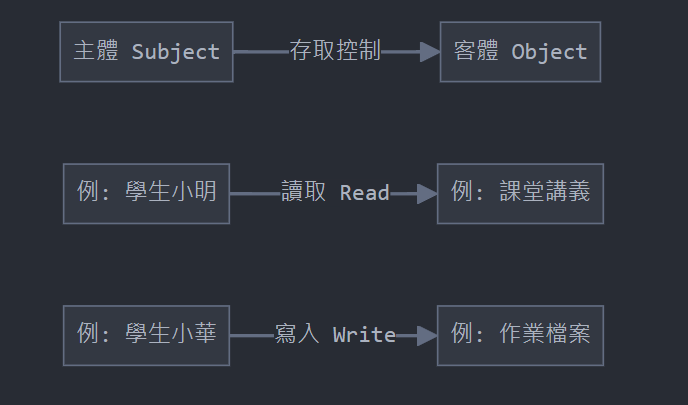
存取控制要素和原則

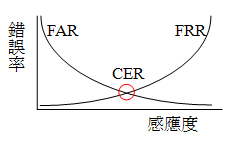
**存取控制四要素 (IAAA)**

* 存取控制相關概念
  + 主體(Subject)：主動發起存取要求者，如使用者、程序。
  + 客體(Object)：被存取的資源，如檔案、印表機、記憶體。
  + 存取權限(Access Control List, ACL)：主體對客體的操作類型，包含讀取、寫入、執行等。

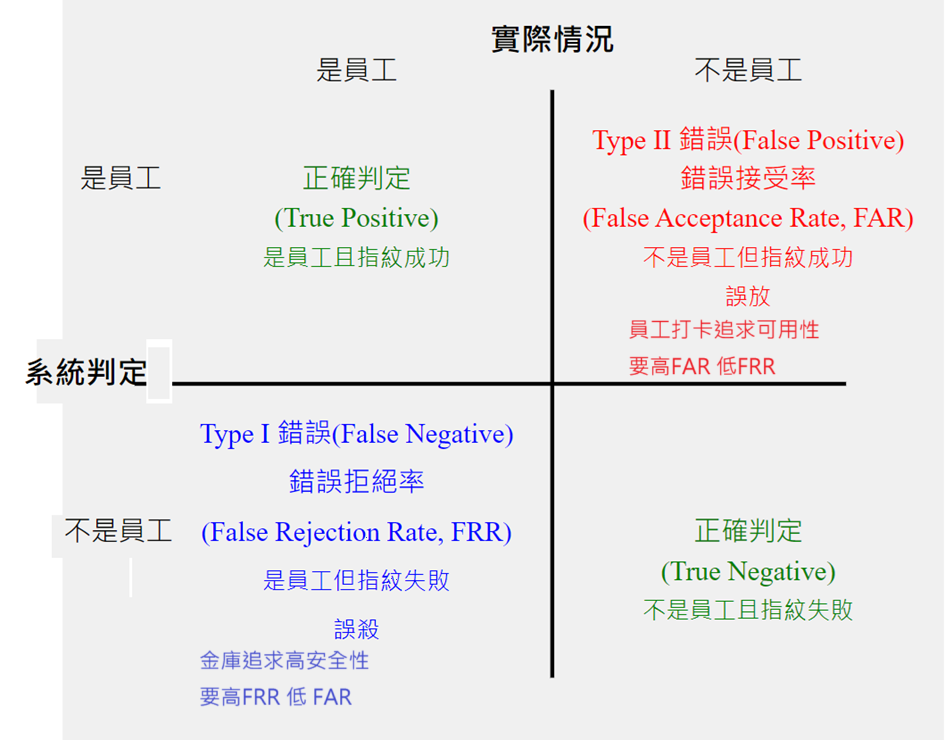


(資料來源：筆者自行整理)

