臺灣省各級漁會第七次新進暨升等人員考試試題（乙卷）

考試科目：資訊電腦實務
職等類別：新進第十一職等(資訊管理)
考試時間：80 分鐘

1. 答案以橫式由左至右書寫。 2. 請依題號順序作答。

---

1. (10 分) 檔案系統（file system）的功用為何？請寫出 3 種常見的檔案系統名稱。

2. (10 分) 請簡述 TCP 與 UDP 的主要區別。

3. (10 分) NAT（Network Address Translation）技術及 IPv6 都可以解決 IP 位址不足的問題。請說明這二種解決方式的主要差異及優缺點為何。

4. (10 分) 請說明下列演算法的用途：(1) DES (2) MD5 (3) Diffie-Hellman (4) RSA

5. (10 分) 若要提供一個安全的無線上網環境，請問可以使用哪些機制或作法？請舉出三種可以提升無線網路安全的相關標準，並說明其用途。

6. (10 分) 對稱式區塊加密演算法在實務上運作時，通常會需要搭配一個指定的運作模式（mode of operations）。請說明搭配運作模式的主要用途為何，並舉出二個運作模式的名稱。

7. (20 分) 請解釋下列名詞：(1) PKI；(2) DDoS；(3) 殭屍網路；(4) 網路釣魚。

8. (20 分) 給定下列資料表，請問下列查詢的結果為何？

(1) `SELECT Name FROM common WHERE relation = 1`

(2) `SELECT common.Name, mem_class.clname, member.enterdate FROM common, member, mem_class WHERE common.Memid = member.memid AND member.classid = 100 AND mem_class.classid = 100`

common：自然人

Memid	Name	belong	relation
1	張三	1	1
2	李四	2	1
3	小山	3	1
6	小六	1	3
7	王五	1	2
8	任天	2	3
26	大刀	26	1
27	非也	27	1
102	中山	102	1

member ：會員檔

memid	classid	enterdate	outdate	statusid
2	100	1987/02/05		100
3	100	1978/08/11	2014/08/08	400
6	200	1954/02/06		100
9	200	1963/08/08	2014/06/45	400
26	100	1988/12/01		100
102	200	2013/21/1		100

comm_relation

belid	belname
1	會員本人
2	會員父母
3	會員子女

mem_class

classid	clname
100	甲類
200	乙類
300	贊助

mem_statusid

statusid	stname
100	入會
200	復會
300	停權
400	出會

(參考答案)

臺灣省各級漁會第七次新進暨升等人員考試試題（乙卷）

考試科目：資訊電腦實務

類別職等：新進人員十一職等

1. 答案以橫式由左至右書寫。 2. 請依題號順序作答。

---

1. (10 分) 檔案系統（file system）的功用為何？請寫出 3 種常見的檔案系統名稱。

檔案系統的用途主要為提供使用者一個便利存取及管理磁碟空間的界面。使用者透過「檔名」存取磁碟上的資料，而資料空間的安排則由檔案系統負責。常見的檔案系統包括 NTFS、FAT、ext2、ext3、UFS 等等。

2. (10 分) 請簡述 TCP 與 UDP 的主要區別。

UDP 為無連接導向的傳輸層協定，資料傳輸單位為 datagram（數據包）
TCP 為連接導向傳輸層協定，傳輸前需要先建立建線，以串流方式傳輸資料。此外，TCP 亦額多提供如可靠傳輸、流量控制、壅塞控制等功能。

3. (10 分) NAT（Network Address Translation）技術及 IPv6 都可以解決 IP 位址不足的問題。請說明這二種解決方式的主要差異及優缺點為何。

NAT：使用者使用虛擬 IP 位址，由 NAT 技術將內部網路的 IP 位址和連接埠和外部（實體）IP 位址和連接埠進行轉換，以達到 IP 分享的目的。優點是建置容易，而缺點是需要額外的裝置、單一 IP 有連接埠上限的問題、且用戶端主機無法對外提供服務（需要額外設定）
IPv6：提供長達 128-bit 的 IP 位址，優點是可以真正解決 IP 不足的問題，而缺點是建置成本較高，且目前的普及率還不足。另外，軟體（如作業系統）和硬體（如路由器）可能都需要升級以支援 IPv6。

