

*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本項測驗僅得使用簡易型電子計算器(不具任何財務函數、工程函數、儲存程式、文數字編輯、內建程式、外接插卡、攝(錄)影音、資料傳輸、通訊或類似功能)，且不得發出聲響。應考人如有下列情事扣該節成績 10 分，如再犯者該節不予計分。1.電子計算器發出聲響，經制止仍執意續犯者。2.將不符規定之電子計算器置於桌面或使用，經制止仍執意續犯者。

⑥答案卷務必繳回，未繳回者該節以零分計算。

第一題：

軟體測試(Software Testing)是指在規定的條件下操作程序，發掘程序是否有錯誤，用以衡量軟體的品質、正確性、完整性，並評估軟體是否滿足使用者需求的過程。請回答下列問題：

- (一) 何謂單元測試(Unit Testing)、系統測試(System Testing)、整合測試(Aggregate Testing)與驗收測試(Acceptance Testing)?【12 分】並說明於系統開發過程中，上述測試進行的先後順序為何?【3 分】
- (二) 測試模式中的白箱測試(White Box Testing)與黑箱測試(Black Box Testing)運作方式為何?請分別說明之。【6 分】
- (三) 單元測試、系統測試、整合測試和驗收測試，分別採用的測試模式為白箱測試或黑箱測試?【4 分】

第二題：

由於軟硬體技術進步，資訊系統的需求量與複雜度大幅提升，因此資訊系統開發愈來愈重要。請回答下列問題：

- (一) 瀑布模式(Waterfall Model)軟體開發週期分為哪幾個階段?【10 分】
- (二) 雛型模式(Prototyping Model)系統開發程序和參與人員為何?【7 分】
- (三) 何謂敏捷軟體開發(Agile Software Development)主要開發理念和價值觀的敏捷宣言(Agile Manifesto)?【8 分】

第三題：

網路攻擊日益嚴重，防火牆為企業組織非常重要的網路安全機制。請回答下列問題：

- (一) 封包過濾防火牆的運作機制為何?【10 分】
- (二) 封包過濾防火牆是否能抵擋 SQL Injection 的攻擊?原因為何?【5 分】
- (三) 利用防火牆建置安全區域(Demilitarization Zone, DMZ)的目的為何?【10 分】

第四題：

DES(Data Encryption Standard)與 AES(Advanced Encryption Standard)都屬於秘密金鑰密碼系統且都使用區塊加密法。請回答下列問題：

- (一) 這兩種加密法在秘密金鑰可使用的金鑰長度及加密區塊長度有何不同?【10 分】
- (二) 現代電腦硬體技術的進步，傳統 DES 加密法在安全性上受到挑戰；因此美國標準技術局在 1999 年提出 Triple-DES (三重 DES) 密碼系統，請說明 Triple-DES 的四種實作法為何?【15 分】