臺灣港務股份有限公司

104 年度獎學從業人員甄試測驗題命題單

考試科目	網路與資訊安全概要	命題老師	(請簽名)
題　　型	測驗題: ■單選題　□多選題	題　　數	20 題
電子計算器	□可使用　■禁止使用		

備註：

一、 本次考試時間為 90 分鐘。

二、 請以命題大綱為範圍出題，並請就出題內容予以保密，以維護本測驗之公平與公正性。

三、 選擇命題原則：

1. 每個試題必須獨立存在，內容不宜相互重疊、不要提供正確答案的線索。
2. 試題排序由易到難。
3. 命題請儘量以不超出命題大綱為原則。
4. 儘可能以正面、肯定、簡短、清晰字詞來敘述試題題幹。
5. 每題之選項：本次考試統一為四個選項，選項代號以英文 A、B、C 及 D 表示，正確答案為單一選項。
6. 錯誤選項應具有誘答性(錯誤選項的敘述要有似真性或合理性) 。
7. 如屬最佳答案類型，必須確信只有一個最清楚的最佳答案。
8. 謹慎使用「以上皆是」或「以上皆非」。
9. 各選項長度應接近。
10. 正確答案宜隨機排列，出現次數儘量相同。
11. 若題幹要求學生從選項中選出一正確者或錯誤者，請使用以下之固定敘述方式：

(1)下列有關...的敘述，哪一個是正確的？(哪一個是錯誤的？)

(2)(引言)...，哪一個敘述(或選項)是正確的？(哪一個是錯誤的？)

答案	題號	題目及選項
D	1、	下列哪一種網路硬體裝置可以透過電話線將電腦連上 ISP（Internet Service Provider）與網際網路？（A）網路卡（B）路由器（C）閘道器（D）數據機
C	2、	常見的 IP 位址(Internet Protocol Address)分為 IPv4 與 IPv6 兩大類，請問這兩類網路位址的長度分別有幾個位元？(A) 16 與 32 (B) 16 與 64 (C) 32 與 128 (D) 64 與 128
A	3、	TCP/IP 是目前網際網路（Internet）廣泛使用的協定，下列有關 TCP（Transmission Control Protocol）的敘述，哪一個是正確的？（A）會重送遺失的封包 (B) 不須建立連線即可進行傳輸 (C) 缺乏流量控制 (D) 缺乏阻塞控制（Congestion Control）
B	4、	在國際標準組織(ISO)所訂定的 OSI 通訊協定中，負責資料加密和壓縮是哪一層？(A)應用層（Application Layer)(B) 展示層（Presentation Layer)(C) 網路層（Network Layer)(D) 實體層（Physical Layer）
B	5、	從郵件伺服器收取電子郵件時，常使用的通訊協定可能為下列哪一項？（A）SMTP（B）IMAP（C）IPX（D）FTP
D	6、	下列有關加密演算法的敘述，哪一個是錯誤的？（A）對稱式加解密法使用相同的金鑰進行加密、解密（B）AES (Advanced Encryption Standard) 屬於對稱式加解密法（C）一般而言，非對稱式加解密法執行速度較對稱式慢（D）非對稱式加解密法必須同時保護兩把金鑰以保證安全性
C	7、	下列有關 RSA 加密演算法的敘述，哪一個是錯誤的？（A）RSA 屬於非對稱式加解密法 (B) 安全性建立在分解大數的困難度上 (C) 在現今的應用中，使用很短的金鑰長度（< 64 位元)即可達到難以破解的安全性（D）以質數同餘有限體的指數運算為基礎
A	8、	資訊安全領域中有關雜湊函數（Hash Function）的敘述，哪一個是錯誤的？(A) 接收固定長度的訊息並且產生固定長度的雜湊值 (B) 將輸入訊息壓縮成訊息摘要(Digest),使得資料量變小(C)屬於單向函數(One-way Function)(D) SHA-1 是常用的雜湊函數演算法
C	9、	當傳送敏感的電子資料時，有必要防止來源端及目的端的否認行為。下列哪一種安全防護機制可以達到不可否認(Non-repudiation)之安全特質？（A）對稱式加解密法（B）非對稱式加解密法（C）數位簽章（Digital

