《電子交易條例草案》審議委員會

數碼簽署

一九九九年十一月四日

人手簽署

簽署的定義是：「在文件上寫上名字，用作認證，確定和認可該份文件」。

簽署有三項主要的功用：

- σ 認證
- σ 保障不可被推翻
- σ 保持完整無缺

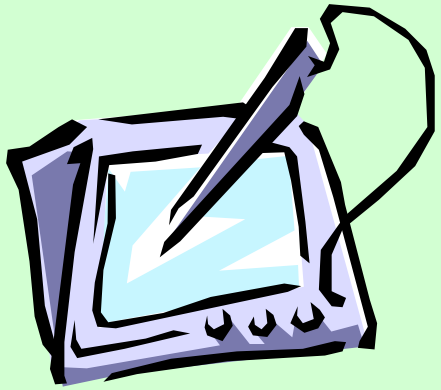
人手簽署的可靠性

在於

- 人手簽署的特徵
- 油墨透入紙張的纖維
- 作出修改或刪除後易被發現

電子簽署

「指與電子紀錄相連的或在邏輯上相聯的數碼形式的任何字母、字樣、數目字或其他符號，而該等字母、字樣、數目字或其他符號是爲認證或承認該紀錄的目的而簽立或採用的。」



數碼簽署

「就電子紀錄而言，指簽署人的電子簽署，而 該簽署是用非對稱密碼系統及雜湊函數將該電子紀錄作數據變換而產生的，使持有原本未經數據變換的電子紀錄及簽署人的公開密碼匙的人能據之確定—

