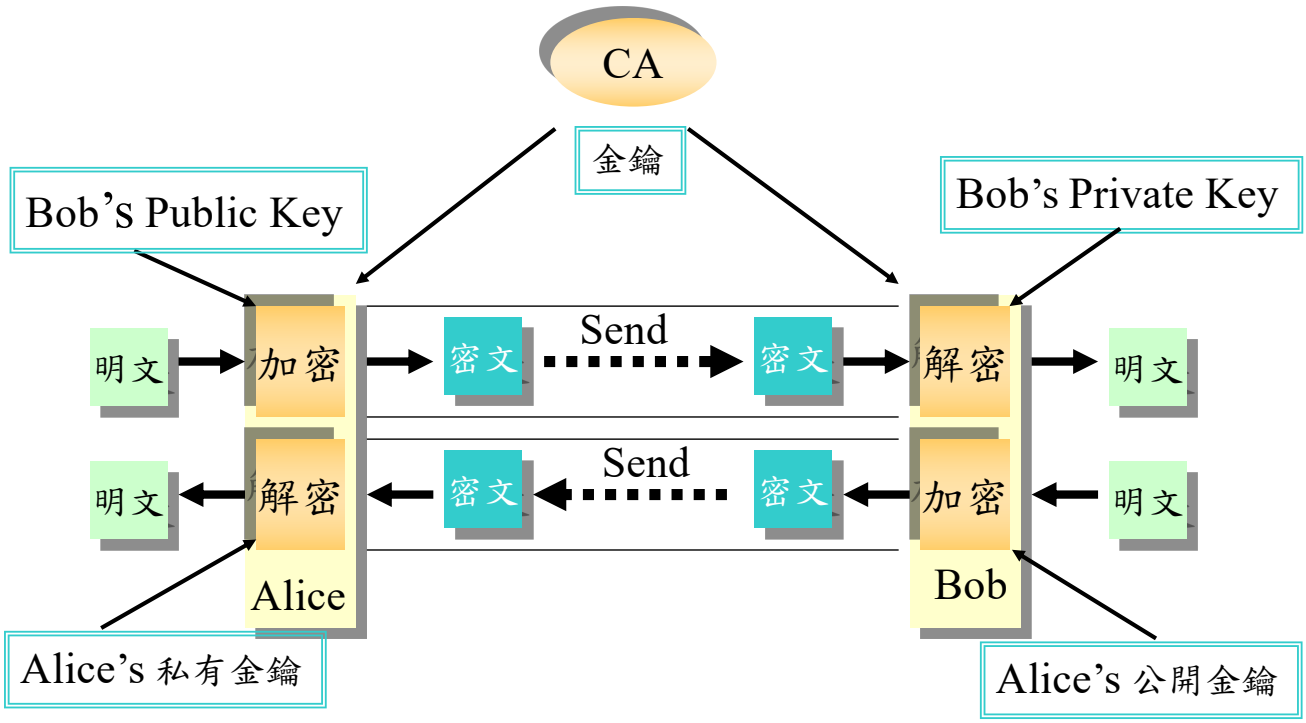
- 對稱式密碼系統有金鑰的管理問題
  - 例如要與N個人做秘密通訊，那麼就必須握有N把秘密金鑰
- 為了改善對稱式密碼系統問題，於是便有公開金鑰密碼系統(Public-Key Cryptosystems)的產生

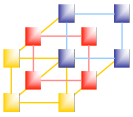


公開金鑰密碼系統

- 著名之公開密碼系統
  - RSA密碼系統
  - ElGamal密碼系統
  - Elliptic Curve Cryptosystem, ECC橢圓曲線的密碼系統
- 公開密碼系統優點
  - 沒有金鑰管理的問題
  - 高安全性
  - 有數位簽章功能
- 公開密碼系統缺點
  - 加解密速度慢

公開金鑰加密系統

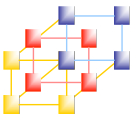




RSA 加密法

- 非對稱式密碼系統的一種。
  - 1978年美國麻省理工學院三位教授Rivest、Shamir、Adleman (RSA) 所發展出來的。
- 利用公開金鑰密碼系統作為資料加密的方式，可達到資料加密及數位簽署的功能。

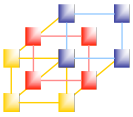
- Encryption
  - RSA 加密演算法，明文加密使用區塊為每次加密的範圍，使用對方公開金鑰 (Public Key) 將明文加密。
- Decryption
  - RSA 解密演算法，必須使用自己的私有金鑰 (Private Key) 才能將密文解出。