		Signature)(D) 數位摘要 (Digital Digest)
A	10、	防止電子郵件被未經授權者讀取最常用的方法是使用軟體加密,下列何者可以為電子郵件進行加密？(A) PGP (B) POP3 (C) HTTP (D) FTP
D	11、	數位憑證(Digital Certificate)一般由憑證機構(Certification Authority, CA)頒發，下列有關數位憑證與憑證機構的敘述，哪一個是錯誤的？(A) CA 提供的服務主要包含憑證簽發、更新與終止等 (B) 數位憑證內含有憑證持有者的公開金鑰(Public Key) (C) 因為不易被偽造，一般可以將憑證放在公開的目錄 (D) 憑證持有者可以自行修改憑證
C	12、	下列有關安全傳輸協定 (Secure Socket Layer, SSL) 的敘述，哪一個是錯誤的？(A) SSL 最初創始於網景公司(Netscape) (B) Web 瀏覽器普遍將 HTTP 和 SSL 相結合以實作安全通訊(C)是由傳輸層安全協議(Transport Layer Security, TLS) 修改而來 (D) 可依環境不同使用適當的加密演算法
B	13、	IP 安全協定 (Internet Protocol Security, IPsec) 工作於 OSI 模型的哪一層以提供安全通訊保密機制？(A) 資料鏈結層(Data link Layer) (B) 網路層(Network Layer) (C) 會談層(Session Layer) (D) 應用層(Application Layer)
A	14、	有關電腦病毒的敘述，下列何者正確？(A) 能夠自我複製 (B) 皆為可獨立存在與執行的完整程式 (C) 電腦關機即會自動消失 (D) 一經感染硬碟即遭破壞
B	15、	下列哪一種惡意程式 (Malicious Programs) 會偷偷控制網際網路上其他的電腦，並且利用被控制的電腦來發動攻擊？(A) 蠕蟲 (B) 僵屍 (C) 後門程式 (D) 木馬程式
D	16、	下列有關分散式阻斷服務 (DDoS) 攻擊的敘述，哪一個是錯誤的？(A) 耗盡網路上目標電腦的網路資源與系統資源 (B) 使目標電腦暫時中斷或停止服務 (C) 可能對企業造成嚴重的資安威脅 (D) 使用單一主機或網路節點發動攻擊
A	17、	下列有關防火牆的敘述，哪一個是錯誤的？(A) 可以防止防火牆內部的不法行為 (B) 利用預先設定的規則，對遠端連接的封包進行檢查並決定是否允許通過 (C) 通常建置於網際網路與內部網路之間 (D) 無法有效阻擋病毒攻擊，尤其是隱藏在資料中的病毒
C	18、	有關防毒軟體的敘述，下列何者錯誤？(A) 主要功能為防範病毒、尋找病毒、清除病毒 (B) 隨時監控電腦程式的舉動及掃瞄系統是否含有病毒 (C) 病毒特徵碼掃描可以檢測出未知的病毒 (D) 無法防止系統與應用程式漏洞攻擊
D	19、	有關特洛依木馬 (Trojan Horse) 的敘述，下列何者錯誤？(A) 通常不會自我複製 (B) 當特洛伊木馬程式被執行，攻擊者即可間接取得系統存取權限 (C) 可用於散播病毒、蠕蟲 (D) 無法被防毒軟體識別清除
B	20、	下列有關資訊安全的敘述，哪一個是錯誤的？(A) 通行碼 (Password) 系統是防禦入侵的方法之一，通行碼經常會先加密再儲存 (B) 入侵偵測系統 (Intrusion Detection System, IDS) 監控網路和系統，可主動偵測入侵行為並主動防禦 (C) 防毒軟體無法防止分散式阻斷服務攻擊 (D) SET(Secure Electronic Transaction)協定可用於保護網際網路信用卡交易之安全性