

試卷範圍：1002Ch3-3 班級：\_\_\_\_\_ 姓名：\_\_\_\_\_ 座號：\_\_\_\_\_

一、選擇題 共 41 題 每題 0 分

01. 要確保資料在傳輸過程中，不會被人從中竄改，確保送出和收到的內容完全一致，必須注意下列哪一事項？ (A)不可否認性 (B)完整性 (C)隱私性 (D)認證性
02. 可過濾、監視網路上的封包與通聯狀況，達到保護電腦的軟體為何？ (A)防毒軟體 (B)防火牆 (C)瀏覽器 (D)即時通
03. 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
04. 下列哪一種技術，不論加密或解密的金鑰，都使用同一把金鑰？ (A)非對稱加密 (B)對稱加密 (C)遠端存取限制 (D)入侵偵測
05. 經過加密演算法處理後的資料稱為 (A)甲骨文 (B)明文 (C)密文 (D)散文
06. 憑證中心(CA)在電子商務中扮演什麼角色？ (A)網際網路身分確認者 (B)網路銀行 (C)特約商家 (D)網際網路服務提供者
07. 下列何者是數位簽章的應用範圍？ (A)軟體認證 (B)PDF 文件檔案 (C)電子郵件 (D)以上皆是
08. 下列何者是兩大國際信用卡發卡機構 Visa 及 MasterCard 聯合制定的網路信用卡安全交易標準？ (A)私人通訊技術(PCT)協定 (B)安全超文字傳輸協定(S-HTTP) (C)電子佈告欄(BBS)傳輸協定 (D)安全電子交易(SET)協定
09. 下列何者不是一個完整的安全電子交易(SET)架構所包括的成員之一？ (A)電子錢包 (B)商店伺服器 (C)商品轉運站 (D)認證中心
10. 網站的網址以 https://開始，表示該網站具有何種機制？ (A)使用 SET 安全機制 (B)使用 SSL 安全機制 (C)使用 small Business 機制 (D)使用 XOOPS 架設機制
11. 下列哪一種技術，可以建立安全通道，確保資料在網路的傳輸過程不會被人竊聽？ (A)防火牆 (B)入侵偵測系統 (C)虛擬專用網路 (D)虛擬主機
12. 何者是錯誤的系統安全措施？ (A)系統操作者統一保管密碼 (B)資料加密 (C)密碼變更 (D)公佈之電子文件設定成唯讀檔
13. 關於「金鑰加密技術」之敘述中，下列何者不正確？ (A)非對稱加密技術的金鑰，可分為公開金鑰與私密金鑰 (B)對稱加密技術的加密、解密速度很快 (C)對稱加密技術不論加密或解密，都只用同一把鑰匙 (D)使用非對稱加密技術，不論加密或解密，都只用同一把鑰匙
14. 安全電子交易(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
15. 建民想要透過家中的電腦存取公司內部的網路資料，透過哪一種技術進行資料傳輸，可保障資料不會被人竊取？ (A)HTTP (B)VPN (C)FTP (D)BT
16. 下列何者有運用到加密技術？ (A)虛擬專用網路(VPN) (B)數位簽章(Digital Signature) (C)安全通道層(SSL) (D)以上皆是
17. 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 (A)不可否認性 (B)完整性 (C)隱私性 (D)認證性

