《資訊管理概要》

一、在資訊安全（Information Security）上提到利用密碼系統保護資訊必須提供下列功能：機密性（Confidentiality）、鑑定性（Authenticity）、完整性（Integrity）與不可否認性（Non-repudiation），請定義此四個功能。（20分）

試題評析	此題爲98年地特、100年關務及100地特之類似題，但與以往不同是此題點出「密碼系統」提供之功能，且使用了一個前所未見的中文翻譯「鑑定性」，增加考生困惑。實際上密碼系統即是密碼學，鑑定性即爲不可否認性，都是考生熟悉的範圍。 由於此題配了20分，因此在作答時除了寫出基本的定義，還要搭配防護技術與案例，才能拿到高分。
考點命中	102年《資訊管理與資通安全》講義第五回，金乃傑編著，P.80 102年《資訊管理與資通安全》總複習講義，金乃傑編著，考點26

答：

資訊安全是組織爲保護其資訊資源的一套技術與管理流程。依提意以下說明透過密碼系統達到之機密性、鑑定性、完整性與不可否認性的定義及內容：

(一)機密性（Confidentiality）：確保只有獲得授權的使用者才能存取資訊，保護資訊不被未授權存取或揭露。密碼系統提供了加密機制，可以確保資訊在傳輸與儲存時，不會被未授權的使用者檢視其內容。例如我們透過SSL（Secure Sockets Layer）對網頁瀏覽加密，可以避免駭客竊取我們在網頁上輸入的信用卡號碼；此外也可以在Windows系統中使用EFS（Encrypting File System）對個人資料夾加密，避免其他使用者讀取該資料夾之內容。

(二)鑑定性（Authenticity）：即爲身分認證性，當傳送方送出資訊時，就必須能確認傳送者的身分是否爲冒名。密碼系統使用公開金鑰基礎建設（PKI）確保網路使用者身分的有效性，在PKI架構中，有成對之公開金鑰與私密金鑰，兩金鑰可互爲加解密。如此設計當使用者以自己的私密金鑰加密時，唯有他的公開金鑰可以爲此資訊解密，即可確認他人無法假冒使用者發訊息。

(三)完整性（Integrity）：保護資訊與處理方法的精確性與完整性，確保資訊沒有不適當的修改或損毀。密碼系統使用MD5或SHA1等雜湊（Hash）演算法對資訊進行摘要（Digest）。當資料只要有一個bit差異時，所產生的訊息摘要就完全不同。如此只要比對訊息摘要是否相符，便可以確認資料爲操竄改。例如網路上的開放軟體常在下載處公布其軟體之MD5摘要編碼，讓下載者比對下載後之檔案與網站上之編碼是否相符，若相符則代表下載到的是正確版本的軟體。

(四)不可否認性（Non-Repudiation）：使用者已使用或接受某項服務時，不能否認其未使用過。不可否認性是鑑定性的延伸，鑑定性代表的是確認使用者是誰（Who you are?），而不可否認性還要進一步確認使用者從事了那些操作行爲（What you do?）。在密碼系統中，由於PKI的架構可以確保無法假冒他人發送訊息，因此當有訊息時，也可以確定「此訊息的確由此人發出」之不可否認性。

密碼系統是資訊安全中最基礎的技術環節，提供著技術面的基礎架構。但上述四個特性仍需要仰賴妥善的管理才能發揮作用。例如若私密金鑰遭竊，則就算有再高級的系統環境，仍然難以完成所需之安全目標。

二、順向工程及逆向工程提供了不同的方式來發展系統模型，請解釋何謂順向工程（Forward Engineering）及逆向工程（Reverse Engineering），並說明什麼是功能性需求（Functional Requirement）與非功能性需求（Nonfunctional Requirement）？（20分）

試題評析	此題爲系統分析的考題，需比較區分兩組相關的名詞並加以定義。由於名詞有相關，在說明時便需要強調他們各自的特性及如何加以區分。此外，由於題目配20分，也應平均分配作答版面，並加上舉例以具體描述名詞的意義及功能。
考點命中	101年《資訊管理與資通安全》第三回 P.11，金乃傑編著 102年研究所《管理資訊系統》第五回 P.21，金乃傑編著

