105年專門職業及技術人員高等考試建築師、
技師、第二次食品技師考試暨普通 代號：01360
考試不動產經紀人、記帳士考試試題

全一張
（正面）

等　　別：高等考試
類　　科：資訊技師
科　　目：系統分析與資訊安全
考試時間：2 小時　　座號：_____

※注意：㈠可以使用電子計算器。
㈡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、書本（Book）由作者（Author）撰寫，再由出版商（Publisher）出版，並由書店（Book Store）出售，最後由讀者（Reader）閱讀。而讀者必須先由銷售的書店購買書本，方可閱讀之。請針對此情境繪製使用案例圖（Use Case Diagram），並顯示不同使用案例間之關係。（10 分）

二、電梯控制器（Elevator Controller）依據各按鈕被按壓與否，控制 N 層樓大樓中之電梯（Elevator）動作。電梯系統說明如下：

- 除一樓和頂樓外，各樓層皆有位於電梯外之樓層升降按鈕（Floor Button），其中 1 個請求電梯上升，另 1 個請求電梯下降。乘客（Passenger）按壓按鈕後，按鈕會亮，而當電梯沿所要求方向移動至乘客所處樓層時，門（Door）將打開，且按鈕燈會熄滅。
- 每部電梯中有一組 N 個按鈕之電梯按鈕（Elevator Button）。乘客按壓對應樓層之電梯按鈕後，按鈕會亮，並使電梯移動至相對應樓層。當電梯到達相對應樓層時，門（Door）將打開，且按鈕燈會熄滅。
- 當無請求時，門會保持關閉，電梯停留將在目前樓層。

㈠請畫出與樓層升降按鈕相關之循序圖（Sequence Diagram）。（5 分）
㈡請畫出與電梯按鈕相關之循序圖。（5 分）

三、請說明階段式（Staged）能力成熟度整合模型（Capability Maturity Model Integration, CMMI）將軟體組織分成那幾個成熟度等級？各成熟度等級之意涵為何？（10 分）

四、某資訊系統專案建置成本為 1,500,000 元，完成後每年帶來之利益及維護成本如下表：

年度	第 0 年（建置）	第 1 年	第 2 年	第 3 年	第 4 年
利益		800,000	1,000,000	1,300,000	1,500,000
成本	1,500,000	300,000	400,000	500,000	600,000
淨獲利					
累積淨現金流					

假設年利率（Interest Rate）為 10%，並需考量貼現現金流（Discounted Cash Flow），請回答下列問題：

㈠此專案之各年度淨獲利（Net Profit）及累積淨現金流（Cumulative Net Cash Flow）為何？（10 分）
㈡此專案 4 年後之整體投資報酬（Return on Investment, ROI）為何？（5 分）
㈢此專案之損益平衡點（Break Even Point, BEP）時間為何？（5 分）
（提示：可能會用到這些計算值：$(1.1)^2=1.21$, $(1.1)^3=1.331$, $(1.1)^4=1.4641$）

（請接背面）

105年專門職業及技術人員高等考試建築師、
技師、第二次食品技師考試暨普通 代號：01360
考試不動產經紀人、記帳士考試試題

全一張
（背面）

等　　別：高等考試
類　　科：資訊技師
科　　目：系統分析與資訊安全

五、下表所描述為簡易對稱式密碼系統的加密函數（Encryption Function）。K = M = C = {a, b, c, d}，其中 M 集合中之明文，透過 K 集合中之金鑰，轉換為 C 集合中之密文。例如：明文 c 經由金鑰 b，變成密文 a；明文 b 經由金鑰 d，變成密文 c。請寫出對應之解密函數（Decryption Function）表格。（10 分）

		M			
		a	b	c	d
K	a	d	a	c	b
	b	b	d	a	c
	c	c	b	a	d
	d	a	c	d	b

六、迪菲赫爾曼（Diffie-Hellman）金鑰交換演算法可使通訊雙方通過不安全通道，建立一把雙方共用之秘密金鑰（secret key）。

㈠請描述迪菲赫爾曼金鑰交換演算法之內容。（5 分）

㈡迪菲赫爾曼演算法之安全性係基於何種計算複雜性？（3 分）

㈢迪菲赫爾曼演算法易受何種攻擊？如何防止？（4 分）

㈣假設 Alice 與 Bob 欲使用迪菲赫爾曼演算法建立共用秘密金鑰。雙方事先約定模數（modulo）p=203，生成元素（generator）g=17。於秘密金鑰建立期間，Alice 送出之訊息為 75，而 Bob 送出之訊息為 88。請問 Alice 與 Bob 之共用秘密金鑰為何？（8 分）

七、㈠通行密碼（password）長度為 8 個字元，每個字元可為大寫英文字母、小寫英文字母或是十進制數字（0-9）之一。若使用暴力攻擊法（Brute-force Attack）猜測通行密碼，請問最多需嘗試多少種組合？（5 分）

㈡假設使用算術加法函數儲存通行密碼：先將各字元轉換為其 ASCII 數字代碼（例如：'A'變成 65，'a'變成 97 等），再將其加上一固定整數，並將結果儲存於 `/etc/passwords` 檔案中。請問以此機制儲存通行密碼是否安全？原因為何？（5 分）

八、請說明組織實作對保護個人隱私權之原則中的「同意及選擇原則」與「資料極小化原則」之實務處理程序。（10 分）