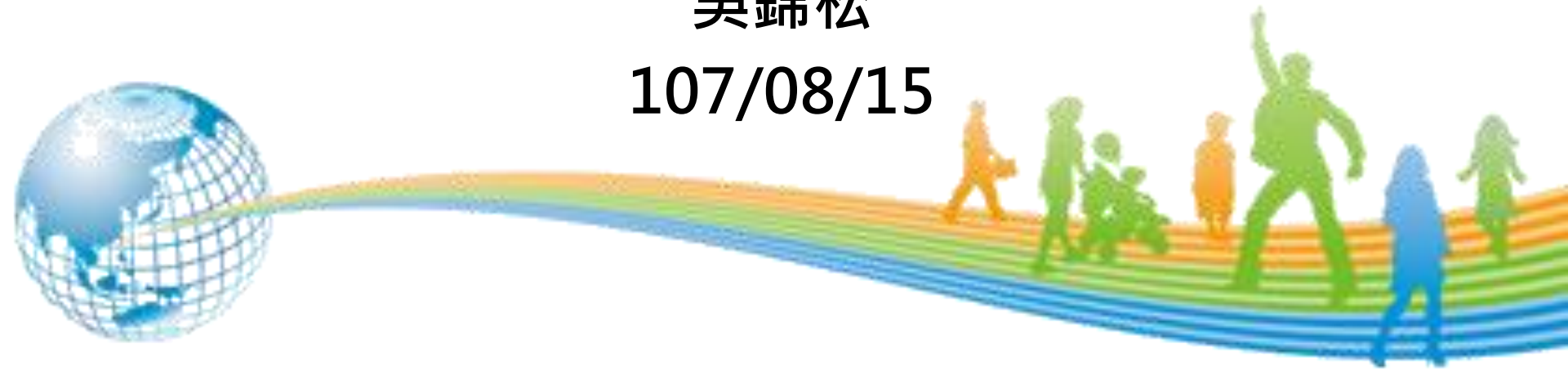
PKI基礎技術與應用

報告單位：資安所

吳錦松

107/08/15



Contents

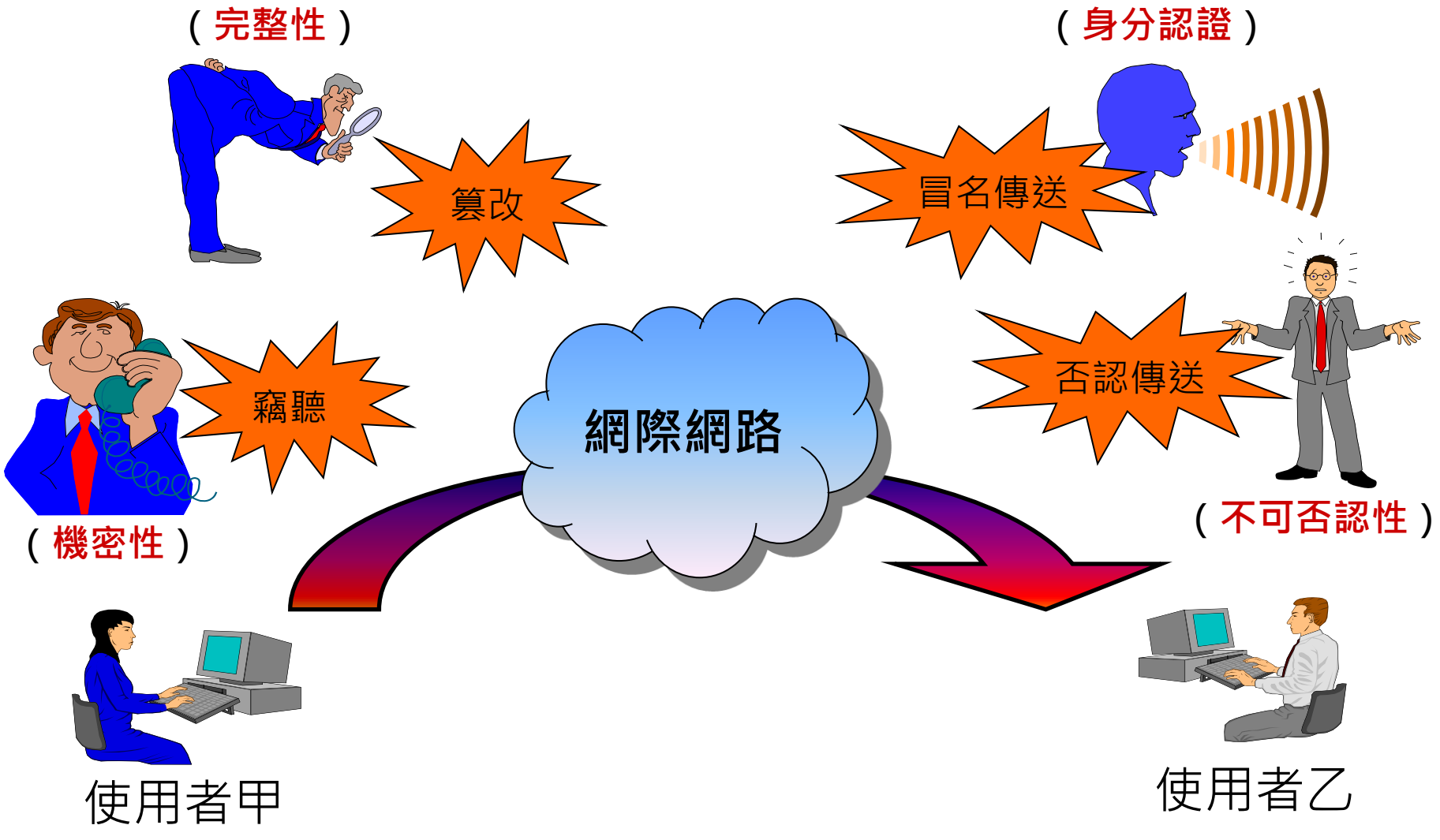
- **密碼學概論**
- 對稱式密碼系統
- 非對稱式密碼系統
- 雜湊函數
- 公開金鑰基礎建設架構(PKI)

在網際網路上，沒人知道你是一隻狗

"On the Internet, nobody knows you're a dog."

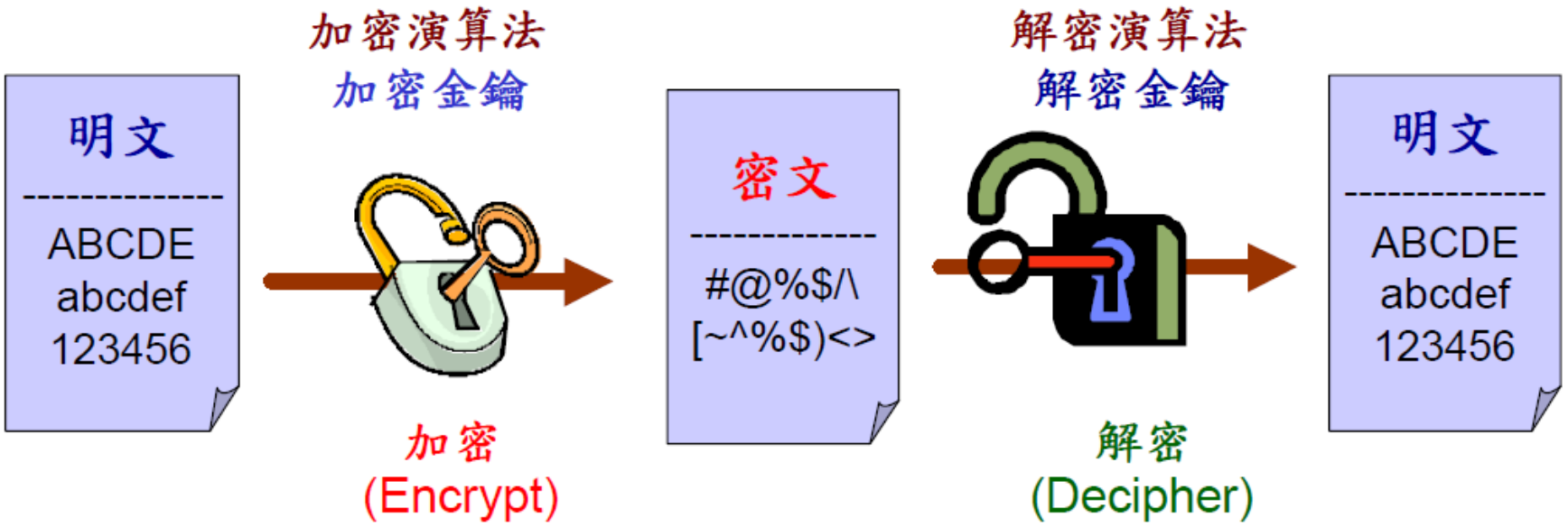
- 1993年7月5日《紐約客》刊登的一則漫畫，此漫畫是由 Peter Steiner 所創作。漫畫的標題是：「On the Internet, nobody knows you're a dog.」
- 這則漫畫體現了一種對網際網路的理解，強調用戶能夠以一種不透露個人信息的方式，來發送或接受信息的能力。