答：

(一)順向工程與逆向工程：在資訊管理領域中，順向工程與逆向工程說明如下：

1.順向工程（Forward Engineering）：即爲建構目標資訊系統的流程。從分析、設計、編碼、單元測試、整合測試、驗收測試等階段逐步完成一個資訊系統。我們所見到大部份的資訊系統都是使用順向工程建構的。其主要應用如下：

(1)建立組織專用之資訊系統：爲組織專屬流程設計的資訊系統，因爲必須完整考量組織需求，因此必須從分析、設計等階段逐步完成，故須採取順向工程。

(2)建立策略型資訊系統：策略型資訊系統須讓組織擁有敵無我有的專屬優勢，故需從無到有開創，沒有其他系統可以參考，故須使用順向工程。

2.逆向工程（Reverse Engineering）：與順向工程相反，是對目標資訊系統進行解構，並了解其處理流程、組織結構、功能效能規格等設計要素，以製作出功能相近，但又不完全一樣的產品。逆向工程源其主要目的是，在不能輕易獲得必要的生產訊息下，直接從成品的分析，推導出產品的設計原理。其主要應用如下：

(1)模仿或盜版現有之資訊系統：此爲逆向工程最有爭議之處，因爲可能會破壞智慧財產權。透過逆向工程，開發者可以很快的獲取其他系統的流程設計，甚至原始程式碼，便可以修改他人所撰寫的系統成爲新的資訊系統。

(2)檢驗現有資訊系統的安全性：逆向工程解構資訊系統，使資訊系統不再是黑箱。我們可以透過逆向工程分析既有系統的漏洞，以預防或修復安全性問題。

(3)保護智慧財產權：可透過逆向工程取得程式原始碼的特性，分析競爭對手資訊系統的原始碼，了解競爭對手是否有在原始碼中抄襲，便能進一步的主張智慧財產權。

(二)功能性與非功能性需求：

1.功能性需求（functional requirement）：定義一個軟體系統或元件的功能，是計算、技術細節、資料處理或其他說明系統希望達成功能的內容，可以用一組輸入、行爲及輸出的組合來表示，常以非功能性需求爲基礎。功能性需求是定義系統的行爲，告訴系統需要完成那些任務，有哪些流程。例如會員系統必須要有「註冊」、「檢視會員資訊」、「管理會員資料」等功能。一般而言功能性需求會在系統設計（Systems Design）書中詳細的列出計劃。

2.非功能性需求（Non-functional requirement）：依一些條件判斷系統運作情形或其特性，而不是針對系統特定行爲的需求。可視爲爲了滿足客戶業務需求而需要符合，但又不在功能需求以外的特性。非功能性需求主要定義系統的特性，在系統架構（Systems Architecture）書中詳細列出計劃。通常可分爲：

(1)執行品質（Execution qualities）：可以在系統運作時觀察到的品質，例如安全性及易用性等。

(2)發展品質（Evolution qualities）：和軟體系統結構及開發過程有關的品質，例如定義系統測試所採用的方式及人員等。

三、在UML系統分析與設計上，必須了解屬性的定義、類別的定義及類別間的關係。試以紅色汽車、白色貨車及藍色漁船來說明何謂類別及屬性？並以車子、車輪和行動電腦為例來說明類別間關係Part-of和Has-a之定義為何。（20分）

試題評析	此題爲系統分析考題，測驗學生對物件導向塑模觀念的了解。必須清楚區分物件與屬性、物件間不同類型的關係。此題除了概念要清楚外，還必須要加以舉例說明，才能拿到高分。
考點命中	《系統分析與設計 理論與實務應用》四版 P.342-363，吳仁和、林信惠編著

