103 年特種考試交通事業鐵路人員考試試題

等 級：高員三級鐵路人員考試
類 科：電子工程
科 目：計算機概論

一、計算機的內部設計架構，依 Flynn 所提出的論述，可分成四類：SISD、SIMD、MISD 及 MIMD。
㈠請問其中那一種架構最不常見？為什麼？
㈡大多數計算機內部只含有單一的處理器，應將之歸類為那一種架構？為什麼？
㈢請寫出 SIMD 的英文全名。

【擬答】：
㈠MISD（Multiple Instruction Single Data）：多指令（CPU）處理單資料（流），效率差，無實作。
㈡目前 CPU，常內建多媒體指令集如 MMX、SSE，可用單一指令處理多個資料流，以提升多媒體資料處理能力，故可歸類在 SIMD 架構。
㈢SIMD（Single Instruction Multiple Data）：單指令（CPU）處理多資料（流）。

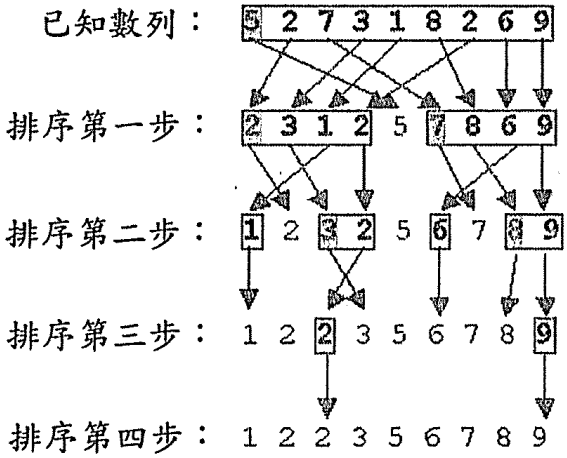
二、internet documents 有三種：㈠static documents ㈡dynamic documents ㈢active documents。請說明這三者最主要的差別為何？

【擬答】：
㈠static documents：靜態文件，文件內容一經發佈，不會自動反應最新內容，實例如一般靜態網頁。
㈡dynamic documents：動態文件，文件內容自動保持在最新狀態，實例如 WIKI、股票報價。
㈢active documents：主動文件，依據使用者的輸入（包括手勢與鍵盤滑鼠相關操作），決定文件內容，實例如 ASP（Active Server Page）網頁。

三、作業系統中常發生一些狀況如下，請說明其發生的原因。
㈠死結（dead lock）
㈡飢餓（starvation）
㈢分頁錯誤（page fault）
㈣記憶體外部碎片問題（external fragmentation）及內部碎片問題（internal fragmentation）

【擬答】：
㈠死結：多筆交易（行程）相互等待對方所持有資源的僵局現象，條件有四，如互斥、持有並等待、不可搶先、循環等待，可用預防（Prevention）或偵測（Detection）技術解決。
㈡飢餓：一筆交易，被無止盡凍結（Indefinite Blocking），如動態環境下，低優先權行程持續等待高優先權行程先執行，可改用公平等待機制（如先到先服務；First Come First Serve，FCFS）或老化（Aging，等愈久優先權愈高）技術解決。
㈢虛擬記憶體中的需求分頁（Demand Paging），為分頁法變形；分頁先存硬碟，有需求時，因分頁不在主記憶體，稱分頁錯誤（Page Fault），需以分頁程式（Pager，又稱懶惰置換程式，Lazy Swapper）載入。
㈣記憶體管理技術，若採固定大小靜態區塊，會因行程過小，造成區塊內部有未使用的閒置空間，稱內部破碎（Internal Fragmentation）；若採動態分割，因多次記憶體分割、配置與回收，易有多個洞，即總空間足夠，但因不連續而無法使用，稱外部破碎（External Fragmentation），可以聚集（Compaction，小碎片合成大的連續區塊）或改用不連續記憶體配置策略（簡單分頁｜分段）解決。

四、下圖是某種排序演算法執行的範例。



㈠請問這個排序演算法的名稱為何？

㈡此排序演算法在處理 n 個資料時，其平均時間複雜度為何？

㈢此排序演算法在處理 n 個資料時，其最壞的時間複雜度為何？

㈣這個排序演算法採用 divide and conquer 的解題策略，請說明如何由上圖看出它是 divide and conquer 的解題策略？

㈤這個排序演算法並不是一種 in-place algorithm，請說明其理由。

【擬答】：

㈠依題意（圖示），以串列第 1 個元素為樞紐（Pivot，P），分（切割）左（<P）、右（>P），遞迴處理，故為快速排序（Quick Sort），又稱分割交換排序法。