資訊及通訊安全的問題



何謂密碼學

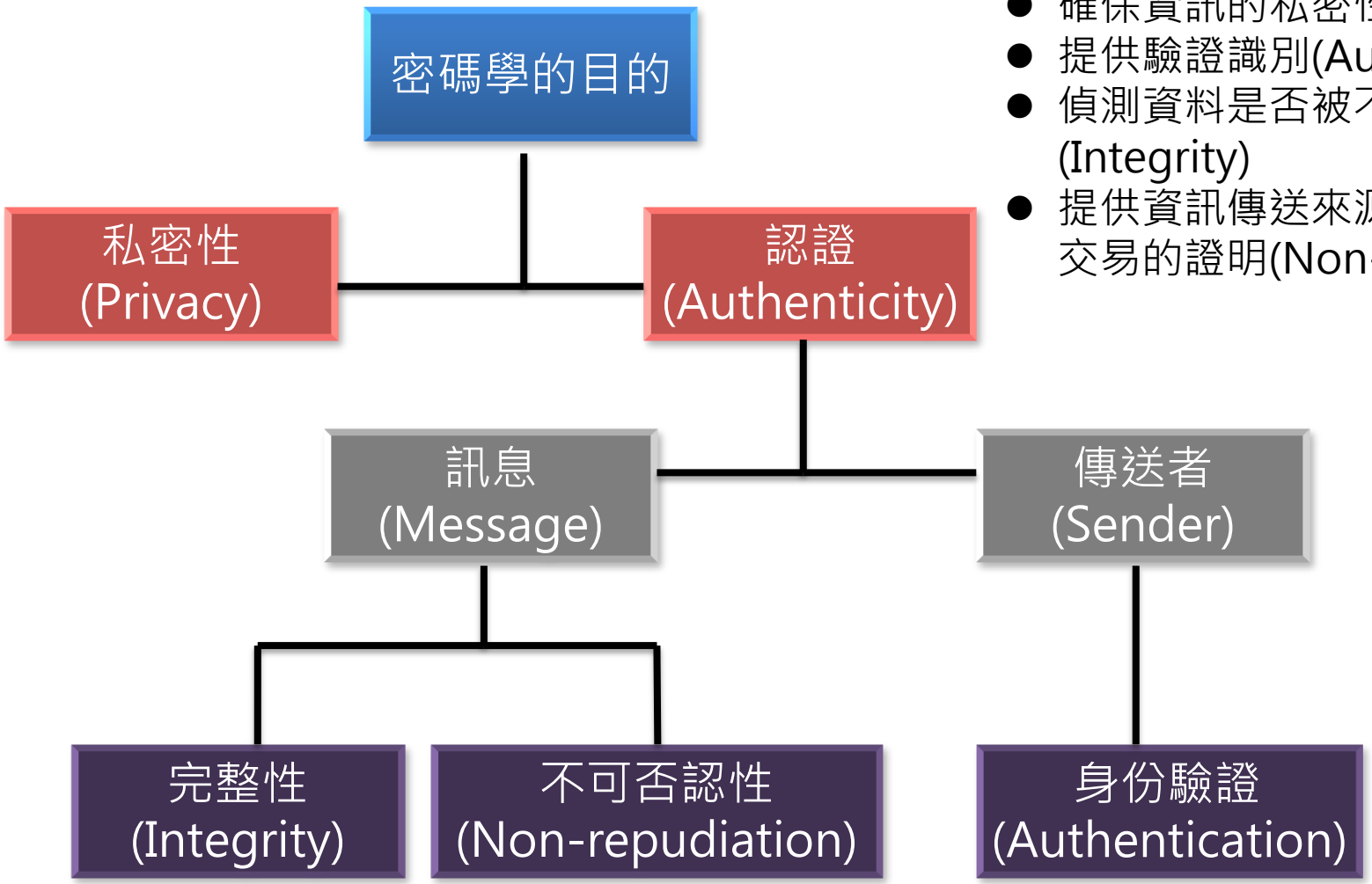
- 由希臘文“kryptos” (隱藏) 和“graphein” (寫字)組成，代表"隱藏的字" 。
- 密碼學為一種利用數學方法來對資料加密和解密的科學。



密碼學基本名詞

- 明文(Plaintext)
  - ✓ 加密前的原始資料，為加密演算法的輸入，解密演算法的輸出。
- 密文(Ciphertext)
  - ✓ 加密之後的資料，為加密演算法的輸出，解密演算法的輸入。
- 加密演演算法(Encryption Algorithm)
  - ✓ 利用金鑰對明文進行加密的編碼動作的演算法。
- 解密演算法(Decryption Algorithm)
  - ✓ 利用金鑰對密文進行解密的解碼動作的演算法。

密碼學的目的



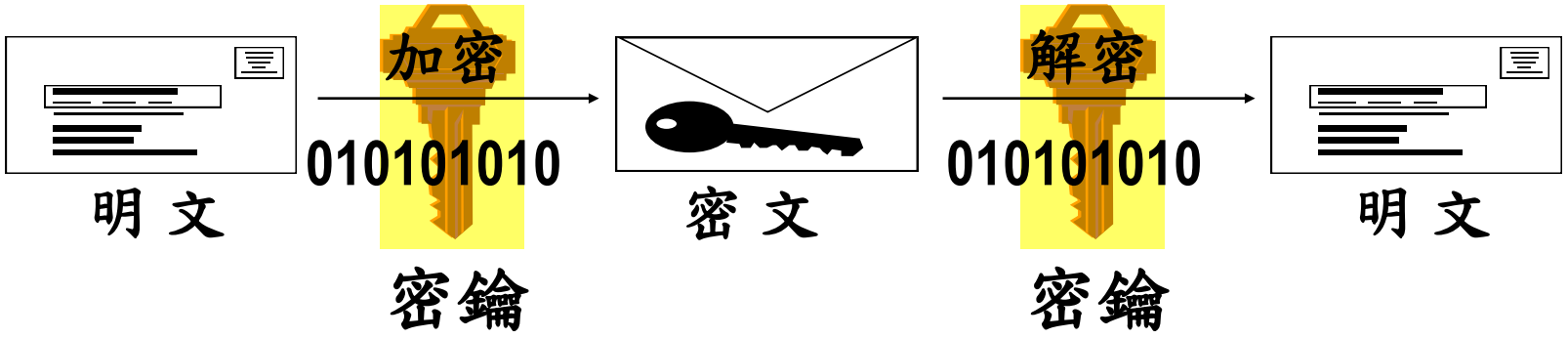
- 確保資訊的私密性(Privacy)
- 提供驗證識別(Authentication)
- 偵測資料是否被不當的竄改(Integrity)
- 提供資訊傳送來源、接收目的或交易的證明(Non-repudiation)

Contents

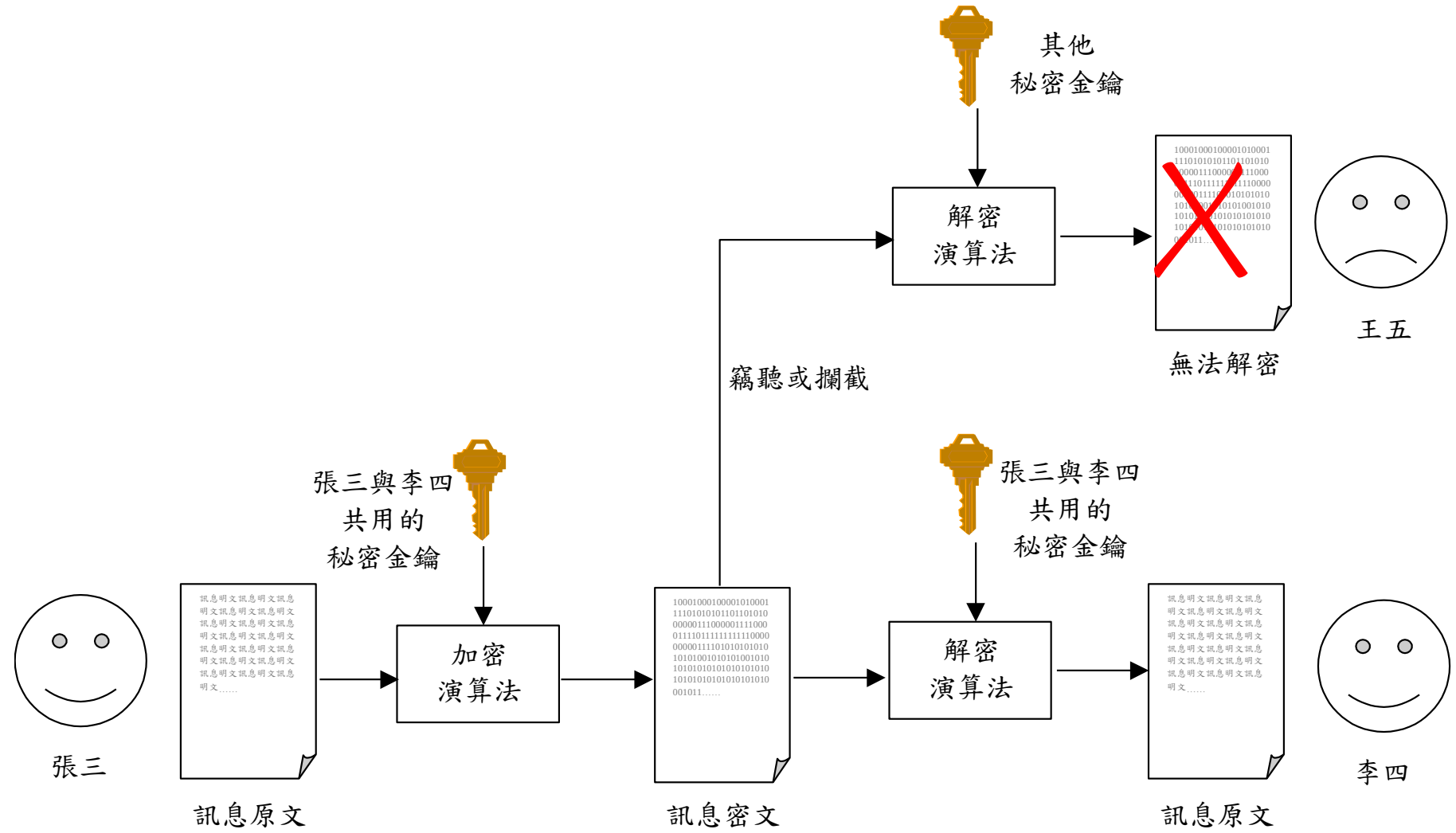
- 密碼學概論
- **對稱式密碼系統**
- 非對稱式密碼系統
- 雜湊函數
- 公開金鑰基礎建設架構(PKI)

對稱式密碼系統

- 加密與解密使用同一把金鑰
- 我們稱這把金鑰為密鑰(Secret Key)

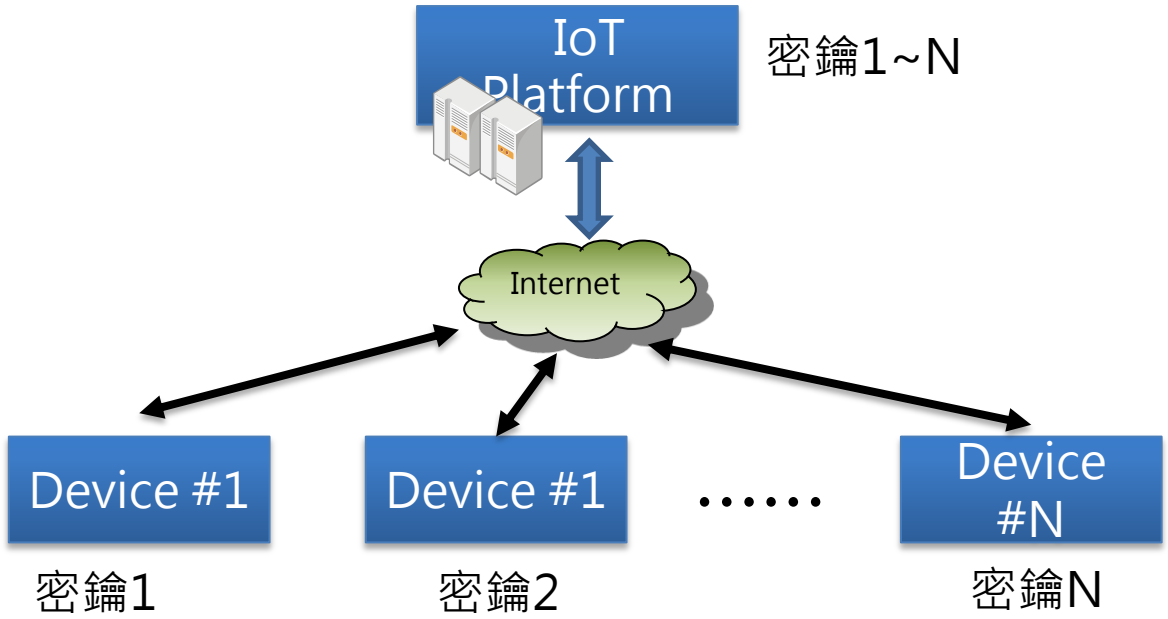


對稱式密碼系統


其他
秘密金鑰
解密
演算法
王五
無法解密
竊聽或攔截
張三與李四
共用的
秘密金鑰
張三與李四
共用的
秘密金鑰
加密
演算法
解密
演算法
張三
李四
訊息原文
訊息密文
訊息原文