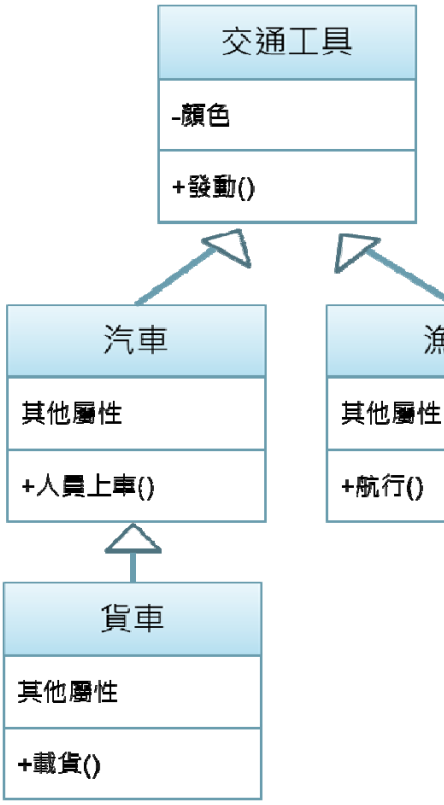
答：

(一)屬性的意義：題目中所列之物件：紅色汽車、白色貨車及藍色漁船，其中交通工具類型即爲「類別」；顏色即爲「屬性」，整理如下：

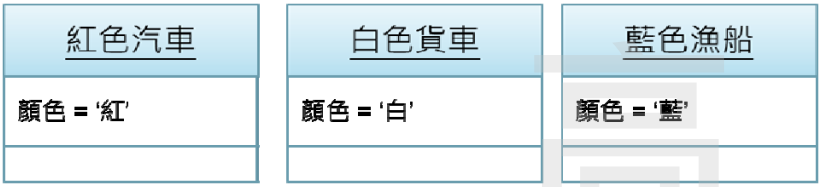
1.類別：交通工具的類型，如「汽車」、「貨車」與「漁船」

2.屬性：交通工具的顏色，如「紅色」、「白色」與「藍色」

以UML物件圖可能表示如下（爲了符合物件導向特性，且讓例子更具表達性，加入父類別與其他方法）：



而UML物件圖可以表示如下：



(二)Part-of與Has-a關係的意義：Has-a與Part-of是相反的觀念如題目中例子，車輪是Part-of車子；而車子Has-a車輪。其關係整理如下：

1.Part-of：車輪Part-of車子；行動電腦Part-of車子

2.Has-a：車子Has-a車輪；車子Has-a行動電腦

以UML描述其關係如下：

四、知識管理裡，Nonaka & Takuichi提出知識創造為SECI模式，請描述其內容。（20分）

試題評析	此題爲考古題，與98年地特、93年退役相似，解釋SECI模式的意涵。只要考生能掌握既有考題，應該很容易回答得當。但由於配分亦爲20分，除了說明其每個模式的定義，還需要加以舉例，並畫出SECI不通階段關聯的轉換圖，才能拿到高分。
考點命中	102年《資訊管理與資通安全》第二回 P.28-29，金乃傑編著 102年《考前30分鐘好題神》考點4，金乃傑編著

答：

SECI爲四個詞彙的縮寫：社會化（Socialization）、外化（Externalization）、組合化（Combination）與內化（Internalization）。是野中鬱次郎（Ikujiro Nonaka）於1989年《知識創造的企業》提出，組織動員個人的內隱知識，經由四種知識轉換模式在組織內部加以擴大，成爲較高層次的知識本體、知識轉移與創造的過程。其目的有二：從既有知識追求目標知識；減緩知識落差或跨越知識鴻溝。

詳述其內容：

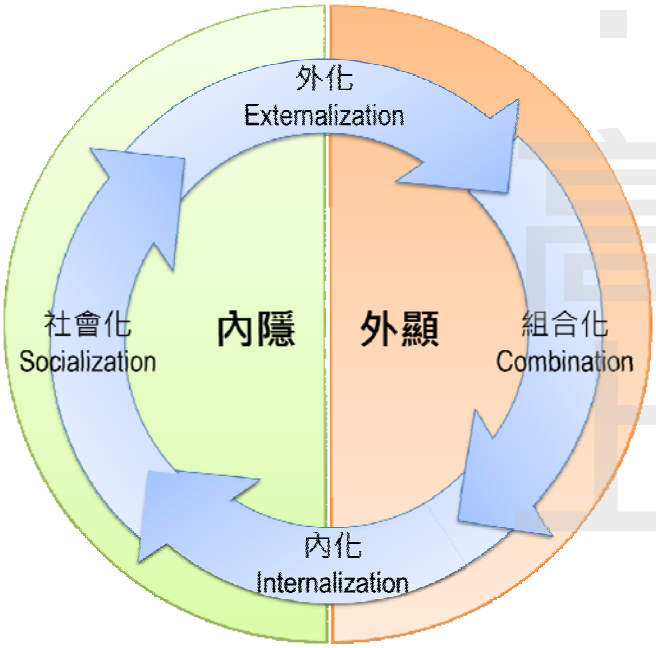
1.社會化：將內隱知識經由內隱學習與同化轉化到不同族群。例如同事習慣吃比較貴的餐點，也會潛移默化影響其他成員的消費習慣。

