密碼學的應用

1.數位信封Digital Envelope| 數位簽章Digital Signature

2.PKI 公開金鑰基礎建設 Public Key Infrastructure

自然人憑證

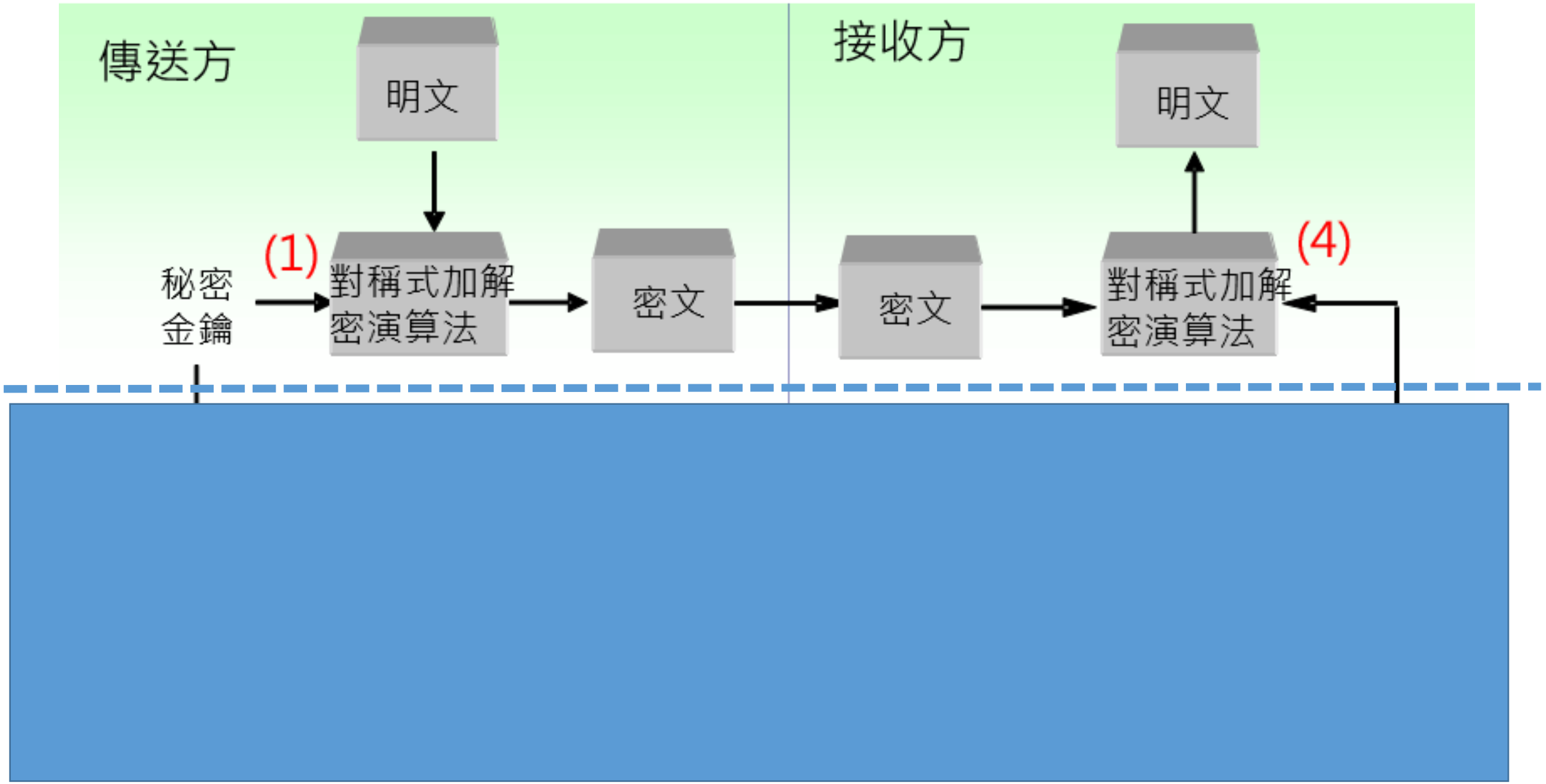
各式各樣的安全協定

S/MIME 電子郵件加密協定

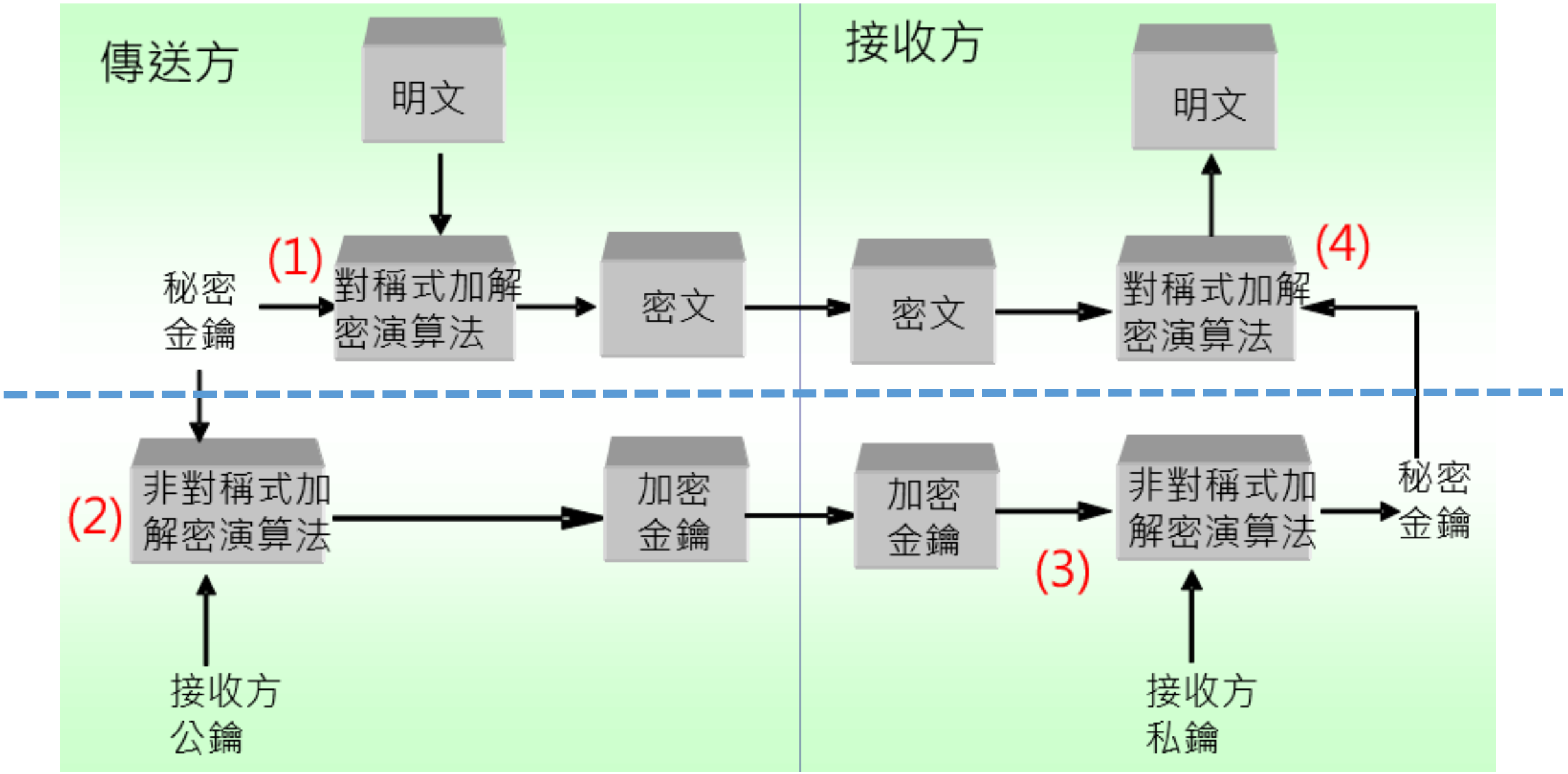
Https/TLS 網站加密協定

IPsec

數位信封的運作流程



數位信封的運作流程


傳送方
明文
(1)
秘密
金鑰
對稱式加解
密演算法
密文
非對稱式加
解密演算法
(2)
加密
金鑰
接收方
公鑰
接收方
明文
密文
對稱式加解
密演算法
(4)
加密
金鑰
非對稱式加
解密演算法
(3)
秘密
金鑰
接收方
私鑰

數位信封Digital Envelope

- 數位信封是結合**對稱式加解密演算法**速度快與**非對稱式加解密演算法金鑰管理方便**兩項優點的一種技術
- RFC2315
- 數位信封是以密碼學的方法，用**收信人的公鑰**對某些機密資料進行加密，收信人收到後再用自己的私鑰解密而讀取機密資料。
- 除了擁有該私鑰的人之外，任何人即使拿到該加密過的訊息都無法解密，就好像那些資料是用一個牢固的信封裝好，除了收信人之外，沒有人能拆開該信封。

