

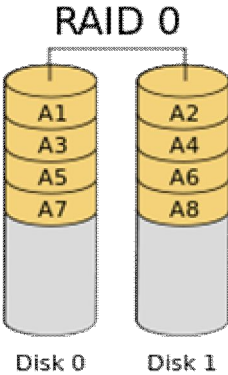
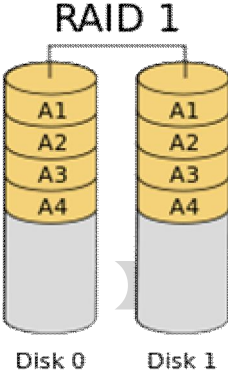
《資訊管理與資通安全》

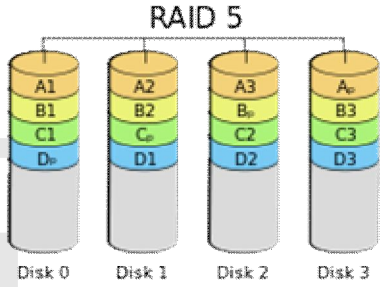
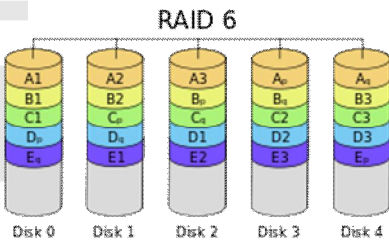
試題評析	<p>今年的題目與往年差異相當大，第一題考出RAID，較常出現在資料庫考題中，屬於資管中較冷門的範圍；第二題出現99年時比較熱門的實體隔離議題，對考生而言實屬難掌握，但因配合防火牆出題，認真準備的考生應可拿到部份分數；第三題和第四題都是資管常見的考古題，考對稱與非對稱加密及CMMI五個層級，都是課程中重要的概念。最後這兩題共佔50分，屬於較容易把握的題目。</p> <p>綜觀而論，今年題目偏向記憶，程度中等的考生應可以拿到50分以上，程度好的考生拿到80分也絕非難事。</p>
考點命中	<p>第一題：《高點·高上資訊管理與資通安全講義》第四回，金乃傑編撰，頁130-132與上課補充。</p> <p>第二題：《高點·高上資訊管理與資通安全講義》第四回，金乃傑編撰，頁83-85。</p> <p>第三題：《高點·高上資訊管理與資通安全講義》第四回，金乃傑編撰，頁24-27。 《高點·高上資訊管理與資通安全總複習講義》，金乃傑編撰，議題2，頁56-57。</p> <p>第四題：《高點·高上資訊管理與資通安全講義》第三回，金乃傑編撰，頁53-54。</p>

一、試敘述磁碟陣列RAID 0、RAID 1、RAID 5及RAID 6的功能與運作原理。它們分別最少需要多少個硬碟才能實現？（30分）

答：

RAID（Redundant Array of Independent Disks），容錯式磁碟陣列，透過將多個相對便宜的硬碟組合成為一個硬碟陣列組，使效能達到甚至超過一個價格昂貴、容量巨大的硬碟。下表說明RAID 0、RAID 1、RAID 5及RAID 6的功能、運作原理及最少實現的硬碟數：

RAID種類	功能	運作原理	示意圖	最少硬碟數
RAID 0	形成一個巨大的儲存空間。 高速的資料讀取與寫入。	將兩個以上的磁碟串聯起來，成為一個大容量的磁碟，將資料分段後分散儲存在這些磁碟中，因為讀寫時都可以並列處理，所以在所有的級別中速度最快。	 <p style="text-align: center;">RAID 0</p> <p style="text-align: center;">Disk 0 Disk 1</p>	2
RAID 1	提供最高的安全性。 高速的資料讀取。	在主硬碟上存放資料的同時也在映像硬碟上寫一樣的資料。當主硬碟（物理）損壞時，映像硬碟則代替主硬碟的工作。	 <p style="text-align: center;">RAID 1</p> <p style="text-align: center;">Disk 0 Disk 1</p>	2

RAID 5	是RAID 0和RAID 1的折衷方案，讀取速度接近RAID 0，但寫入速度稍慢；安全性RAID 1稍低，但磁碟利用率較高，儲存成本相對較便宜。	把資料和相對應的奇偶校驗資訊儲存到組成RAID 5的各個磁碟上，並且奇偶校驗資訊和相對應的資料分別儲存於不同的磁碟上。當RAID 5的一個磁碟資料發生損壞後，可以利用剩下的資料和相應的奇偶校驗資訊去恢復被損壞的資料。		3
RAID 6	極高度的安全性。	使用二個獨立的奇偶校驗資訊塊，並以不同的演算法實作，安全性相當高，即使兩塊磁碟同時失效也不會影響資料的使用。但因為需要分配給奇偶校驗資訊更大的磁碟空間，較差的效能和複雜的實作方式使得RAID 6很少得到實際應用。		4

二、什麼是網路實體隔離 (Network Physical Isolation) 設備？它與防火牆 (Firewall) 設備有何不同？(20分)

答：

- (一)網路實體隔離設備是實體隔離設備的一種，強調在網路資料上的實體隔離，主要目的是確保內部資料不會被外部竊取，或內部員工不會洩露資料。在政府機關中，常見的網路實體隔離設備是使用網路線做區隔，一條網路線連結對外的網際網路，一條網路線連接內部網路。在使用內部網路時，使用者就無法連上網際網路；反之亦然。若使用者電腦無法儲存資料，則可以完全確保內部機密不會被傳送至網際網路。值得一提的是，網路實體隔離技術是一套發展已久的技術，因此設備型態也相當多樣，如早期的「完全實體隔離」，使用使用兩台電腦，一台電腦連接外部網路，一台電腦連接內部網路，兩個網路無任何聯絡。當使用者要使用內部網路時，必須使用隨身碟或磁片將資料複製到內部網路中使用，亦屬網路實體隔離設備。
- (二)網路實體隔離設備與防火牆相異處如下表所示：