18. 爲了避免類似 911 事件的重演，如果你是一家投資公司的老闆，應採取什麼措施來保護重要的交易資料？ (A)將資料放到保險箱 (B)隨身攜帶資料 (C)將備份資料分散到不同地點存放 (D)將資料用紙本記錄
19. 爲了避免人爲所造成的網路安全損害，下列哪項不是人員控制的要素？ (A)身份辨識系統 (B)溫、濕度控制 (C)密碼管制 (D)網路安全訓練
20. 下列何者是錯誤的系統安全措施？ (A)將資料備份並分別存放於不同位置 (B)對員工進行教育訓練，熟悉各種程序性安全措施 (C)使用 UPS 穩定電壓設備，避免斷電意外 (D)統一使用一個密碼管理所有系統，避免密碼太多管理不易
21. 光良架設一個網路購物網站，老是遭到駭客的網路攻擊，爲了防堵未經授權的使用者隨意存取內部資料，可以使用何種網路設備？ (A)集線器 (B)光纖數據機 (C)防火牆 (D)擋土牆
22. 未經過加密處理的資料內容，稱爲 (A)電文 (B)散文 (C)明文 (D)條文
23. 在網路上傳輸信用卡的資料，可以使用何種技術，將內容變成不易解讀的亂碼，以避免被人從中竊取？ (A)解壓縮 (B)分段傳送 (C)加密 (D)明文傳送
24. 要解開加密的資料前必須先取得下列何者才能順利解密？ (A)明文 (B)金鑰 (C)演算法 (D)密文
25. 添賓想要設定資料加密的金鑰，選擇何種長度的金鑰，能夠提供較佳的安全性，較不易被破解？ (A)256 bits (B)2048 bits (C)512 bits (D)1024 bits
26. 下列敘述何者指的是對稱加密？ (A)加密與解密使用不同的金鑰 (B)加密與解密後內的內容完全一致 (C)加密與解密的時間一致 (D)加密與解密使用同一把金鑰
27. 小菁使用非對稱加密技術進行資料加密，若對方收到小菁用私鑰加密後的資料，要如何進行解密？ (A)使用小菁上傳的私鑰 (B)使用小菁上傳的公鑰 (C)用自己生成的私鑰 (D)以上皆否
28. 要避免上傳的金鑰被駭客冒用，需透過何種機構來驗證使用者的身分？ (A)客服中心 (B)資料中心 (C)認證機構 (D)交換中心
29. 下列何者是常用的網路安全防護機制？ (A)SSL (B)POS (C)RFID (D)ATM
30. 小茜要在某個拍賣網站進行帳號登錄，發現該網頁的開頭是「https」，這表示該網站支援何種功能？ (A)FTP (B)SSL (C)MSN (D)VPN
31. 林經理想傳一份文件給董事長簽核，擔心傳送過程會被人竄改內容，可用什麼方式來驗證文件內容是否有遭到竄改？ (A)郵件附件 (B)數位圖檔 (C)數位典藏 (D)數位簽章
32. 孫排長承辦民間的招標業務，擔心重要資料透過網路傳送容易被人從中竊取，應建議連上使用何種功能的網路設備，才能防止洩密？ (A)CNN (B)VPN (C)MSN (D)DHCP
33. 下列何者不是應用在電子商務上的加密保護技術？ (A)XML (B)SET (C)TLS (D)SSL
34. 下列何者是兩大信用卡發卡機構 Visa 及 Master Card 聯合制定的網路信用卡安全交易標準，負責維護網路上的交易安全性？ (A)HTTPS (B)SSL (C)VPN (D)SET
35. 某個網站的 URL 開始爲 https://，這代表該網站使用何種安全機制？ (A)SAT (B)SAP (C)SET (D)SSL
36. 蘋果公司的執行長想透過電子郵件傳送 iPad 2 的採購清單給鴻海公司，他擔心採購清單會被人動手腳，可以利用哪種技術防止內容被竄改？ (A)數位典藏 (B)數位簽章 (C)

數位分析 (D)數位壓縮

37. 下列何者有使用到金鑰加密的技術？ (A)MAC 位址過濾 (B)禁用 Cookie (C)網域名稱轉址 (D)SSL
38. 志鴻經營購物網站，發現顧客在傳送訂單時容易被駭客竊取信用卡資料，他可以使用何種安全機制進行加密保護？ (A)RFID (B)HTTP (C)BBS (D)SSL
39. 羅剛要從國外傳報價單給總公司，他擔心在網路傳送的過程，會被人竊取，可以使用以下何種技術保護機密資料？ (A)RFID (B)VPN (C)FTP (D)HTTP
40. 下列何種網路設備可以提供網路存取控管，防止外人入侵內部網路，並能阻擋內部人員存取未經允許的網站？ (A)防火牆 (B)中繼器 (C)集線器 (D)交換器
41. 下列何者是認證機構，可驗證金鑰與網路使用者的身分？ (A)教育部 (B)中華電信 (C)經濟部 (D)Google

二、填空题 共 18 格 每格 0 分

01. \_\_\_\_\_能根據過濾規則過濾內、外部網路的各種封包，可阻擋未經授權的使用者入侵內部電腦隨意存取資訊。
02. \_\_\_\_\_指的是加密之前的原始資料，未經過任何處理的資訊。
03. \_\_\_\_\_是用來進行加密及解密的資料，是由一組相當長的數字或符號字串所組成的，它的長度通常以位元為單位。
04. 加密處理後的結果稱為\_\_\_\_\_，像是一堆亂碼所組成的內容，若不了解資料解密的方法就無法順利解讀其中的意義。
05. \_\_\_\_\_指的是用來對明文資料進行加密編碼動作的演算法，能使欲保密的資料變成難以解讀的內容。
06. \_\_\_\_\_(Symmetric Encryption)不論是加密或解密的過程，都是使用同一把金鑰來處理。
07. \_\_\_\_\_(Asymmetric Encryption)會產生兩種金鑰，一種稱為\_\_\_\_\_，可以放到網路上供人使用；另一種稱為\_\_\_\_\_由使用者自行保管。
08. \_\_\_\_\_(英文簡稱\_\_\_\_\_ )通常是具有公信力的第三方單位，擔任金鑰管理的把關工作，負責驗證金鑰與使用者的關係。
09. \_\_\_\_\_可用來確認發送者身分及內容，能確定資料來源及交易之不可否認性，達到「保密」及「簽章」的效用。
10. \_\_\_\_\_(英文簡稱\_\_\_\_\_ )是 Netscape 公司推出的網路安全傳輸標準，可提供用戶端與伺服器之間的傳輸安全服務，防範外界的竊聽或竄改訊息。
11. \_\_\_\_\_(英文簡稱\_\_\_\_\_ )是由 VISA 與 MasterCard 兩大信用卡組織提出的規範，被應用在網際網路上以信用卡為基礎的電子付款系統。
12. \_\_\_\_\_(英文簡稱\_\_\_\_\_ )是利用加密技術在網際網路中建構一條安全的通訊管道，能夠防止駭客從中竊取或竄改資料。