* 識別(Identification)：用戶宣稱自己是誰。
* 例子：輸入使用者帳號。
* 認證(Authentication)：驗證用戶是否為其所宣稱的身份。
  + 生物辨識種類：指紋、臉型、虹膜。
  + 辨識錯誤類型
    - 第一型錯誤-誤殺(False Rejection Rate, FRR)
      * 拒絕合法使用者
    - 第二型錯誤-誤放(False Acceptance Rate, FAR)
      * 接受非法使用者
    - 交叉錯誤率(Crossover Error Rate, CER)
      * FAR 與 FRR 的交叉點，也稱相等錯誤率 (Equal Error Rate, EER)，通常表示辨識的效能最好。

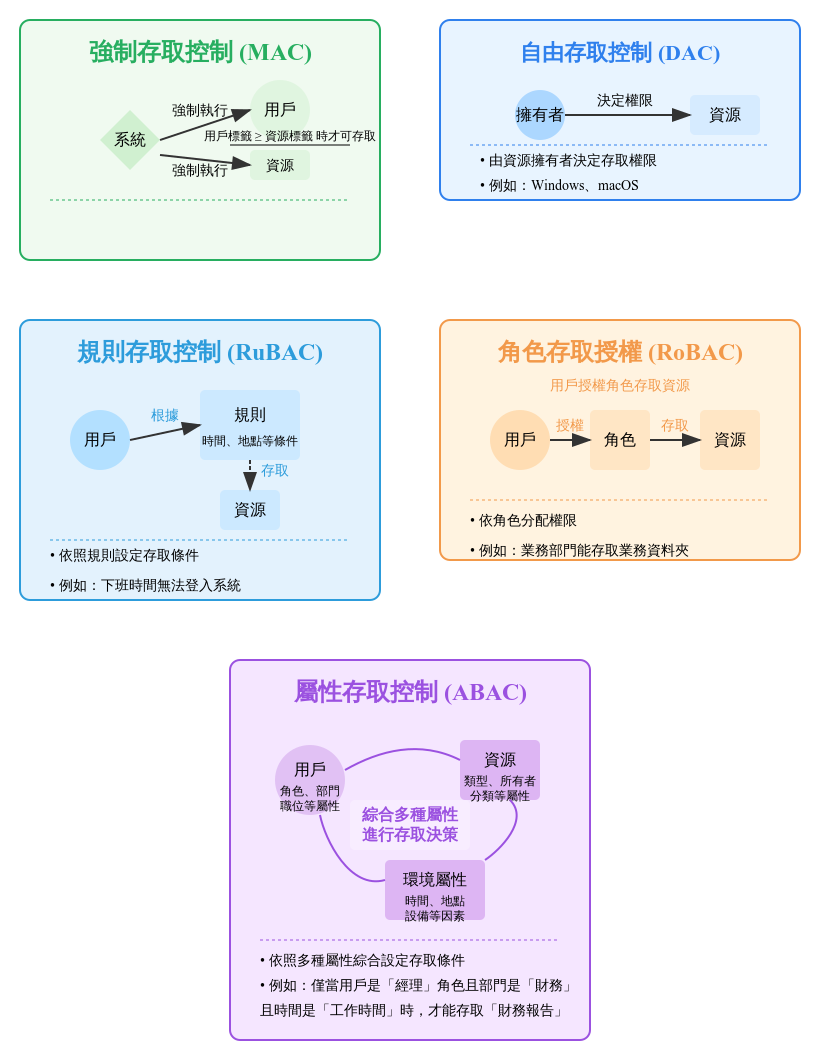


(資料來源：網際網路)



(資料來源：筆者自行整理)

