第13章 電子商務安全機制

13-1 資料傳輸安全

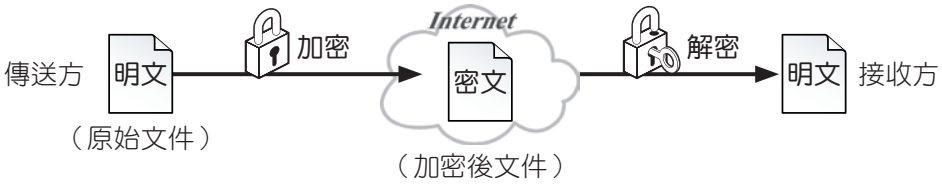
一、資料傳輸安全的要件

安全要件	說明
隱密性（confidentiality）	確保交易資料在傳輸過程中不被他人窺知
完整性（integrity）	確保交易雙方接收到的資料正確且未被篡改
認證性（authentication）	確認交易者的身分（消費者、商家、銀行），避免冒名頂替
不可否認性（non-repudiation）	交易雙方不可事後否認其交易的事實
可用性（availability）	確保系統正常運作不中斷服務

五秒自測　維護資料傳輸安全的要件為何？

二、資料傳輸安全的保護 103 105 106 112

1. **資料加／解密**：將資料加密成無法閱讀的格式，再進行傳送，接收者收到後再加以解密，以回復成原資料內容。



   a. 資料加密的目的是為了符合**資料隱密性**的要求，避免被他人窺知。
   b. 資料加／解密是使用特定的演算法，將明文轉換成密文。
   c. 資料加／解密的演算法再搭配**金鑰**的使用，可強化加密的安全性。

2. **金鑰**（key）：由一串文字或數字組成的密碼，**金鑰的長度（單位為bit）越長，安全性越高**。金鑰分為兩種，一種是**單一金鑰**，另一種是一對**私鑰與公鑰**。
   a. 單一金鑰：每次傳輸資料時由程式（如瀏覽器）自動產生，產生的金鑰可用在**對稱式加解密**。
   b. 私鑰與公鑰：一般是由認證中心（CA）同時產生，並封存於**數位憑證**中，常用在**非對稱式加解密**。

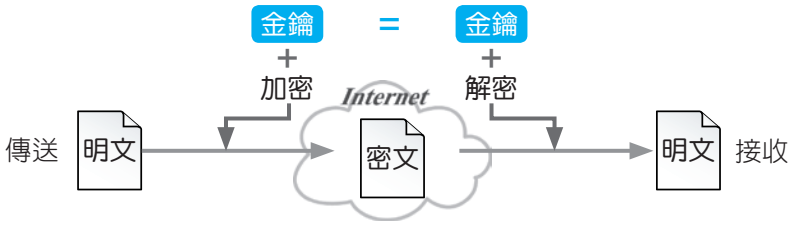
c. **公鑰可公開給任何人取得，私鑰則需私密保管**。兩者間有**配對**關係，使用私鑰加密的資料只能用對應的公鑰解密；同樣地，使用公鑰加密的資料也只能用對應的私鑰解密。

d. **認證中心**是具有公信力的第三團體（如內政部憑證管理中心），負責核發及管理數位憑證。

3. 加／解密的技術：

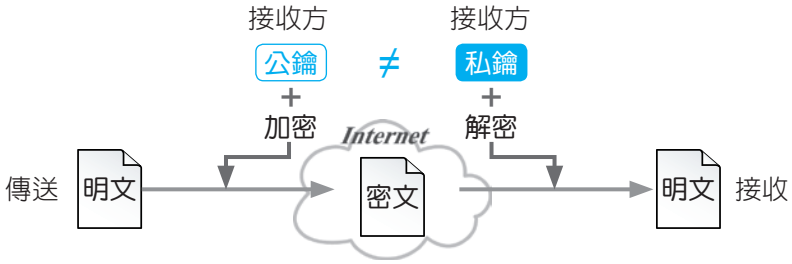
a. **對稱式加／解密**：又稱私密金鑰加密法，傳送者與接收者約定使用**同一把**金鑰加、解密。

解題密技 「對稱式」是指雙方使用同一把金鑰加／解密。



b. **非對稱式加／解密**：又稱公開金鑰加密法，使用一對**公鑰**與**私鑰**來進行加／解密，運算過程較複雜，但安全性較高。**秘密通訊**（secret communication）即是採用此種技術。

解題密技 「非對稱式」是指雙方使用不同金鑰，一般是使用接收方的公鑰與私鑰加／解密。



c. 比較：

比較項目	對稱式加／解密	非對稱式加／解密
安全性	較低	較高
用相同金鑰	是	否
金鑰可公開	否	公鑰可，私鑰不可
運算速度	較快	較慢
應用	較長的資料，如E-Mail	較短的資料，如數位簽章
常見的演算法	AES、DES	RSA

4. **雜湊函數**（hash function）：特定的資料轉換規則，資料透過雜湊函數轉換，可產生固定長度的**訊息摘要**（Message Digest）。