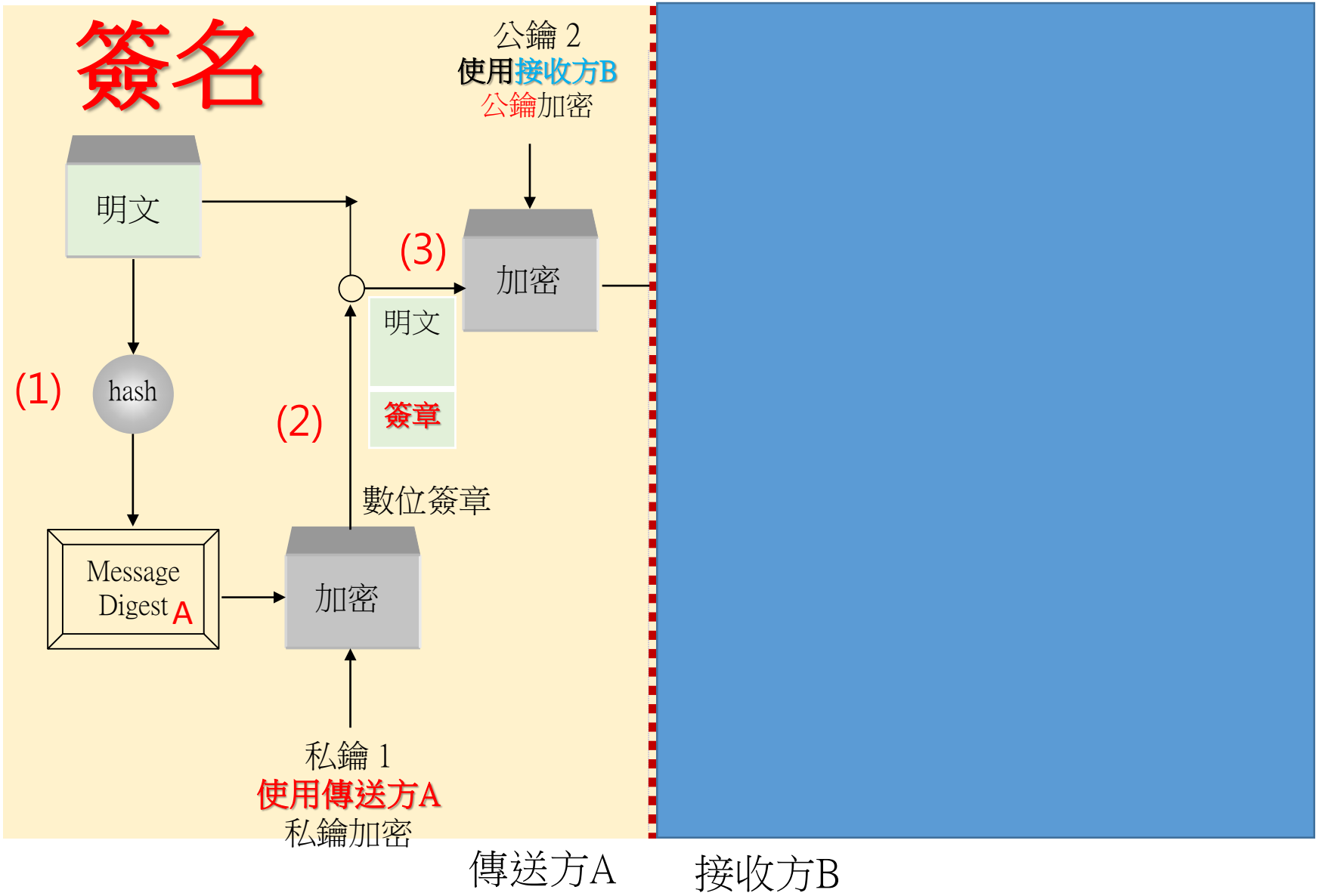
數位信封的運作流程：

1. 使用「秘密金鑰」以「對稱式加解密演算法」對「明文」加密後，得到「密文」
2. 利用接收方的「公開金鑰」以「非對稱式加解密演算法」將「秘密金鑰」加密，得到「加密金鑰」(如同製作一個數位信封)。
3. 再將「密文」與「加密金鑰」傳送到接收方(如同兩者都一起放入數位信封內)，以提高訊息加密的效率

