密碼學介紹

主講人：陳靖德

日期：2014/11/14

這份投影片

- 沒有艱深的數學
- 不能讓你變成密碼學專家
- 概念為主

主題

- 對稱式加密〈Symmetric-key encryption〉
  - 凱撒密碼〈Caesar cipher〉
- 雜湊函數〈Hash Function〉
  - 應用
- 非對稱式加密〈Asymmetric-key encryption〉
- 密碼學應用
- 名詞介紹

凱撒密碼

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 Z

↓ ↓

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 C

The quick brown fox jumps over the lazy dog

↓

WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ

↓

The quick brown fox jumps over the lazy dog

* 實務上會捨掉空白

DES、AES

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

＊ 有興趣可以去研究

雜湊函數

- 雜湊函數是輸入不定長度的資料，會輸出固定長度的資料
- 很少發生不同資料對應到相同Hash值(碰撞)
- 很難從輸出資料反推輸入資料
- 常見的雜湊函數有MD5、SHA系列

Example

MD5("hello, world!!") => 9fe4fa1a9c66b49ffef769c595bfd9ec

MD5("hello, world!?") => 9631637dabe36824f8b715fa7692a26d

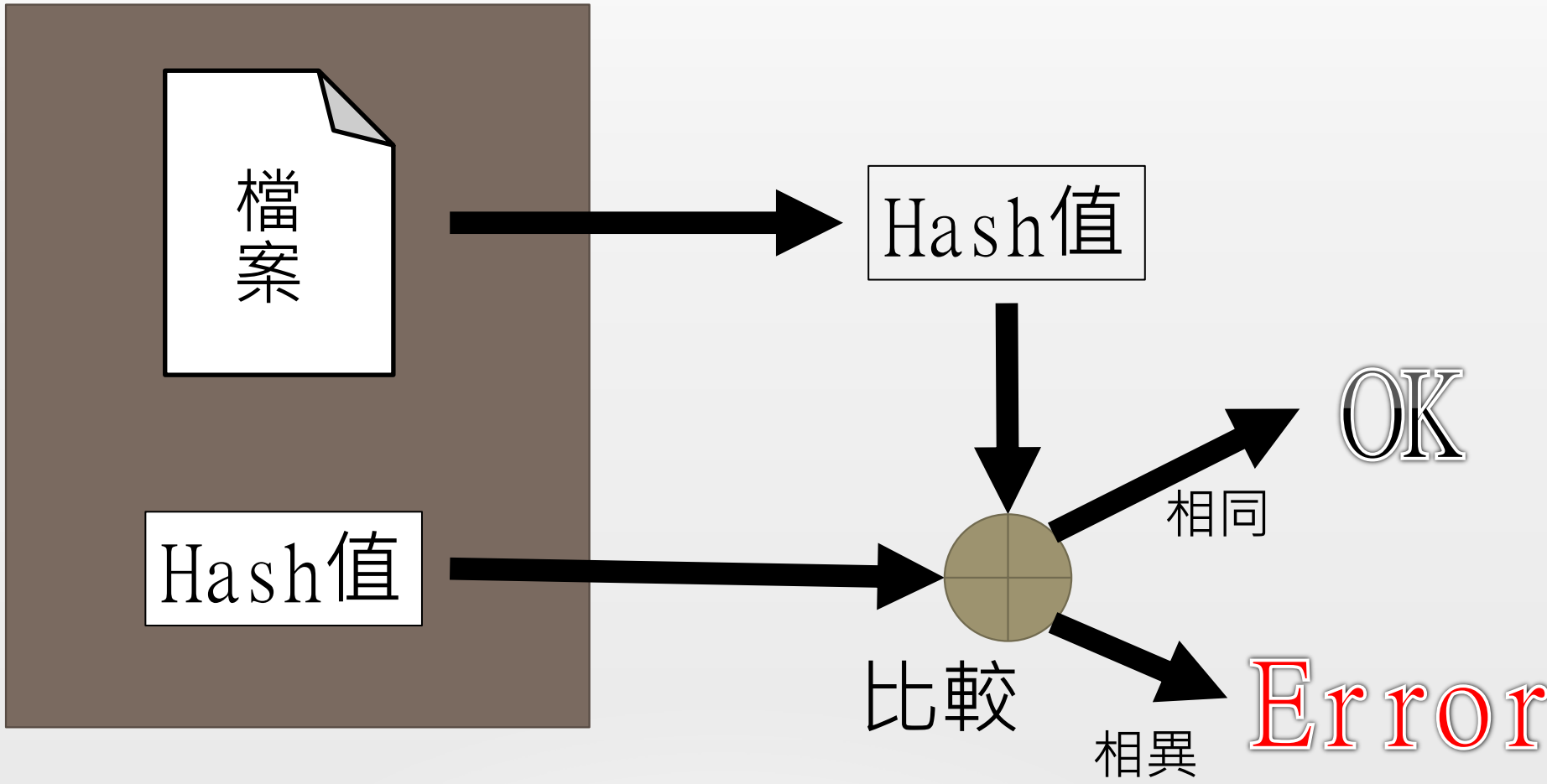
Google(md5 online)

