

中華郵政股份有限公司 111 年職階人員甄試試題

職階／甄選類科【代碼】：專業職(一)／系統操作(1)【U3209】、系統操作(2)【U3210】
 第一節／專業科目(1)：資訊科學概論(含電腦基礎知識、資料結構、網路基本知識、資訊安全)

*入場通知書編號：_____

注意：①作答前先檢查答案卷，測驗入場通知書編號、座位標籤、應試科目等是否相符，如有不同應立即請監試人員處理。使用非本人答案卷作答者，該節不予計分。
 ②本試卷為一張單面，非選擇題共 4 大題，每題 25 分，共 100 分。
 ③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，並請依標題指示之題號於各題指定作答區內作答。
 ④請勿於答案卷上書寫姓名、入場通知書編號或與答案無關之任何文字或符號。
 ⑤答案卷務必繳回，未繳回者該節以零分計算。

第一題：

請回答下列問題：

- (一) 當今計算機的通用架構，都是基於所謂的馮紐曼架構。此架構定義了電腦的五大單元，請問是哪五大單元？【5 分】
- (二) 以下用虛擬碼撰寫的演算法，當輸入值為(0,1)時，請問輸出值為何？【5 分】
 Procedure TEST (A, B)
 if (B < 100) then
 (print the value assigned to B;
 temp ← A+B;
 apply TEST(B, temp)
- (三) 下列之時間複雜度請由“小到大”依序排序（例：O(A) < O(B) < O(C)）。【5 分】
 $O(n^3), O(2^n), O(n!), O(n \log n), O(\log n), O(n)$
- (四) 管線化(pipelining)是一種能讓多個指令同步執行的實做技巧，也是讓處理器(CPU)效能更快的主要關鍵。但管線化確有可能發生所謂的危障(hazard)。(1)請說明何謂危障？(2)危障有三種不同類型，請問是哪三種類型？【10 分】

第二題：

有一數列 35, 46, 59, 26, 47, 34, 10, 32, 14, 20, 16 要依序儲存至下列雜湊表(Hashing Table)中，雜湊函式 $f(x) = x \text{ mod } 11$ ，請回答下列問題：

- (一) 使用線性探測法(Linear Probing)處理碰撞，請說明最後的雜湊表為何？【10 分】
- (二) 使用平方探測法(Quadratic Probing)處理碰撞，請說明最後的雜湊表為何？【10 分】本方法中，該數列中最大搜尋次數為何？【5 分】

0	1	2	3	4	5	6	7	8	9	10

第三題：

請回答下列問題：

- (一) OSI 模型的七層架構是哪七層？請由上而下依序列出(請寫出每一層之正式名稱，中英文皆可)。【7 分】
- (二) TCP/UDP 協定是執行在 OSI 模型中的哪一層(請寫正式名稱，中英文皆可)？並說明此層之主要工作為何？【8 分】
- (三) 請針對 TCP 與 UDP 協定做說明，並比較兩者之優劣(至少兩項)。【10 分】

第四題：

請回答下列問題：

- (一) 進階持續性攻擊(Advanced Persistent Threat, APT)簡單的說就是針對特定組織所作的複雜且多方位的網路攻擊。近年來，APT 攻擊手法逐漸由傳統社交工程轉向水坑式攻擊。請問何謂水坑式攻擊(Watering hole)？【4 分】
- (二) 密碼學中有一種加密方法叫做替換加密法(substitution cipher)。其做法就是一種以特定方式改變字母表上字母順序，並以此順序替換原始訊息的加密方式。這樣一張改變了字母次序的字母表即為『替換表』。替換表可以說就是加解密的金鑰。因為知道替換表才能正確加密，接收方也才能正確解密。下表是一個金鑰的範例。

替換前	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
替換後	Z	E	B	R	A	S	C	D	F	G	H	I	J	K	L	M	N	O	P	Q	T	U	V	W	X	Y

用上表的金鑰加密訊息 HELLO，則得出密文為 DAILL，

- (1) 請問替換加密法的替換表，也就是金鑰的變化有多少種？【3 分】
- (2) 請問這種加密方式是否安全？請說明原因。【3 分】
- (三) 數位簽章(digital signature)是一種公開金鑰密碼技術。請問數位簽章提供的三大功能為何？【6 分】
- (四) 請說明 SYN flooding 洪水攻擊的原理及可能的防禦機制。【9 分】