TQC 電子商務概論 V4 第六類

1. 下列有關「數位信封」的敘述哪些錯誤？(複選)
(A) 只用到對稱式加密演算法
(B) 只用到非對稱式加密演算法
(C) 數位信封的觀念可簡化為「加上金鑰的金鑰」
(D) 大型文件大多使用非對稱式演算法來進行全文加密
Ans: A B D

2. 下列有關 Apply Pay 的敘述哪些正確？(複選)
(A) 採用 Token 代碼化服務，防止真實信用卡卡號被竊取
(B) 在 Android 系統上運作
(C) 需透過 QR Code 進行通訊
(D) 將傳統信用卡數位化，消費者不須攜帶實體信用卡，透過手機即可使用
Ans: A D

3. 下列有關 CERT 協調中心的敘述哪些正確？(複選)
(A) 位於美國麻省理工學院
(B) 監看並追蹤尋求其協助之私人公司或政府機關所報告的線上犯罪活動
(C) 協助機構找出安全問題
(D) 包含產品評估、報告及訓練大眾對資訊安全的重視
Ans: B C D

4. 下列哪一項是 DES 使用的金鑰位元數？
(A) 8
(B) 16
(C) 32
(D) 56
Ans: D

5. 下列有關阻斷服務（DoS）攻擊的敘述哪一項正確？
(A) DoS 會以無用的連線流量壅塞網站並癱瘓網路
(B) 這種攻擊將會使網路上的伺服器全遭破壞
(C) Smurf 攻擊屬於監聽攻擊的方式之一
(D) DoS 不會威脅系統運作
Ans: A

6. Handshake Protocol Specification 與 Record Protocol Specification 屬於下列哪一項技術或制度？
(A) SET（Secure Electronic Transaction Protocol）
(B) EFT（Electronic Funds Transfer）
(C) TLS（Transport Layer Security）
(D) TFTP（Trivial File Transfer Protocol）
Ans: C

7. 下列有關 Host Card Emulation（HCE）的敘述哪一項錯誤？
(A) 由 Apple 提出
(B) 在 Android 系統上運作
(C) 不需要換發 SIM 卡即可使用
(D) 採用軟體式的安全元件
Ans: A

8. 下列哪一種是將交易的安全元件（Secure Element）放在手機的 SIM 卡中來確保安全的行動支付機制？
(A) Host Card Emulation
(B) 3D Secure
(C) Trusted Service Manager
(D) 以上皆非
Ans: C

9. 下列有關 Java Applet 的敘述哪些錯誤？(複選)
(A) 從瀏覽器執行的程式
(B) 使網頁互動化
(C) 可防止電腦感染所有病毒
(D) 無法由網頁下載
Ans: C D

10. Kerberos 系統主要是用來提供下列哪一項資訊安全服務？
(A) 安全稽核與警示
(B) 存取控制
(C) 金鑰管理
(D) 身分鑑別
Ans: D

11. 下列哪些項目可用於提供電子郵件的安全傳輸？(複選)
(A) PGP（Pretty Good Privacy）
(B) SET（Secure Electronic Transaction Protocol）
(C) S/MIME（Secure/Multipurpose Internet Mail Extensions）
(D) TLS（Transport Layer Security）
Ans: A C D

12. 下列有關網路付款安全的敘述哪一項正確？
(A) 對稱性加密是指收送雙方都擁有一對公開金鑰與私密金鑰，公開金鑰可傳送給對方，用公開金鑰加密的密文資料一定要取得對應的私密金鑰才能將資料轉為原本的交易資料
(B) 非對稱性加密是指收送雙方都擁有相同的私密金鑰，由自己保管，發送傳送交易資料時，以私密金鑰將交易資料轉為密文的資料，接收端以自己的私密金鑰將密文轉為原文的交易資料
(C) DES 是非對稱性加密的方法之一
(D) RSA 是非對稱性加密的方法之一
Ans: D