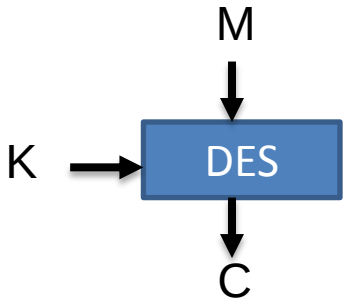
對稱式密碼系統

- 在網際網路上建立安全通道是一大問題，且每一把密鑰必須由共用該把密鑰的通訊雙方同時秘密保存而不可外洩
- 當一方可能與多方通訊時，則他必須與各方先協商產生各自的密鑰，再安全送達多方設備

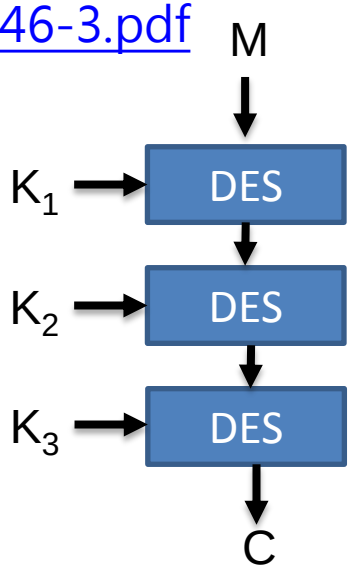


對稱式密碼系統

- **常見的對稱式密碼系統演算法有：**
  - ✓ DES (Data Encryption Standard)
    - 明文64位元，密文64位元，金鑰56位元。
    - 安全性(金鑰的組合)=2^{56}。
    - http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf



  - ✓ 三重DES (Triple-DES)
    - DES重複執行3次。
    - 第一把金鑰＝第三把金鑰相同≠第二把金鑰不同。
      - 安全性(金鑰的組合)=2^{112}。
    - 第一把金鑰≠第二把金鑰相同≠第三把金鑰不同。
      - 安全性(金鑰的組合)=2^{168}。



  - ✓ AES (Advanced Encryption Standard)
    - 目前全世界使用最廣泛的密碼系統。
    - 明文128位元，密文128位元，金鑰有128、192、256位元。
    - 安全性(金鑰的組合)=2^{128}、2^{192}、2^{256}。
    - http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

對稱式密碼系統

- 對稱加密演算法比較

	DES	3DES	AES
資料區塊	64bits	64bits	128bits
金鑰長度	56bits	112bits 168bits	128bits 192bits 256bits
重複運算次數	16次	48次	10次 12次 14次 (隨金鑰長度而異)

對稱式密碼系統

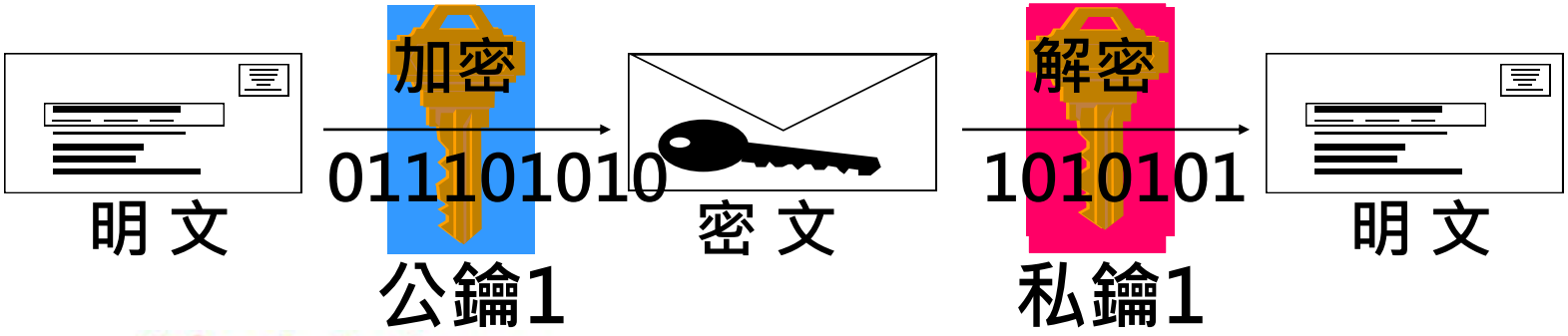
- 區塊加密演算法，有五種操作模式用來提供保密性，包括：
  - ✓電子密碼本(Electronic CodeBook，ECB) 模式。
  - ✓計數器(CounTeR，CTR)模式。
  - ✓密文區塊鏈結(Cipher Block Chaining，CBC) 模式。
  - ✓密文反饋(Cipher FeedBack，CFB)模式。
  - ✓輸出反饋(Output FeedBack，OFB) 模式。
- 參考文件：
  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

Contents

- 密碼學概論
- 對稱式密碼系統
- **非對稱式密碼系統**
- 雜湊函數
- 公開金鑰基礎建設架構(PKI)

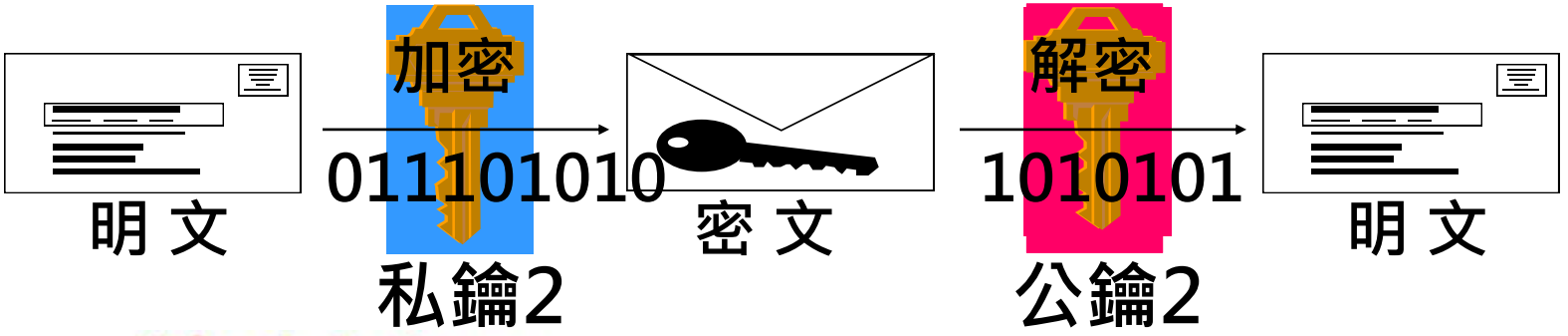
非對稱式密碼系統

- 加密與解密使用不同的金鑰。
- 我們稱這2把金鑰為公開金鑰(Public Key)與私密金鑰(Private Key) 。
- 每一對公鑰與私鑰皆是唯一成對的(key pairs)，任何兩個金鑰對，都不會共用同一把公鑰或私鑰
- 利用某一把公鑰編碼過的資料，唯有利用其相對應的私鑰才能解碼。



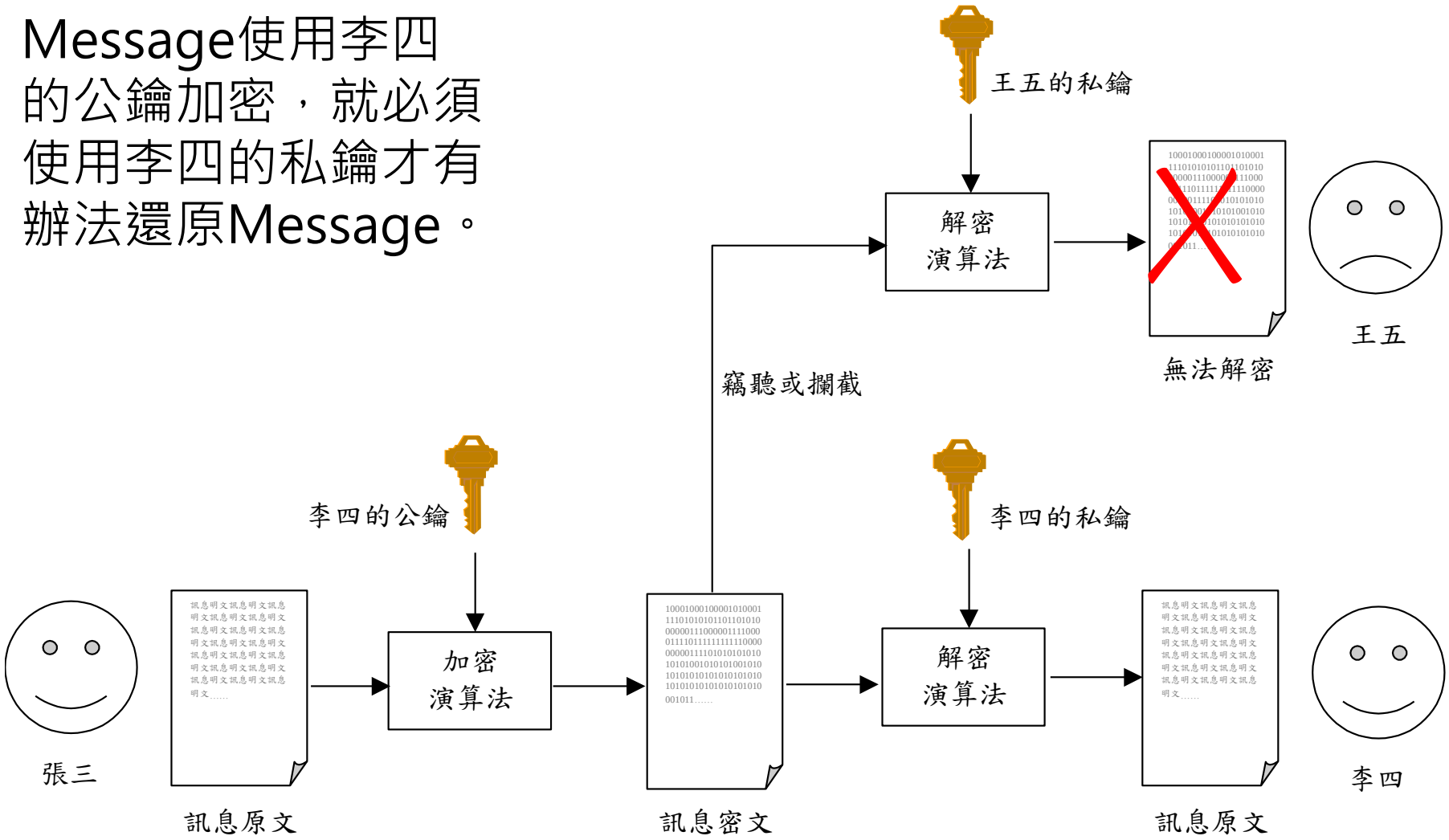
非對稱式密碼系統

- 利用某一把私鑰編碼過的資料，唯有利用其相對應的公鑰才能解碼。
- 公鑰與私鑰雖然具有數學上的對應關係，但其產生方法是不可逆的，即無法由公鑰推算得到其相對應的私鑰。