* 有安全需求時，不要使用MD5

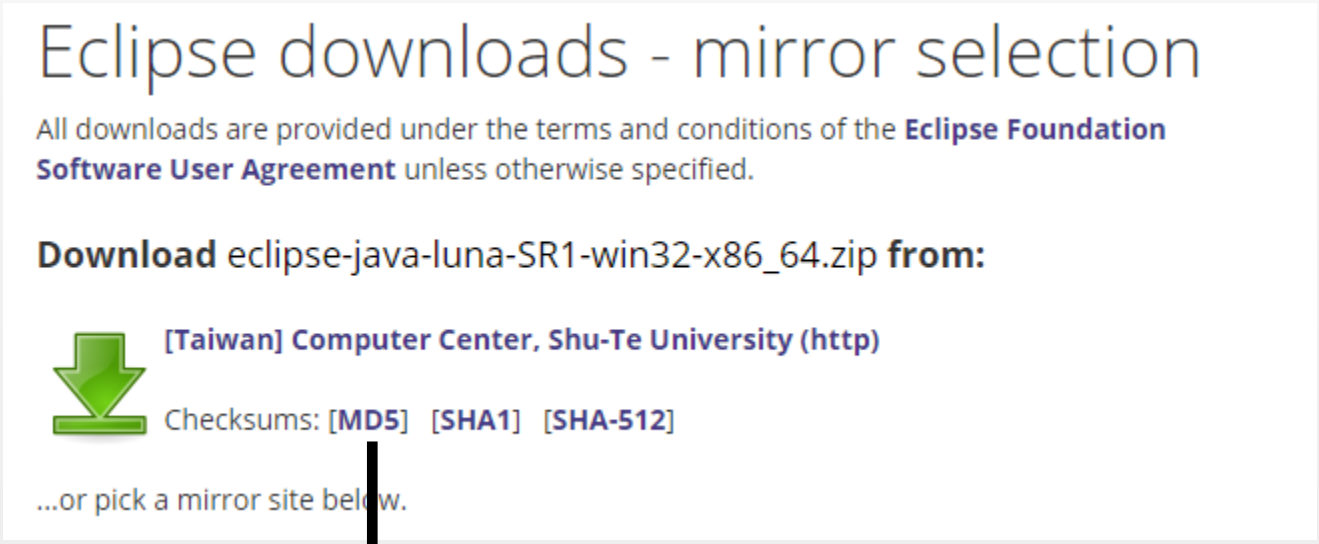
雜湊函數的應用

- 雜湊表〈資料結構〉
- 驗證資料的正確性
- 後台儲存使用者密碼

驗證資料的正確性



例子

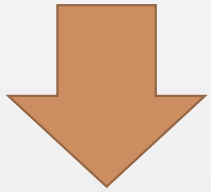



```
98e9c87b78cc0efb1dd45beb157e73f9  eclipse-java-luna-SR1-win32-x86_64.zip
```

* openssl dgst -md5 eclipse-java-luna-SR1-win32-x86_64.zip
*
https://www.eclipse.org/downloads/download.php?file=/technology/epp/downloads/release/luna/SR1/eclipse-java-luna-SR1-win32-x86_64.zip