13. 下列有關 Smurf 攻擊的敘述哪一項正確？
(A) 不屬於 DoS 攻擊之一
(B) 攻擊方式是針對多台網路位置送出一個請求（Ping），來檢查這個網路位置是否正確，並捏造特定公司的 IP 位置作為回應請求的位置
(C) 又稱為 Sniffer 攻擊
(D) 最常被企業內部的人員拿來攻擊公用資料庫
Ans: B

14. 下列哪些可以用來確保網際網路通訊管道的安全？(複選)
(A) TLS（Transport Layer Security）
(B) S-HTTP（Secure HyperText Transfer Protocol）
(C) VPN（Virtual Private Network）
(D) Proxy
Ans: A B C D

15. 下列哪一項是利用 TCP 來提供點對點的安全服務？
(A) SET（Secure Electronic Transaction Protocol）
(B) TLS（Transport Layer Security）
(C) VPN（Virtual Private Network）
(D) PKI（Public Key Infrastructure）
Ans: B

16. TLS（Transport Layer Security）協定具有下列哪些特質，可保護交易資料的安全？(複選)
(A) 提供顧客身分認證
(B) 提供不可否認性
(C) 用來解決身分辨識的問題
(D) 提供了交換訊息的完整性
Ans: C D

17. 下列有關 TLS（Transport Layer Security）協定的敘述哪一項正確？
(A) 採 RSA 法則加密
(B) 採 DES 法則加密
(C) 採 RSA 與 DES 並用
(D) 不採用 RSA 與 DES
Ans: C

18. 下列哪一項不是 TLS（Transport Layer Security）安全協調程序中的項目？
(A) 交握（Handshake）
(B) 使用數位信封傳送顧客產生的程序金鑰
(C) 交換憑證
(D) 使用程序公開金鑰進行加密
Ans: D

19. 下列哪一項不是一個成功且安全的網際網路交易的基本要求？
(A) 隱私性（Privacy）
(B) 可否認性（Repudiation）
(C) 身分驗證（Authentication）
(D) 完整性（Integrity）
Ans: B

20. 一種軟體程式，介於網際網路與內部網路間作安全保護用，所指的是下列哪一個項目？
(A) Firewall
(B) VPN（Virtual Private Network）
(C) Proxy Server
(D) PPTP（Point to Point Tunneling Protocol）
Ans: A

21. 入侵偵測系統中，下列哪一項是統計在一段時間內某個事件所發生的次數，如果發生的次數超過合理的範圍，就認定是異常行為？
(A) 門檻偵測
(B) 紀錄檔偵測
(C) 規則分析偵測
(D) 特徵入侵偵測
Ans: A

22. 電子商務的六項特性中，讓參與電子商務的參與者無法拒絕承認他們線上行為的能力，這被稱為下列哪一項特性？
(A) 可否認性（Repudiation）
(B) 機密性（Confidentiality）
(C) 可獲得性（Availability）
(D) 不可否認性（Non-Repudiation）
Ans: D

23. 下列敘述哪些正確？(複選)
(A) 在網路安全環境中，過去最常使用的加密演算法為資料加密標準（Data Encryption Standard，DES），其有效位元數為 56 位元
(B) 公開金鑰密碼是對稱的，乃使用兩把相似的金鑰，一把為公開金鑰，另一把為私密金鑰
(C) 公開金鑰演算法的缺點為在傳送大量資料時缺乏效率，需要極大量的電腦運算能力而降低通訊的速度
(D) PGP（Pretty Good Privacy）為公開金鑰加密系統，可用來對電子郵件或檔案加密，供商業使用並收取費用
Ans: A C D

24. 下列有關公開金鑰的敘述哪一項正確？
(A) 公開金鑰通常會與私密金鑰同時產生
(B) 金鑰產生者除了自己保留公開金鑰與私密金鑰之外，同時會一起送給通訊的對方
(C) 公開金鑰只可作加密動作，不能作解密動作
(D) 不可配合雜湊函數使用
Ans: A

