

※請填寫入場通知書編號：_____

注意：①作答前須檢查答案卡（卷）、入場通知書編號、桌角號碼、應試類別是否相符，如有不同應立即請監試人員處理，否則不予計分。

②本試卷為一張雙面，測驗題型分為【四選一單選擇題 30 題，每題配分 2 分，共 60 分】與【非選擇題 2 題，每題配分 20 分，共 40 分】，合計 100 分。

③選擇題限以 2B 鉛筆於答案卡上作答，請選出最適當答案，答錯不倒扣；未作答者，不予計分。

④非選擇題限以藍、黑色鋼筆或原子筆於答案卷上採橫式作答，並請從答案卷內第一頁開始書寫，違反者該科酌予扣分，不必抄題但須標示題號。

⑤請勿於答案卡（卷）上書寫姓名、入場通知書編號或與答案無關之任何文字或符號。

⑥本項測驗僅得使用簡易型電子計算器(不具任何財務函數、工程函數功能、儲存程式功能)，但不得發出聲響；若應考人於測驗時將不符規定之電子計算器放置於桌面或使用，經勸阻無效，仍執意使用者，該節扣 10 分；該電子計算器並由監試人員保管至該節測驗結束後歸還。

⑦答案卡（卷）務必繳回，違反者該節成績以零分計算。

壹、四選一單選擇題 30 題（每題配分 2 分）

【4】1.下列何者並非網際網路控制訊息協定 ICMP 的錯誤回報(error reporting)訊息？

- ①時間逾時(time exceeded)
- ②重新導向(redirection)
- ③來源抑制(source quench)
- ④資料遺失(data loss)

【3】2.假設一路由器(router)其內部之路由表如下，今有一封包其目的地地址為 01110001，則此封包將會被傳送到哪個鏈結介面？

前綴匹配(prefix match)	鏈結介面(link interface)
01110	A
011100	B
0111000	C
其他	D

- ① A
- ② B
- ③ C
- ④ D

【1】3.假設有一 F 位元大小之檔案，今欲將其從主機 A 傳送到主機 B ， A 跟 B 之間透過一個路由器(router)連接（亦即有兩道連結(link)，每道連結的傳輸速率是 R bps），若將檔案分割成大小皆為 S 位元的區段，並且在每個區段中加入 20 位元的標頭(header)，今假設檔案傳輸延遲(transmission delay)為： $(F/S + 1)$ 個區段所需之傳輸時間，試求能令此傳輸延遲最小之 S 值。

- ① $(20F)^{1/2}$
- ② $(10F)^{1/2}$
- ③ $(20F)^{1/4}$
- ④ $(10F)^{1/4}$

【3】4.考量發生於路由器中的佇列延遲(queueing delay)，假設有 N 個封包(packet)同時抵達路由器中的空白佇列(queue)，所有封包都是 L 位元，而路由器從佇列中依先進先出方式將封包逐個傳輸出去的速率是 R bps，試求所有封包在佇列中被傳輸出去前的平均佇列延遲（等待時間）。

- ① $(N+1)/2 L/R$
- ② $(2N+1)/2 L/R$
- ③ $(N-1)/2 L/R$
- ④ $(2N-1)/2 L/R$

【1】5.考量網頁瀏覽器下載 2 個 HTML 網頁、每個網頁內含 5 個不同圖片(jpeg)，若瀏覽器採用永久性連線(persistent connection)的 HTTP 協定，則此瀏覽器最少需要建立多少次 TCP 連線，以將此 2 個網頁及其內含總共 10 個圖片下載完成？

- ① 1 次
- ② 2 次
- ③ 11 次
- ④ 12 次

【2】6.考量發生於路由器中的封包刪除（造成封包遺失，packet loss），下列敘述何者錯誤？

- ①封包由輸入介面(input interface)傳送進入路由器的輸入埠(input port)後，由於輸入埠內的佇列(queue)已滿，故而此封包被刪除
- ②封包由輸入埠的佇列移至交換結構(switching fabric)後，由於交換結構已滿，無法進行交換，故而此封包被刪除
- ③封包於交換結構完成交換後，移至輸出埠(output port)的佇列，由於輸出埠內的佇列已滿，故而此封包被刪除
- ④封包於交換結構完成交換後，移至輸出埠(output port)的佇列，由於輸出埠內的佇列已滿，故而某一原已存放於佇列內之封包被刪除，以空出空間來存放此一新的封包

【3】7.目前多種網路採用 CRC (Cyclic Redundancy Check)技術來執行錯誤偵測，今假設所要傳送的資料為“101110”，而所使用的 CRC 函數為 $f(x) = x^2 + 1$ ，試求此資料的 CRC 檢查碼。