後台儲存使用者密碼

~~Hash(password)~~



Hash(password + salt)*

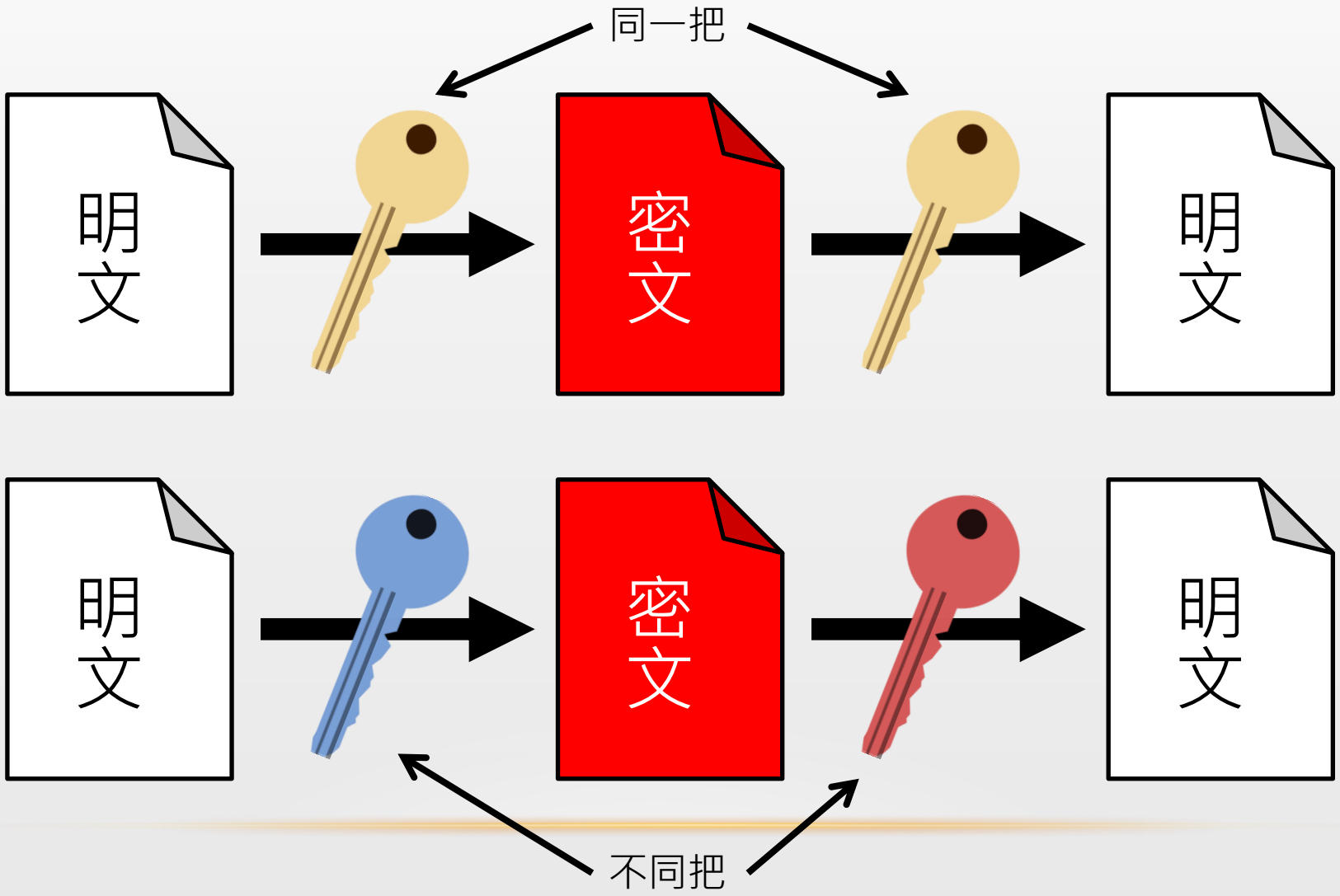
需具有唯一性

- 只能減緩攻擊者的速度，來爭取防禦的時間

我的密碼沒加密 http://plainpass.com/

* 也有其他方法

對稱與非對稱

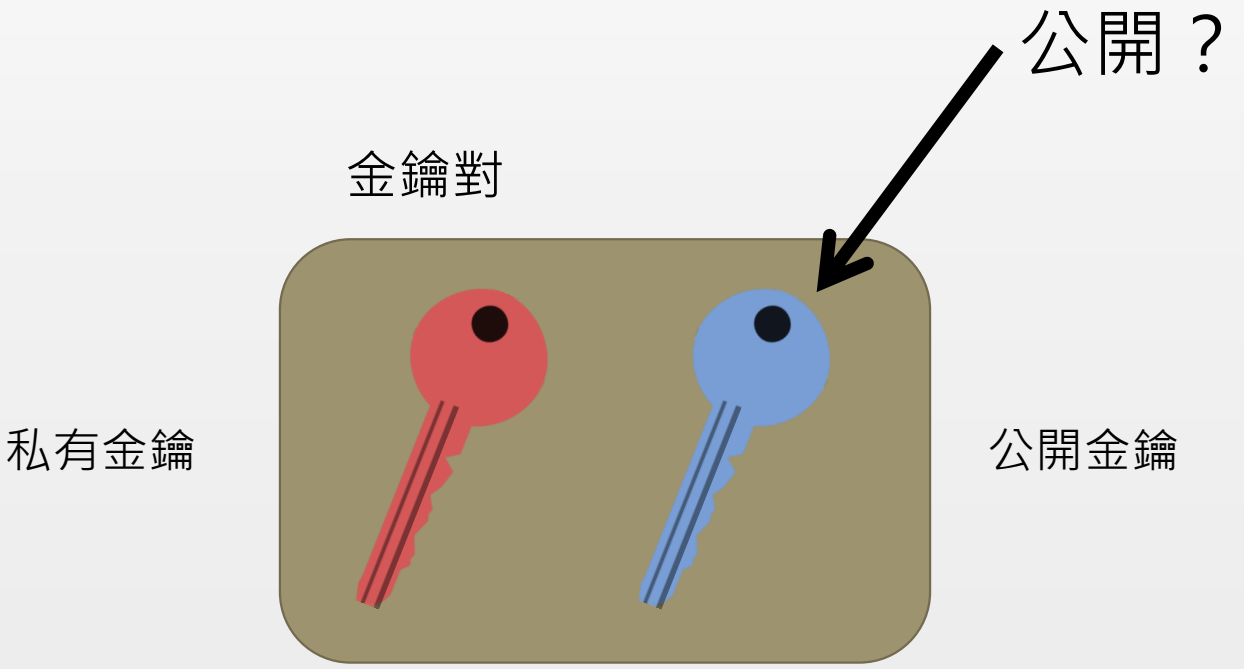