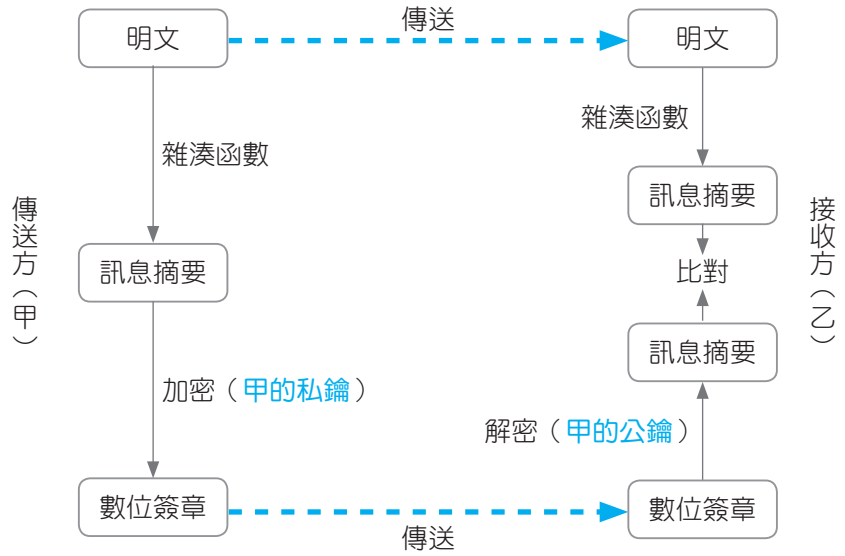
a. 雜湊函數不能讓人由訊息摘要反推出原資料內容。

b. 不同資料透過雜湊函數的轉換，不可產生出同樣的訊息摘要。

5. **數位簽章**（digital signature）：具有簽名效力，這種技術**可符合資料完整、身分驗證、不可否認等安全要件**。其運作方式如下：

   a. **產生數位簽章**：傳送者利用雜湊函數將資料運算後產生訊息摘要，再以傳送者的**私鑰**進行加密，以產生數位簽章，然後連同資料一起傳送給接收者。

   b. **比對訊息摘要**：接收者收到資料後，利用同一雜湊函數產生另一個訊息摘要，並使用傳送者的**公鑰**將原數位簽章解密，以便比對兩個訊息摘要內容是否一致。



   c. 為推動電子簽章之普及運用，確保電子簽章之安全，我國制定有**電子簽章法**，並明定數位簽章屬於電子簽章的一種，因此數位簽章具有等同書面簽章的法律效力。

   d. 電子郵件、PDF檔、Word文件…等檔案可加入數位簽章，以證明傳送者身分。加入數位簽章後，文件檔案會顯示  圖示。

   e. 採用非對稱式加密法技術的秘密通訊與數位簽章之比較：

比較項目	秘密通訊	數位簽章
用途	確保資料在傳輸過程中不被未經授權者窺知	證明自己的身分，等同書面簽章，僅本人可加密
金鑰擁有者	接收方	傳送方
加密	公鑰	私鑰
解密	私鑰	公鑰
可確保	機密性	完整性、認證性、不可否認性

6. **數位憑證**：內含持有人的姓名、公鑰、私鑰、雜湊函數…等簽章驗證資料（如網路報稅用的自然人憑證、網路下單用的金融憑證），可用來辨識持有人身分，有了它，才能用來產生數位簽章。數位憑證有一定期限，需定期申請更換。

有「背」無患

1. 「非對稱式加／解密技術」一般是使用接收方的公鑰加密，再以接收方的私鑰解密，以達到避免資料被窺知的目的（如祕密通訊技術就是使用此種方法來保護資料）。若反過來使用傳送方的私鑰加密、再以傳送方的公鑰解密，則可達到證明資料確實為傳送方傳送的目的（因私鑰僅本人持有）。
2. 「非對稱式加／解密技術」也可做到不可否認傳送，加／解密順序為：①接收方公鑰加密、②傳送方私鑰加密、③傳送方公鑰解密、④接收方私鑰解密。其中①、②順序若對調，③、④順序也要對調。
3. 數位簽章技術就是使用傳送方的私鑰對訊息摘要加密，再以其公鑰解密，故可證明傳送方身分。
4. 由上頁圖可看出，數位簽章技術並未將明文加密，因此在實務上應用數位簽章時，明文在傳送前，多半會先另外加密，再傳送給接收方，避免資料外洩。

得分區塊練

( )1. 下列保護資訊安全的技術，何者主要是將檔案資料做特殊編碼？
(A)資料加密 (B)密碼 (C)網路認證 (D)防毒軟體。

( )2. 下列何者不是「數位簽名」的功能之一？
(A)證明了信的來源 (B)做為信件分類之用
(C)可檢測信件是否遭竄改 (D)發信人無法否認曾發過信。 [丙級軟體應用]

( )3. 有關數位簽章（digital signature）的敘述，下列何者錯誤？
(A)可達到網路安全目標的不可否認性（non-repudiation）
(B)可達到網路安全目標的資料完整性（integrity）
(C)利用雜湊函數（hash function）將欲傳送的資料加以運算，以產生訊息摘要（message digest）
(D)採用對稱式加密法（symmetric encryption）。

( )4. 為了避免交易雙方否認已送出或已接收到的資料，會透過一套機制驗證雙方是否有收到或發出訊息，這種原則稱為下列哪一項？
(A)不可否認性 (B)完整性 (C)隱私性 (D)認證性。 [技藝競賽]