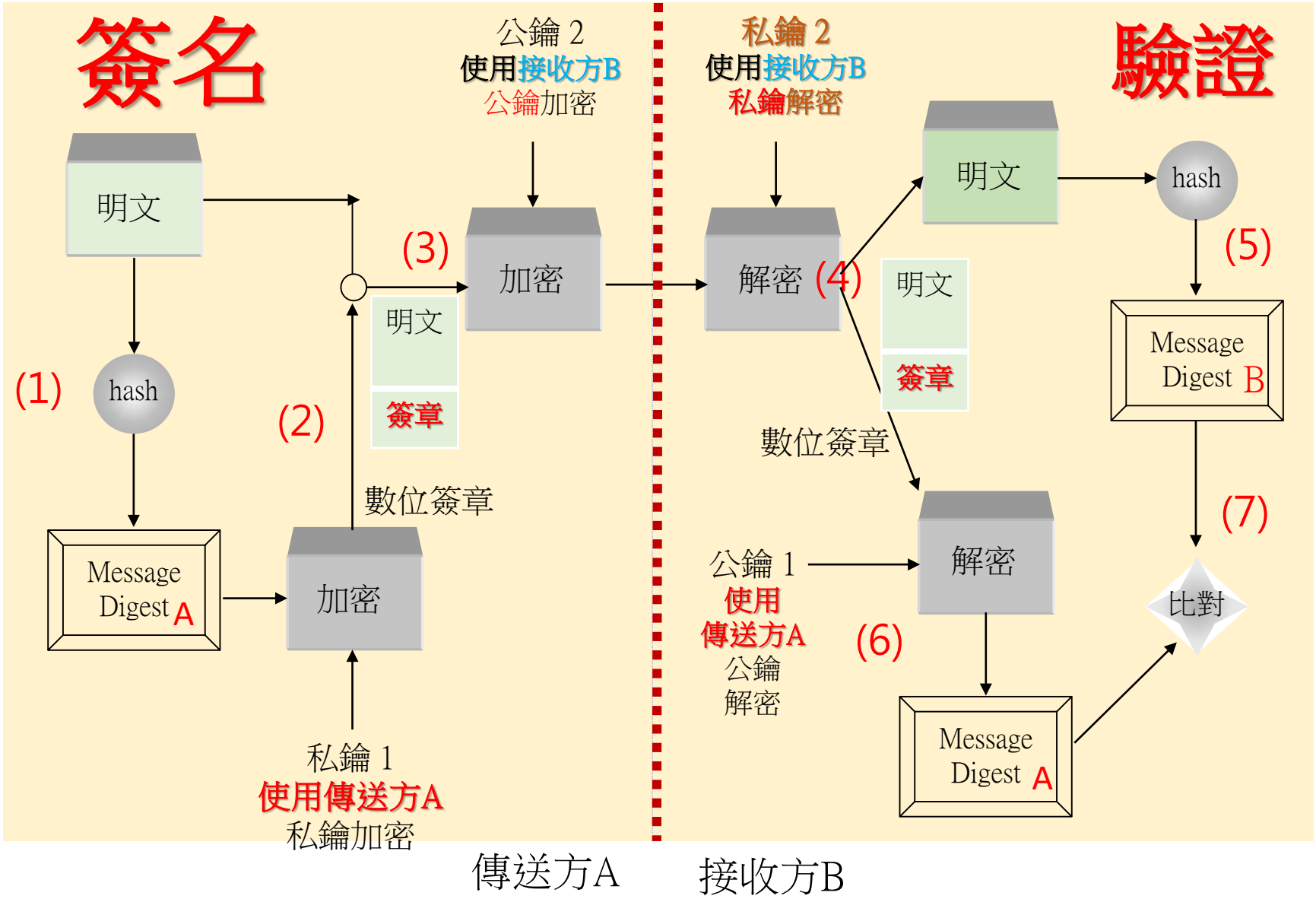
接收方

1. 用自己的「私密金鑰」以「非對稱式加解密演算法」將「加密金鑰」解密後，得到「秘密金鑰」
2. 使用「秘密金鑰」以「對稱式加解密演算法」解開「密文」後，得到「明文」

數位簽章Digital Signature



數位簽章Digital Signature



數位簽章Digital Signature

- 數位簽章又稱**公鑰數位簽章**
- 是一種功能類似寫在紙上的簽名、但使用**公鑰加密**的技術，用於鑑別數位訊息的方法。
- 一套數位簽章通常會定義兩種互補的運算，一個用於**簽名**，另一個用於**驗證**。
- 目的
  - ✓ 證明電子檔案為簽章者所傳送 == >**鑑別性authenticity |不可否認性 Non-Repudiation**
  - ✓ 資料被竄改時可以發現 == >**完整性 Integrity**
  - ✓ **使用公鑰加密**的技術加解密 == >**機密性(Confidentiality)**
- **簽名**

  甲方要把電子檔案簽章後傳送給乙方
  - ✓ 1.甲方使用 hash 算出電子檔案的message digest
  - ✓ 2.甲方用自己的**私密金鑰**對message digest作簽章
  - ✓ 3.甲方將電子檔案與簽章一起傳送給乙方
- **驗證**
  - ✓ 乙方用甲方的公開金鑰解開簽章 == > 得到(message digest)乙

    可驗證出電子檔案沒有被竄改，的確是由甲方所傳送

- 數位簽章技術同時提供**訊息的完整性 Integrity**、**鑑別性authenticity** 、**機密性(Confidentiality)**及**不可否認性 Non-Repudiation**

	1	若要僅有收件者能開啟，並確認內容未遭篡改的信件，下列敘述何者 正確？ (A) 信件以雜湊(Hash)演算後，以寄件者的私密金鑰(Private Key) 加密後寄出 (B) 信件以雜湊(Hash)演算後，以收件者的私密金鑰(Private Key)加密後寄出 (C) 信件以雜湊(Hash)演算後，以收件者的公開金鑰(Public Key) 加密後寄出 (D) 使用收件者的公開金鑰(Public Key)加密信件
	2	電子郵件常用的數位簽章(Digital Signature)，其目的是保護下列哪些資訊安全要素？ (A) 機密性（Confidentiality）與完整性（Integrity） (B) 完整性（Integrity）與可用性（Availability） (C) 完整性（Integrity）與不可否認性（Non-Repudiation） (D) 機密性（Confidentiality）與不可否認性（Non-Repudiation）
	3	關於數位簽章(Digital Signature)，下列敘述何者「不」正確？ (A) 使用了公開金鑰基礎建設(Public Key Infrastructure, PKI） (B) 簽章時用公鑰(Public Key)加密 (C) 公鑰(Public key)必須向接受者信任的數位憑證認證機構 (Certificate Authority, CA)註冊 (D) 可以用 EIGamal 演算法來實做數位簽章
	4	關於數位簽章（Digital Signature）及數位信封（Digital Envelop），下 列敘述何者正確？ (A) 數位簽章與數位信箱皆運用雜湊函式（Hash Function）達成效果 (B) 數位簽章主要是將訊息摘要加密後運用對稱金鑰加密 (C) 數位信封將資料以對稱金鑰加密，再將金鑰透過公開金鑰加密技術傳輸供收訊方解密 (D) 數位簽章及數位信封技術在訊息傳遞時皆已加密訊息