Key Image: http://pixabay.com/en/key-security-locked-lock-admin-150079/

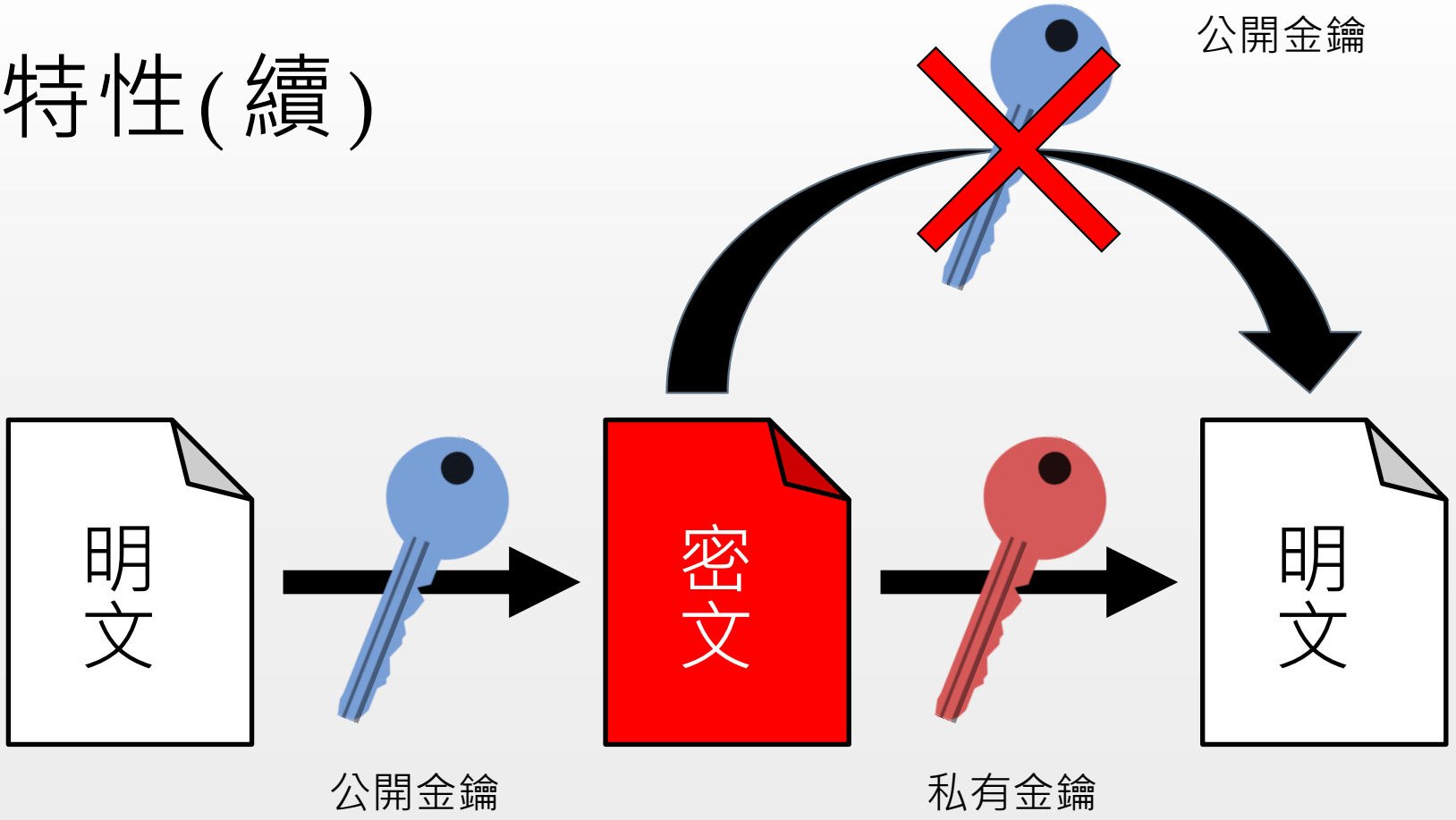
非對稱式加密

- 常見名稱為「公開金鑰加密」〈public-key cryptography〉
- 常見的有RSA、ElGamal、Elliptic curve cryptography

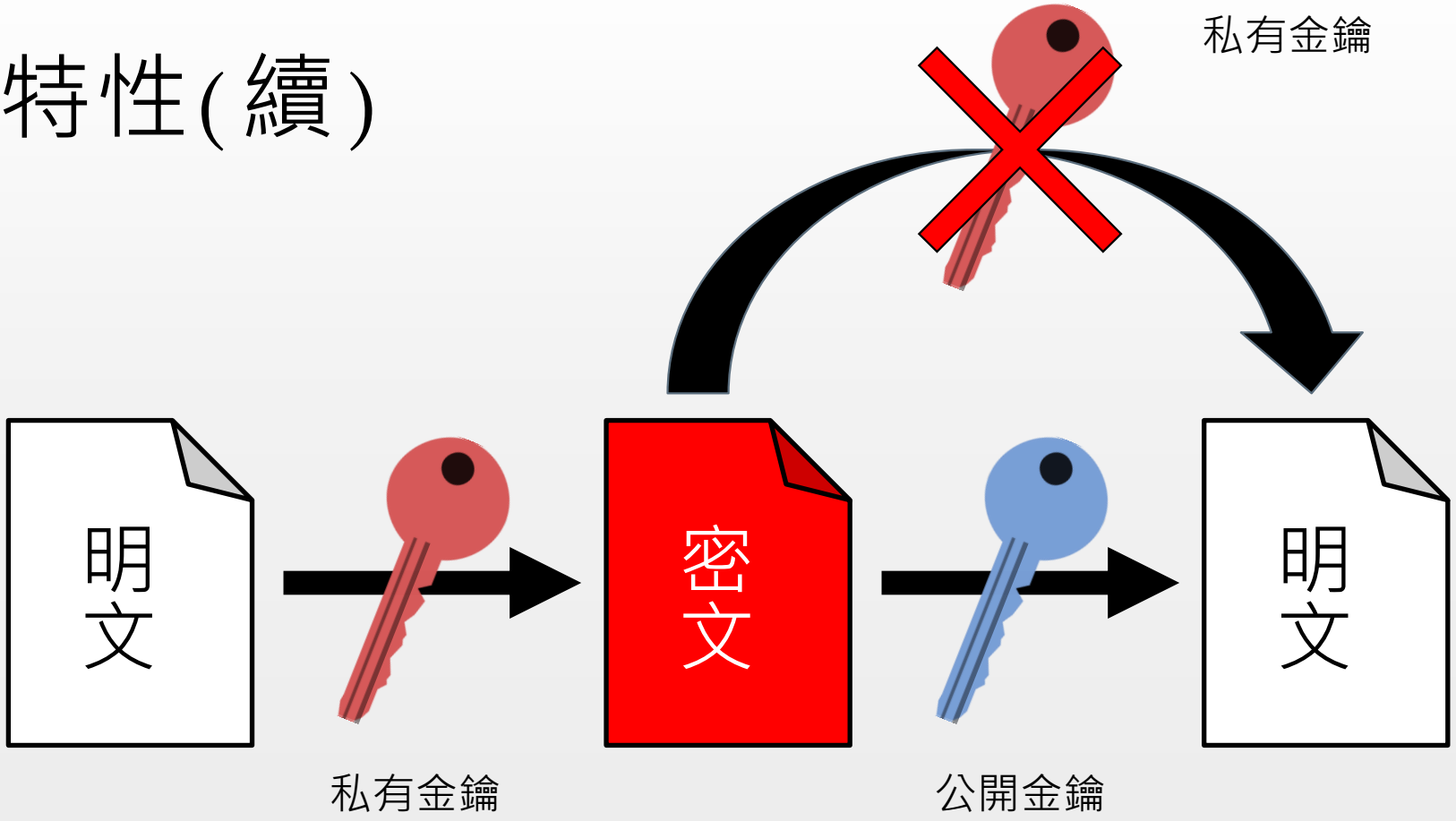
特性



特性(續)



特性(續)