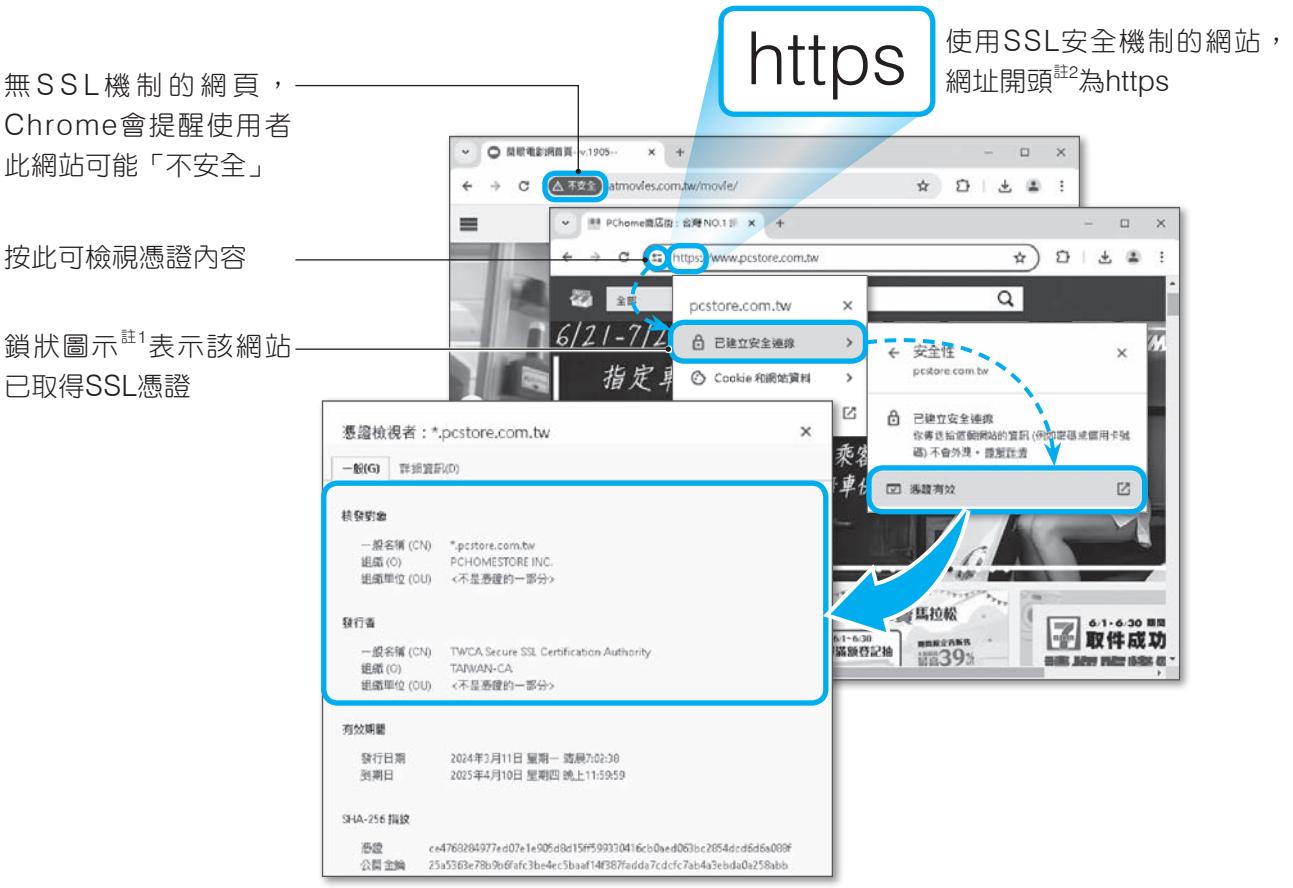
( )5. 為了要保護資料傳輸的安全，防止資料被人窺視，使用下列哪一種方式最佳？
(A)將資料備份（Backup） (B)將資料做好編號及命名
(C)將資料加密（Encryption） (D)將資料檔案的屬性設成隱藏（Hiding）。

( )6. 公開金鑰密碼系統中，要讓資料傳送時以亂碼呈現，並且傳送者無法否認其傳送行為，需要使用哪兩個金鑰同時加密才能達成？
(A)傳送者及接收者的私鑰 (B)傳送者及接收者的公鑰
(C)接收者的私鑰及傳送者的公鑰 (D)接收者的公鑰及傳送者的私鑰。 [丙級軟體應用]

13-2 電子商務常見的安全機制

一、安全資料傳輸層（Secure Socket Layer, SSL） 104 108 111 114

1. Netscape公司為了保護網路上資料傳輸安全而制定的一種安全機制。
2. SSL可用來確認商家身分，確保交易資料的隱密性及完整性。
3. 登錄資料（如註冊、訂單資料）的網頁，大多採用SSL安全機制來保護。
4. 使用SSL機制，網站業者須先向認證中心（CA）申請SSL數位憑證，再將它安裝至網站伺服器中，才能保護資料在傳輸過程中不被他人窺知或篡改。
5. 使用SSL安全機制保護的網頁，瀏覽器會出現**鎖狀圖示**，且網址中的通訊協定為**https**。