三、簡答題 共 2 題 每題 0 分

01. 請將下列英文名詞與正確的敘述配對：

A) UPS      B) IDS      C) ATM      D) TLS      E) Decryption Algorithm

(1) \_\_\_\_\_能提供緊急電力，幫助穩定設備電壓，避免突然地電源中斷造成資料損毀、遺失等意外。

- (2) 網拍得標的買家，可透過\_\_\_\_\_的方式匯款給賣家。
- (3) \_\_\_\_\_能偵測監控網路或系統是否有異常存取活動，並隨時紀錄使用者對網路資源的存取狀。
- (4) \_\_\_\_\_是由 IETF 採用 SSL 規格所發展出來的協定，可用於用戶端與伺服器之間的傳輸安全服務。
- (5) \_\_\_\_\_指的是能進行解密動作的演算法，使加密後的資料能還原成一般人可以解讀的內容。

02. 請將下列電子商務的注意事項對應至符合敘述的名詞。

保護個人隱私資料不會外流出去的機制。	•	•	完整性
驗證雙方是否有收到或發出訊息，避免交易雙方否認。	•	•	認證性
保障資料送出和收到的內容能夠一致。	•	•	隱私性
確認交易雙方的身分，當身分確認無誤時才能進行交易。	•	•	不可否認性
規範使用者存取網路資源的權利與限制。	•	•	存取控制

試卷範圍：1002Ch3-4 班級：\_\_\_\_\_ 姓名：\_\_\_\_\_ 座號：\_\_\_\_\_

一、選擇題 共 2 題 每題 0 分

01. 下列何者是線上拍賣常見的交易模式？ (A)面交 (B)便利超商代收 (C)貨到付款 (D)以上皆是
02. 下列關於網路拍賣的敘述何者錯誤？ (A)合法經營網拍必須有稅籍登記與營業登記 (B)在 Yahoo!拍賣網站刊登商品拍賣，必須收取手續費 (C)只能設定以直購價方式拍賣 (D)業者必須經過身分驗證，方能使買家安心購買

二、填充題 共 2 格 每格 0 分

01. 請任舉二個有提供拍賣服務的網站：\_\_\_\_\_、\_\_\_\_\_。

解答

一、選擇題 共 41 題 每題 0 分

01	B	02	B	03	A	04	B	05	C	06	A	07	D	08	D	09	C	10	B
11	C	12	A	13	D	14	D	15	B	16	D	17	A	18	C	19	B	20	D
21	C	22	C	23	C	24	B	25	B	26	D	27	B	28	C	29	A	30	B
31	D	32	B	33	A	34	D	35	D	36	B	37	D	38	D	39	B	40	A
41	B																		

二、填充題 共 18 格 每格 0 分

- |         |                     |                  |
|---------|---------------------|------------------|
| 01. 防火牆 | 05. 加密演算法           | 09. 數位簽章         |
| 02. 明文  | 06. 對稱加密            | 10. 安全通道層,SSL    |
| 03. 金鑰  | 07. 非對稱加密,公開金鑰,私密金鑰 | 11. 安全電子交易標準,SET |
| 04. 密文  | 08. 認證機構,CA         | 12. 虛擬專用網路,VPN   |

三、簡答題 共 2 題 每題 0 分

01. A、C、B、D、E  
02.

保護個人隱私資料不會外流出去的機制。	●	●	完整性
驗證雙方是否有收到或發出訊息，避免交易雙方否認。	●	●	認證性
保障資料送出和收到的內容能夠一致。	●	●	隱私性
確認交易雙方的身分，當身分確認無誤時才能進行交易。	●	●	不可否認性
規範使用者存取網路資源的權利與限制。	●	●	存取控制

一、選擇題 共 2 題 每題 0 分

01	D	02	C
----	---	----	---

二、填充題 共 2 格 每格 0 分

01. Yahoo!奇摩拍賣,露天拍賣