113 年公務人員國家安全局國家情報人員考試試題

考　試　別：國家安全情報人員考試
等　　別：三等考試
類科組別：資訊組（選試英文）
科　　目：資料庫應用
考試時間：2 小時

一、有一連鎖商店使用[訂單資料表]儲存訂單，並將訂單所訂購的產品明細使用[訂單明細資料表]儲存，產品名稱、庫存數量、採購部門等資料則儲存於[產品資料表]，[訂單資料表]、[訂單明細資料表]和[產品資料表]的欄位如下所示：
訂單（訂單編號，商店編號，訂單年，訂單月，訂單金額，付款方式，運送編號）
訂單明細（訂單編號，產品編號，數量，單價，小計）
產品（產品編號，產品名稱，庫存數量，單價，部門）
請使用結構化查詢語言（SQL）的子查詢（Subquery）和內隱聯合查詢（Implicit Join）兩種方式，分別列出 2024 年各部門販售多少種產品。（20 分）

【解題關鍵】
《考題難易》：★★★(最多五顆星)
《破題關鍵》：分群統計 SQL 語法及子查詢與內隱聯合查詢的差異；要求依指定方式寫出 SQL 語法歷年罕見，需留意。

【擬答】

㈠ 子查詢語法：

```
SELECT   部門，COUNT(產品編號)
FROM     產品
WHERE    產品編號 IN（
             SELECT  產品編號
             FROM    訂單，訂單明細
             WHERE  訂單.訂單編號＝訂單明細.訂單編號  AND
                    訂單年＝2024）
GROUP BY  部門；
```

㈡ 內隱聯合查詢：

```
SELECT   產品.部門，COUNT(DISTINCT  訂單明細.產品編號)
FROM     訂單，訂單明細，產品
WHERE    訂單.訂單編號＝訂單明細.訂單編號  AND
         訂單明細.產品編號＝產品.產品編號  AND
         訂單.訂單年＝2024
GROUP BY  產品.部門；
```

DB—8。

二、某一學校有一[實驗室分配資料表]，內含三個欄位，分別為學生學號、實驗室編號和教授姓名，已知學生學號和實驗室編號為主鍵（PK），以字下線表示，如實驗室分配資料表（學生學號，實驗室編號，教授姓名），內容如下表所示。請列出功能相依性（Functional Dependency），並將[實驗室分配資料表]依序轉換成符合 BCNF（Boyce-Codd Normal Form），其正規化後的結果必須標示出必要的主鍵（PK）和外部鍵（FK）。（30 分）

學生學號	實驗室編號	教授姓名
11301	RM01	劉一
11302	RM02	陳二
11303	RM03	張三
11303	RM04	李四
11304	RM02	陳二
11305	RM03	張三
11306	RM01	王五
11301	RM02	陳二

【解題關鍵】
《考題難易》：★★★(最多五顆星)
《破題關鍵》：本題給定欄位數少，依 BCNF 定義，所有決定因子皆為候選鍵，分解資料表即可，參考講義第 6 章正規化。

【擬答】

㈠ 由表格內容，得下列 FD：

1. （學生學號，實驗室編號）→教授姓名。

2. 教授姓名→實驗室編號。

㈡BCNF 化簡如下：屬性加底線為主鍵，外鍵以 FK 表示。

1. 由 教授姓名→實驗室編號，得 R1（教授姓名，實驗室編號）；

2. 由剩餘屬性[實驗室分配資料表]－（實驗室編號），得R2（學生學號，教授姓名）；FK：教授姓名→R1.教授姓名。

㈢ 上述分解，所有決定因子皆為候選鍵，符合 BCNF。

DB—6。

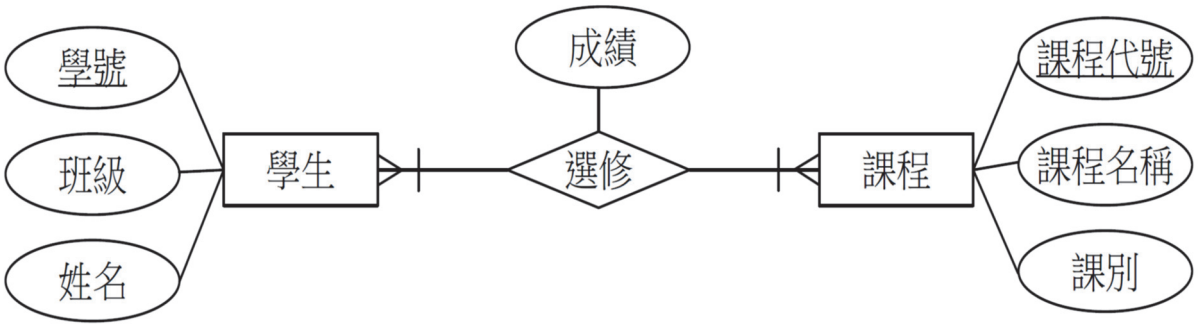
三、下表為 ABC 學校 113 學年第一學期學生修課紀錄表的一部份，經詢問業務承辦人得知，每位學生至少選一門課，每一門課最少需有一人選修，請使用 1 對多（1：N）關係的烏鴉腳表示法（Crow'S Foot Notation）畫出 ABC 學校 113 學年第一學期學生修課紀錄表的實體關係圖（Entity-Relationship Diagram）。（30 分）