25. 下列有關電子交易安全中認證中心的敘述哪一項錯誤？
(A) 主要是以公開金鑰為保障基礎
(B) 它的功能是在提供產生、分配與管理所有持卡人、特約商店與參與電子交易之銀行所需的電子簽證
(C) 以私密金鑰為保障基礎
(D) 發給信用卡持卡人的電子證書稱為 CCA（Consumer CA）
Ans: C

26. 下列有關代碼化技術（Tokenization）的描述哪些正確？(複選)
(A) 代碼化技術可讓行動支付使用者免換 SIM 卡
(B) 代碼化技術是將虛擬的信用卡卡號在線上傳輸
(C) 代碼化技術是將真實信用卡卡號加密後，在線上傳輸
(D) 代碼化技術可降低卡號被竊風險
Ans: A B D

27. 以附加數位指紋的方式提供資料完整性保護的評估，可用於反制下列哪些破壞性操作？(複選)
(A) 資料修改
(B) 資料新增
(C) 資料部分刪除
(D) 資料偽造
Ans: A B C

28. 下列哪些加密方法常被使用於 WWW 電子商務交易的安全保護中？(複選)
(A) TLS（Transport Layer Security）
(B) PGP（Pretty Good Privacy）
(C) SET（Secure Electronic Transaction Protocol）
(D) S-HTTP（Secure HyperText Transfer Protocol）
Ans: A C D

29. 加密（Encryption）是保護網際網路通訊安全的重要方法之一，下列哪些項目是加密的主要功能？(複選)
(A) 訊息完整性（Integrity）
(B) 身分鑑別性（Authenticity）
(C) 不可否認性（Non-Repudiation）
(D) 竊聽對方的通訊資料
Ans: A B C

30. 下列有關加密演算法的敘述哪一項正確？
(A) NSA 與 IBM 在 1950 年代開發出一種 128 位元的 DES 演算法（資料加密標準）
(B) 加密演算法不可與雜湊函數一起使用
(C) 非對稱式演算法中將公開金鑰發送給通訊對方，私密金鑰則自己持有
(D) 公開金鑰可用來仿造出數位簽章
Ans: C

31. 包括各種像病毒、蠕蟲、特洛伊木馬等威脅的程式，稱為下列哪一項？
(A) 閘道器（Gateway）
(B) 駭客（Hacker）
(C) 惡意程式（Malicious Code）
(D) 怪客（Cracker）
Ans: C

32. 下列哪一項不可以用來作為身分驗證（Authentication）的方法？
(A) 數位簽章
(B) 數位憑證
(C) 生物特徵
(D) 封包交換
Ans: D

33. 下列有關巨集型病毒的敘述哪一項錯誤？
(A) 巨集病毒可輕易擴散
(B) 巨集病毒感染的是文件檔
(C) 巨集病毒的可行性建立在自動化巨集上
(D) 巨集病毒與作業系統有關
Ans: D

34. 下列有關信用卡 3D 驗證服務的描述哪一項錯誤？
(A) 此機制是使用實體信用卡背後的 CVV（Card Verification Value）三碼
(B) 此機制指的是讓持卡人設定密碼來保護信用卡在網路上的交易
(C) VISA 組織稱此種服務為 Verified by VISA
(D) Master 組織稱此種服務為 MasterCard SecureCode
Ans: A

35. 企業為了達到系統安全檢查的目的，會僱用一群好的電腦高手，由外部網路試著入侵公司系統，這一群人俗稱為下列哪一項名稱？
(A) Black Hat
(B) White Hat
(C) Gray Hat
(D) Red Hat
Ans: B

36. 下列有關 Microsoft Passport 的敘述哪一項錯誤？
(A) 在 Windows 10 中，Microsoft Passport 使用密碼進行驗證
(B) Microsoft Passport 可協助保護使用者身分識別與使用者認證
(C) Passport 是微軟公司的重要策略之一
(D) Passport 讓使用者便利地存取企業資源
Ans: A