* + 認證方式
    - 所知之事(What you know)：如密碼。
    - 所持之物(What you have)：如卡片、OTP。
    - 所具之形(What you are)：如指紋、臉型。
    - 多因子認證(MFA)：
      * 結合上述兩種以上，例如密碼 + 指紋。
* 授權(Authorization)：確定用戶可執行的操作範圍。
  + 自由存取控制(DAC)：
    - 由資源擁有者決定權限。
    - 例如：Windows、macOS、Linux。
  + 強制存取控制(MAC)：
    - 系統強制執行用戶和資源的權限，只有用戶高於資源才可以存取。
    - 例如：SELinux。
  + 角色存取控制(RoBAC)
    - 依角色分配權限。
    - 例如：業務部門能存取業務資料夾。
  + 規則存取控制(RuBAC)
    - 依照規則設定存取條件。
    - 例如說下班時間無法登入系統。
  + 屬性存取控制(ABAC)
    - 依照屬性設定存取條件。
    - 例如僅當使用者是「經理」角色且部門是「財務」且時間是「工作時間」時，才能存取「財務報告」。



(筆者自行整理)

* 紀錄(Accounting)：記錄存取行為。
  + 可歸責性 (Accountability)：追蹤使用情況，產生稽核報表，主要是要追朔到誰使用這個行為，產生問題時可歸責。

**存取控制原則**

* 職責區隔 (Segregation of Duties, SOD)：
* 同一業務由不同人負責不同部分，避免單人掌握所有權限。
* 例如：程式開發和上線由兩個人負責。
* 例如：管帳的不能管錢。
* 最小權限原則 (Principle of Least Privilege, PoLP)：
* 僅給予完成工作所需的最低權限。
* 例如：操作員不應擁有管理系統的權限。
* 僅知原則 (Need to Know)：
* 只能接觸工作所需的資訊。
* 例如：就算是主治醫生也只能查看自己的病人資料。
* 職務輪調 (Job Rotation)：
* 定期調動職務，避免單人長期掌握權限，有助於發現異常。
* 例如：銀行經理輪調後發現監守自盜行為。
* 強制休假 (Mandatory Vacation)：
* 要求員工強制休假，由他人代理工作，可發現異常行為。
* 例如：金庫管理員休假後發現款項短缺。
* 責任分擔 (Dual Control)：
* 避免高機密資訊由某人完整的持有，重要操作需兩人以上完成，相互監督。
* 例如：核彈發射需指揮官與總統同時在場。
* 例如：密碼頭尾由兩個人持有。
* 縱深防禦 (Defence in depth)：
  + 單一安全產品無法完全保護網路免受可能面臨的每一次攻擊。有時候也可稱為「分層式安全性」，它依賴於多個控制層 (實體、技術和管理) 的安全解決方案，來防止攻擊者存取受保護的網路或內部部署資源
  + 例如：公司結合防火牆、登入驗證和教育訓練來防止網路入侵。

考古題：

9. 下列關於「縱深防禦」的描述，何者較「不」合適？

(A) 縱深防禦是一種網路安全策略，它使用多種安全產品和做法來保護組織的網路、Web資產和資源

(B) 縱深防禦有時與「分層式安全性」一詞互換使用，因為它依賴於多個控制層（實體、技術和管理）的安全解決方案

(C) 縱深防禦透過實作多種安全產品和做法可以幫助偵測和阻止出現的攻擊，使組織能夠有效地緩解各種威脅

(D) 縱深防禦安全策略中，運用一個功能強大的產品來阻止攻擊者和其他威脅

規劃 114-1 答案D

(縱深防禦（Defense in Depth）強調利用多重防禦層次，結合各種技術、實體與管理措施來保護資訊資產，不依賴單一產品或控制措施。選項 (D) 表示僅依靠一個功能強大的產品來阻止攻擊者，這與縱深防禦的多層防護理念背道而馳，因此較不合適。)

10. 設計職務區隔（SoD）控制措施時，宜考量共謀之可能性。小型組織可能發現難以實施職務區隔，但於可能及可行之情況下，宜儘可能使用此原則。難以區隔職務時，宜考量採行相關控制措施來輔助，下列何者控制措施較「不」適切？