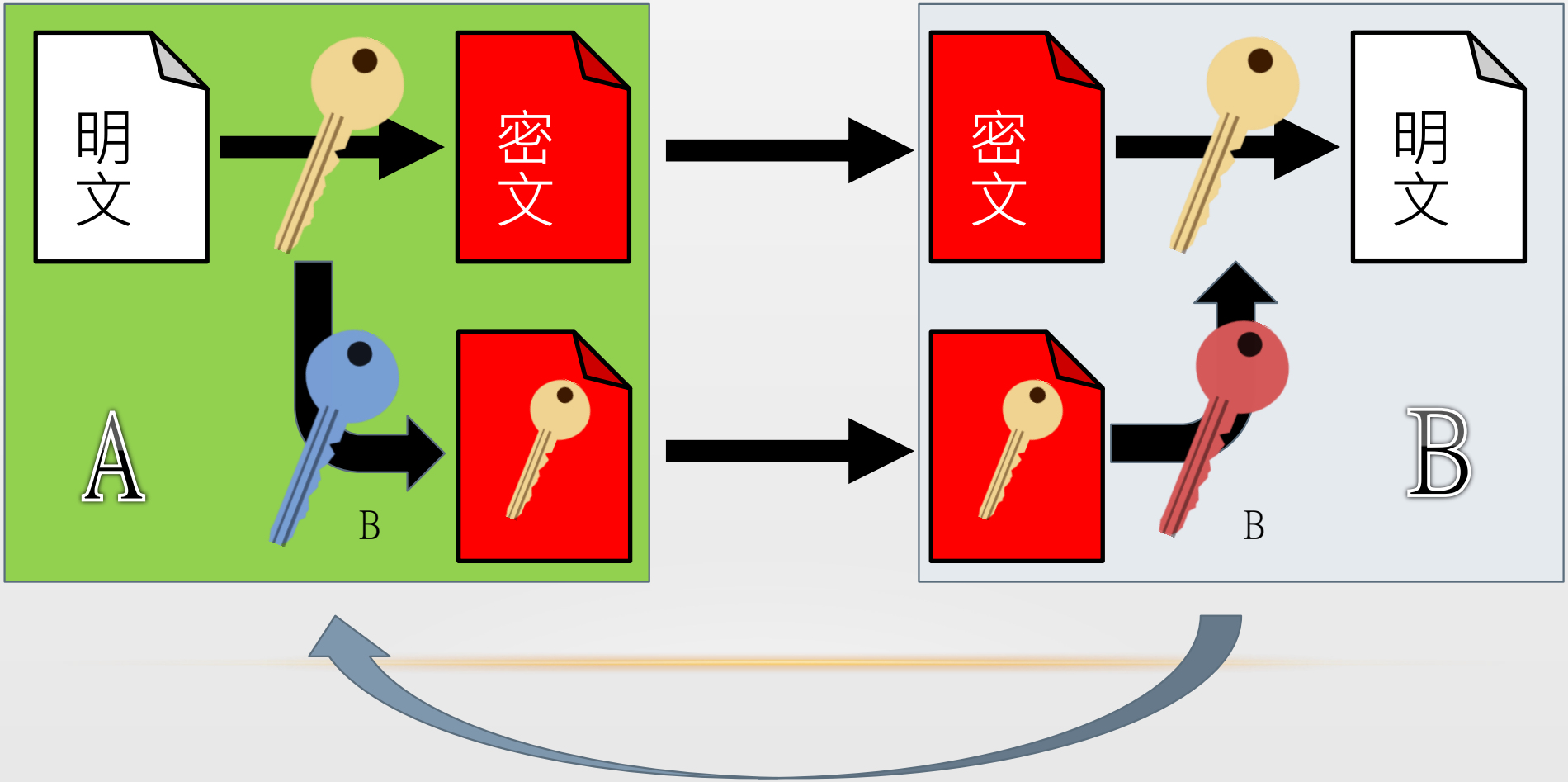
- 用途？　數位簽章

小總結

- 雜湊函數
  - 無法反推，對輸入資料很敏感
- 對稱加密法
  - 速度相對快，但鑰匙不好發送
- 非對稱加密法
  - 解決鑰匙發送問題，但速度較慢