	網路實體隔離設備	防火牆
功能	使用軟體或硬體設備確保內部網路與外部網路不會有任何連通，以防止內部網路的重要資訊傳送到外部網路或外部網路的惡意連線存取內部網路資源。依照技術演進，可分為完全的實體隔離、網路卡隔離、資料傳送隔離、空氣開關隔離與專用通道隔離等五種。	可由軟體或硬體來實作的一種安全機制，用來隔離兩個安全信任度不同的網路。利用系統所建立的安全性規則，有效的控制對內與對外流量。依照實作方式，可分為封包過濾路由器、狀態檢視防火牆與應用層閘道器等三種。
限制	無法阻止未經網路的威脅，例如使用USB記錄內部資料、偷拍照等。即使操作非機密的資料，也無法將資料在內外部網路間流通。在不同網路間切換需要額外的時間成本，如重新開機、軟硬體採購等，並增加使用者操作的	無法阻止未經防火牆或全新的威脅。無法防止內部使用者利用其合法的身分作破壞系統的行為。無法防範病毒（木馬、蠕蟲）、緩衝區溢位攻擊、通訊埠掃瞄攻擊、碎片封包攻擊、系統與應用程式漏洞攻擊。

	難度。	易形成網路上的交通瓶頸；防火牆本身可能也存在弱點，以及其他安全性的設定錯誤。
使用者	操作內部重要資源的人員，內部人員具有主控權，決定使用內部網路電腦還是外部網路電腦。	防火牆具通透性，一般使用者無法感到防火牆存在。主要使用者是網管人員對其進行設定。
實體位置	使用到機密資源的辦公室內。	硬體防火牆存在於機房中；軟體防火牆安裝在需要防護的電腦上。
邏輯位置	內部網路與外部網路間。	在兩個安全性不同的網路間。

三、解釋何謂對稱式加密技術與非對稱式加密技術。請說明其優缺點，並說明這兩種加密技術分別適合的應用場合；此外，請針對這兩種加密技術各舉一個加密標準。（20分）

答：

將對稱式加密（Symmetric Encryption）與非對稱式加密（Asymmetric Encryption）之定義、優缺點、適用性及加密標準以表格整理如下：

	對稱式加密	非對稱式加密
內容	雙方持有同樣的金鑰來加密和解密。	使用兩把成對的金鑰，其中一把加密的資料可由另一把解密。由於運作上有一組金鑰被公開（Public key），另一把金鑰私密保存（Private key），所以又稱為「公開金鑰加密法」。
優點	較快速。 密文長度小於等於原始文章。 如果使用足夠大的金鑰，將難以破解。	公開金鑰可以公開分送。 無論與多少人交換訊息，僅需保管好私鑰。 提供私密性、驗證與不可否認性等服務。
缺點	不同對象要使用不同組金鑰，管理複雜，與N個使用者交換訊息，必須保管N把金鑰。 需要有一個安全性機制將金鑰安全性的分送至交易的雙方。 不支援數位簽章（不可否認性）。	速度較慢。 密文長度大於原始文章。 只要取得私鑰則可破解所有交易。
加密標準	DES（Data Encryption Standard）	RSA（Rivest、Shamir and Adleman）

四、請問能力成熟度模型集成（CMMI）將工作程序的改善（process improvement）分成那五個等級（level）？請說明每個等級的特色。（30分）

答：

能力成熟度模型集成（CMMI）是共通性之整合架構，支援整合不同專業領域之特定能力成熟度模式及相關產品，應用在軟體、系統工程、整合產品及流程發展等領域。CMMI將企業的軟體開發能力，依其執行的承諾度（Commitment）、品質與能力成熟度，分成下列五個層級：初始（Initial）、管理（Managed）、定義（Defined）、量化管理（Quantitatively Managed）與最佳化（Optimizing），特色與內容說明如下：

(一)初始層級：

- 1.軟體開發程序未被清楚定義，流程充滿了不確定性及混亂無章的狀態。
- 2.軟體的成敗主要靠幾個核心人物的聰明才智與努力，充滿個人英雄主義。

(二)管理層級：

- 1.具備基本的專業管理能力，對於軟體開發程序中的成本、時程及功能都有追蹤與管理。
- 2.已有能力依據以前的成功經驗與程序來複製開發類似的應用系統。

(三)定義層級：

- 1.軟體發展的工程活動和管理活動已標準化，且集結成爲組織標準流程資產（文件化）。
- 2.所有軟體的發展和維護都在這個標準基礎上制訂與執行。

(四)量化管理層級：

1. 量化評估：能以客觀、明確的量化指標，來清楚衡量軟體開發的活動與品質。
2. 品質保證：透過量化評估資料的蒐集與分析，來改善製造流程與品質，並能界定流程變異之特殊原因，適當的矯正該特殊原因之癥結，以防再度發生。

(五)最佳層級：

1. 持續改善：此階段主要特點在於利用量化評估資料的回饋，來分析成敗的原因與解決方案，並能持續地改善軟體開發的各流程及預防錯誤的發生。
2. 組織創新：此階段已可利用實驗性的先導計畫來嘗試新的開發方法。

一般而言，必須要達到熟度第三等級（定義層級），因為具有標準化與文件化，所產出的產品的可靠度才會較有保障。

高
點
·
高
上

【版權所有，重製必究！】