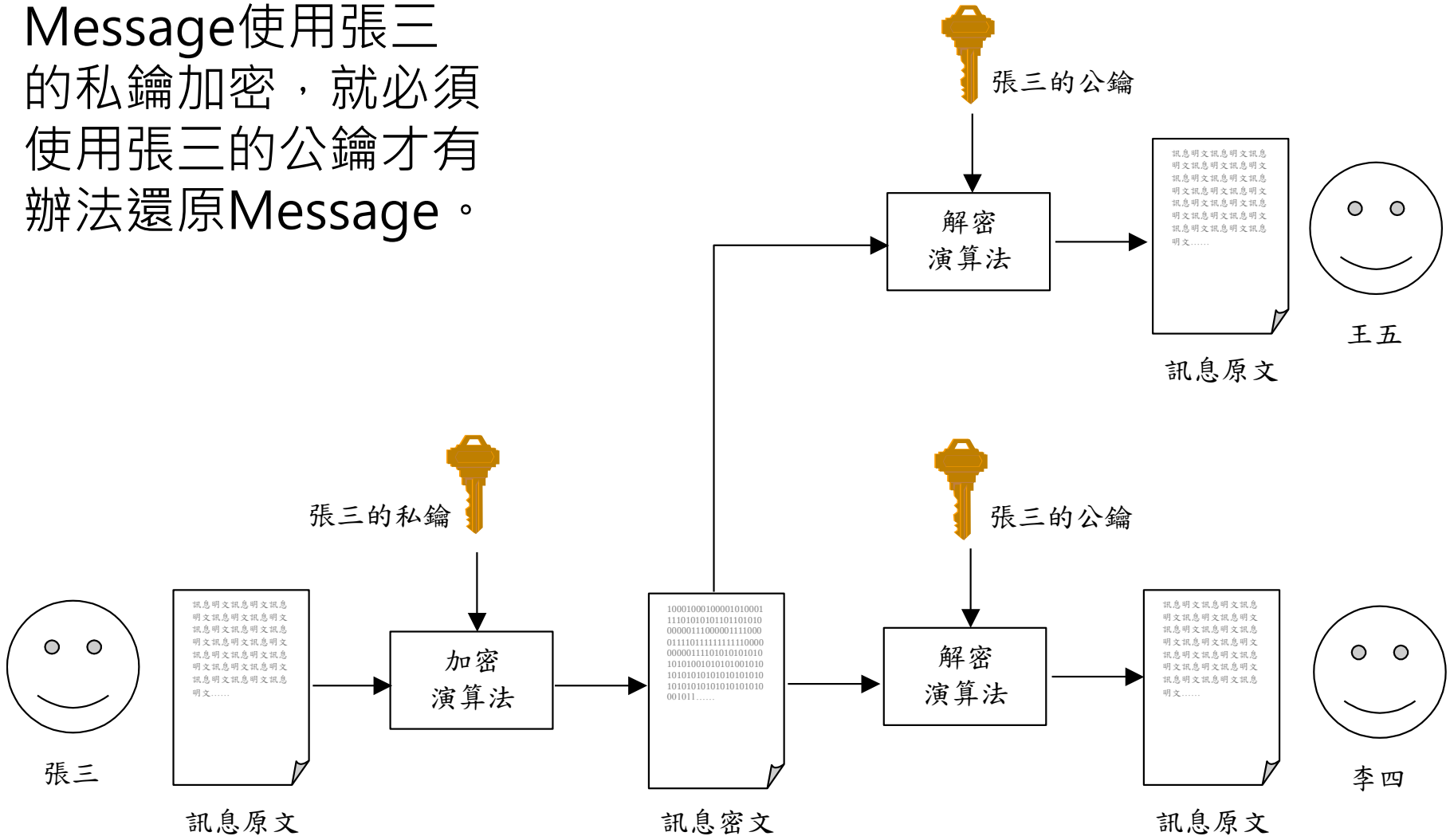
非對稱式密碼系統

Message使用李四的公鑰加密，就必須使用李四的私鑰才有辦法還原Message。



非對稱式密碼系統

Message使用張三的私鑰加密，就必須使用張三的公鑰才有辦法還原Message。



非對稱式密碼系統

- 常見的公開金鑰密碼系統演算法有：
  - ✓ RSA密碼系統
  - ✓ 橢圓曲線(ECC)密碼系統
- RSA密碼系統
  - ✓ 公開金鑰是兩個正整數(E、N)，私密金鑰則是一個數字(D)。N=P*Q，P與Q是大質數。
  - ✓ $D=E^{-1} \bmod ((P-1)*(Q-1))$
  - ✓ 加密公式 $C = M^E \bmod N$，M is Message。
  - ✓ 解密公式 $M = C^D \bmod N$，C is Cipher。
  - ✓ https://www.emc.com/collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-standard-wp.pdf

非對稱式密碼系統

橢圓曲線(ECC)密碼系統

- ✓公開金鑰：雙方同意之系統橢圓曲線參數、基準點G、基準點G 的階數(N)、公鑰Q(Q=d·G)。
- ✓私密金鑰：使用者的私密金鑰為d，1<d<N。
- ✓加密公式
  - $C_1 = M + r \cdot Q$。
  - $C_2 = r \cdot G$。
- ✓解密公式
  - $M = C_1 - d \cdot C_2$
- ✓http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

- r是隨機取的自然數，0<r<n。
- M is message
- C_1&C_2 is Cipher

非對稱式密碼系統

- 相同安全性時，RSA與ECC金鑰長度比較

安全性 / 演算法	2^{80} (2TDEA)	2^{112} (3TDEA)	2^{128} (AES128)	2^{192} (AES192)	2^{256} (AES256)
RSA長度 (位元)	1024	2048	3072	7680	15360
ECC長度 (位元)	160-223	224-255	256-383	384-511	512以上
RSA:ECC 金鑰長度比	6:1	9:1	12:1	20:1	30:1

密碼系統的優點與缺點

- **對稱式密碼系統**
  - ✓ **優點**
    - 較快速。
    - 如果使用足夠大的金鑰，將難以破解。
  - ✓ **缺點:**
    - 需要有一個安全性機制將金鑰安全性的分送至交易的雙方。
    - 提供私密性(Confidential)的安全性能力，無法提供不可否認的能力。
- **非對稱式密碼系統**
  - ✓ **優點**
    - 公開鑰匙可以公開分送
    - 提供私密性、驗證與不可否認性等服務
  - ✓ **缺點**
    - 效率較差

對稱式加密法vs.非對稱式加密法

- 非對稱性加密技術並非要用來取代對稱性加密技術，而是用來彌補其不足，並加強安全性。
- 二者各有優劣，實務上經常合併使用。

	對稱式加密法	非對稱式加密法
其它名稱	秘密金鑰加密法	公開金鑰加密法
加解密的key是否相同	相同	不同
key可否公開	不可公開	公開鑰匙可以公開 私有鑰匙不可公開
key保管問題	如果與N個人交換訊息,需保管好N把加解密鑰匙。	無論與多少人交換訊息，只需保管自己的私密鑰匙。
加解密速度	快	慢
應用	常用於加密長度較長的資料，例如：e-mail	常用於加密長度較短的資料、數位簽章。

Contents

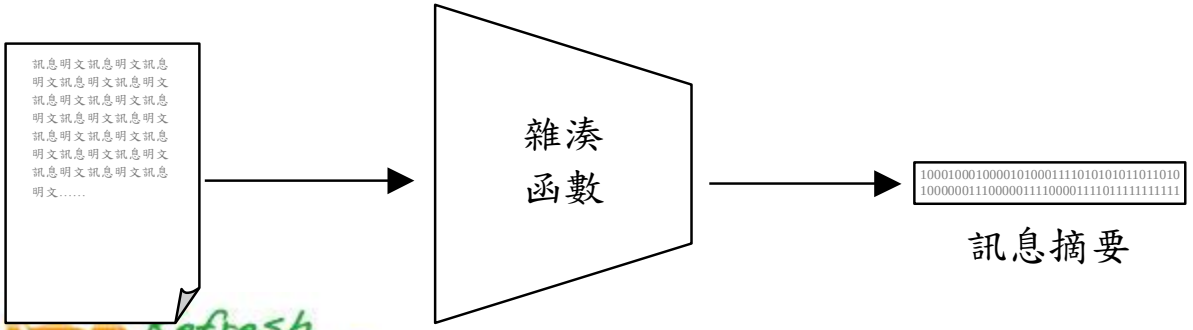
- 密碼學概論
- 對稱式密碼系統
- 非對稱式密碼系統
- **雜湊函數**
- 公開金鑰基礎建設架構(PKI)

雜湊函數

- 雜湊函數將任何長度的訊息輸入後加以濃縮，轉換而成為一個長度較短且固定的輸出，此輸出訊息為雜湊值(Hash Value)或訊息摘要(Message Digest)。
- 應用：
  - ✓確保資料傳送的完整性
  - ✓數位簽署
  - ✓密碼儲存
  - ✓訊息確認

雜湊函數

- 輸入任意大小的訊息，輸出固定大小的訊息摘要(Message Digest)
- 單向函數(one-way function)
  - ✓無法由訊息摘要再回覆到原文
- 抗碰撞(collision resistance)
  - ✓不同的原文不可以得出相同的訊息摘要
- 計算速度快
- 著名的雜湊函數有MD5、SHA-1、SHA-2。



雜湊函數

- 常見單向雜湊函數的比較

	MD5	SHA-1	SHA-256	SHA-384	SHA-512
摘要長度(位元組)	16	20	32	48	64
安全性	不安全	有疑慮	2^{128}	2^{192}	2^{256}
最大訊息長度(位元)	$2^{64}-1$	$2^{64}-1$	$2^{64}-1$	$2^{128}-1$	$2^{128}-1$
標準公佈年份	1992	1995	2002	2002	2002

雜湊函數

- 金鑰雜湊訊息確認碼(HMAC)
  - ✓HMAC是一種利用單向雜湊函數提供私密金鑰訊息防偽。
  - ✓訊息發送者與訊息接收者有共同訊息防偽用秘密金鑰，而希望能偵測訊息在傳送過程是否被竄改。
  - ✓設計的概念是發送者先將私密金鑰與訊息透過某種計算過程算出所謂的訊息認證碼(message authentication code， MAC)後附加在訊息中。
  - ✓訊息與訊息認證碼將傳送給接收者，而兩者皆可能在傳送過程中被竄改，然而接收者可以重新計算訊息認證碼及與收到訊息認證碼做比較，符合時才接受，不符合時則代表 至少訊息或認證碼之一被竄改。
  - ✓http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf