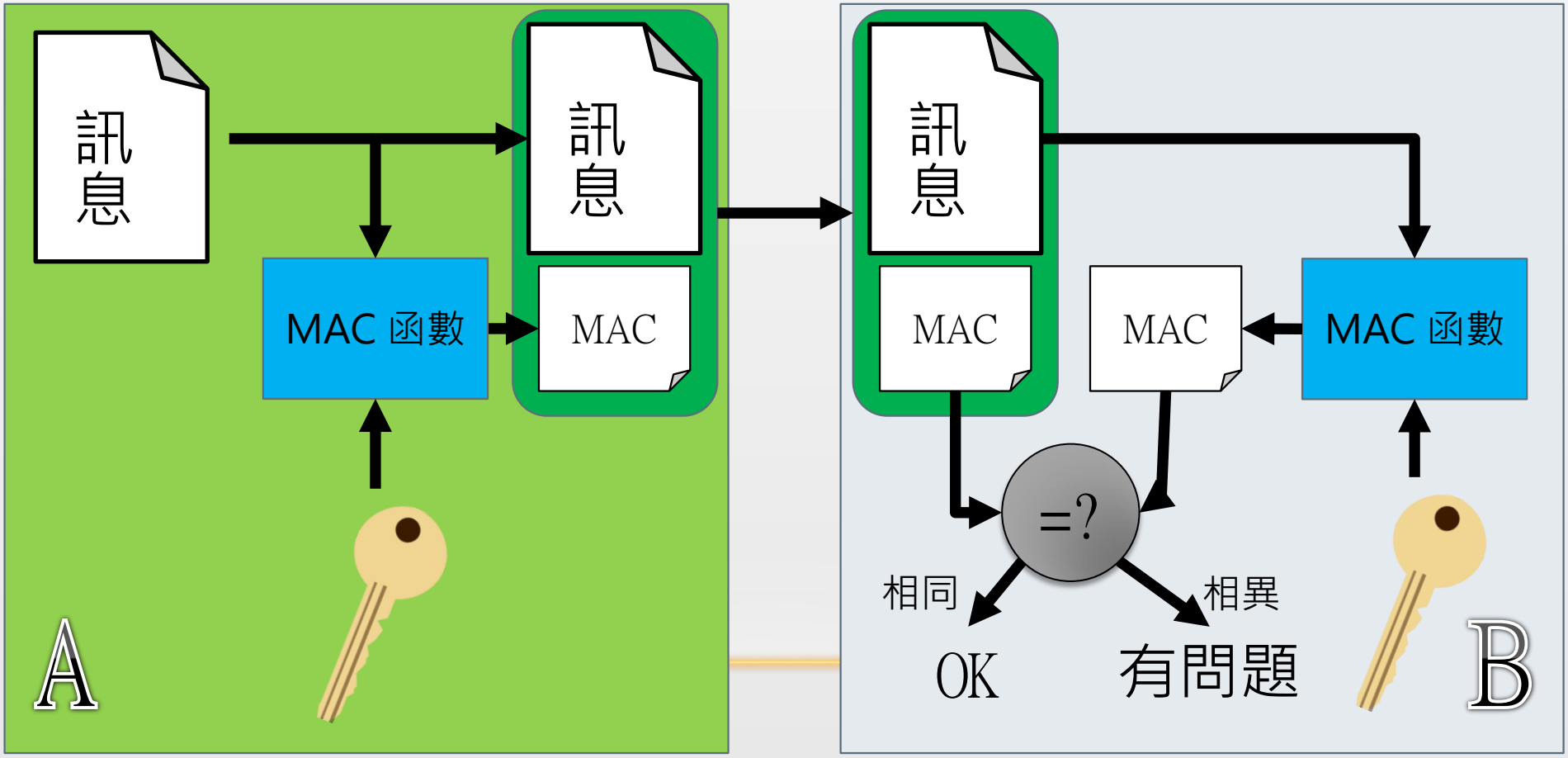
密碼學應用 – 混和加密

- 因為非對稱加密速度較慢……

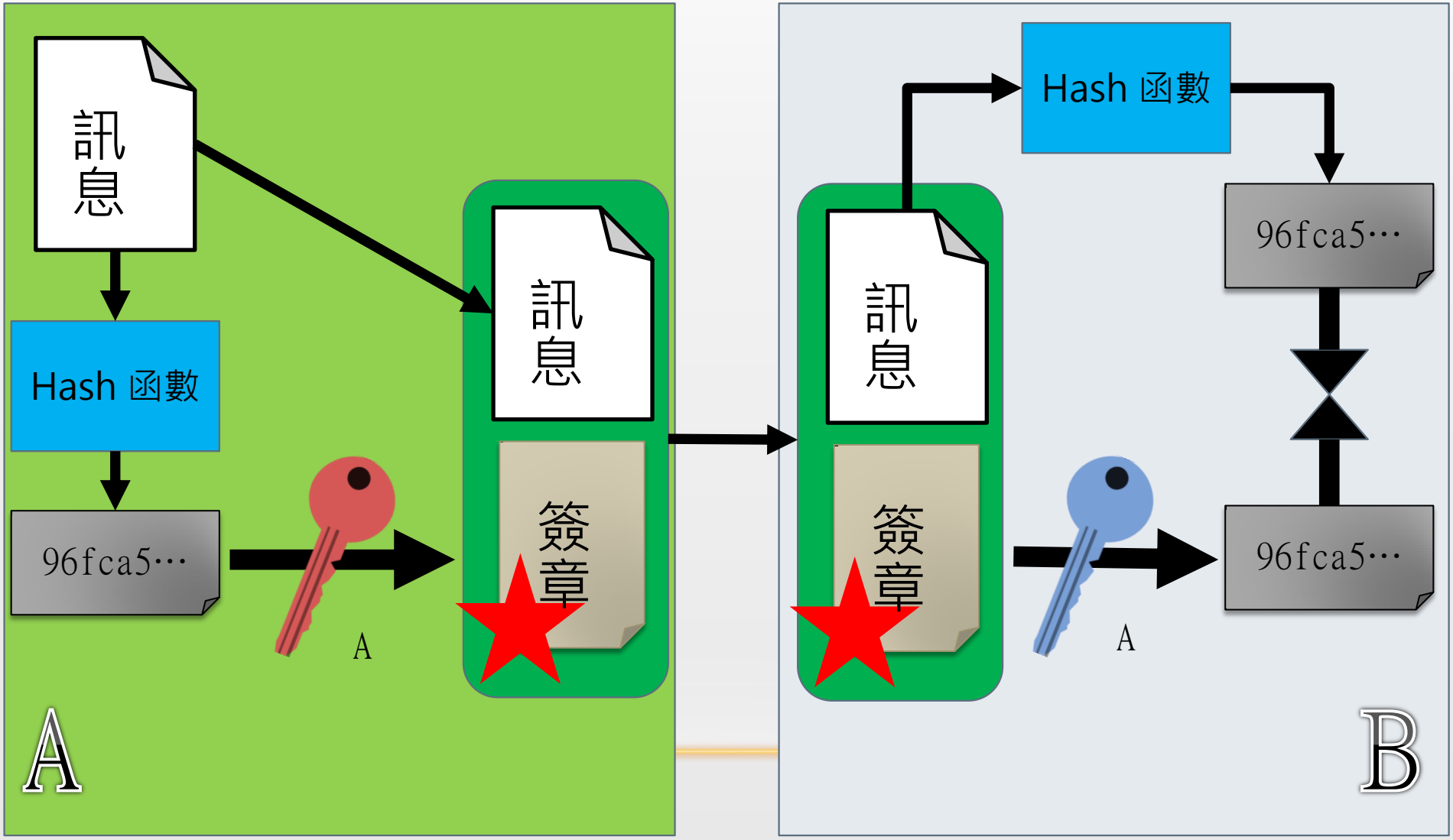


密碼學應用 – MAC

- Message Authentication Code (訊息認證碼)