37. 在 Internet 服務的安全問題中，下列哪一項傳輸方式是最具危險性的，因為其在傳送帳號及密碼時，並未對內容進行加密編碼，使傳輸內容易被攔截而破解？
(A) 遠端登錄（Telnet）
(B) 全球資訊網（WWW）
(C) 檔案傳輸協定（FTP）
(D) 電子郵件（E-mail）
Ans: A

38. 在虛擬私人網路（VPN）的機制中，將一個通訊協定（PPTP）接上另一個通訊協定 IP 的過程，稱為下列哪一項？
(A) 通道（Tunneling）
(B) 頻道（Channel）
(C) 安全協定（Security Protocol）
(D) SSL（Secure Socket Layer）
Ans: A

39. 在網路的保全方式中，下列哪一項是最常見的第一線安全措施？
(A) 信任式保全
(B) 生物特徵識別系統
(C) 主機保全
(D) 密碼設定
Ans: D

40. 作業系統的安全模式中，可以讓使用者對自己所擁有的檔案及其他週邊設備資源，自行決定是否提供或授權他人存取，其權限包括讀、寫、執行等三種，這是指下列哪一項存取控制模式？
(A) 任意性存取控制（DAC）
(B) 強制性存取控制（MAC）
(C) 以角色為基礎的存取控制（RBAC）
(D) 貝爾-拉帕杜拉（Bell-Lapadula）安全模式
Ans: A

41. 電子商務有六項特性，能夠確保網站上顯示的、或者是 Internet 上收發的資訊，沒有被未獲許可的人士以任意方式更改的特性，這被稱為下列哪一項特性？
(A) 不可否認性（Non-Repudiation）
(B) 身分鑑別性（Authenticity）
(C) 隱私性（Privacy）
(D) 完整性（Integrity）
Ans: D

42. 下列有關防火牆的敘述哪些正確？(複選)
(A) 防火牆的工作原理是在 Extranet 和 Internet 之間建立一個屏障
(B) 防火牆的工作原理是在 Intranet 和 Internet 之間建立一個屏障
(C) 防火牆的工作原理是在 Extranet 和 Intranet 之間建立一個屏障
(D) 防火牆系統通常是置於網路閘道點上
Ans: B D

43. 下列敘述哪一項錯誤？
(A) 數位簽章具有交易者身分的識別
(B) 防火牆是針對資料庫的保護而設計
(C) 電子簽章具有不可否認性
(D) 電子錢包一般應用於小額付款
Ans: B

44. 下列有關防火牆的敘述哪一項錯誤？
(A) 防火牆的目的是用以保護區域性網路（LAN）不被網路外的人所入侵
(B) 防火牆可以防止企業本身內部的安全威脅且可防範病毒入侵
(C) 防火牆的功能像是一個控制資料流入和流出的安全屏障
(D) 封包過濾式防火牆可檢視所有從 LAN 外來的資料，自動拒絕任何有 LAN 位址的資料
Ans: B

45. 具有安全性之電子付款系統有下列哪些安全保密要求？(複選)
(A) 身分認證
(B) 加密
(C) 完整性
(D) 防止拒付
Ans: A B C D

46. 下列有關信用卡 3D 驗證服務與公開金鑰基礎建設（Public Key Infrastructure，PKI）技術比較的敘述哪些正確？(複選)
(A) 信用卡 3D 驗證服務比公開金鑰基礎建設來得安全
(B) 信用卡 3D 驗證服務較方便，不須本人親自到特定地點辦理
(C) 信用卡 3D 驗證服務使用了數位憑證技術，較為先進
(D) 信用卡 3D 驗證服務相較於公開金鑰基礎建設，更易於普及
Ans: B D

47. 下列有關屏障式閘道器（Screen Host Gateway）防火牆過濾規則之敘述哪些正確？(複選)
(A) 不允許外界封包輸入至內部閘道器
(B) 不允許外界封包輸入至內部其他主機
(C) 不允許閘道器的封包輸出至外界網路
(D) 不允許其他內部主機的封包輸出至外界網路
Ans: B D