(A) 全權負責

(B) 活動監視

(C) 稽核存底

(D) 管理監督

規劃 114-1 答案A

(在職務區隔（SoD）的設計中，目的是減少單一個體對所有關鍵流程的控制權，從而降低共謀或內部欺詐的風險。對於小型組織而言，雖然難以完全實施職務區隔，但可以採用其他輔助控制措施，如活動監視、稽核存底和管理監督來彌補不足。相比之下，讓某個人全權負責則完全無法防範共謀的風險，因此較不適切。)

11. 請問下列對於資訊安全管理實務的描述何者較「不」正確？

(A) 縱深防禦（Defense in Depth）指在整實體、系統、網路或網宇（Cyberspace）中建置了多層的防禦機制

(B) 零信任架構（ZTA）已成為國內主流，目前國內企業組織的資訊及工控系統都已廣為採用零信任架構

(C) 僅知原則（Need-to-Know Principle）與最小權限原則（Principle of Least Privilege，POLP）仍然是可供參考的資安管理實務原則

(D) 職務區隔（Separation of Duties，SoD）也是管理層面的安全機制，也可以透過技術層面來加強使得工作分成多人分層負責避免個人進行非授權的工作或提升偵測的能力

114-1 規劃 答案B

(雖然零信任架構（Zero Trust Architecture，ZTA）在資訊安全領域逐漸受到關注，但目前並未成為國內的主流安全架構，國內許多企業及工控系統仍在傳統安全模型下運作或正處於試點階段。因此，選項 (B) 描述不正確。其他選項則描述了現行資訊安全管理實務中的正確概念。)

2. 下列何項「不」是帳號管理的安全政策？

(A) 定期檢視超過一定期間未登入之使用者帳號

(B) 定期檢視管理者帳號

(C) 要求使用者密碼須為複雜性密碼 (要求使用者密碼須為複雜性密碼是一項重要的安全措施，但它屬於**密碼管理**的範疇，而不是**帳號管理**的安全策略)

(D) 依申請期限，關閉臨時帳號

規劃 113-2 答案C

9. 關於縱深防禦（Defense in Depth）的敘述，下列何者錯誤？

(A) 係透過應用多種的安全機制來建立一系列的安全屏障

(B) 可以防止、延遲或阻止攻擊行為

(C) 主要安全機制可以包含邊界防禦、身份驗證和授權、主機和端點保護、應用程式保護、資料保護、安全監控與事件回應等機制

(D) 可以完全取代資安託管服務 (縱深防禦是一種安全策略和架構，而資安託管服務 (Managed Security Services, MSS) 是一種將資安運維工作外包給專業的第三方服務提供商的模式。兩者並不互斥，反而是可以相輔相成的。)

規劃 113-2 答案D

10. 公司採用聲紋辨識器作為門禁控制措施，因員工感冒，導致其被拒絕進入，這種現象稱為下列何項？

(A) False reject (指系統錯誤地拒絕了合法使用者，也稱為 Type I error)

(B) False accept (指系統錯誤地接受了非法使用者，與題目情況不符)

(C) Type-II error (統計學中對應「False accept」（未拒絕錯誤的假設))

(D) CER (這是 FAR 和 FRR 的交叉點，是一個系統性能指標)

規劃 113-2 答案A

11. 職務區隔及責任範圍區隔，旨在分隔不同個人間相互衝突之職務，以防止一個人獨自執行潛在衝突的職務。下列何者的應用情境較「不」適當？

(A) 啟動、核可及執行變更

(B) 使用及列印應用程式說明文件 (此操作僅屬於資訊文件的查閱或列印，並無涉及潛在的權限濫用或作業衝突，因此沒有必要實施職務區隔。)

(C) 設計、實作及審視程式碼

(D) 請求、核可及實作存取權限

規劃 113-2 答案B

12. 下列哪些措施的採用「有助於」職務區隔（Separation of Duties ，SOD）控制措施有效的施行？（複選）

(A) 職務定期輪調

(B) 多因素驗證（MFA） (MFA 主要是增強使用者的身份驗證安全性，但並不直接影響或支援職務區隔的實施，因此不屬於有助於 SOD 控制措施的項目)