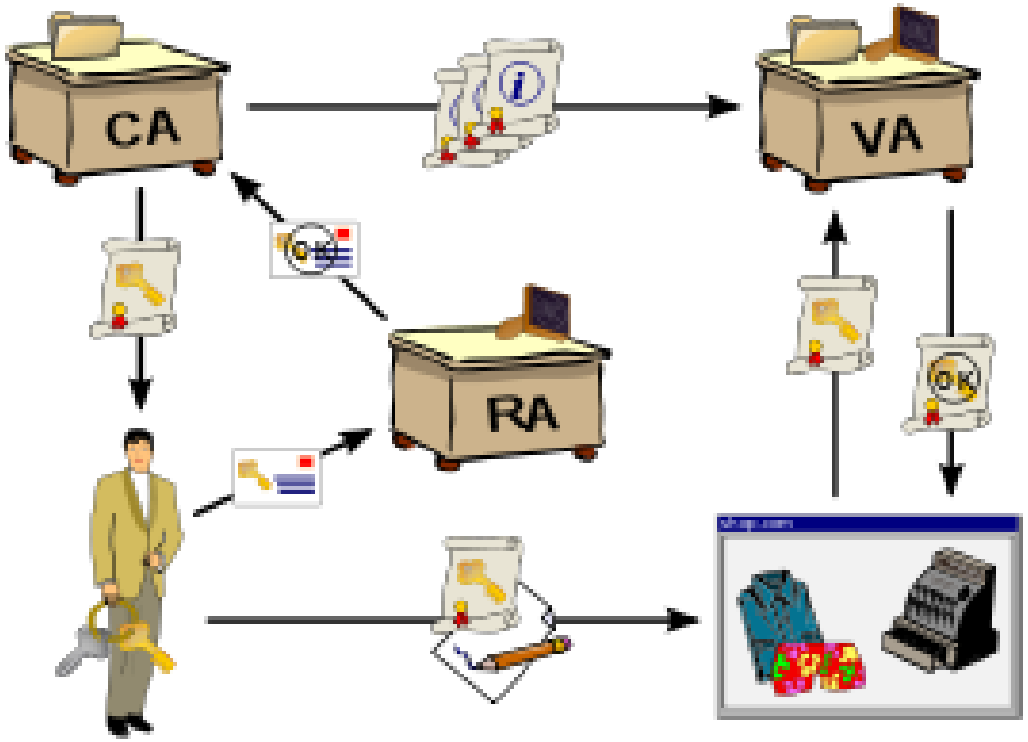
C	1	若要僅有收件者能開啟，並確認內容未遭篡改的信件，下列敘述何者 正確？ (A) 信件以雜湊(Hash)演算後，以寄件者的私密金鑰(Private Key) 加密後寄出 (B) 信件以雜湊(Hash)演算後，以收件者的私密金鑰(Private Key)加密後寄出 **(C) 信件以雜湊(Hash)演算後，以收件者的公開金鑰(Public Key) 加密後寄出** (D) 使用收件者的公開金鑰(Public Key)加密信件
C	2	電子郵件常用的數位簽章(Digital Signature)，其目的是保護下列哪些資訊安全要素？ (A) 機密性（Confidentiality）與完整性（Integrity） (B) 完整性（Integrity）與可用性（Availability） **(C) 完整性（Integrity）與不可否認性（Non-Repudiation）** (D) 機密性（Confidentiality）與不可否認性（Non-Repudiation）
B	3	關於數位簽章(Digital Signature)，下列敘述何者「不」正確？ (A) 使用了公開金鑰基礎建設(Public Key Infrastructure, PKI） **(B) 簽章時用公鑰(Public Key)加密** (C) 公鑰(Public key)必須向接受者信任的數位憑證認證機構 (Certificate Authority, CA)註冊 (D) 可以用 EIGamal 演算法來實做數位簽章
C	4	關於數位簽章（Digital Signature）及數位信封（Digital Envelop），下 列敘述何者正確？ (A) 數位簽章與數位信箱皆運用雜湊函式（Hash Function）達成效果 (B) 數位簽章主要是將訊息摘要加密後運用對稱金鑰加密 **(C) 數位信封將資料以對稱金鑰加密，再將金鑰透過公開金鑰加密技 術傳輸供收訊方解密** (D) 數位簽章及數位信封技術在訊息傳遞時皆已加密訊息

PKI 公開金鑰基礎建設
Public Key Infrastructure

- 是一組由硬體、軟體、參與者、管理政策與流程組成的**基礎架構**
- 目的在於創造、管理、分配、使用、儲存以及復原**數位憑證(digital certificates)**。