(a) 該數據變換是否用與簽署人的公開密碼匙對應的私人密碼匙產生 的；及

(b) 在產生數據變換之後，該原本的電子紀錄是否未經變更 。」

非對稱密碼技術

原文

簽署的定義是在文件上寫上一個名字。

加密

密文

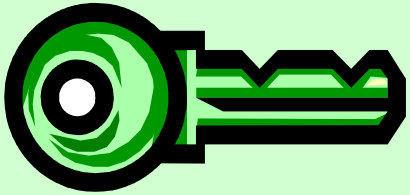
Abx uha
jDKAJS
LKwimJ
129x1s

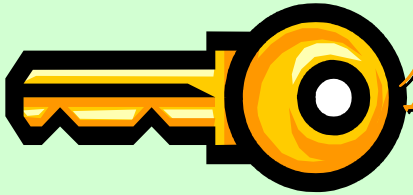
解密

原文

簽署的定義是在文件上寫上一個名字。

私人密碼匙





公開密碼匙

解密

簽署的定義是在文件上寫上一個名字。

原文

Abx uha
jDKAJS
LKwimJ
129x1s

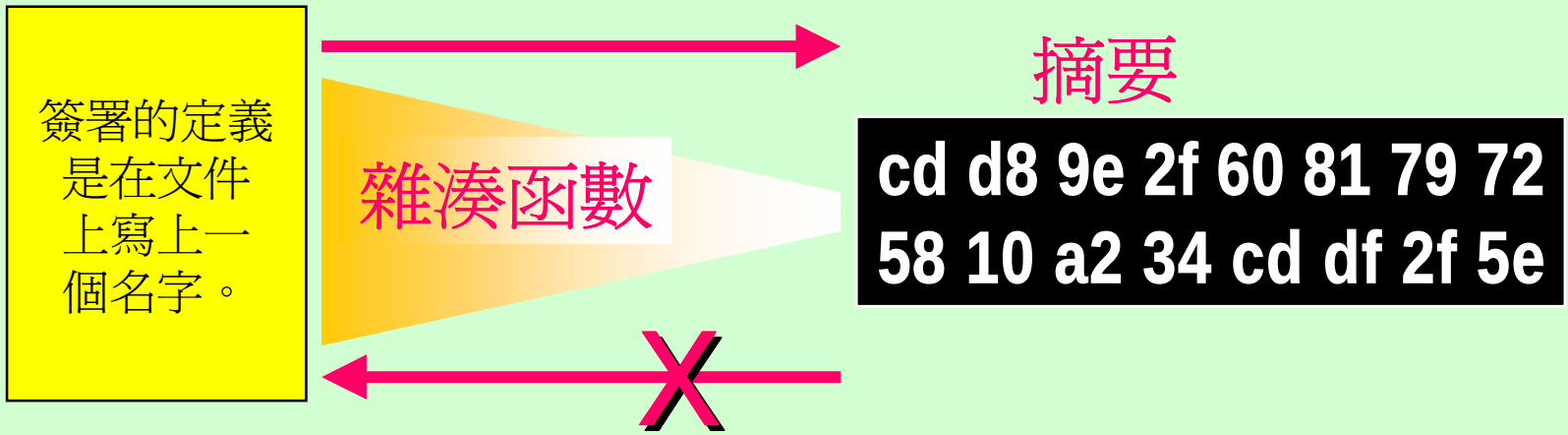
密文

加密

簽署的定義是在文件上寫上一個名字。

原文

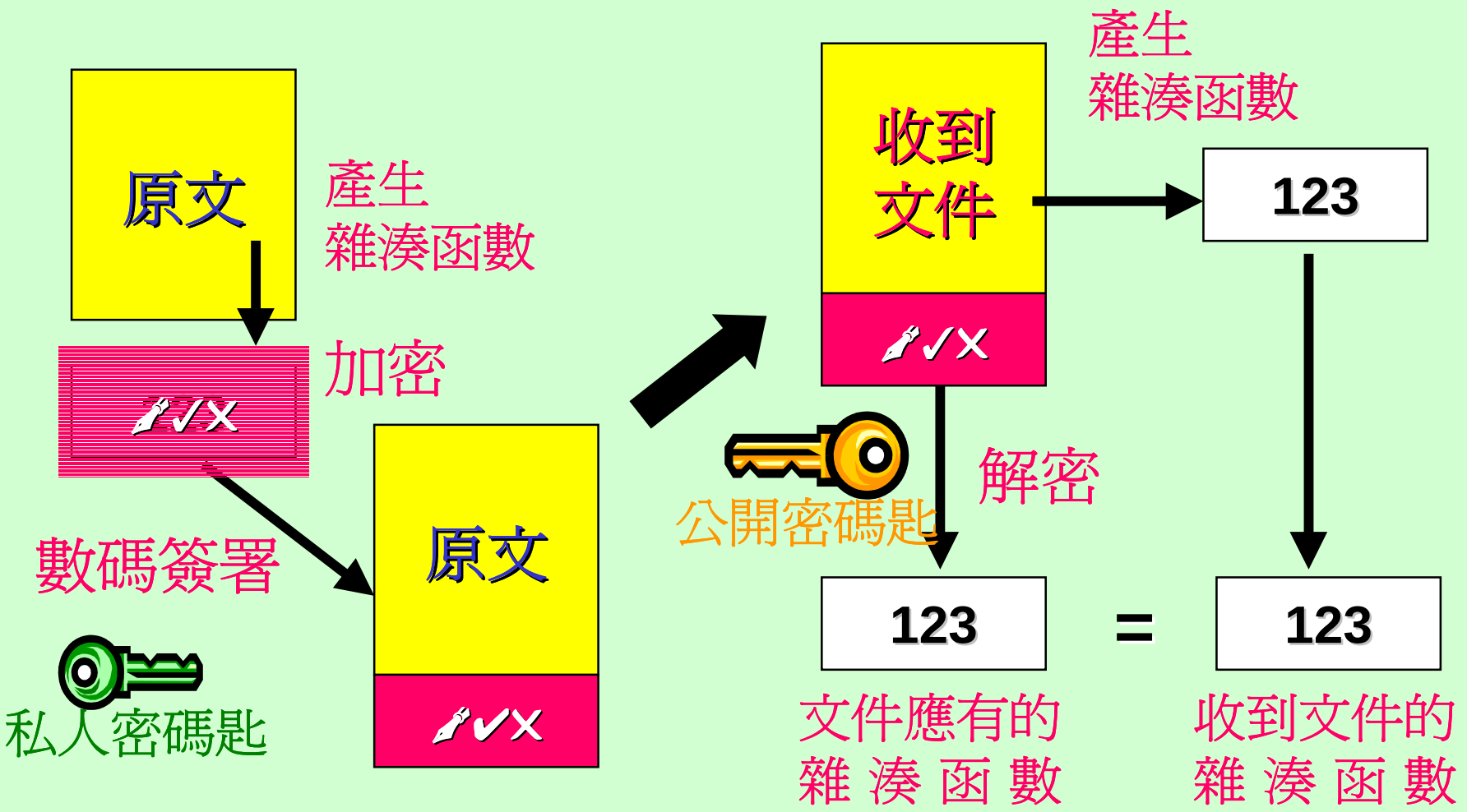
雜湊函數 (Hash Function)