RSA 演算法

- 張三選 2 個大質數 p 和 q (至少100位數)，
  令 N = p ・ q
- 再計算Ø(N)=(p-1)(q-1)，並選一個與Ø(N)互質數 e
  - Ø(N)為Euler's Totient函數，其意為與N互質之個數
- (e, N) 即為張三的公開金鑰
- 加密法為 $C = M^e \bmod N$
- 張三選 1 個數 d，滿足 e ・ d $\bmod$ Ø(N) = 1
- d 即為張三的解密金鑰(亦稱私有金鑰或祕密金鑰)
- 解密法為 $M = C^d \bmod N$

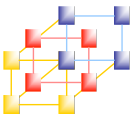
- **RSA之安全性取決於質因數分解之困難度**
- **要將很大的N因數分解成P跟Q之相乘，是很困難的**



RSA 演算法- 例子

- 張三選 p = 3 ， q = 11
  此時 N = p ・ q = 3 x 11 = 33
- 張三選出一個與 (p-1) x (q-1) = (3-1)(11-1) = 20互質數 e = 3
- (e, N) = (3,33) 即為張三的公開金鑰
- 張三選一個數 d = 7 當作解密金鑰，
  滿足 e ・ d ≡ 1 mod 20 (7 x 3 ≡ 1 mod 20)

- 令明文 M = 19
  - 加密 : $C = M^e \bmod N = 19^3 \bmod 33 = 28$
  - 解密 : $M = C^d \bmod N = 28^7 \bmod 33 = 19$



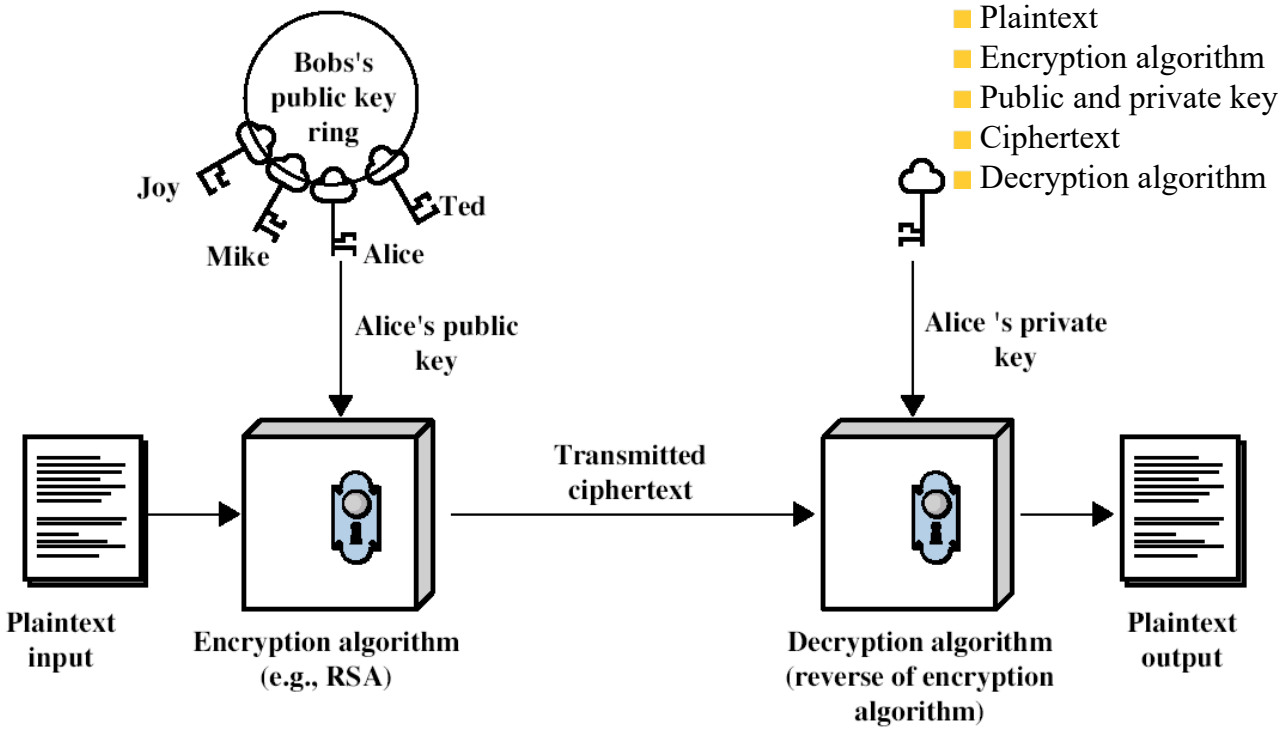
公開金鑰加密系統之特性 (1/2)