(C) 以角色為基礎的存取控制（RBAC）

(D) 定期實施權限審查

規劃 113-2 答案ACD

14. 身分驗證機制是利用帳戶密碼進行作為識別使用者的機制，是多數資訊系統驗證使用者身分的基礎。關於身分驗證機制的敘述，下列那些正確？ （複選）

(A) 設定「最小密碼長度」的原則主要是要產生更多的密碼組合，提高被破解的難度。美國國家標準暨技術研究院（ National Institute of Standards and Technology, NIST）建議最小長度為 8 個字元

(B) 設定「密碼歷程記錄」的原則為了方便使用者自己找到以前使用過的密碼 (**錯誤**。密碼歷程記錄的目的是**防止使用者重複使用舊密碼**，提高密碼的安全性。如果使用者可以輕易找到並使用以前的密碼，那麼密碼歷程記錄就失去了意義，安全性也會降低)

(C) 設定「密碼最短使用效期」的原則是指該密碼必須使用一段時間後才能再次進行變更，通常是配合密碼歷程機制啟用

(D) 「圖形驗證碼」是設計一組對人類能夠輕易回答而對電腦是困難的題目，以作為區分執行動作的是電腦還是人類的行為 (圖形驗證碼 (CAPTCHA) 的設計目的是區分人類和機器人程式。它利用人類擅長而電腦難以處理的任務，例如圖像識別、扭曲文字識別等，防止自動化程式進行惡意操作，例如刷票、灌水、大量註冊帳號等，猜測是因為AI出來後越來越無法區分)

防護 113-2 答案 A、C

26. 關於存取控制技術的描述，下列何者錯誤？

(A) 任意型存取控制（Discretionary Access Control, DAC）是主體存取客體之權限由擁有者設定

(B) 強制型存取控制（Mandatory Access Control, MAC）是依照主體與客體之分類標籤（Classification Label）給予權限，即使是管理者也無法給予特別權限

(C) 角色為基礎的存取控制（Role-Based Access Control, RBAC）使用角色（Role）來管理權限，對於使用者位於同一個單位或執行相關的工作十分方便有效

(D) 基於屬性的存取控制（Attribute Based Access Control, ABAC）僅能透過單一屬性設定存取控制來達到安全的管控

管理 113-2 答案D

(ABAC 的核心優勢在於其靈活性和細粒度。它可以使用多個屬性的組合來定義存取控制策略，這些屬性可以來自使用者、資源、環境等。例如，可以設定規則：「僅當使用者是『經理』角色且部門是『財務』且時間是『工作時間』時，才能存取『財務報告』」。因此，說 ABAC 只能透過單一屬性設定存取控制是錯誤的)

27. 採用生物識別作為身分認證機制時，生物特徵識別系統的辨識精確度會有其誤差值的存在，如果組織需要加強進出人員安全管控時，下列何項是生物特徵識別系統要分別增加及減少誤差值的種類？

(A) 增加FRR（False Rejected Rate）、減少FAR（False Acceptance Rate）

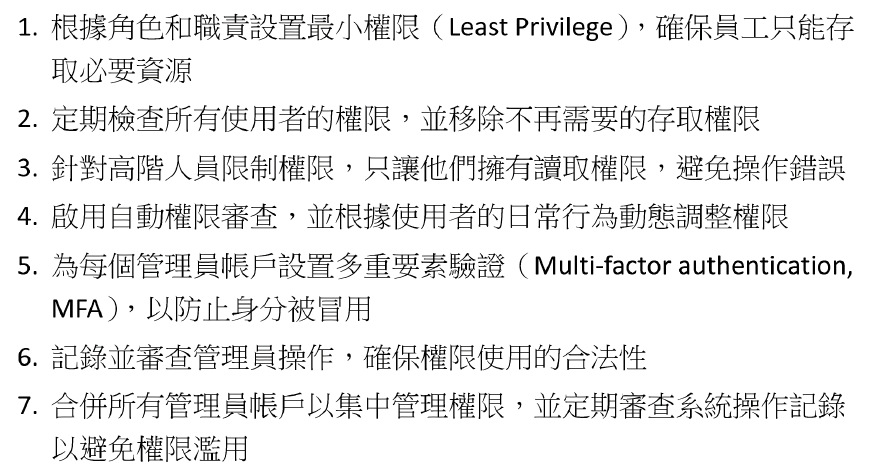
(B) 增加FRR（False Rejected Rate）、減少CER（Crossover Error Rate）