Contents

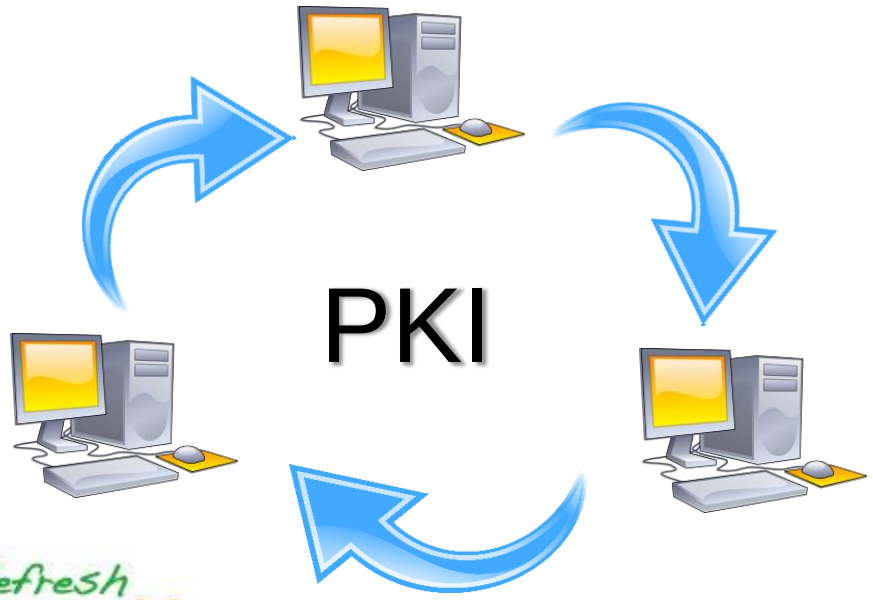
- 密碼學概論
- 對稱式密碼系統
- 非對稱式密碼系統
- 雜湊函數
- **公開金鑰基礎建設架構(PKI)**

何謂 PKI

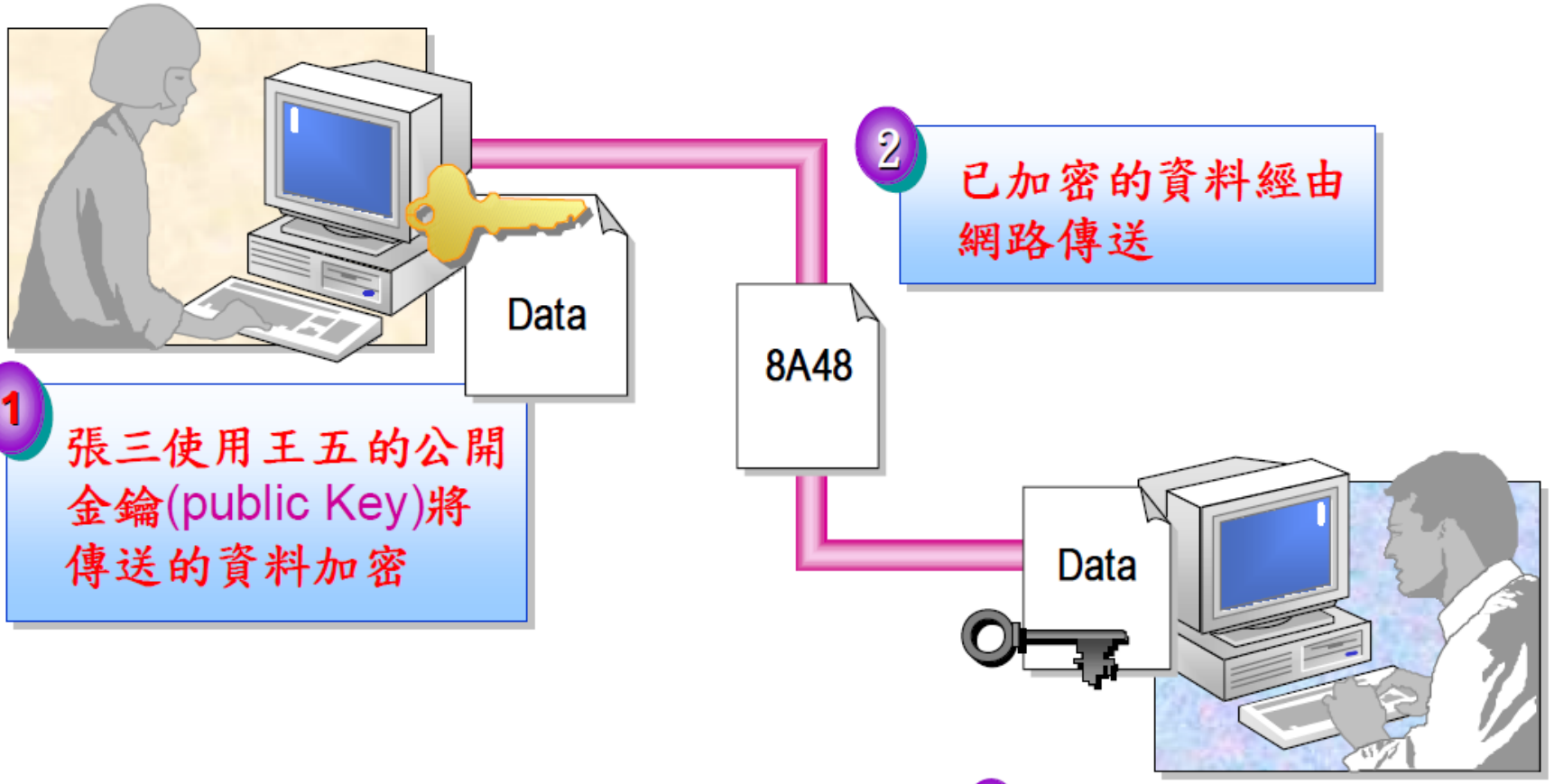
- PKI是一種非對稱性密碼學、軟體和網路服務的整合技術，主要是用來提升保障網路通訊和電子交易的安全性。
- PKI 也是一種支援數位憑證和公開金鑰各項標準或協定的安全性整合服務與架構。

為何需要使用PKI

- PKI 提供了分送公開金鑰的實務技術
- 資訊環境下需要更多層面和更高安全性的交易機制。
  - ✓需要比傳統密碼系統更嚴謹的驗證機制
  - ✓需要提供不可否認機制