1. D(d, E(e, M)) = M，可還原性
2. d 和 e很容易求得
3. 若公開(e, n)，別人很難從(e, n)求得d，即只有自己知道如何解密(以e加密)
4. E(e, D(d, M)) = M

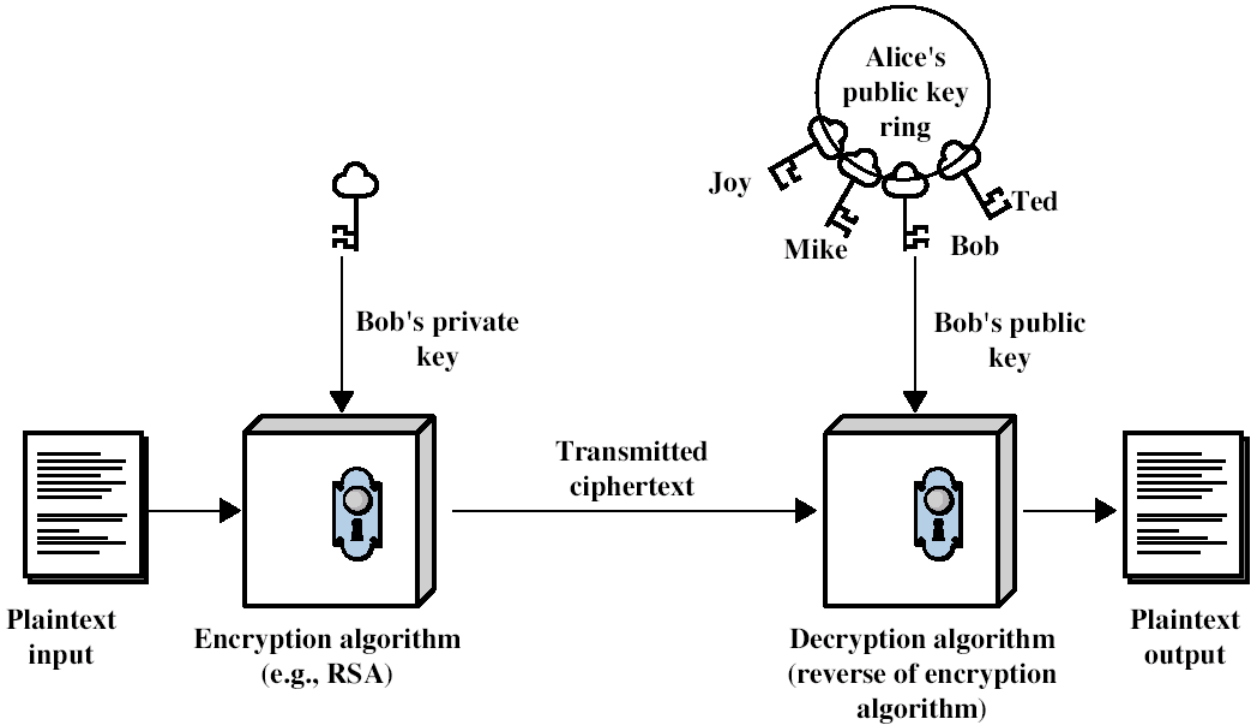
公開金鑰加密系統之特性 (2/2)

- 滿足1~3項稱之為trap-door one-way function
  - “one-way”因易加密而不易解密
  - “trap-door”若知一些特別資訊即可解密
- 滿足1~4項稱之為trap-door one-way permutation
- 1~3項為public-key cryptosystems之要求
- 若同時滿足第4項要求，則該保密法可用來製作數位簽章。

Public-Key Cryptography -- Encryption

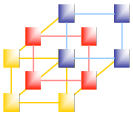


Public-Key Cryptography -- Authentication



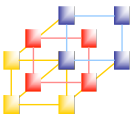
雜湊函數

- 在網路上公開的傳送文件訊息(Document or Message)很容易遭到駭客攔截竄改、新增、或刪除等攻擊。
  - 需對文件訊息作完整性(Integrity)驗證。
- 該文件訊息是否確實為某人所送過來的文件訊息，而非由他人假冒。
  - 需驗證訊息的來源是否正確。
- 這兩項功能可藉由訊息鑑別碼 (Message Authentication Code，MAC) 的輔助來達成