ABC 學校 113 學年第一學期學生修課記錄						
學號	班級	姓名	修課資料			
			課程代號	課程名稱	課別	成績
9901001	國貿二	劉一	C01	國文	必修	80
			C02	英文	必修	75
9901002	國貿二	陳二	C02	英文	必修	60
			C03	會計學	必修	50
			C04	計量經濟	選修	65
9901003	國貿三	張三	C01	國文	必修	85

【解題關鍵】
《考題難易》：★★★(最多五顆星)
《破題關鍵》：掌握 Crow Foot 中基數比&參與限制的特殊表示法，繪製 ERD 即可，參考講義第 3 章概念設計－實體關係模型。

【擬答】

ERD 以 Crow Foot 表示，如下圖，屬性加底線為主鍵；學生—選修—課程，多對多關係。



DB—3。

四、有一電子商務網站，前端網頁讀入使用者輸入的會員帳號變數為 acc，密碼變數為 pwd，呼叫後端動態網頁程式。其中會員資料的帳號和密碼存於 member 資料表，其欄位名稱分別為 account 和 password。有一使用者在前端表單帳號欄輸入任一字串，密碼欄輸入特定字串，雖然該使用者所輸入的帳號和密碼組合，並未儲存於 member 資料表中，卻可以通過程式檢核而進入會員區，請問這種對資料庫的入侵行為的攻擊名稱為何？解釋造成此攻擊效果的原因，並說明二種防制的方法。（20 分）

【解題關鍵】
《考題難易》：★★★(最多五顆星)
《破題關鍵》：SQL Injection，近年常考重點題型，完整實例可參考「110 年—警察二—資料庫—第四題」；SQL Injection 防制方式，歷年首見，需留意。

【擬答】

㈠ 可能會有 SQL Injection（資料隱碼）的資安風險 SQL，即以 SQL 語法缺失（將攻擊指令放入資料庫命令中藉以竊取或竄改資料），入侵資料庫。

㈡ 常見攻擊手法：以網址 http://someASP.asp?acc=xxx pwd=yyy，且 SQL 語法 SELECT* FROM member WHERE(account='xxx') and (password='yyy');為例。

1. 略過權限檢查（Authorization Bypass）：在 acc 欄位輸入「'OR 1=1);--」，得 SQL 語法「SELECT* FROM memberWHERE(account="OR 1=1);-- and(...);」，查詢結果必成立（--為 SQL 註解），即可跳過權限檢查，進入系統。
2. 注入 SQL 子語法（Injecting SQL Sub-Statements into SQL Queries）：在 acc 欄位輸入「'OR 1=1); DROP TABLE member; --」，得 SQL 語法「SELECT* FROM member WHERE(account="OR 1=1); **DROP TABLE member;**-- and(...);」，先略過權限檢查後，再將另一個惡意 SQL 指令注入執行，破壞系統（如刪除 police 表格）。
3. 利用預存程序（Exploiting Stored Procedures）：在 acc 欄位輸入「'OR 1=1);EXEC master.dbo.xxSP; --」，得 SQL 語法「SELECT* FROM member WHERE(account="OR 1=1); **EXEC master.dbo.xxSP;**-- and(...);」，先略過權限檢查後，再呼叫已知預存程式，進行破壞。

㈢ 防制方式：

1. 參數化查詢（Parameterized Query）：SQL 語法中，在需要填入資料的地方，使用參數（Parameter）給值，語法如下；此法已被視為預防 SQL Injection 攻擊最有效防禦方式。
SELECT * FROM myTable WHERE myID = @myID;
2. 跳脫字元使用：將所有的網頁傳入參數，單引號字元前自動加上跳脫字元，避免視為 SQL 語法的一部份。

DB—18。