公開金鑰加密原理

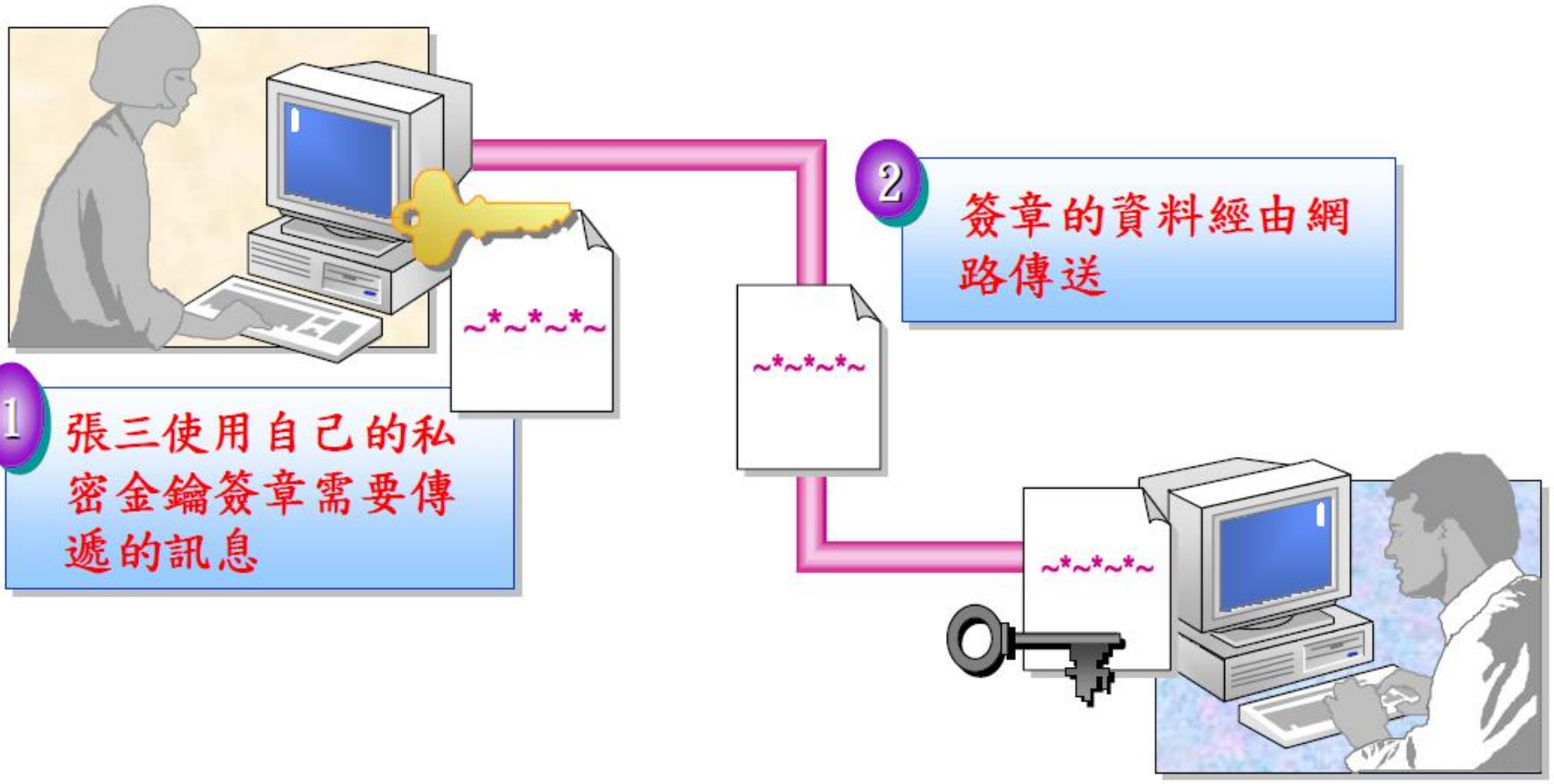


1 張三使用王五的公開金鑰(public Key)將傳送的資料加密

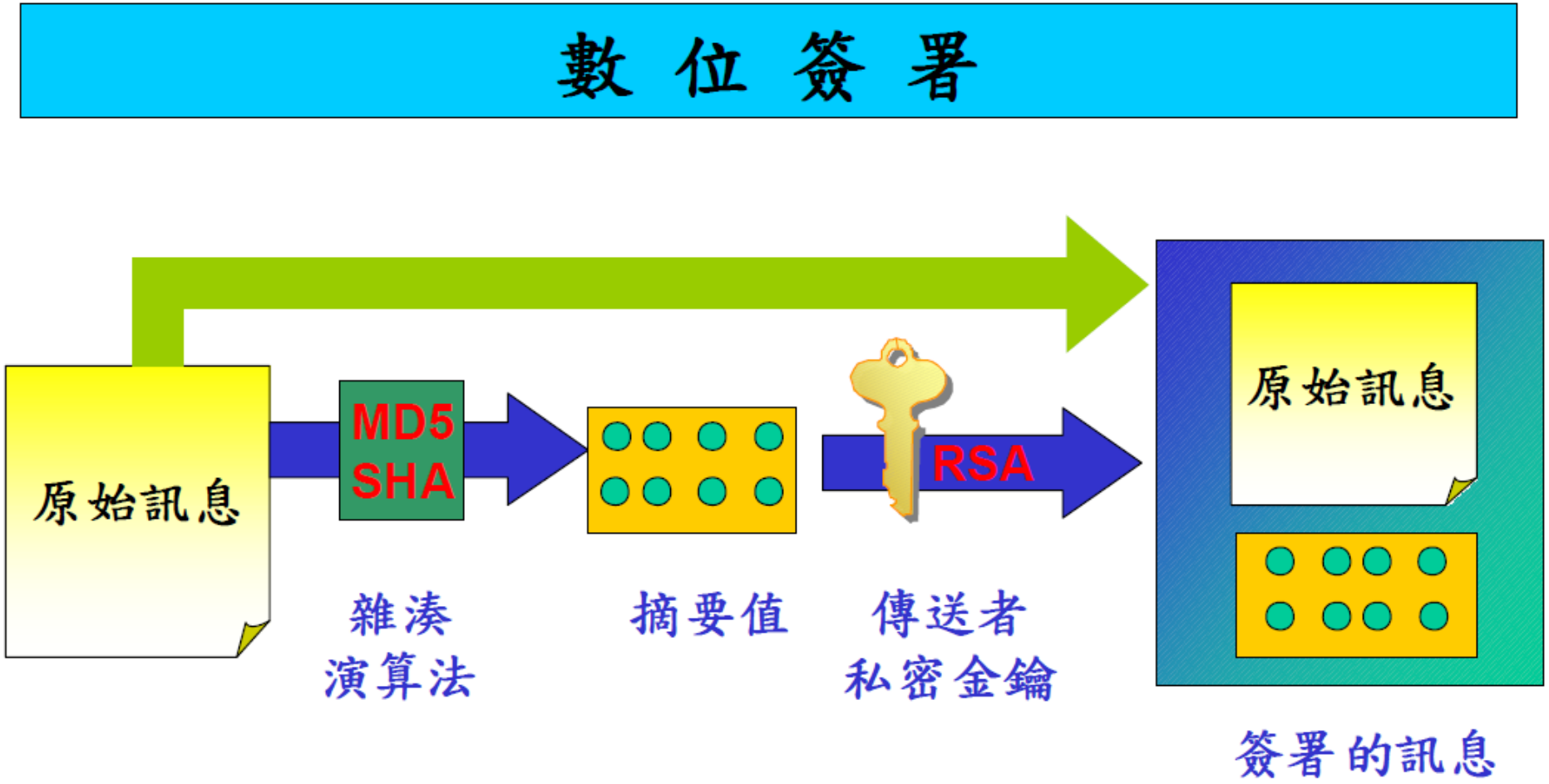
2 已加密的資料經由網路傳送

3 王五使用自己的私密金鑰(Private Key)解除加密的資料

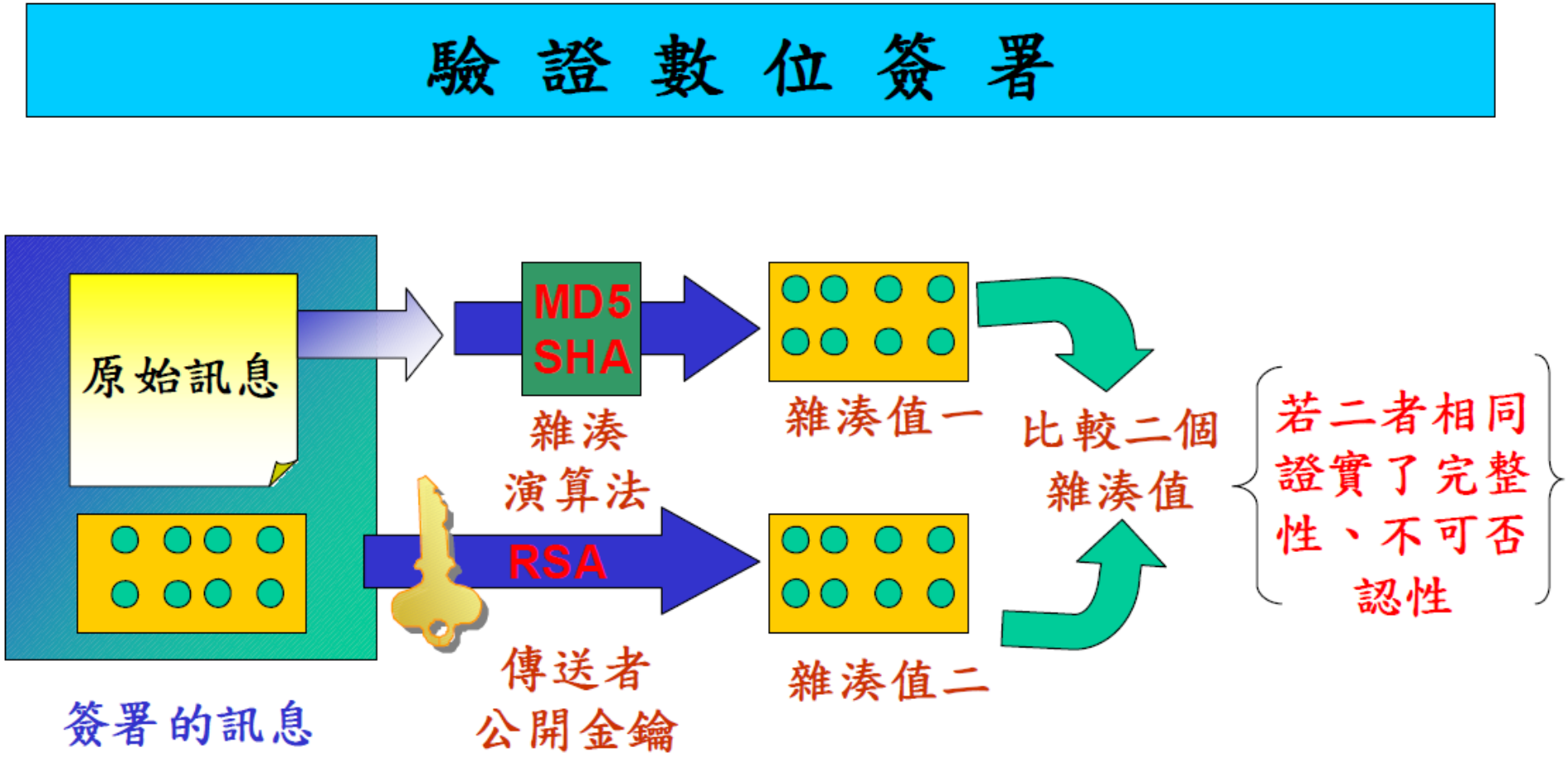
公開金鑰驗證原理


~*~*~*~
~*~*~*~
~*~*~*~
1
張三使用自己的私密金鑰簽章需要傳遞的訊息
2
簽章的資料經由網路傳送
3
王五利用張三的公開金鑰確認信息是發自張三

產生數位簽署



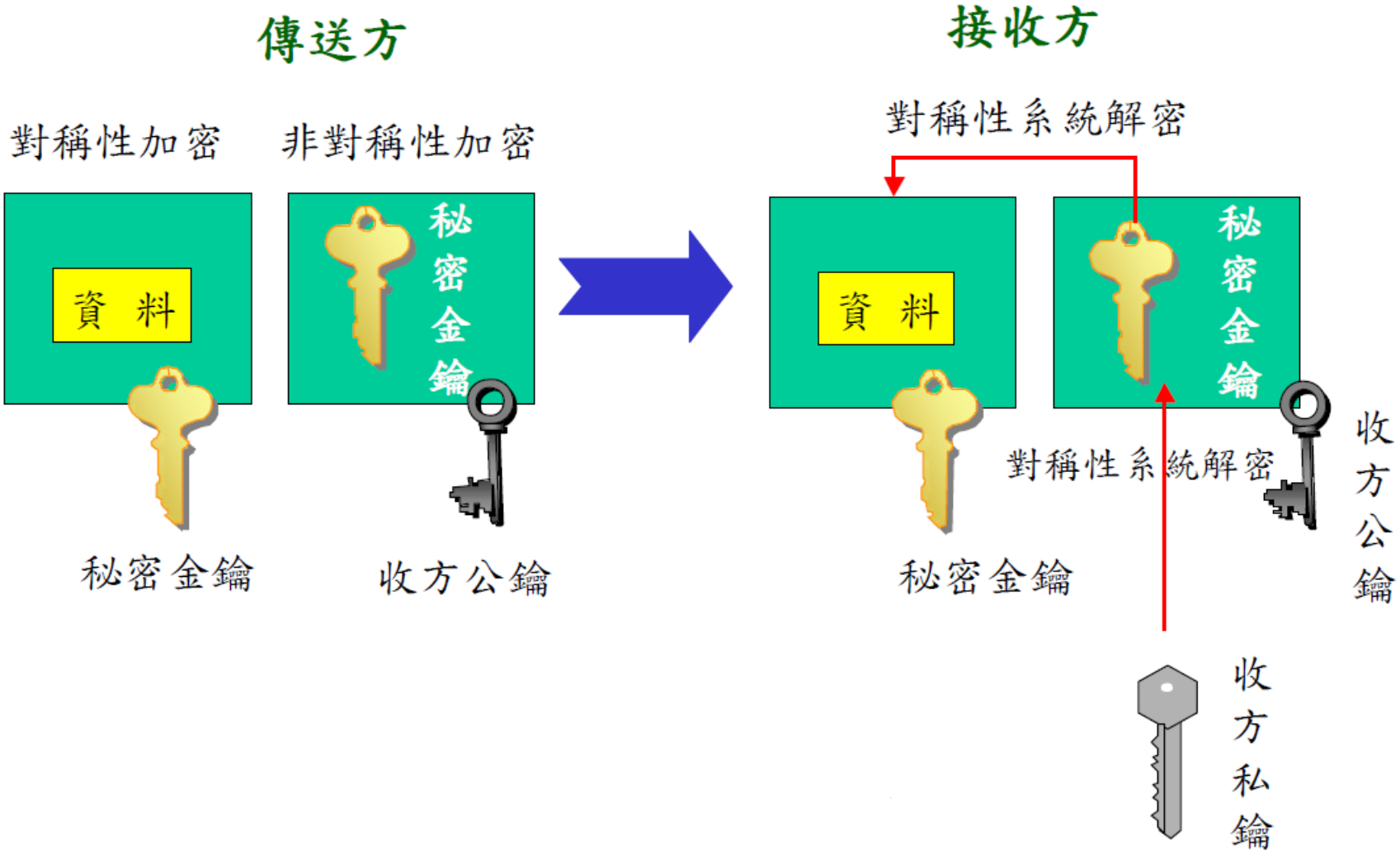
驗證數位簽署


驗 證 數 位 簽 署
原始訊息
MD5
SHA
雜湊
演算法
RSA
傳送者
公開金鑰
簽署的訊息
雜湊值一
雜湊值二
比較二個
雜湊值
若二者相同
證實了完整
性、不可否
認性

數位信封(Digital Envelope)