單向雜湊函數

- 單向雜湊函數二個主要功能
  - 將文件訊息打散及重組，使其不能再還原為原始文件訊息。
  - 將任意長度的文件訊息壓縮成固定長度的訊息摘要(Message Digest，MD)。
- 數學式子
  - MD=H(M)　　H(.)：一單向雜湊函數
M　：表一任意長度文件訊息
  - Ex: $E(M) = M^2 \bmod 1024$，不管文件 M 多大，經由 E(.) 計算的結果都是一個 10 bits 的數

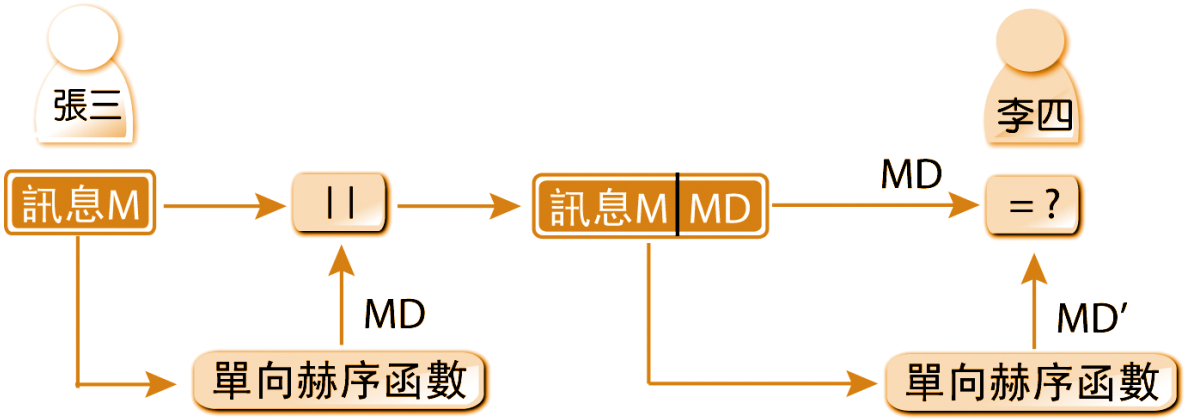


單向雜湊函數特性

- 單向雜湊函數三種特性
  - 給定文件訊息M，可很容易算出其對應的訊息摘要MD 。
  - 給定一訊息摘要MD ，很難從MD去找到一個文件訊息M’，使H(M’)= MD。
  - 給定一文件訊息M，很難再找到另一文件訊息M’，使H(M)=H(M’)。
    - 避免碰撞的情況發生 (Collision-resistance)

文件訊息完整性驗證 (1/2)