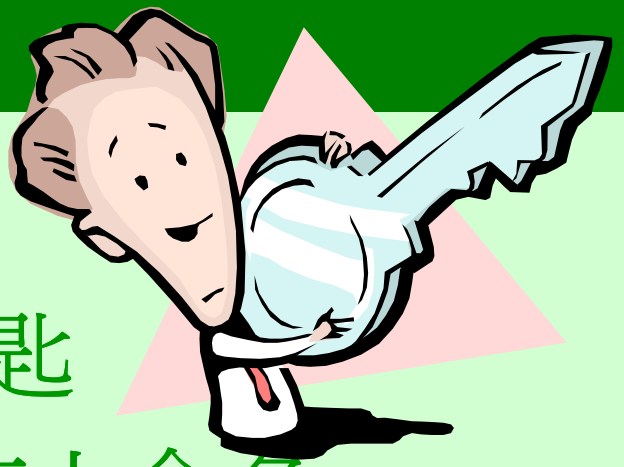
雜湊函數算法

Message Digest 5 (MD5)	***128 bits***（16字節）
Secure Hash Algorithm (SHA-1)	***160 bits***（20字節）

數碼簽署的應用及運作

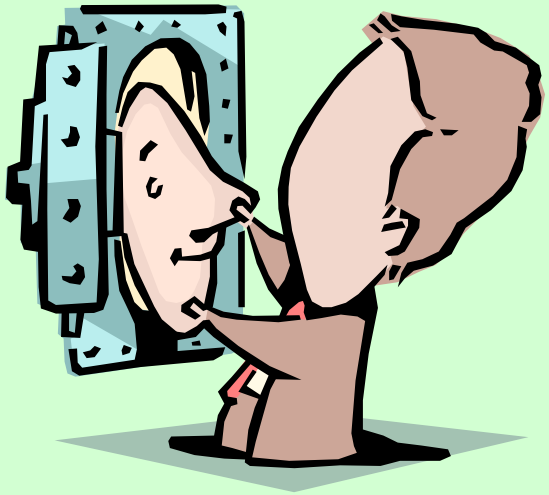

原文
產生
雜湊函數
加密
數碼簽署
私人密碼匙
原文
收到
文件
產生
雜湊函數
123
公開密碼匙
解密
123
=
123
文件應有的
雜 湊 函 數
收到文件的
雜 湊 函 數