憑證(**certificates)** == >個人的身分證，
其內容包括憑證序號、使用者名稱、公開金鑰（Public Key）、憑證有效期限等

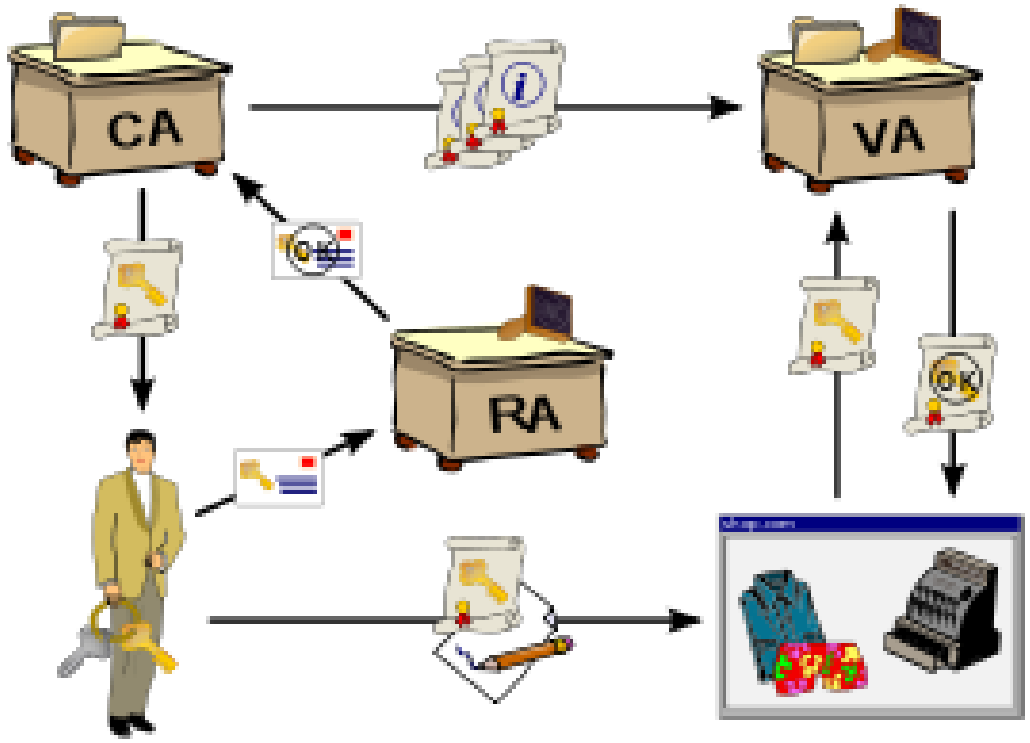
最常見的憑證格式標準: X.509



- PKI是以公鑰密碼學為基礎衍生出來的架構
- 基礎建置包含
  1. 憑證機構(Certification Authority ,CA) 頒發憑證的人或機構
  2. 註冊中心(Register Authority, RA)
     - ✓ 審核使用者的憑證申請
     - ✓ 將憑證申請送至CA處理
  3. 目錄服務(Directory Service ,DS)伺服器
     倉庫repository是存放憑證的資料庫。倉庫也叫憑證目錄
  4. 驗證機構(Validation Authority)
     A PKI Validation Authority (VA) provides validation of PKI certificates.

https://zh.wikipedia.org/zh-tw/%E5%85%AC%E9%96%8B%E9%87%91%E9%91%B0%E5%9F%BA%E7%A4%8E%E5%BB%BA%E8%A8%AD

- CA須同時為傳送者與接收者所信任，由具**公信力的第三者**來擔任
- 由CA經過認證，簽發公開金鑰憑證，以作為檢驗私密金鑰的憑證。
- PKI包含一支公開金鑰（Public Key）與一支私密金鑰（Private Key）， Public Key公開給大眾知道， Private Key由持有者保管。
- 這一組金鑰為一組電子密碼，可作為檢驗身分之用，且具有相對應的關係，其中一支金鑰將訊息進行加密，另一支金鑰則可進行解密而得到原來的訊息。



私密金鑰應如何保管才能兼顧安全、便利性以及成本考量？
私鑰儲存設備 == > 電腦之硬碟或軟碟、**Smart Card(智慧卡)**或 Token(權杖)等相關儲存元件。

憑證授權中心 Certification Authority, CA

發出憑證的單位（或公司）

- CA 中心必須是個可信賴的公正單位（私人或政府）
- CA會依據合法申請者的請求，發出數位憑證。
  數位憑證裡包含了申請人的辨識資料（姓名、地址、或身份字號）、申請人的公開鑰匙、序號與其他資料，並保證不會造假
- CA 中心利用自己的私有鑰匙向上述資料簽署，所得到的數位簽章亦存放於憑證裡。
- 每一張數位憑證必須有發行 **CA 的數位簽章**，而此數位簽章是利用 CA 中心的私有鑰匙簽署保證。
- 如果懷疑某一張數位憑證的真實性，便可以利用 CA 的公開鑰匙來認證它的正確性。
- 如何取得 CA 的公開鑰匙? == > 必須先拿到該 CA 的數位憑證，再由它的數位憑證取得它的公開鑰匙
- 但數位憑證的真實性如何？ == > 需仰賴另一個較高權威的 CA 來證實

台灣較具權威的認證中心有：

- ✓ **政府憑證管理中心 (www.pki.gov.tw)**：這是官方發行單位，可以針對個人(自然人)或公司行號(法人)發行數位憑證，所發行的憑證較具有權威性，它的用途也較為特殊。譬如，透過網路向政府單位承標各種工程或器材，便需要此 CA 中心所發行的憑證來證明自己的身份。
- ✓ **內政部憑證管理中心(moica.nat.gov.tw)**：官方發行單位，這是針對個人所發行的憑證，功能就如同個人身分證一樣，又稱為『電子身分證 IC 卡』。個人（或稱自然人）欲透過網路向政府機關申辦任何事項，便以此憑證來確認身份。
- ✓ 工商憑證管理中心moeaca.nat.gov.tw
- ✓ 台灣網路認證中心 (www.taica.com.tw)：這是民間發行單位（主要是台灣證券交易所），主要用途是使用於透過網路來執行股票交易（下單買賣）時，認證下單者的真正身份、也發行電子錢包；但目前也有許多網路銀行，利用此 CA 所發行的憑證來確認客戶的身份。