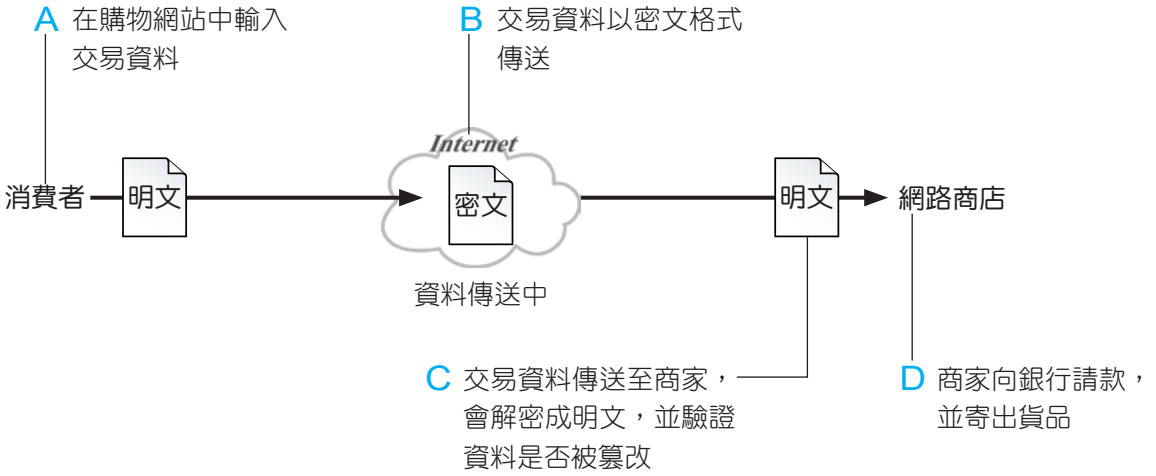
註1：不同的瀏覽器（如Chrome、Firefox、Microsoft Edge）或版本，鎖狀的圖示與位置可能會有差異。

註2：有些瀏覽器（如Chrome）會將網址開頭的http://或https://隱藏，使用者雙按**網址列**即會顯示完整的網址。

6. 使用SSL安全機制保護的網站，其首頁通常會置入SSL標章。如『PChome 24h購物』網站的首頁，即有如下的標章。按此類標章可檢視網站的名稱、憑證有效期限等資料。

Norton SECURED powered by Symantec　VeriSign Secured　McAfee SECURE　Certification Authorities WebTrust Baseline　ePKI Authentic Site

7. 使用SSL安全機制的交易流程：



8. **傳輸層保全（Transport Layer Security, TLS）**：以SSL v3.0為基礎改良而來，目前國外有許多金融機構將TLS應用在電子郵件傳送的安全保護。

有肖無患

- 數位憑證（Digital Certificate）：可用來證明持有者的身分，並確保資料在傳輸過程中不被他人窺知或篡改，常見的憑證種類如下：

憑證種類	應用	申請單位
自然人憑證（可視為網路身分證）	網路報稅、申辦戶籍謄本、查詢個人健保資料	內政部憑證管理中心、戶政事務所
工商憑證	營利事業所得稅申報、政府採購	經濟部工商憑證管理中心
金融憑證	網路下單、網路銀行轉帳	經濟部核准的金融機構（如銀行）

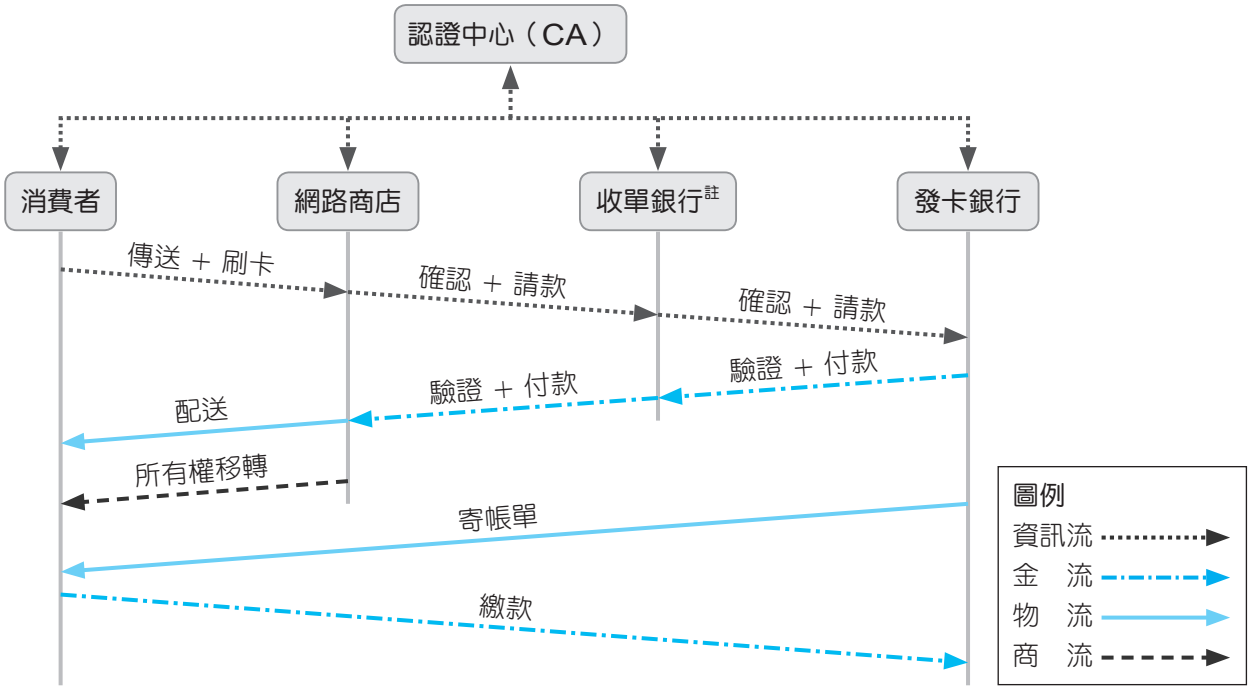
得分區塊練

(　)1. HTTPS與HTTP通訊協定兩者差異為何？
(A)HTTPS加強執行速度
(B)HTTPS加強安全性
(C)HTTPS加強資料傳輸量
(D)HTTPS可允許更多人同時上網使用。 [技藝競賽]