2.外化：將內隱知識外顯化，轉換爲可定義、可訴諸文字的外顯知識。例如吃過許多高級餐廳後，也可能訓練出較挑剔的味蕾，並將實用美食的經驗在網路上用文字加以分享。

3.組合化：由現有不同的外顯知識，經由分析、分類、分享及重組產生新的外顯知識。例如整理網路上眾多的美食食記，便可成爲美食地圖，供網友參考選擇美食餐廳。

4.內化：將知識透過實做、學習，改善其技能與知識，外顯知識轉換爲內隱知識。例如網友將網路上美食餐廳的彙整資料記在腦海裡，當有需要選餐廳的時候就可以憑藉印象選擇，即爲將外部知識變爲自己的知識。

以圖示呈現SECI的關係如下：



SECI將群體中部份人對餐廳選擇的變號轉化到組織其他成員中，在藉由不斷嘗試、分享、整合而創造完整的美食地圖，並使之成爲更多人生活的一部分，便是知識螺旋的價值。

五、正規化的目的簡單的說法是要將資料的重覆性降至最低，試說明資料庫正規化概念裡第一正規

化（INF）、第二正規化（2NF）及第三正規化（3NF）的重點。（20分）

試題評析	此題爲資料庫或系統分析中基礎的「資料正規化」知識，只要考生有充分準備資料庫或計算機概論，應不難應答。維此題亦須舉例說明每個正規化階段的具體變化，才能獲得完整的分數。
考點命中	《系統分析與設計 理論與實務應用》四版 P.174~186，吳仁和、林信惠編著

答：

資料庫正規化降低資料的重複性，並去降低發生資料異常的可能性。在正規化的過程中，每一層級的正規化都建立在上一層及之上，例如第二正規化（2NF）是建立在第一正規（1NF）化之上，因此也必須滿足第一正規化的所有條件，以此類推。以下說明1NF、2NF與3NF：

假設某公司建立銷售資料表，欄位內容如下：
銷售(訂單序號，訂貨日期，送貨日期，客戶代號，客戶名稱，客戶地址，產品代號，訂購數量，產品名稱，單價，庫存量)

第一正規化（1NF）：第一正規化是爲了要排除重複資料的出現，所採用的方法是要求資料庫的每個欄位都只能存放單一值，而且每筆記錄都要能利用一個唯一的主鍵來加以識別。例如上述資料表由於每筆訂單的產品代號、訂購數量、產品名稱、單價與庫存量都會重複且相同，因此可以將之獨立爲一個表，第一正規化後變爲：
訂單_客戶 (訂單序號，訂貨日期，送貨日期，客戶代號，客戶名稱，客戶地址)
訂單_產品 (訂單序號，產品代號，訂購數量，產品名稱，單價，庫存量)

第二正規化（2NF）：要求資料表裡的所有資料都要和該資料表的主鍵有完全相依關係；如果有哪些資料只和主鍵的一部份有關的話，就得把它們獨立出來變成另一個資料表。例如將上述第一正規化「訂單_產品」資料表中，僅以「產品代號」就可決定產品的名稱，單價，庫存量，存在部分功能相依，故可以將該表切開成兩個資料表：
訂單明細 (訂單序號，產品代號，訂購數量)
產品 (產品代號，產品名稱，單價，庫存量)

第三正規化（3NF）：檢驗是否所有非鍵屬性都只和候選鍵有相關性，也就是說所有非鍵屬性互相之間應該是無關的。例如上例中「訂單_客戶」資料表，雖然客戶代號不是主鍵，但卻可以決定「客戶名稱」與「客戶地址」，故應把它獨立出來，可將「訂單_客戶」拆成如下兩個表：
訂單 (訂單序號，訂貨日期，送貨日期，客戶代號)
客戶 (客戶代號，客戶名稱，客戶地址)

上述範例，原本的銷售資料表可以被拆爲四張表，如此當修改客戶地址的時候，就不需要到每筆產品訂單中修改，可以節省時間，並能增加正確性。資料表如下：
訂單明細 (訂單序號，產品代號，訂購數量)
產品 (產品代號，產品名稱，單價，庫存量)
訂單 (訂單序號，訂貨日期，送貨日期，客戶代號)
客戶 (客戶代號，客戶名稱，客戶地址)