- 指電子文件採用對稱金鑰加密產生密文，再利用收文者的公開金鑰將對稱金鑰加密保護，將密文與加密後之對稱金鑰傳送給接收者，以達到秘密通訊之目的者。
- 公開金鑰密碼系統的缺點是其編碼與解碼速度較慢，所以在實際運用上，通常均以公開金鑰密碼系統搭配私密金鑰密碼系統來對訊息作加解密，以兼顧安全與效率。

數位信封(Digital Envelope)



PKI 使用範圍

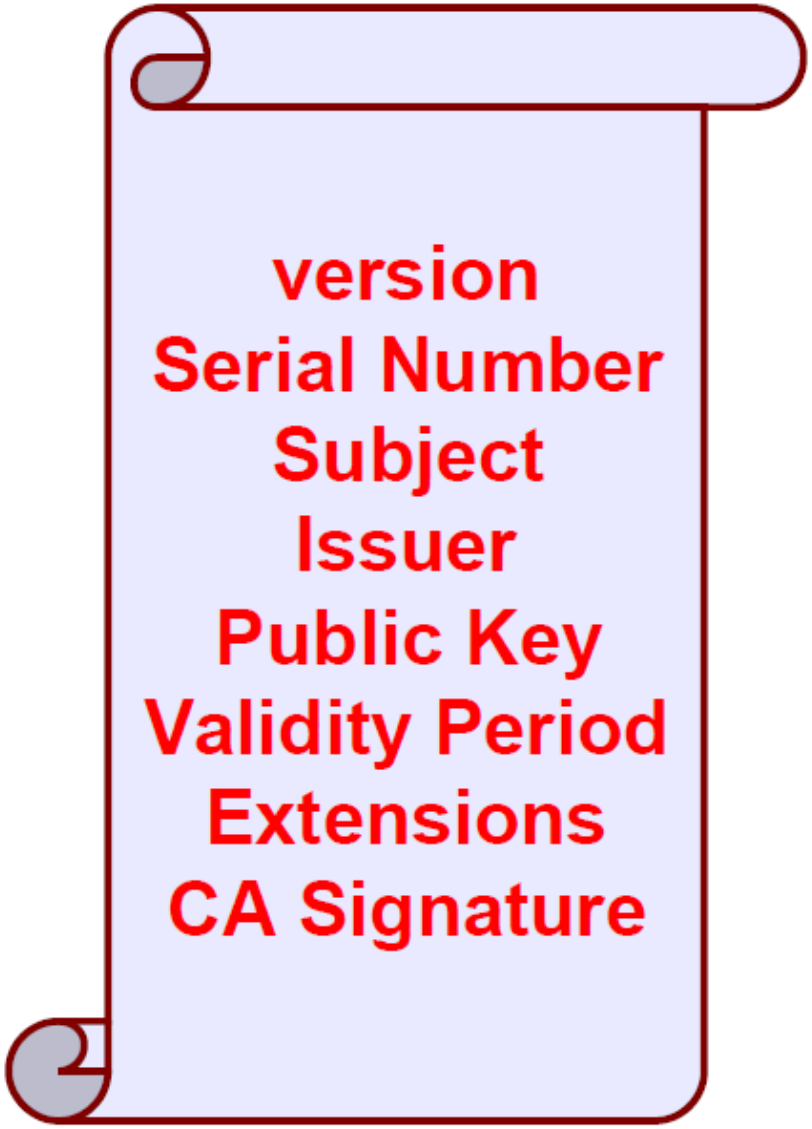
- 提供遠端存取系統及資源的身份驗證機制
- 確保各種資料於網路上傳送的私密性(confidentiality)和完整性(integrity)
- 軟體簽章(Code Signature)
- 安全性的各項電子交易
  - ✓內部公文電子化
  - ✓電子商務
  - ✓網路銀行
  - ✓網路下單

憑證管理中心(Certification Authority)

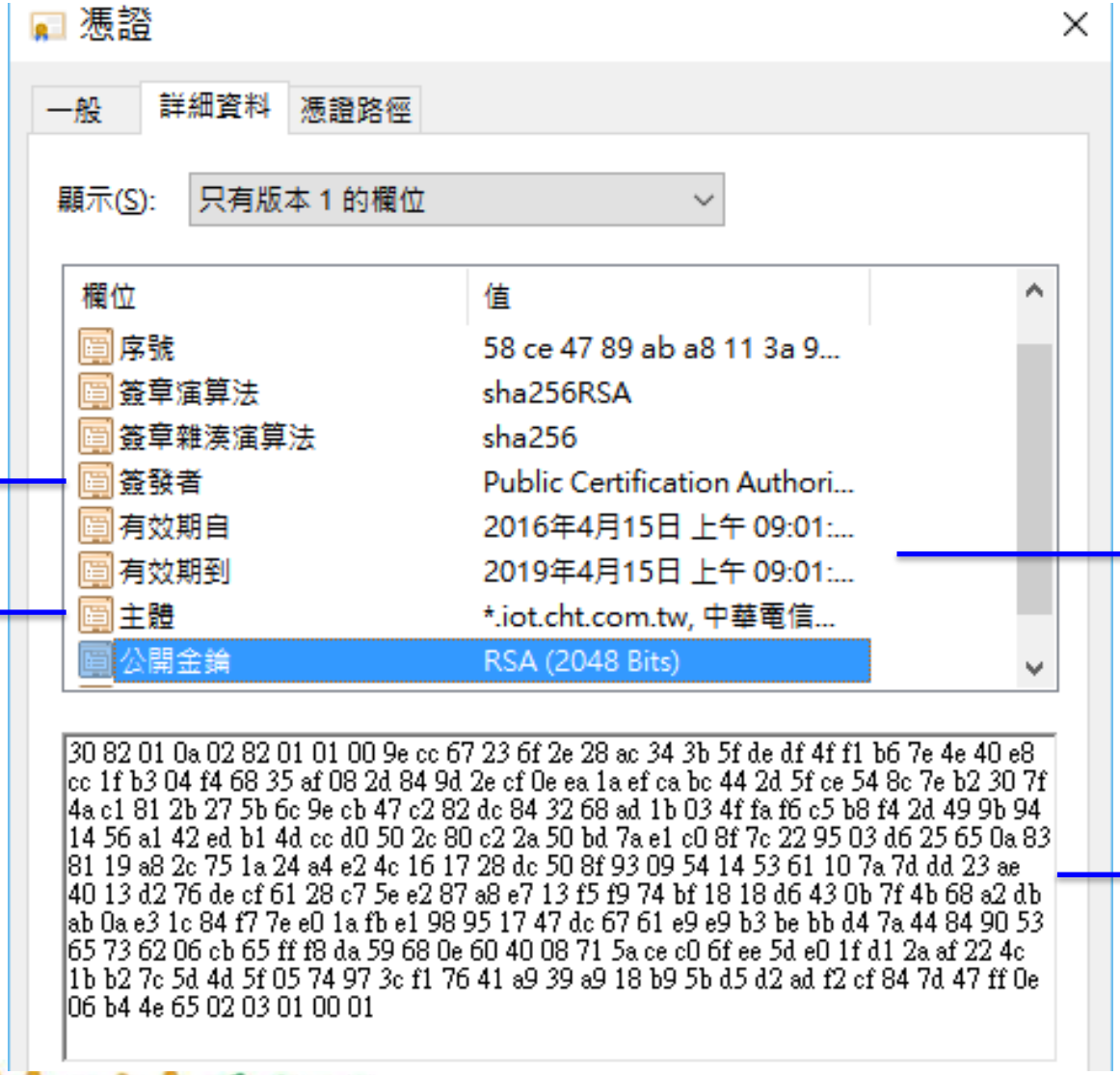
- 為了使公開金鑰密碼系統得以順利運作，必需設法緊密結合並證明某一把公開金鑰確實為某人或某單位所擁有，讓他人無法假冒、偽造。解決方法是模仿印鑑證明的方式，由可信賴的第三者或機構(Trusted Third Parity)來當作公鑰授權單位，以簽發公鑰電子憑證的方式來證明公鑰的效力
- CA就是一個用來提供發行、撤銷管理憑證的服務單位。
- 可由政府、商業機構(如verisign)或組織內自行架設以提供各項憑證相關的服務。

憑證(Certificates)

- 數位憑證是一份經由CA簽章的電子文件。
- 用來證明公開金鑰和特定的個人或單位(擁有者)的連繫關係。
- 標準：ITU-T X.509格式
- 憑證內容包括使用者名稱、公開金鑰、發證者(issuer)、生效和到期日期、擁有者... .等資訊。



憑證內容



憑證發行者

憑證持有者

憑證的
有效期限

公開金鑰

X.509數位憑證格式

- X.509數位憑證乃以ASN.1符號表示法(Abstract Syntax Notation 1)定義，詳細記載了組成該數位憑證的二進位資料。
- ASN.1可以用多種方式加以編碼，現今標準多為使用簡單的DER (Distinguished EncodingRules)，可以產生二進位數位憑證；BASE64產生文字模式編碼格式。

數位憑證的編碼內容

- 數位憑證通常以Base64編碼，產生出如下所列的ASCII內容文件：

-----BEGIN CERTIFICATE-----
MIICWDCCAgICAQAwDQYJKoZIhvcNAQEEBQAwgbYxCzAJBgNVBAYTAlpBMRUwEwYD
VQQIEwxXZXN0ZXJuIENhcGUxEjAQBgNVBAcTCUNhcGUgVG93bjEdMBsGA1UEChMUV
Ghhd3RlIENvbnN1bHRpbmcgY2MxHzAdBgNVBAsTFkNlcnRpZmljYXRpb24gU2VydmljZX
MxFzAVBgNVBAMTDnd3dy50aGF3dGUuY29tMSMwIQYJKoZIhvcNAQkBFhR3ZWJtYXN0
ZXJAdGhhd3RlLmNvbTAeFw05NjExMTQxNzE1MjVaFw05NjEyMTQxNzE1MjVaMIG2MQs
wCQYDVQQGEwJaQTEVMBMGA1UECBMMV2VzdGVybiBDYXBlMRIwEAYD
VQQHEwlDYXBlIFRvd24xHTAbBgNVBAoTFFRoYXd0ZSBDb25zdWx0aW5nIGNjMR8wHQ
YDVQQLExZDZXJ0aWZpY2F0aW9uIFNlcnZpY2VzMRcwFQYDVQQDEw53d3cudGhhd3Rl
LmNvbTEjMCEGCSqGSIb3DQEJARYUd2VibWFzdGVyQHRoYXd0ZS5jb20wXDANBgkqhki
G9w0BAQEFAANLADBIAkEAmpIl7aR3aSPUUwUrHzpVMrsm3gpI2PzIwMh39l1h/RszI0/0q
C2WRMlfwm5FapohoyjTJ6ZyGUUenICllKyKZwIDAQABMA0GCSqGSIb3DQEBBAUAA0EA
fI57WLkOKEyQqyCDYZ6reCukVDmAe7nZSbOyKv6KUvTCiQ5ce5L4y3c/ViKdlou5BcQYAb
xA7rwO/vz4m51w4w==
-----END CERTIFICATE-----