(　)2. 在網路銀行網站的首頁，常可看到SSL標章，請問按下標章後可瀏覽下列哪一項資訊？
(A)該公司的當季營業額 (B)該網站的名稱、憑證的有效期限
(C)該網站是否為優良網站 (D)該網站是否為公營的單位。

二、安全電子交易（Secure Electronic Transaction, SET） 103 104 111

1. VISA、MasterCard、IBM、Microsoft、Netscape等公司共同制定的安全機制。
2. SET可用來保護在網路上使用**信用卡交易的安全**，確保交易資料的隱密性、完整性、身分的識別、交易的不可否認性。
3. 要使用SET機制，網路業者與消費者都必須申請相關的數位憑證，且消費者需安裝電子錢包軟體。
4. SET機制交易流程：



註：收單銀行是與網路商店合作的銀行，負責向發卡銀行驗證消費者的信用卡資料，以協助網路商店完成電子商務的交易。

5. SSL與SET安全機制的比較：

比較項目 \ 安全機制	SSL	SET
資料傳輸的隱密性	✓	✓
資料的完整性	✓	✓
身分的識別	只能驗證商家身分	可驗證商家、消費者、發卡／收單銀行的身分
交易的不可否認性		✓
安全等級	較低	較高
應用領域	網路資料傳輸、信用卡線上交易	信用卡線上交易

→ 結論：SSL申請程序簡易（只要商家申請憑證即可使用），但只能驗證商家身分，無法避免盜刷或否認交易的行為，安全等級較低。SET申請程序複雜（商家和使用者皆需申請憑證才可使用），但其安全等級較高。

6. 線上交易的安全性，是電子商務賴以發展的基礎。

有背無患

3D-Secure是SET的簡化版，它是透過消費者向發卡銀行申請取得識別身分的密碼，來避免信用卡被盜刷。消費者在線上刷卡時，還必須輸入此組密碼，來進行身分確認。華南銀行、中國信託等皆提供有此種安全驗證機制。

得分區塊練

(　)1. 由Visa與Master兩信用卡組織所提出的一種應用在網際網路上，以信用卡為基礎的電子付費系統規範，為下列哪一項？
(A)EDI (B)SSL (C)SET (D)VAN。 [技藝競賽]

(　)2. 下列關於電子商務SET之描述，何者為真？
(A)病毒防護 (B)文書處理
(C)資料備份 (D)為一種通訊協定，用於信用卡交易。

(　)3. 下列有關SSL與SET的敘述，何者有誤？
(A)SET機制可避免買方事後否認交易的事實
(B)SSL機制可確認賣方身分
(C)欲使用SET機制，買賣雙方都必須具有憑證
(D)SSL提供的安全等級較SET高。

13-3 電子商務常見的觸法行為

1. 在未經他人授權下，擅自將他人著作收錄於線上資料庫中
2. 網頁內容使用未經授權的文字、照片、音樂、動畫等
   →商品編號、售價等不具原創性的資料，不需授權即可使用

（1、2 → 侵犯智慧財產權）

3. 盜賣個人資料
4. 蒐集、販售電子郵件帳號
5. 販售儲存在瀏覽者電腦中記錄登入帳號、瀏覽訊息等資料的**cookie**檔案

（3、4、5 → 侵犯隱私權）

6. 使用他人已註冊的商標
7. 在網域名稱中，使用他人商標中的文字

（6、7 → 侵犯商標權）

有背無患

- 網路商家保護消費者隱私權的常見做法：
  - » 使用安全機制保護個人資料的隱密性，避免資料被窺視、不當使用。
  - » 告知消費者個人資料的使用原則，不將個人資料使用於其它用途。
  - » 賦予消費者選擇只提供部分個人資料的權利。
- 網路蟑螂：是指搶先登記一些公司、品牌名稱或人名等網域名稱，意圖日後再以高價售出的不法人士。
  - 例 某網路蟑螂搶先註冊取得麥當勞網域名稱，麥當勞公司耗費巨資購回自家的網域名稱使用權。

得分區塊練

(　)1. 下列關於「對客戶資料的保護」，何者正確？
(A)予以保密　(B)提供給關係企業做行銷
(C)告知同事給予參考　(D)讓其他客戶瞭解。

(　)2. 小優網路服飾商店所使用的各種衣服資料中，哪一項需要取得原廠商的授權？
(A)原廠的商品品名　(B)原廠的價格
(C)原廠的照片　(D)原廠的貨號。

滿分晉級

情境素養題

▲ 閱讀下文，回答第1至2題：

電子商務詐騙頻傳，讓許多人對於電子商務安全機制的討論度提高不少，以下是幾位同學在討論電子商務安全機制的發言：

- 天立：「維護資料傳輸安全的要件有隱密性、完整性、認證性、不可否認性、可用性。」
- 崴宇：「金鑰的長度越長，安全性越高；金鑰分成2種，一種是單一金鑰，另一種是私鑰與公鑰。」
- 吉米：「對稱式加／解密又稱私密金鑰加密法，傳送者與接收者約定使用同一把金鑰加、解密。」
- 小安：「非對稱式加／解密法是使用一對公鑰與私鑰來進行加／解密，過程較為複雜。」

( )1. 請問上述情境中，哪些同學敘述有關電子安全機制的內容是錯誤的？
(A)吉米 (B)天立、吉米 (C)天立、崴宇、吉米 (D)四位同學的觀念皆正確。 [13-1]

( )2. 下列哪一種加密演算法屬於小安所說的非對稱式加／解密技術？
(A)AES (B)DES (C)DOS (D)RSA。 [13-1]