4. (10 分) 請說明下列演算法的用途：(1) DES (2) MD5 (3) Diffie-Hellman (4) RSA

(1) DES：對稱式密碼加密演算法，用來進行資料加解密。使用一組密碼。
(2) MD5：密碼學的雜湊函數，可以任意長度資料計算出相對應的雜湊值。
(3) Diffie-Hellman：提供在公開場合進行密碼交換的功能，基於離散對數的解題難度而設計。
(4) RSA：非對稱式密碼加密演算法，用來進行資料加解密。使用二組密碼。

5. (10 分) 若要提供一個安全的無線上網環境，請問可以使用哪些機制或作法？請舉出三種可以提升無線網路安全的相關標準，並說明其用途。

IEEE 802.1x：提供帳號密碼認證的功能。
WEP：傳統的無線網路資料傳輸加密標準。
WPA 或 WPA2：較新版的無線網路資料傳輸加密標準。
RADIUS：可配合 802.1x 標準，提供帳號密碼認證。
Captive Portal：使用網站的方式要求使用者登入後才得以存取 Internet。

6. (10 分) 對稱式區塊加密演算法在實務上運作時，通常會需要搭配一個指定的運作模式（mode of operations）。請說明搭配運作模式的主要用途為何，並舉出二個運作模式的名稱。

主要用途：避免相同的資料，在相同的演算法和密碼下，得到相同的結果。
舉例：如 CBC、CFB、OFB、CTR、GCM 等等。

7. (20 分) 請解釋下列名詞：(1) PKI；(2) DDoS；(3) 殭屍網路；(4) 網路釣魚。

(1) PKI：公開金鑰密碼基礎建設，提供用戶對取得的公開金鑰進行認證的功能。
(2) DDoS：分散式服務阻斷攻擊，指利用大量且分散於各處的網路主機，對特定對象發動的大規模攻擊，以癱瘓服務。
(3) 殭屍網路：攻擊者入侵大量用戶端主機，並透過一指令伺服器，下達命令給被入侵的主機執行。這些受害的用戶端主機組成的網路即殭屍網路。
(4) 網路釣魚：指建立一個與真正的服務網站相同的網站，以騙取使用者的私密資料如信用卡號、帳號、密碼、銀行戶頭等資訊。

8. (20 分) 給定下列資料表，請問下列查詢的結果為何？

(1) `SELECT Name FROM comon WHERE relation = 1`

(2) `SELECT comon.Name, mem_class.clname, member.enterdate FROM comon, member, mem_class WHERE comon.Memid = member.memid AND member.classid = 100 AND mem_class.classid = 100`

comon：自然人

memid	Name	belong	relation
1	張三	1	1
2	李四	2	1
3	小山	3	1
6	小六	1	3
7	王五	1	2
8	任天	2	3
26	大刀	26	1
27	非也	27	1
102	中山	102	1

member ：會員檔

memid	classid	enterdate	outdate	statusid
2	100	1987/02/05		100
3	100	1978/08/11	2014/08/08	400
6	200	1954/02/06		100
9	200	1963/08/08	2014/06/45	400
26	100	1988/12/01		100
102	200	2013/21/1		100

comm_relation

belid	belname
1	會員本人
2	會員父母
3	會員子女

mem_class

classid	clname
100	甲類
200	乙類
300	贊助

mem_statusid

statusid	stname
100	入會
200	復會
300	停權
400	出會

(1) 列出會員本人的姓名，執行結果包括：

張三、李四、小山、大刀、非也、中山

(2) 列出甲類會員的姓名及入會日期，結果包括：

李四　甲類　1987/02/05

小山　甲類　1978/08/11

大刀　甲類　1988/12/01