- ① 101
- ② 010
- ③ 011
- ④ 111

【2】8.有關 Ethernet 區域網路技術，下列敘述何者錯誤？

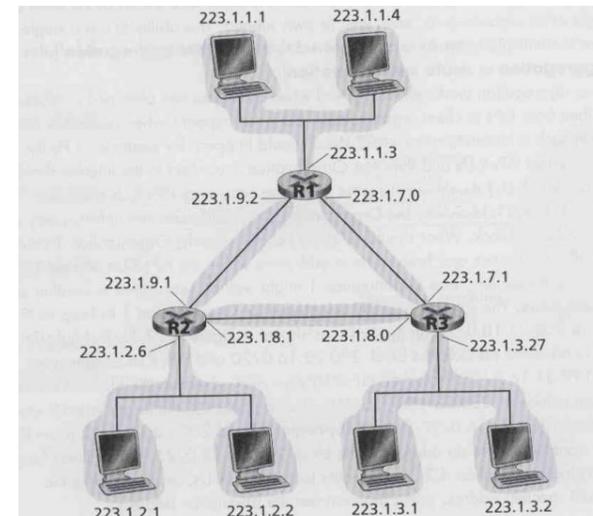
- ① Ethernet 是目前最通行的有線區域網路技術
- ② Ethernet 目前實體上多採用 bus 架構(topology)
- ③ Ethernet 成本較 FDDI、ATM 低
- ④ Ethernet 目前多採用 CSMA/CD 多重存取協定

【3】9.考量具有 3 個路由器(router, R1/R2/R3)的網路如【圖 9】，總共形成多少個子網路(subnet)？

- ① 4 個
- ② 5 個
- ③ 6 個
- ④ 7 個

【4】10.有關藍芽(Bluetooth)網路技術，下列敘述何者錯誤？

- ①定義於 IEEE 802.15.1 標準
- ②以 TDM 方式運作於 2.4 GHz 的無線電頻寬上
- ③不需要網路基礎設施連接運作中的裝置
- ④同一環境中，最多可以容納 16 個裝置同時運作



【圖 9】

【4】11.有關 IPv4 及 IPv6 的差異，下列敘述何者錯誤？

- ① IPv6 擴增 IPv4 之位址位元數，從 32 位元提昇到 128 位元
- ② IPv6 修正 IPv4 之資料前置欄位(header fields)，並固定為 40 bytes 長
- ③ IPv6 新增資料流量標籤(flow label)，以註明資料傳送之品質要求
- ④ IPv6 新增資料於傳送過程中，各 router 可對資料進行分解或組合

【3】12.今有一關聯資料表內含{A, B, C, D}四個欄位，其 3 組功能相依(functional dependency)關係為 $A, B \rightarrow C$ ； $B \rightarrow D$ ； $C \rightarrow A$ ，請將此資料表分解成 BCNF 資料表。

- ① {A, C}, {A, B}, {B, D}, {C, A}
- ② {B, C}, {A, B}, {B, D}, {C, A}
- ③ {B, C}, {B, D}, {C, A}
- ④ {B, C}, {A, B}, {C, A}

【1】13.在磁碟矩陣階層(RAID level)中，下列何者採用同位檢查碼(parity code)概念，以位元組為分置單位，將資料分置於不同磁碟，而檢查碼則另置於其他磁碟？

- ① RAID Level 3
- ② RAID Level 4
- ③ RAID Level 5
- ④ RAID Level 6

【請接續背面】

【2】14.有關資料整體性(Integrity)，不包括下列哪個特性？

- ①緊密性(Atomicity) ②重覆性(Redundancy) ③一致性(Consistency) ④持久性(Durability)

【1】15.考量下列關聯資料表 ABC

分行名稱	借款代號	顧客姓名	借款總額
------	------	------	------

今有一 SQL 指令

```
Select 分行名稱 sum(借款總額) as 分行借款總額
From ABC
Group By 分行名稱
Having 借款總額 > 2000
```

下列有關此指令之敘述，何者正確？

- ①列印所有顧客的借款總額超過 2,000 的分行名稱、分行借款總額
②列印所有顧客的借款總額超過 2,000 的分行名稱、借款總額、分行借款總額
③列印至少一個顧客的借款總額超過 2,000 的分行名稱、分行借款總額
④列印至少一個顧客的借款總額超過 2,000 的分行名稱、借款總額、分行借款總額

【4】16.若某一資料表內容被切割為數份（可依據欄位切割為數份、如欄位 A-E 可被分為 A-B 及 C-E 等兩個資料表；另外也可依據資料錄切割為數份、如資料錄 1-10 可被分為 1-5 及 6-10 等兩個資料表）、分別存放於不同地方，今若想將這些分散於各地的資料表整合還原回原來的單一資料表，則下列有關 SQL 指令敘述，何者正確？