CRL憑證吊銷列表 與 OCSP線上憑證狀態協定

CRL憑證吊銷列表

- **Certificate revocation list**
- 尚未到期就被憑證頒發機構**吊銷**的數位憑證的名單。
- 在憑證吊銷列表中的憑證不再會受到信任。
- **線上憑證狀態協定(OCSP)**已經替代憑證吊銷列表（CRL）成為**檢查憑證狀態**的主流。

OCSP線上憑證狀態協定

- Online Certificate Status Protocol
- OCSP是一個用於**檢查**X.509**憑證狀態**的網際協定
- 協定資料傳輸過程中使用ASN.1編碼，並通常建立在HTTP協定上
- 此訊息類型分為「請求訊息」和「回應訊息」

.	一般而言，公開公鑰會透過憑證管理中心發行公開憑證來傳遞，對於仍在有效期內，卻因為某些因素造成憑證廢止的情形，可以透過下列何項協定來查詢？ (A) Online Certificate Status Protocol(OCSP) (B) Online Certificate Register Protocol(OCRP) (C) Online Certificate Revoke Protocol(OCRP) (D) Certificate Transmit Protocol(CTP)

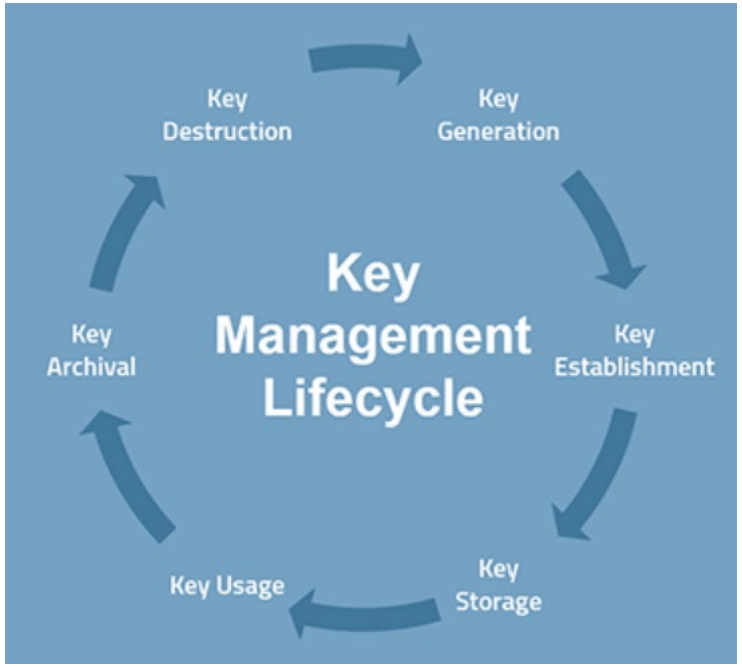
金鑰管理Key Management

金鑰生命週期管理(Key Management Lifecycle)
金鑰與憑證管理

- Key management是一個密碼系統中加密金鑰的管理部分。
- Key management包括**金鑰的生成、交換、儲存、使用**、**金鑰銷毀**以及**金鑰更替**的處理。
- 金鑰管理關注 使用者層面 或 使用者與系統之間的金鑰。
- 金鑰管理在某種意義上比純數學的密碼學更加具有挑戰，因為它涉及到系統策略、使用者培訓、組織和部門的相互作用，以及上述所有元素之間的協調，而這些過程往往和密碼學的其他元件不同，因為這些過程無法自動完成。

Key Management有許多解決方案,請參看**WIKI |金鑰管理** 說明
金鑰管理系統(key management system，KMS)
密碼學金鑰管理系統（crytographic key management system，CKMS）

金鑰可以通過金鑰管理系統、HSM硬件安全模組(Hardware security module)或受信任的協力廠商（TTP）生成



NIST SP 800-57 Recommendation for Key Management

- Part 1 Rev. 5 Recommendation for Key Management: Part 1 – General
  - https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final
- Part 2 Rev. 1 Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations
  - https://csrc.nist.gov/publications/detail/sp/800-57-part-2/rev-1/final
- Part 3 Rev. 1 Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance
  - https://csrc.nist.gov/publications/detail/sp/800-57-part-3/rev-1/final

1	**關於金鑰與憑證管理，下列敘述何者「不」正確？** **(A)** 金鑰都應受保護不被修改和破壞，並應使用實體安全來保護用於 產生、儲存和歸檔金鑰的設備，以避免金鑰遭受不當修改、不慎遺失或銷毀等情況 **(B)** 基於業務需要，須自行建置、委託建置或選用憑證機構（**Certificate Authority**）時，應綜合考量憑證機構之技術、管理、人員及財務 **(C)** 憑證機構資訊系統（含應用系統、密碼模組等）之安全驗證，應遵照權責主管機關訂定之規範作業，以確保其安全性 **(D)** 憑證機構使用之電子簽章或加密金鑰長度，視系統的安全需求， 由組織自行決定
2	關於金鑰生命週期管理(Key Management Lifecycle)，於儲存階段之最佳實務的敘述，下列何項錯誤？ (A) 金鑰不應以明文形式(Plaintext)進行儲存 (B) 金鑰若留存於系統記憶體(Memory)中，其暫存特性能達成保護目的 (C) 金鑰離線儲存須以「金鑰加密密鑰」(Key Encryption Keys)加密保護 (D) 金鑰應儲存於密碼庫(Cryptographic Vault)，如：硬體安全模組(HSM, Hardware Security Module)