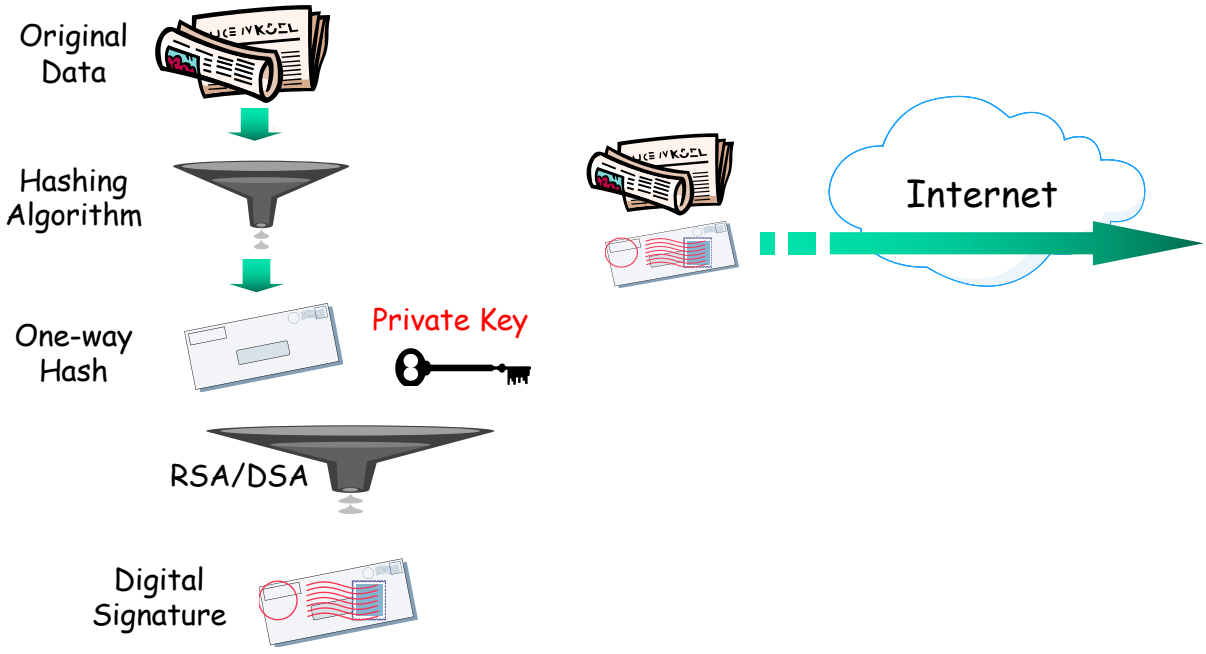
- 以單向赫序函數做文件訊息的完整驗證，其驗證方式如下：



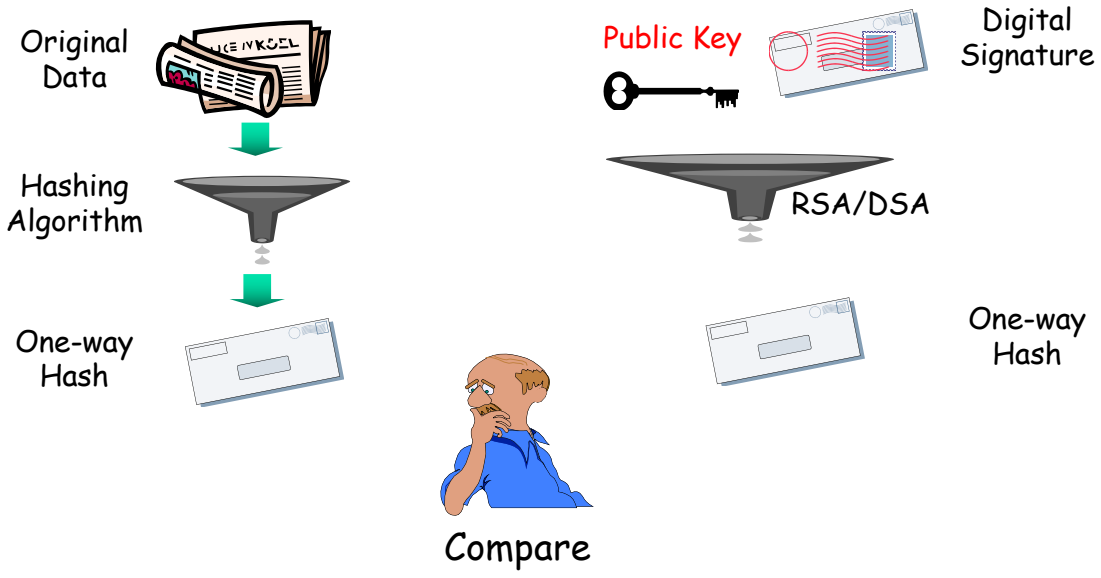
文件訊息完整性驗證 (2/2)

- 首先張三先將要傳送給李四的文件訊息M，經單向赫序函數運算後得到一訊息摘要MD，再將文件訊息M與訊息摘要MD一起送給李四
- 李四收到後先將文件訊息M用同樣的單向赫序函數運算，假設得到一訊息摘要MD’ ，李四再比較MD’ 是否與收到的MD相同，若相同，則李四則可確認此文件之完整性。

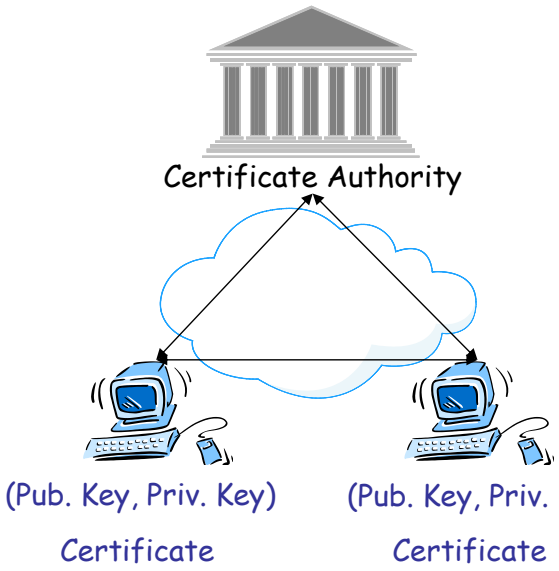
Digital Signature -- Sender



Digital Signature -- Receiver



Public-Key Infrastructure



- X.509 (ITU-T)
  - Directory service
  - Authentication Framework
  - Lightweight Directory Access Protocol (LDAP; RFC1777)
- Certification Revocation List (CRL)
  - Lightweight Directory Access Protocol (LDAP; RFC1777)
  - Online Certificate Status Protocol (OCSP;RFC2560)

Certificate