- ①若資料表係依據欄位被切割為數份，則可使用 EXCEPT 指令以還原回單一資料表
②若資料表係依據欄位被切割為數份，則可使用 INTERSECT 指令以還原回單一資料表
③若資料表係依據資料錄被切割為數份，則可使用 JOIN 指令以還原回單一資料表
④若資料表係依據資料錄被切割為數份，則可使用 UNION 指令以還原回單一資料表

【2】17.下列有關變更關聯資料表 ABC 內容的 SQL 指令，何者正確？

- ① Update ABC as ② Update ABC set ③ Update set ABC as ④ Update as ABC set

【3】18. NoSQL(Not only SQL)是下一代的資料庫概念，下列有關 NoSQL 敘述，何者錯誤？

- ① NoSQL 以分散式(distributed)為主，以便於在不中斷資料庫運行的情況下擴充資料儲存空間
② NoSQL 欄位定義深具彈性(schema-free)，以便於隨時進行資料庫欄位的調整
③ NoSQL 資料一致性深具彈性(consistency-free)，以便於隨時進行資料儲存空間的擴充
④ NoSQL 支援大量資料的運算，以便於處理現今網路應用系統的資料分析需求

【2】19.下列何者並非關聯式代數(Relational Algebra)中所使用的運算子(operator)？

- ①聯集(union) ②聚合(aggregation) ③差集(difference) ④投射(project)

【1】20.下列何者並非一般資料庫管理系統所採用的索引(index)技術？

- ①區段索引(block index) ②次索引(secondary index)
③叢集索引(clustering index) ④主索引(primary index)

【1】21.若關聯資料表 A 及 B(主鍵皆為 id)分別有 30 列及 50 列資料，下列 SQL 指令執行最多會產生多少列資料？

(Select id From A) Except (Select id From B)

- ① 30 列 ② 50 列 ③ 80 列 ④ 1,500 列

【4】22.下列何者並非資料操作語言(Data Manipulation Language, DML)的詞彙？

- ① Except ② Insert ③ Exists ④ Alter

【3】23.今有一關聯資料表內含{A, B, C}三個欄位，其 4 組功能相依關係(functional dependency)為 $A \rightarrow BC$ ； $B \rightarrow C$ ； $A \rightarrow B$ ； $AB \rightarrow C$ ，下列何者為簡化此 4 組功能之相依關係？

- ① $AB \rightarrow C$ ； $B \rightarrow C$ ② $A \rightarrow C$ ； $B \rightarrow C$ ③ $A \rightarrow B$ ； $B \rightarrow C$ ④ $AB \rightarrow C$ ； $A \rightarrow C$

【4】24.下列關於滲透測試之敘述，何者錯誤？

- ①模擬駭客攻擊實體環境檢驗安全性 ②屬於資安防護手段
③屬於稽核活動 ④不須取得客戶授權

【3】25.政府組態基準(Government Configuration Baseline, GCB)建議 Windows7 的密碼最小長度為何？

- ① 8 ② 10 ③ 12 ④ 14

【2】26. ISO 27001 資訊安全管理系統導入 PDCA 模型，不包含下列何種程序(process)？

- ① Plan ② Determine ③ Act ④ Check

【2】27.關於雜湊函數的敘述，下列何者錯誤？

- ①碰撞為多個值對應到同一個雜湊值 ②所有應用的安全性都仰賴雜湊函數不會碰撞的特性
③ MD5 已被證明會有碰撞問題 ④ MD5 的長度為 128 位元

【2】28.目前連接網站的 HTTPS 協定主要採用何種非對稱加密演算法？

- ① AES ② RSA ③ ECC ④ 3DES

【3】29. HTTPS 協定在金鑰交換後，一般採用何種演算法加密所傳輸資料？

- ① MD5 ② SHA1 ③ AES ④ RSA

【2】30.透過修改網址參數使受害者點擊後，導致 Session Cookie 被挾持，為下列何種類型問題？

- ① Injection ② Cross-Site Scripting
③ Missing Function Level Access Control ④ Security Misconfiguration

貳、非選擇題二大題（每題配分 20 分）

第一題：

考量 TCP 協定中的 GBN(Go Back N)及 SR(Selective Repeat)等兩種自動重傳請求 ARQ 機制，假設傳送封包的編號空間為 K(也就是封包可被編號為 0 到 K-1)：

(一) 請問此 2 種機制之差異為何？【5 分】

(二) 請說明傳送封包的流動視窗(sliding window)其大小(window size)為何不能超過 K 值的一半？【15 分】

第二題：

今有一拍賣網站會員可透過忘記密碼功能，取回其原始設定通行密碼，請回答下列問題：

(一) 請說明拍賣網站此功能可能有何風險？【5 分】

(二) 請說明改善方式。【5 分】

(三) 請說明何謂一次性通行密碼(One Time Password)，並說明其設計原理。【10 分】