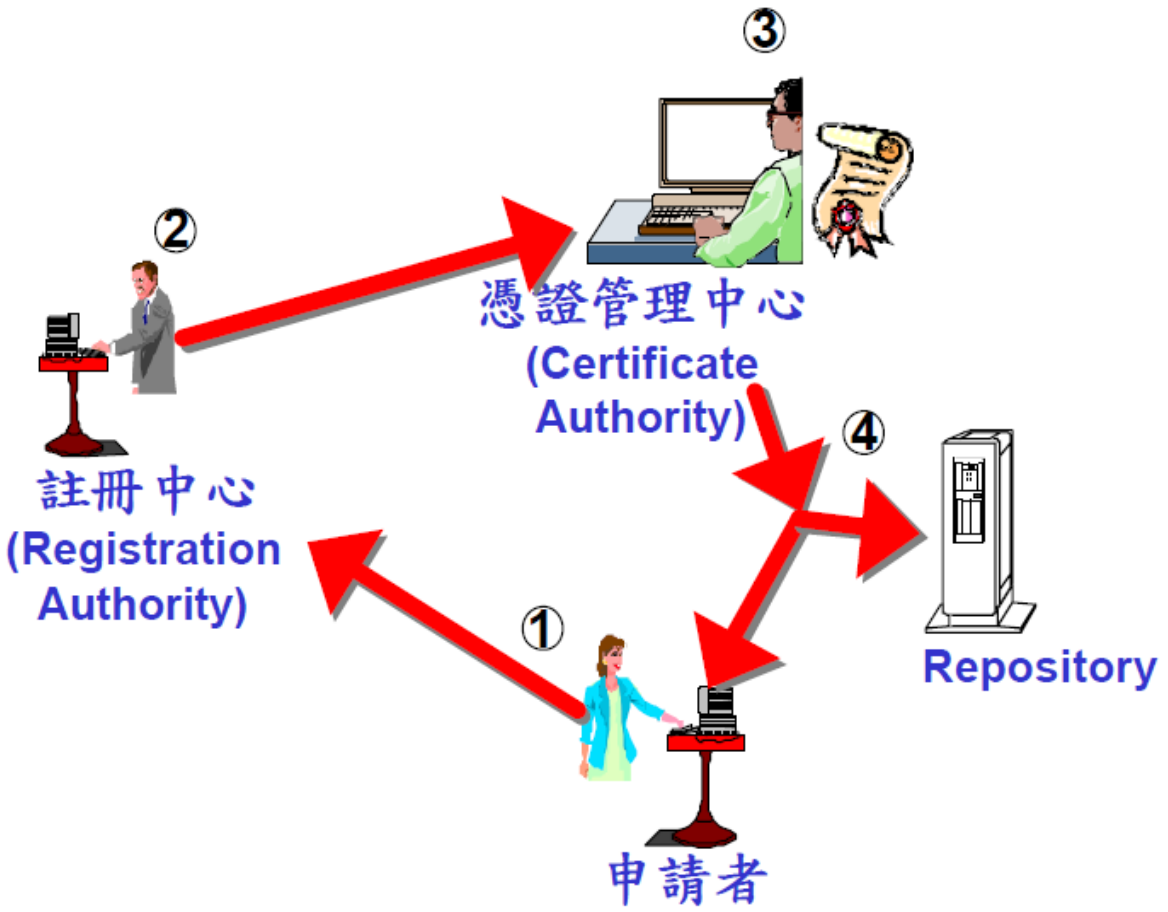
憑證管理中心發行憑證

① 由請者向註冊中心提供身份及申請證明。

② 註冊中心驗證憑證請求人之身分，並授權CA 來簽發憑證，同時也將憑證請求安全地傳給CA。

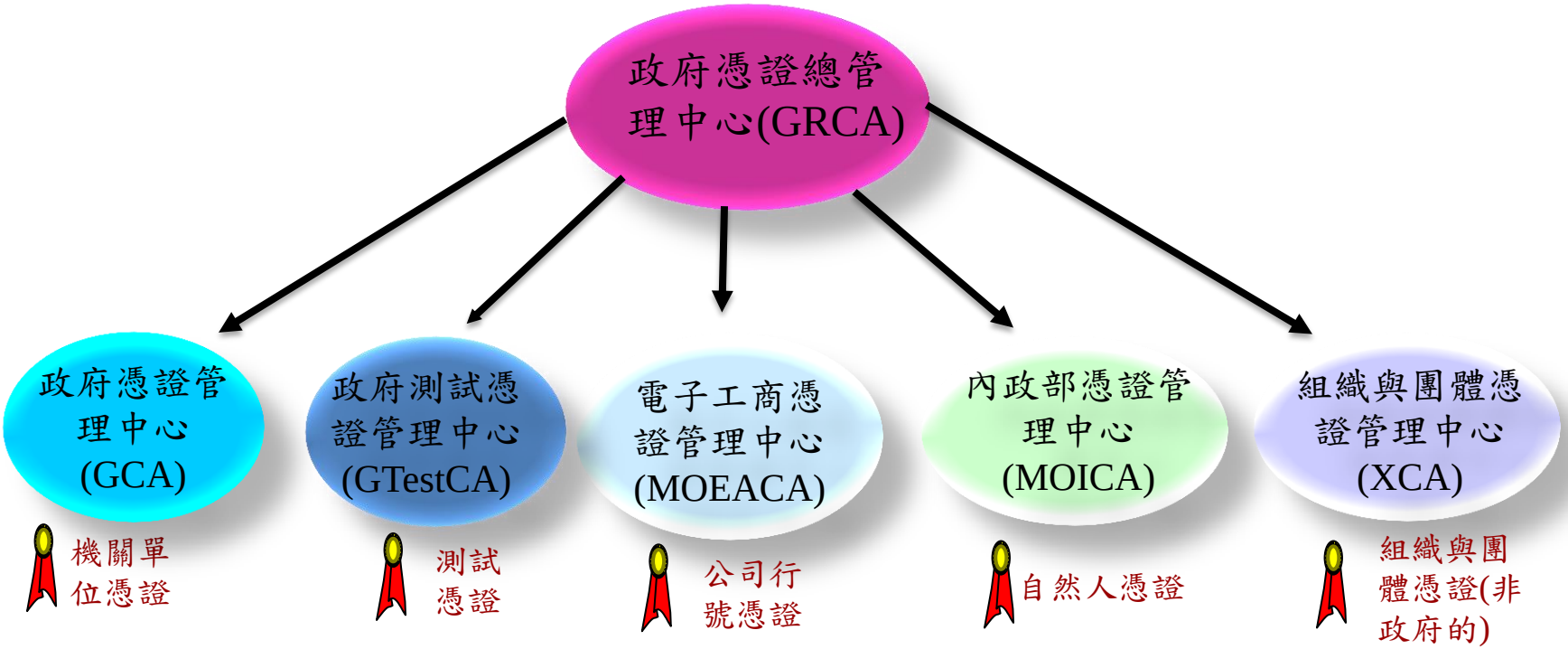
③ 憑證管理中心產生並簽署申請人憑證。

④ 憑證管理中心安全的將憑證傳送給申請人，並將它儲存於資料庫中。

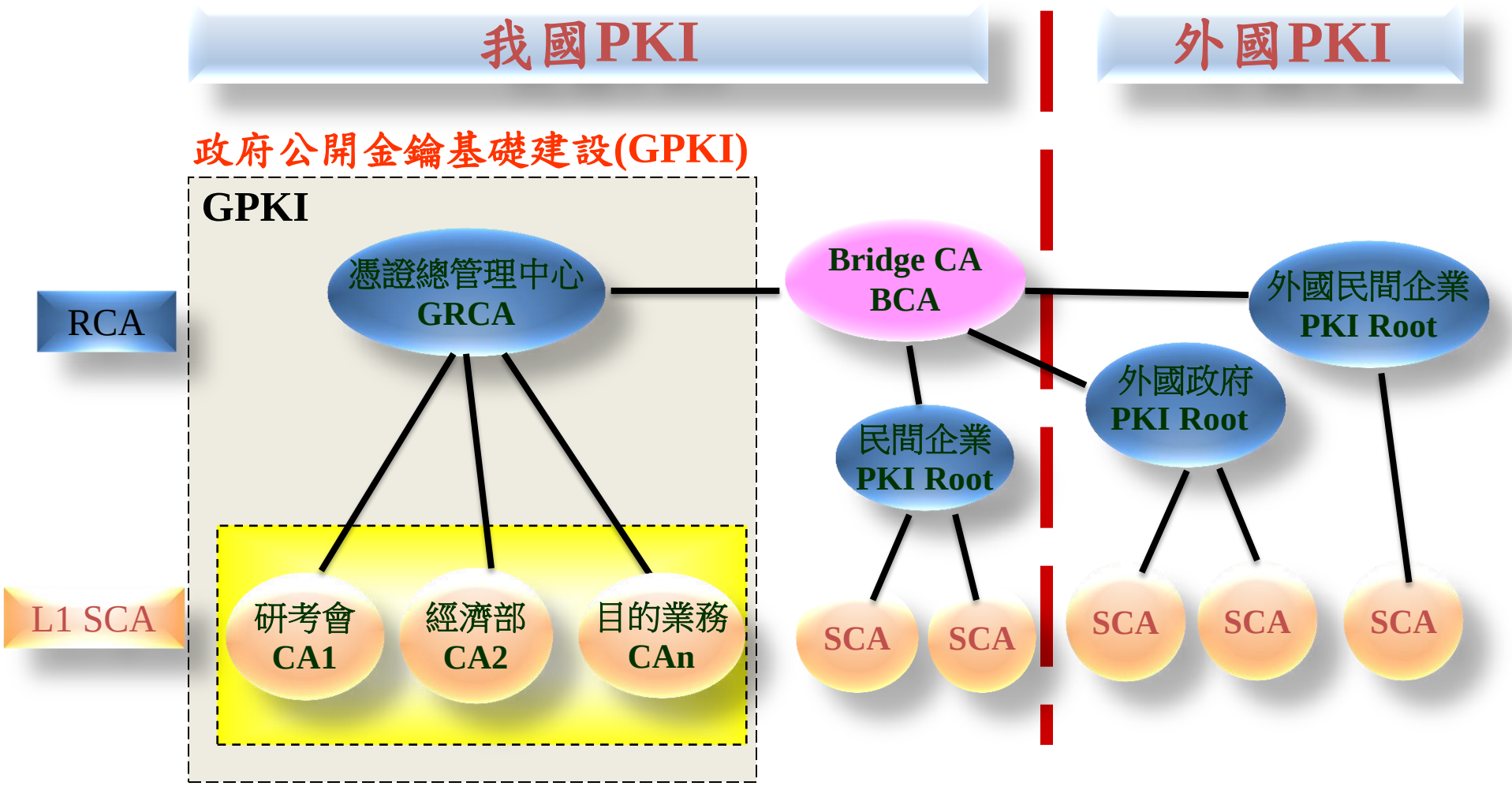


政府機關公開金鑰基礎建設(GPKI)

- 目前政府機關公開金鑰基礎建設(Government Public Key Infrastructure,GPKI)的架構如下圖所示。
- GPKI的發展及建置方式請參考GRCA網站: http://grca.nat.gov.tw



我國整體架構關係圖



L1 SCA: Level 1 Subordinate CA

簡報完畢，敬請指教