

103年公務人員特種考試警察人員考試
103年公務人員特種考試一般警察人員考試
103年特種考試交通事業鐵路人員考試試題

代號：70940 全一張
(正面)

等 別：高員三級鐵路人員考試

類 科：電子工程

科 目：計算機概論

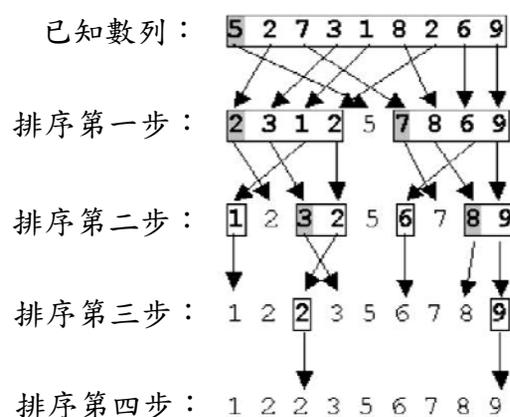
考試時間：2小時

座號：_____

※注意：(一)禁止使用電子計算器。

(二)不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。

- 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。(每小題 5 分，共 15 分)
- (一)請問其中那一種架構最不常見？為什麼？
- (二)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？
- (三)請寫出 SIMD 的英文全名。
- 二、internet documents 有三種：(一) static documents (二) dynamic documents (三) active documents。請說明這三者最主要的差別為何？(15 分)
- 三、作業系統中常發生的一些狀況如下，請說明其發生的原因。(每小題 5 分，共 20 分)
- (一)死結 (dead lock)
- (二)飢餓 (starvation)
- (三)分頁錯誤 (page fault)
- (四)記憶體外部碎片問題 (external fragmentation) 及內部碎片問題 (internal fragmentation)
- 四、下圖是某種排序演算法執行的範例。(每小題 5 分，共 25 分)



- (一)請問這個排序演算法的名稱為何？
- (二)此排序演算法在處理 n 個資料時，其平均時間複雜度為何？
- (三)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？
- (四)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？
- (五)這個排序演算法並不是一種 in-place algorithm，請說明其理由。

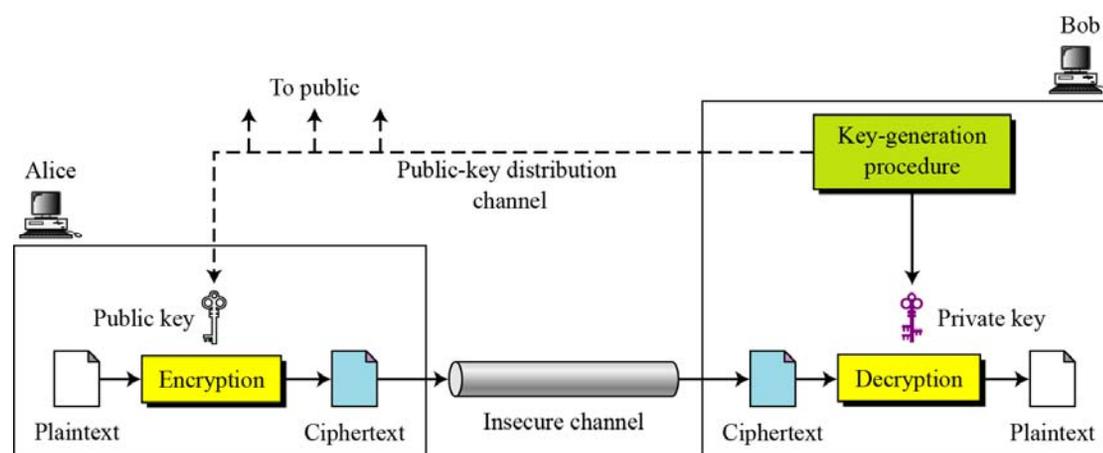
(請接背面)

103年公務人員特種考試警察人員考試
103年公務人員特種考試一般警察人員考試
103年特種考試交通事業鐵路人員考試試題

代號：70940 全一張
(背面)

等 別：高員三級鐵路人員考試
類 科：電子工程
科 目：計算機概論

五、下圖是 RSA public-key cryptosystem 的示意圖。(每小題 5 分，共 25 分)



- (一) 請問 Plaintext 和 Ciphertext 有何不同？
- (二) 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？
- (三) RSA public-key cryptosystem 被歸類為非對稱式密碼系統 (asymmetric cryptosystem)，請問為何是「非對稱式」？
- (四) 另外有一類對稱式密碼系統 (symmetric cryptosystem)，請問它和非對稱式密碼系統的主要差別在那裡？
- (五) RSA public-key cryptosystem 運作時，需先選擇兩個大的質數 p 和 q ，要計算其乘積 $N=p \times q$ 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？