( )3. 展文在購物網站，以信用卡付款方式購買一台單眼相機，當他在填寫交易資料時，發現該網站的網址開頭為https。請依據上述，判斷該網站是使用下列哪一項安全機制，來確保線上交易的安全？
(A)SET (B)Wi-Fi (C)LTE (D)SSL。 [13-2]

( )4. 家中開設炸雞店的曉惠，透過下列做法希望能利用網際網路來增加炸雞的銷售量，請問哪一項做法最有可能觸法？
(A)拍攝店內環境的圖片，上傳至自己的網路商店
(B)在網頁中標示銷售的炸雞產品名稱及金額
(C)註冊使用含有肯德基（KFC）字樣的網域名稱（如KFC_NO1），方便網友記憶
(D)提供炸雞折價券供網友下載。 [13-3]

( )5. 小明想上網拍賣禰豆子的公仔，他直接到網友的拍賣網頁下載同一公仔產品的照片來使用。根據上述，以下何者正確？
(A)小明可任意使用，因為照片不屬於著作品
(B)小明應取得授權，因為照片已被他人先公開於網路上
(C)小明可任意使用，因為產品照片不具原創性
(D)小明應取得授權，因為網頁上的照片屬於著作權保護的範圍。 [13-3]

精選試題

13-1

( )1. 將要傳送的文件先透過雜湊函數運算後產生訊息摘要，並利用傳送者的私鑰將摘要加密後連同文件一起傳送，是屬於下列哪一種資訊安全的防護策略？
(A)數位簽章 (B)防火牆 (C)防毒軟體 (D)密碼管制。

( )2. 能確保資料不被未經授權者取得的管理方法，具有下列何種資訊安全特性？
(A)機密性（Confidentiality）
(B)完整性（Integrity）
(C)友善性（Friendliness）
(D)不可否認性（Non-repudiation）。

( )3. 在公開金鑰密碼系統中，A將機密資料傳給B，B應該使用下列哪一項金鑰來解密？
(A)A的公開金鑰 (B)A的私密金鑰 (C)B的公開金鑰 (D)B的私密金鑰。

( )4. 在寄發電子郵件時，可以使用下列哪一項技術讓電子郵件的收信人確認寄件人的身分，以確認郵件來源，並避免第三人冒名傳遞不實訊息？
(A)郵件加密 (B)開啟標幟 (C)數位簽章 (D)防火牆。

( )5. 以下敘述何者正確？
(A)對稱式加密法有不同的加密與解密金鑰
(B)AES是對稱式加密法
(C)RSA是對稱式加密法
(D)DES是非對稱式加密法。

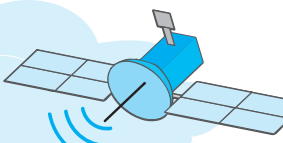
( )6. 為了避免資料傳輸時被竊取或外洩，通常採用何種保護措施？
(A)將資料壓縮 (B)將資料加密
(C)對資料加簽章碼 (D)對資料加檢查碼。

( )7. 有關對稱式加／解密法的敘述，下列何者正確？
(A)需使用到2把金鑰
(B)傳送方需用接收方的公鑰將資料加密
(C)RSA是一種對稱式加／解密法
(D)加／解密速度通常比非對稱式加／解密法快。

( )8. 為了強化加密的安全性，在實務上，加密演算法通常會搭配「金鑰」使用。請問金鑰是指？
(A)一把鑰匙
(B)一個鑰匙形狀的隨身碟
(C)一種可以證明身分的數位圖像
(D)一串文字或數字組成的密碼。

( )9. 非對稱式加解密技術中，「非對稱」是指下列何者非對稱？
(A)使用的金鑰 (B)加密演算法 (C)明文 (D)密文。

( )10. 有關網路安全技術的敘述，下列何者錯誤？
(A)平均而言，RSA演算法處理速率快過DES演算法
(B)「加密與解密使用兩支不同金鑰，且這兩支金鑰是成對的」是非對稱式加／解密法的特色
(C)DES是一種對稱式加／解密法
(D)SET使用非對稱式加／解密法，所以可確認交易者身分。



( )11. 實務上，在傳送較長的資料（如E-Mail）時，通常是使用對稱式加密法來進行加密，請問主要原因為何？
(A)對稱式加密法安全性較高
(B)對稱式加密法可證明寄送者身分
(C)對稱式加密法加密速度較快
(D)對稱式加密法可確保資料完整性。

( )12. 將資料經過「雜湊函數」的運算，可以產生下列何者？
(A)訊息摘要 (B)數位簽章 (C)金鑰 (D)明文。

( )13. 下列保護資料傳輸安全常用的技術或機制中，何者具有檢查資料完整性的功能？
(A)資料加密 (B)資料解密 (C)數位簽章 (D)防火牆。

( )14. 數位簽章的運作流程中，不包含下列哪一項？
(A)利用雜湊函數產生訊息摘要
(B)用傳送者的公鑰將訊息摘要加密
(C)用傳送者的公鑰將訊息摘要解密
(D)比對訊息摘要。

( )15. 利用雜湊函數技術，可檢查透過網路傳輸的資料是否遭到篡改，請問這種技術是用來確保下列哪一項網路傳輸安全的要件？
(A)身分驗證 (B)資料隱密 (C)不可否認 (D)資料完整。

( )16. 數位簽章的技術，必須要使用到下列哪些金鑰？
(A)接收方的公鑰與私鑰
(B)傳送方的公鑰與私鑰
(C)傳送方的公鑰與接收方的私鑰
(D)傳送方的私鑰與接收方的公鑰。