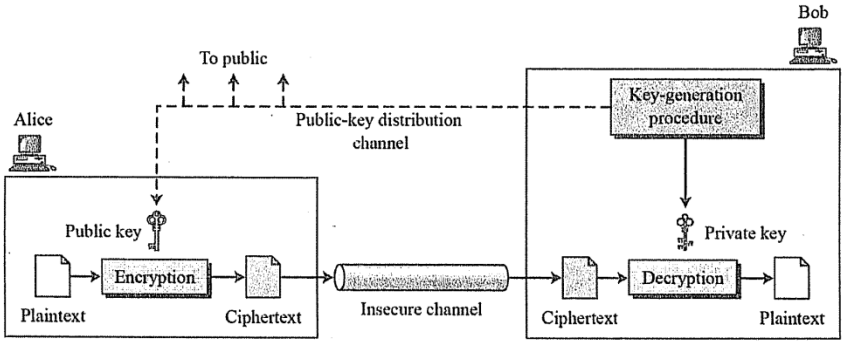
㈡比較次數：最佳（Pivot 均分資料）與平均，皆為 $O(N\log_2 N)$。

㈢比較次數：最差，分割極度不均，左 N－1 右 0，$O(N^2)$。

㈣分而治之（Divide & Conquer）：問題分割、處理再合併（Top-Down）；適用遞迴關係問題，如河內之塔、快速｜合併排序、二元搜尋；由上圖，以串列第 1 個元素為樞紐（Pivot，P），分（切割）左（<P）、右（>P），遞迴處理，故為 Divide & Conquer 的解題策略。

㈤僅需少量（常數等級）的額外空間，轉換資料，稱原地演算法；快速排序，需遞迴呼叫堆疊空間（最差 $O(N)$；最佳 $O(\log_2 N)$；對數以上），故為非原地（Not-In-Place｜Out-Of-Place）演算法。

五、下圖是 RSA public-key cryptosystem 的示意圖。



㈠請問 Plaintext 和 Ciphertext 有何不同？

㈡上圖中 Private key 必須隱密地加以保存，請問需由誰隱密地加以保存？

㈢RSA public-key cryptosystem 被歸類為非對稱式密碼系統（asymmertric cryptosystem），請問為何是「非對稱式」？

㈣另外有一類對稱式密碼系統（symmertric cryptosystem），請問它和非對稱式密碼系統的主要差別在那裡？

㈤RSA public-key cryptosystem 運作時，需選擇兩個大的質數 p 和 q，要計算其乘數積 $N=p\times q$ 是很容易的，但是反過來說，有一個計算問題是非常困難的。故 RSA 之安全性取

決於這個計算問題之困難度。請問這個困難的計算問題為何？

【擬答】：

㈠明文（Plaintext）：一般人可輕易解讀內容的本文，又稱可讀性本文（Readable Text）；非本意密文（Ciphertext）：將明文，以不易解讀的方式呈現，可避免資訊外洩，又稱不可讀本文（Unreadable Text）。

㈡私鑰（Secret Key）為擁有者個人私有，需小心存放；以上圖為例，Private key 需由 Bob 隱密保存。

㈢加解密使用一對金鑰（分公私），公鑰加密私鑰解，私鑰加密公鑰解，故稱非對稱式加密法；公鑰自由傳（對外公開），私鑰小心存（個人私有），又稱公開金鑰加密法，可用於文件保密（機密性）與來源證明（完整性＋驗證性＋不可否認性），常見有 Diffie-Hellman（解決對稱式加密法中金鑰交換問題）與 RSA（使用最廣）演算法。

㈣對稱式加密法：加解密使用相同金鑰，配合相同但逆向計算的演算法，又稱私密金鑰加密法（Secret Key Cryptography），僅可用於文件保密（機密性），常見有 DES、3DES、AES、OTP、RC5。

㈤RSA 演算法，（N，e）為公鑰（已知），（N，d）是私鑰，且 $N=p\times q$，得 p、q 才能計算 d（$(d\times e)MOD((p-1)\times(q-1))=1$；破解私鑰），RSA 安全度建立在將 1 個大整數分解成 2 質因數乘積的難題上。