

類 科：電力工程、電子工程、電信工程

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。

(三)本科目除專門名詞或數理公式外，應使用本國文字作答。

- 一、如果任何布林函數 (Boolean function) 可以藉著重複使用一種邏輯閘或一組邏輯閘來建構，則稱該邏輯閘或該組邏輯閘為通用的 (universal)。例如，集合 {AND, OR, NOT} 是一組通用的邏輯閘。請寫出 AND, OR, 與 NOT 邏輯閘的真值表。然後使用這三種邏輯閘設計與畫出一個 2 對 1 多工器，並說明其動作。所謂的 2 對 1 多工器為一個組合邏輯模組，它由兩個資料輸入端 (I_0 與 I_1)、一個標的選擇線 (S) 與一個資料輸出端 (Y) 組成。當選擇線 (S) 為邏輯 0 時，輸入資料端 I_0 的值即傳送到資料輸出端 (Y)；當選擇線 (S) 為邏輯 1 時，輸入資料端 I_1 的值即傳送到輸出端 (Y)。(20 分)
- 二、目前固態硬碟 (SSD, solid-state disk or solid-state driver) 已經廣泛地使用在計算機 (或稱電腦) 系統或是當作資料儲存的隨身碟。目前用來生產固態硬碟的 NAND Flash 有四種，分別是單層式儲存 (SLC)、多層式儲存 (MLC, 通常用來指稱雙層式儲存)、三層式儲存 (TLC)、四層式儲存 (QLC)。請說明這四種 NAND Flash 的差異，再由使用者觀點，比較它們的讀寫速度、使用壽命與成本。(20 分)
- 三、在計算機 (或稱電腦) 系統或是計算機網路中，資訊傳輸的安全性倍受重視。為此，許多不同的加密與解密技術 (或稱演算法) 廣泛的應用於此等系統中，研究這些技術的專門學問則稱為密碼學 (cryptography)。然而這些技術可以歸納為兩大類：對稱式密碼學 (symmetric cryptography) 與非對稱式密碼學 (asymmetric cryptography)。請說明這兩者的區別。又公鑰 (public key) 與私鑰 (private key) 與上述兩種密碼學有何關連？請說明之。(20 分)
- 四、欲將桌上型計算機 (或稱電腦) 連接到網際網路時，必須設定下列四個 TCP/IP 通訊協定的項目：IP (internet protocol) 位址、子網路遮罩 (subnet mask)、預設閘道 (default gateway) IP 位址、DNS (Domain Name System 或是 Domain Name Server) IP 位址。請說明上述各項目的功能。(20 分)

五、在計算機系統中，搜尋 (search) 資料為一個常用的演算法。今有一個 N 個元素的陣列。請先由計算機科學的觀點定義什麼是演算法，再說明循序搜尋 (sequential search) 與二元搜尋 (binary search) 的適用時機，並使用運算的次數為時間單位，比較兩種搜尋方式在搜尋上述 N 個元素的陣列時的最小搜尋時間、平均搜尋時間與最大搜尋時間。(20 分)