( )17. 在數位簽章的技術中，數位簽章是如何產生的？
(A)將明文用傳送方的公鑰加密
(B)將訊息摘要以傳送方的私鑰加密
(C)將明文以接收方的公鑰加密
(D)將訊息摘要以接收方的私鑰加密。

( )18. 為什麼數位簽章可以證明傳送者的身分？
(A)訊息摘要中包含傳送方姓名
(B)傳送方使用自己的公鑰加密
(C)傳送方使用自己的私鑰加密
(D)接收方可用傳送方的私鑰解密。

( )19. 若要保護線上交易的資料隱密性，下列哪一種作法最有效？
(A)將資料加密 (B)架設防火牆
(C)安裝最新版本的瀏覽器 (D)定期備份資料。

( )20. 好的雜湊函數，必須具有下列哪一項特性？
(A)能證明傳送者的身分
(B)所產生的訊息摘要長度不固定
(C)同樣的一段文字會產生不同的訊息摘要
(D)不能由訊息摘要反推出原資料內容。

( )21. 在公開金鑰密碼系統中，有關公鑰與私鑰的說明，何者錯誤？
(A)用公鑰加密的資料，可再用公鑰解密
(B)我們可向認證中心查詢公鑰的持有人
(C)必須確保不能由公鑰來反推出私鑰的內容
(D)公鑰與私鑰的內容不相同，必須配對使用。

( )22. 在對稱式加／解密技術下，有關金鑰的說明，下列何者錯誤？
(A)金鑰只能產生一次，產生後必須永久保存該金鑰
(B)每次產生的金鑰內容會不一樣
(C)資料的傳送方與接收方都是使用同一把金鑰
(D)資料可用同一把金鑰加密與解密。

13-2 ( )23. 下列何者為常用之網路購物安全防護機制？
(A)SSL (B)POS (C)ATM (D)CAM。

( )24. SET是一個用來保護信用卡持卡人在網際網路消費的開放式規格，透過密碼加密技術（Encryption）可確保網路交易，下列何者不是SET所要提供的？
(A)輸入資料的私密性 (B)訊息傳送的完整性
(C)交易雙方的真實性 (D)訊息傳送的轉接性。

( )25. SET是目前公認Internet上的電子交易安全標準，下列哪一公司未參與SET之發展？
(A)IBM (B)Microsoft (C)American Express (D)Visa。

( )26. 在啟用SSL安全機制的安全認證網站上進行交易，下列描述何者是可確保交易安全的？
(A)在交易過程中所傳輸的資料都是被加密的
(B)該網站不會將個人資料外流
(C)該網站的商品價格一定比市價便宜
(D)該網站不會被駭客入侵。 [乙級軟體應用]

( )27. 下列哪一種技術，主要是希望能確保網路上信用卡交易的安全性？
(A)SET (B)SMTP (C)VoIP (D)WAP。 [技藝競賽]

( )28. 下列哪一個敘述是正確的？
(A)SSL是由VISA公司所制定的一種安全機制
(B)SET可以提供交易的不可否認性
(C)SSL的安全等級比SET高
(D)SET只能驗證商家的身分。 [技藝競賽]

13-3 ( )29. 網路商家在登錄產品資料時，引用下列哪些原廠的資料不需取得授權，即可直接使用？
①產品編號 ②產品照片
③產品單價 ④產品功能介紹的文字
(A)①② (B)①③ (C)②④ (D)①②③。

( )30. 達禮想開設網路書店，下列哪一項做法最沒有侵權之虞？
(A)以「yahoobook」（雅虎書）做為網域名稱
(B)列出銷售之書籍名單
(C)自行將他人出版書籍內容數位化
(D)借用博客來網路書店之商標。

統測試題

( )1. 在網路安全的領域中，「資料完整性（Integrity）」常用來評估資料的接收者所收到的資料是沒有被篡改的。下列哪一個工具或技術，最適合用來確保在網路間交換資料的完整性？
(A)使用防火牆 (B)使用防毒軟體
(C)利用對稱式加密技術 (D)利用數位簽章技術。 [103商管群]

( )2. 在網路交易過程中，有所謂公開金鑰（public key）和私密金鑰（private key），下列有關公開金鑰和私密金鑰的敘述，何者錯誤？
(A)兩者都是由一連串的數字組成
(B)發送方將資料發送給接收方前，先用接收方的公開金鑰將資料加密
(C)在同一演算法下，金鑰越長，加密的強度就越強
(D)公開金鑰和私密金鑰分別打造，彼此沒有配對關係。 [103工管類]

( )3. 小明想要在「GoodBuy」網站刷卡購買一台攝影機，請問下列哪一項技術可以用來提高網站上刷卡交易的安全性？
(A)LTE（Long Term Evolution）
(B)WiMax（Worldwide Interoperability for Microwave Access）
(C)SET（Secure Electronic Transaction）
(D)SRAM（Static RAM）。 [103資電類]

( )4. 下列敘述何者錯誤？
(A)SET安全機制需要憑證管理中心驗證憑證
(B)以https開頭的網頁就是有採用SET安全機制的網頁
(C)SSL採用公開金鑰辨識對方的身份
(D)SET的安全性比SSL高。 [104商管群]

( )5. 下列何者為常見的網路連線安全機制？
(A)DNS（domain name system）
(B)DHCP（dynamic host configuration protocol）
(C)SSL（secure socket layer）
(D)SIP（session initiation protocol）。 [104工管類]