1	關於金鑰與憑證管理，下列敘述何者「不」正確？ **(A)** 金鑰都應受保護不被修改和破壞，並應使用實體安全來保護用於 產生、儲存和歸檔金鑰的設備，以避免金鑰遭受不當修改、不慎遺失或銷毀等情況 **(B)** 基於業務需要，須自行建置、委託建置或選用憑證機構（**Certificate Authority**）時，應綜合考量憑證機構之技術、管理、人員及財務 **(C)** 憑證機構資訊系統（含應用系統、密碼模組等）之安全驗證，應遵照權責主管機關訂定之規範作業，以確保其安全性 **(D) 憑證機構使用之電子簽章或加密金鑰長度，視系統的安全需求， 由組織自行決定**
2	關於金鑰生命週期管理（Key Management Lifecycle），於 儲存階段之最佳實務的敘述，下列何項錯誤？ (A) 金鑰不應以明文形式（Plaintext）進行儲存 **(B) 金鑰若留存於系統記憶體（Memory）中，其暫存特性能達成保護目的** (C) 金鑰離線儲存須以「金鑰加密密鑰」（Key Encryption Keys）加密保護 (D) 金鑰應儲存於密碼庫（Cryptographic Vault），如：硬 體安全模組（HSM, Hardware Security Module）

PKI的應用 PKI可廣泛應用到各種領域

公共領域方面
報稅
環保通報系統
健保
軍方行政相關應用
Smart Card
（例如捷運悠遊卡、高速公路收費自動化）

在企業方面
企業流程(Work Flow)管理、ERP、 SCM 等相關應用
員工差勤門禁系統
企業員工網路資料傳輸的加密及數位簽名
企業內部網路安控與使用權限機制
企業內部安全電子郵件及電子公文系統環境
電子供應商採購系統
電子經銷商訂貨系統
客戶分級與使用權限
安全電子交易加密與數位簽名
安全電子交易市集平台
跨國網路交易認證
交易認證國際漫遊功能

建置PKI技術

PKI介绍及搭建Linux私有CA (SSL 示例)
https://blog.csdn.net/weixin_44983653/article/details/96511856

Windows Active Directory Certificate Services (AD CS)
Windows Server role for issuing and managing public key infrastructure (PKI) certificates

Understanding Active Directory - Active Directory Certificate Services CS
https://www.youtube.com/watch?v=D8cffeiovvc

Windows 驗證概觀
https://learn.microsoft.com/zh-tw/windows-server/security/windows-authentication/windows-authentication-overview

Windows Server 文件
https://learn.microsoft.com/zh-tw/windows-server/

自然人憑證

- 自然人憑證 == 網路身分證
- 使用自然人憑證可透過網路申辦多項政府提供的服務:

網路報稅
勞保年資
個人退休金專戶查詢
個人限制入出境查詢
健保個人資料及欠費查詢
電子公路監理
電子戶籍謄本
身分證掛失及地政e網通等多項便民服務

(請參照內政部憑證中心網站http://moica.nat.gov.tw/link_1.html)。

如何申請自然人憑證：

1.年滿18歲就可辦理，必須本人親自辦理
（不可委託辦理| 也不可授權辦理）
2.應備證件：
(1)身分證正本。
(2)E-mail信箱。
(3)規費250元。
3.可至全國任一戶政事務所辦理。
4.於上班時間申請或補領自然人憑證可當場領取IC卡。

https://ca.gov.taipei/News_Content.aspx?n=59F2E04A34FDA3E8&s=41C4401AABF1E572

	1	關於自然人憑證，下列敘述何者「不」正確？ (A) 自然人憑證是基於公開金鑰基礎建設（Public Key Infrastructure, PKI）架構下之應用 (B) 自然人憑證在網路上使用時，其代表申請人之身分識別上具有法律效力 (C) 自然人憑證申請一次永久有效，無需換發 (D) 自然人憑證於網路上的相關應用具有不可否認性
	2	關於自然人憑證，下列敘述何者「不」正確？ (A) 使用非對稱式演算法產生金鑰對 (B) 簽驗章和加解密是使用同一組金鑰對 (C) 目前自然人憑證設有有效期，但可以展延 (D) 透過自然人憑證進行簽章時，被簽章之資料無長度限制

C	1	關於自然人憑證，下列敘述何者「不」正確？ (A) 自然人憑證是基於公開金鑰基礎建設（Public Key Infrastructure, PKI）架構下之應用 (B) 自然人憑證在網路上使用時，其代表申請人之身分識別上具有法律效力 **(C) 自然人憑證申請一次永久有效，無需換發** (D) 自然人憑證於網路上的相關應用具有不可否認性
B	2	關於自然人憑證，下列敘述何者「不」正確？ (A) 使用非對稱式演算法產生金鑰對 **(B) 簽驗章和加解密是使用同一組金鑰對** (C) 目前自然人憑證設有有效期，但可以展延 (D) 透過自然人憑證進行簽章時，被簽章之資料無長度限制