問題



任何人都可以

- 製造私人/公開密碼匙
- 爲私人密碼匙的持有人命名
- 將公開密碼匙放置在公開目錄中

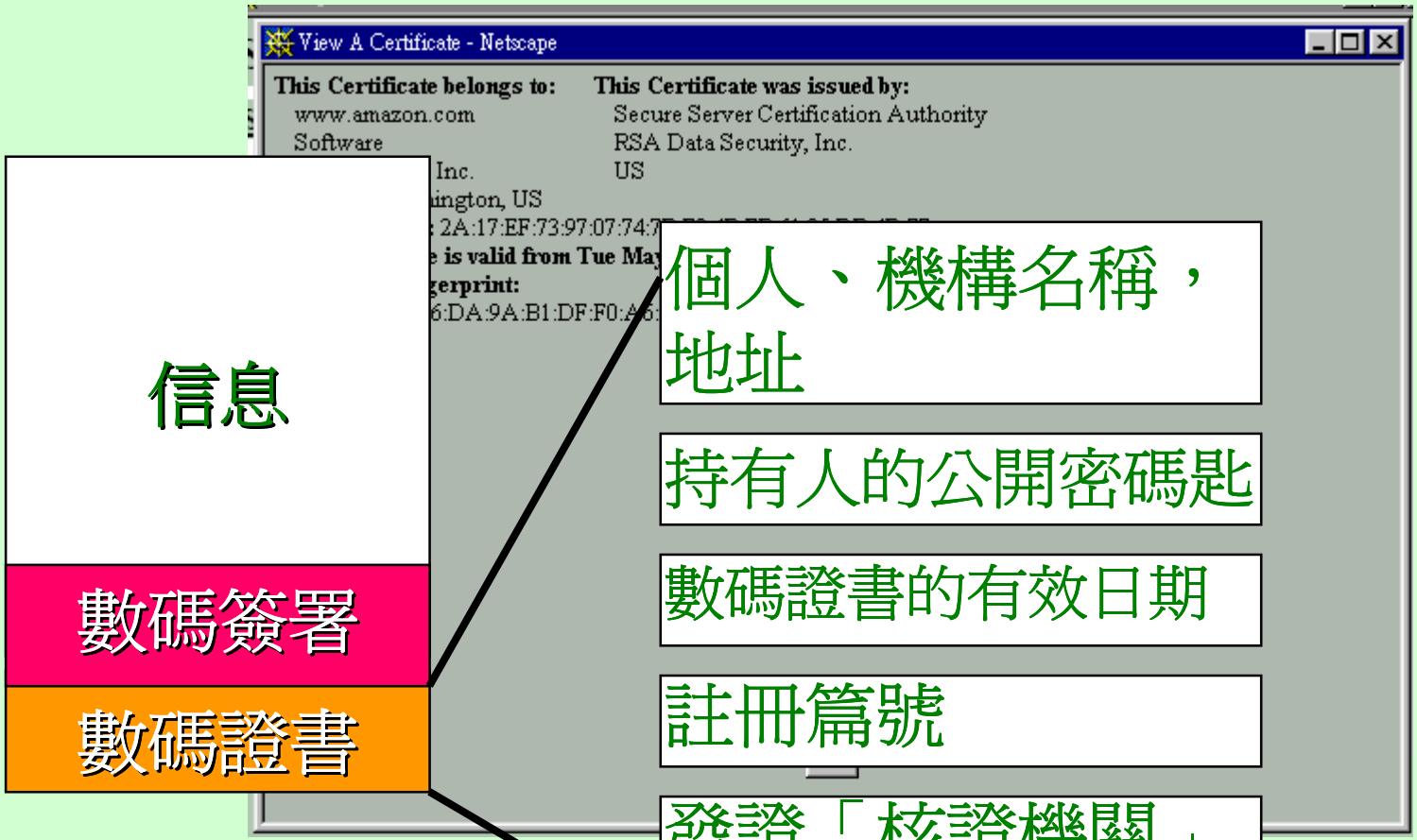


問題在於，如何才能確定私人密碼匙持有人的真正身份。

核證機關

- 數碼證書可証實私人密碼匙與持有人之間的關係
- 由一可信任第三者發出的數碼證書具公信力
- 發出的數碼證書的可信任第三者亦稱爲核證機關

數碼證書


View A Certificate - Netscape
This Certificate belongs to:
www.amazon.com
Software
Inc.
ington, US
2A:17:EF:73:97:07:74:7
is valid from Tue May
gerprint:
6:DA:9A:B1:DF:F0:A6:
This Certificate was issued by:
Secure Server Certification Authority
RSA Data Security, Inc.
US
信息
數碼簽署
數碼證書
個人、機構名稱，地址
持有人的公開密碼匙
數碼證書的有效日期
註冊篇號
發證「核證機關」的數碼簽署