( )6. 某網站的網址為「https://www.ezuniv.com.tw」，這表示該網站使用了何種網路安全機制？
(A)SET（Secure Electronic Transaction）
(B)SSL（Secure Socket Layer）
(C)SATA（Serial Advanced Technology Attachment）
(D)防火牆（Firewall）。 [104資電類]

( )7. 使用者甲與使用者乙約定藉由非對稱加密（asymmetric encryption）進行溝通，假設使用者甲先以甲的私密金鑰（private key）加密原始訊息，再以乙的公開金鑰（public key）加密前一步驟所得之加密訊息，並將所得之結果傳送給使用者乙，則使用者乙要如何才能讀取原始訊息？
(A)先以甲的公開金鑰解密，再以乙的私密金鑰解密
(B)先以乙的公開金鑰解密，再以甲的私密金鑰解密
(C)先以甲的私密金鑰解密，再以乙的公開金鑰解密
(D)先以乙的私密金鑰解密，再以甲的公開金鑰解密。 [105商管群]

( )8. 對於數位簽章的敘述，下列何者錯誤？
(A)傳送前透過雜湊函數演算法，將資料先產生訊息摘要
(B)以傳送方的私鑰將訊息摘要進行加密產生簽章，再將文件與簽章同時傳送
(C)收到資料後，使用接收方的公鑰對數位簽章進行運算，再比對訊息摘要驗證簽章的正確性
(D)加密和解密運算，都是使用非對稱式加密演算法。 [106商管群]

( )9. 具SSL（Secure Sockets Layer）規範的網站與下列哪類URL（Uniform Resource Locator）最相關？
(A)http:// (B)httpd:// (C)httpp:// (D)https://。 [106工管類]

( )10. 下列敘述何者不正確？
(A)防火牆是一種可以過濾資料來源的網路安全防護設施
(B)偽造銀行網站以騙取使用者帳號和密碼的行為稱之為網路釣魚
(C)使用HTTP協定在網路上傳輸的資料會進行加密，確保使用者連線安全
(D)阻斷服務（DoS）攻擊是藉由不斷發送大量訊息，造成被攻擊網站癱瘓而無法提供服務的攻擊手法。 [107工管類]

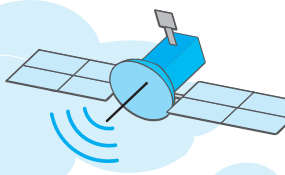
( )11. 某URL網址開頭為https://這表示該網站使用了哪個安全規範？
(A)VPN（Virtual Private Network）
(B)SSL（Secure Sockets Layer）
(C)SATA（Serial Advanced Technology Attachment）
(D)RSS（Really Simple Syndication）。 [107資電類]

( )12. 有關自然人憑證卡的敘述，下列何者錯誤？
(A)由財政部核發
(B)用來證明個人在網路上的身分
(C)使用該憑證卡可進行網路報稅
(D)經由網路及該憑證卡可查詢個人健保資料。 [108商管群]

( )13. 在電子商務交易的安全機制中，下列敘述何者不正確？
(A)SSL協定保護交易資料在網路傳輸過程中不被他人窺知
(B)SET協定在於保障電子交易的安全，客戶端需有電子錢包
(C)消費者透過SSL或SET交易均需事先取得數位憑證
(D)SSL的英文全名為Secure Socket Layer。 [108商管群]

( )14. 有關電子商務安全機制SSL與SET的敘述，下列何者正確？
(A)兩種機制均可達到交易的機密性
(B)兩種機制均為信用卡支付標準協定
(C)兩種機制中，消費者與店家均需要憑證作身分識別
(D)兩種機制均可達到消費者與店家雙方交易的不可否認性。 [111商管群]

( )15. 關於加解密技術的敘述，下列何者正確？
(A)數位簽章僅達到不可否認性與資料來源辨識性
(B)數位簽章除利用對稱式加密法，亦可利用公開金鑰加密法實現
(C)公開金鑰加密法傳送方利用接收方的公鑰將明文加密，接收方收到密文後使用接收方私鑰可解密
(D)公開金鑰加密法傳送方利用自己的私鑰將明文做數位簽章，接收方收到簽章後使用自己的公鑰可解開簽章。 [112商管群]



( )16. 為了保護網路資料傳輸安全，若網站回應網頁的網址是以https為開頭，且可以正常連線的情況下，這代表該網站啟動了哪一種安全機制？
(A)安全外殼（Secure Shell, SSH）
(B)安全電子交易（Secure Electronic Transaction, SET）
(C)安全檔案傳輸協定（Secure File Transfer Protocol, SFTP）
(D)安全通道層（Secure Sockets Layer, SSL）/傳輸層安全性（Transport Layer Security, TLS）。 [113工管類]

( )17. 網址「https://www.tcte.edu.tw」中的英文字母「s」可用下列何者技術來完成？
(A)SSD（solid state disk）
(B)SSL（secure sockets layer）
(C)SKC（secret key cryptography）
(D)SET（secure electronic transaction）。 [114商管群]

( )18. 使用瀏覽器以超文字安全傳輸通訊協定（HyperText Transfer Protocol Secure, HTTPS）瀏覽網站時，下列敘述何者正確？
(A)HTTPS在傳輸數據時僅有針對網頁內文字資訊加密
(B)HTTPS通訊時需要瀏覽器與網站都支援加密的協定
(C)HTTPS不涉及任何加密技術，利用防火牆達成安全傳輸
(D)沒有數位憑證的HTTPS網站可以安心連線，無安全隱患。 [114工管類]

NOTE