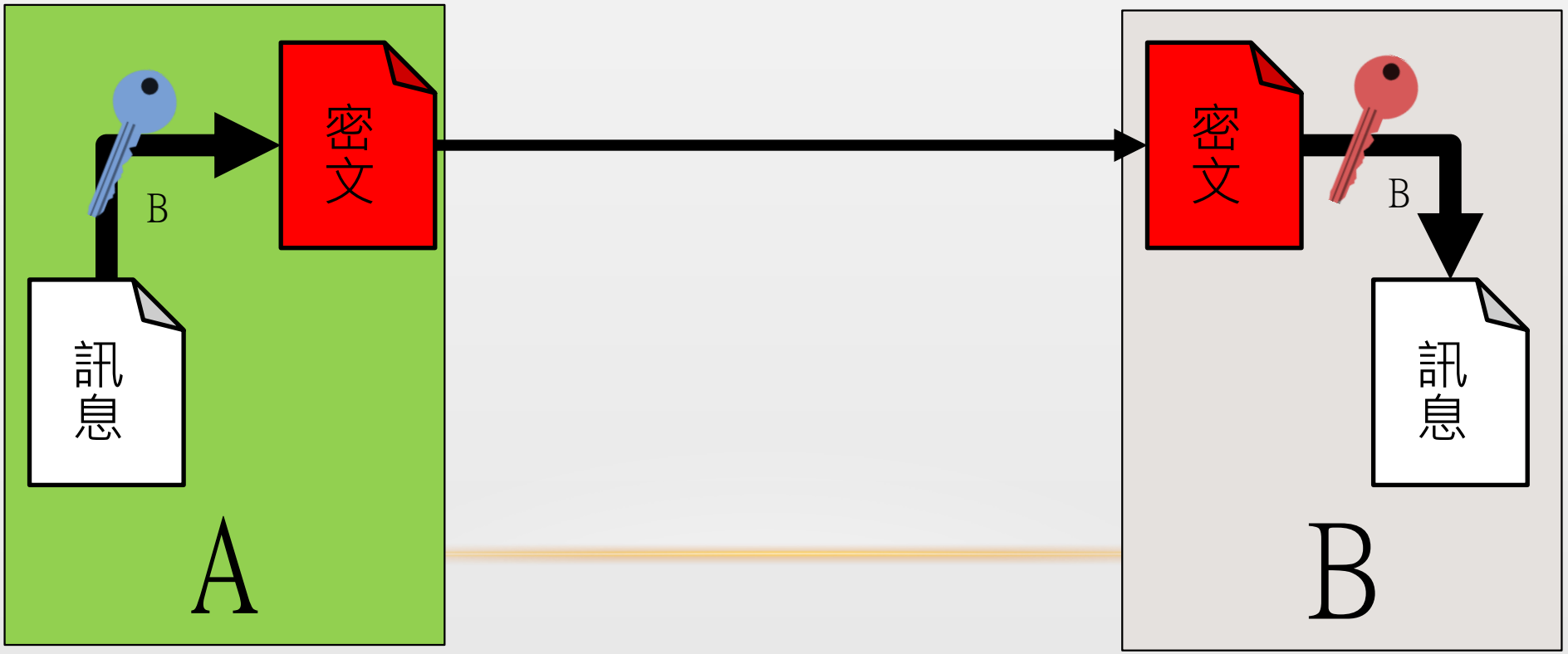


密碼學應用 – 數位簽章



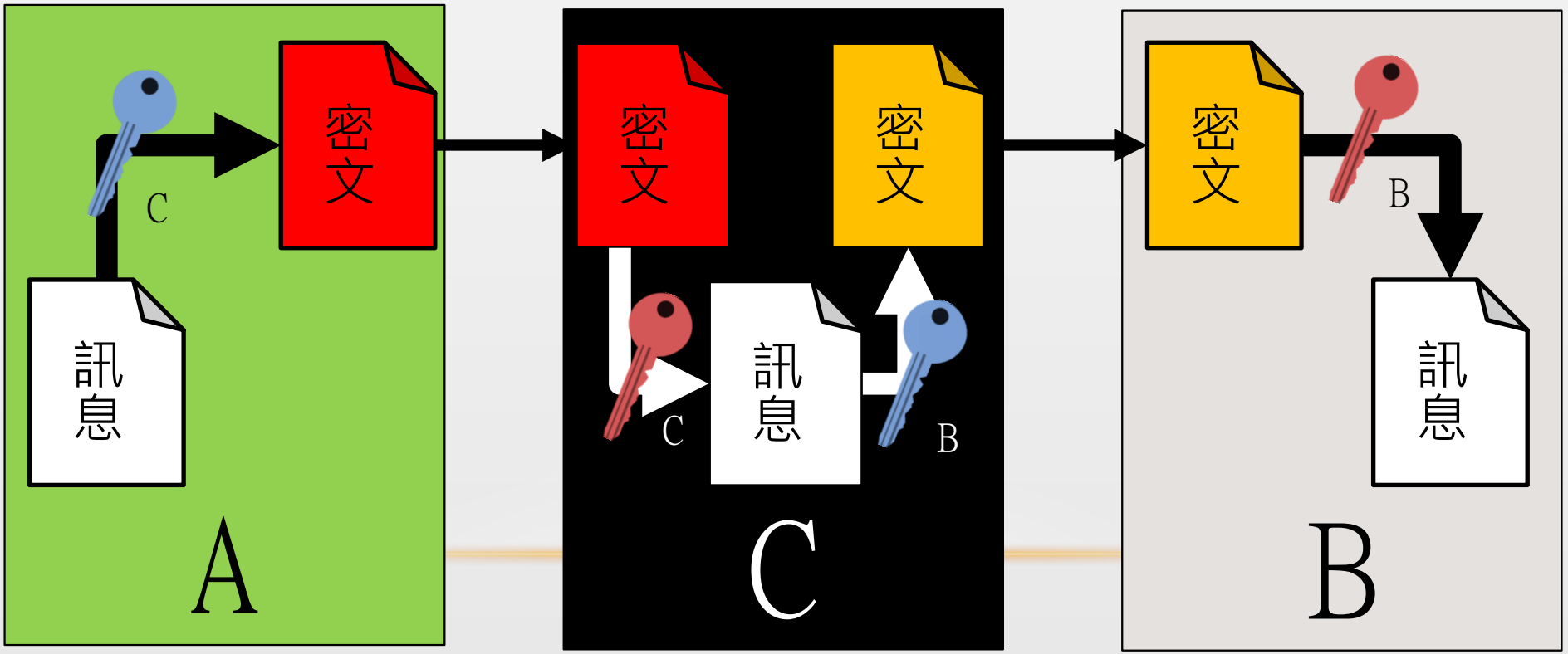
中間人攻擊(MAN-IN-THE-MIDDLE ATTACK)