48. 挑戰與回應（Challenge and Response）機制是用於提供下列哪一項安全服務？
(A) 身分鑑別（Authenticity）
(B) 資料的完整性（Integrity）
(C) 事件的不可否認（Non-Repudiation）
(D) 存取控制（Access Control）
Ans: A

49. 下列哪些工具可用來協助建構安全的網路環境？(複選)
(A) 加密
(B) 防火牆
(C) 虛擬私人網路
(D) 架設 E-mail 伺服器
Ans: A B C

50. 下列哪一項不屬於美國國家電腦安全協會（NCSA）所提之安全電子商務基石？
(A) 隱私性（Privacy）
(B) 身分驗證（Authentication）
(C) 完整性（Integrity）
(D) 可否認性（Repudiation）
Ans: D

51. 根據來源與終點 IP 位址、來源與終點埠位號碼以及封包類型來規範進入封包之接受或拒絕之網路安全系統，指的是下列哪一項？
(A) 郵件伺服器
(B) 封包分封器
(C) 封包過濾器
(D) 封包交換器
Ans: C

52. 下列哪些方法可用來防止重播攻擊（Replay Attack）？(複選)
(A) 數位信封
(B) 唯一序號法
(C) 挑戰與回應
(D) 時間戳記法
Ans: B D

53. 下列有關稽核目標的敘述哪一項錯誤？
(A) 提供非法行為的入侵偵測和防禦
(B) 確保所有的運作均能按照既定的安全政策執行
(C) 確保所有資料的存取都要經過授權
(D) 確保所有資料的正確性
Ans: A

54. 下列有關單向雜湊函數（One-way Hash Function）特性的敘述哪一項錯誤？
(A) 產生固定長度的輸出
(B) 可以處理任意大小的資料區段
(C) 給定一訊息摘要 M，無法找出符合下列條件的 M，即 H(M)=MD
(D) 可以找到二份不同的文件訊息，具有相同的訊息摘要
Ans: D

55. 有關虛擬私人網路（VPN）的敘述，下列哪一項正確？
(A) 利用檔案傳輸協定安全的在網路上存取內部網路
(B) 使用 PPTP 通訊協定在網路上進行私密資料傳送
(C) VPN 是永久的安全線路
(D) VPN 屬於專線的一種，使企業可以在專線上安全的傳送資料
Ans: B

56. 下列有關信用卡 3D 驗證服務的描述哪些正確？(複選)
(A) 台灣的發卡銀行皆提供 3D 驗證服務
(B) 3D 驗證不需定期更換密碼
(C) 3D 驗證服務可在網路上直接申請
(D) 3D 驗證服務使用公開金鑰基礎建設（Public Key Infrastructure，PKI）
Ans: B C

57. 下列哪一項是資訊安全中的 CA（Certificate Authority）的作用與特色？
(A) 發行數位憑證的單位
(B) 只有政府機關可以擔任
(C) 需要與公開金鑰基礎建設分別設置
(D) CA 可由具公信力的司法官來擔任
Ans: A

58. 下列哪些是資訊安全管理的作業要點或系統規範？(複選)
(A) ISO/IEC 17799
(B) TS16949
(C) BS7799
(D) CNS17800
Ans: A C D

59. 下列哪一種方式是使用信用卡在網路上進行刷卡最為安全的機制？
(A) 使用實體信用卡背後的 CVV（Card Verification Value）三碼
(B) 使用 3D 驗證服務
(C) 僅輸入信用卡卡號
(D) 不使用 SSL 加密
Ans: B

60. 電子付款系統所採用的主要安全機制有下列哪些？(複選)
(A) 加密
(B) 電子簽章
(C) 身分認證
(D) 認證授權
Ans: A B C D

61. 下列哪些是電子商務中的安全性威脅？(複選)
(A) 信用卡詐欺
(B) 阻斷服務（DoS）攻擊
(C) 監聽（Sniffer）
(D) 欺騙（Spoof）
Ans: A B C D

62. 下列有關電子現金系統的特性哪一項錯誤？
(A) 不易被複製或篡改
(B) 不可轉換性
(C) 具匿名性
(D) 不可回溯性
Ans: B