- 正常情況



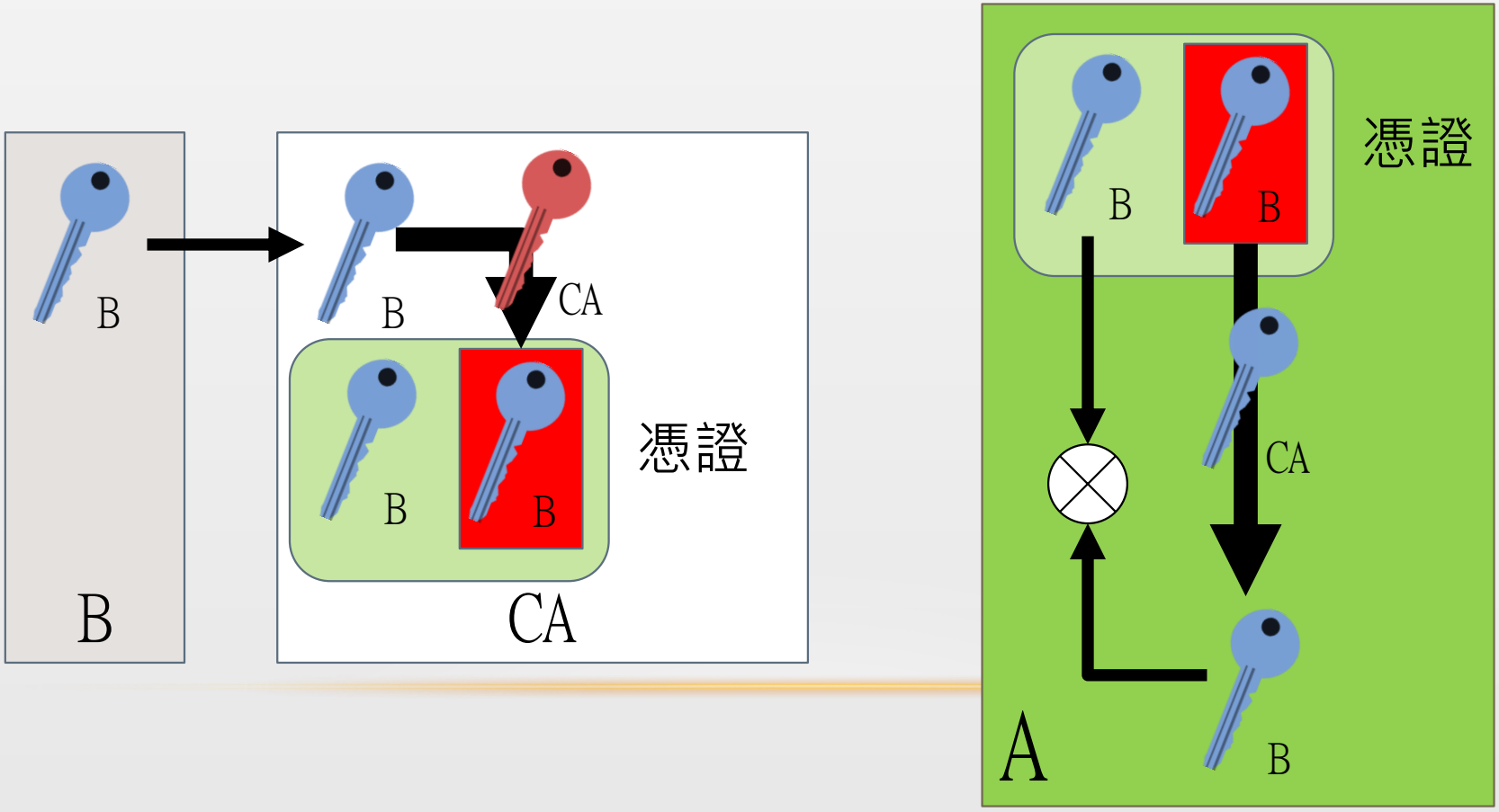
中間人攻擊(MAN-IN-THE-MIDDLE ATTACK)

- 有中間人存在



中間人攻擊 – 解決方案 – CA

憑證管理中心(Certification Authority，CA)



名詞

- 下列攻擊手法的差異：
  - 已知密文攻擊：擁有密文。
  - 已知明文攻擊*：擁有明文與密文的組合。
  - 選擇明文攻擊：能選擇明文加密。
  - 選擇密文攻擊：能選擇密文解密。
- 公開金鑰基礎建設〈Public Key Infrastructure, PKI〉

* Uva 850: Crypt Kicker II (http://uva.onlinejudge.org/external/8/850.html)

結語

- 盡量使用有被大量研究過的安全系統
- 密碼學不是唯一的解決方案[參考資料4]
- 密碼要有8個字元以上，英數字混合

延伸主題

- Random number generator
- 量子密碼學〈Quantum cryptography〉

參考資料

- 改變世界的九大演算法：讓今日電腦無所不能的最強概念 / 約翰．麥考米克〈John MacCormick〉著；陳正芬譯 / 2014.08 / ISBN：9789866031557
- 碼書：編碼與解碼的戰爭 / 賽門・辛〈Simon Singh〉著；劉燕芬譯 / 2000 / ISBN： 9570516720
- 世界第一簡單密碼學 / 三谷政昭、佐藤伸一合著；林羿妏譯 / 2009.05 / ISBN：9789577769817
- 密碼學實務 / Nieis Ferguson, Bruce Schneier 著；許建隆、楊松諺譯 / 2004 / ISBN：9864216171
- Google