(C) 增加FAR（False Acceptance Rate）、減少FRR（False Rejected Rate）

(D) 增加CER（Crossover Error Rate）、減少FAR（False Acceptance Rate）

管理 113-2 答案A

(敏感度調高會讓FFR錯誤拒絕率(誤殺)上升，FAR以降低錯誤接受率(誤放))

28. 如附圖所示。在雲端服務的存取權限控管中，下列哪些做法組合最能有效避免過度授予權限？

(A) 1、2、5、7

(B) 1、3、5、6

(C) 1、2、4、6

(D) 1、2、5、6

管理 113-2 答案D

(

**1. 根據角色和職責設置最小權限 (Least Privilege)，確保員工只能存取必要資源：** 這是一項基本的安全原則，對於防止過度授權至關重要。

**2. 定期檢查所有使用者的權限，並移除不再需要的存取權限：** 定期審查對於確保權限隨著角色和職責的變化保持適當性至關重要。

**3. 針對高階人員限制權限，只讓他們擁有讀取權限，避免操作錯誤：** 雖然限制高階人員的權限在某些情況下可能是有益的，但它並不是防止過度授權的通用最佳方法。這可能會阻礙他們執行必要的任務。

**4. 啟用自動權限審查，並根據使用者的日常行為動態調整權限：** 這是一個好做法，但其有效性取決於自動化系統的準確性和穩健性。最好將其用作其他方法的補充。

**5. 為每個管理員帳戶設置多重要素驗證 (Multi-factor authentication, MFA)，以防止身分被冒用：** MFA 對於保護帳戶（尤其是特權帳戶）至關重要，但它主要解決的是未經授權的存取，而不是合法使用者被授予的過度權限。

**6. 記錄並審查管理員操作，確保權限使用的合法性：** 稽核對於檢測和阻止濫用權限至關重要。

**7. 合併所有管理員帳戶以集中管理權限，並定期審查系統操作記錄以避免權限濫用：** 雖然集中管理可以簡化管理，但合併帳戶可能會增加風險，因為一旦該單一帳戶被攻破，後果更嚴重。)

29. 生物特徵辨識應用在存取權限控制時，所扮演的角色是下列哪一項？

(A) 授權（Authorization）

(B) 身分驗證（Authentication）

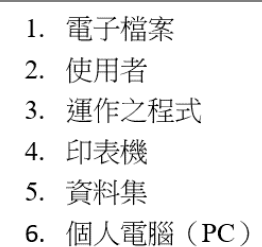
(C) 可問責（Accountability）

(D) 正確率（Accuracy）

管理 113-2 答案B

(生物辨識扮演身分驗證的角色)

30. 存取控制是用以控制使用者與系統、系統與系統之間進行資訊交換和溝通，其概念是作業系統為控制一個主體（Subject），能依照其所得到的權限進行客體（Object）之存取。請問附圖中的選項哪些可以作為客體？



(A) 2、3、4

(B) 1、4、5、6

(C) 2、3、6

(D) 1、2、5、6

管理 113-2 答案B

(客體就是被存取使用的物品，2、3是主體)

34. 關於RuBAC（Rule-based Access Control）、MAC（Mandatory Access Control）、DAC（Discretionary Access Control）、RoBAC（Role-Based Access Control）的描述，下列何者最「不」適切？

(A) RuBAC根據安全規則來決定使用者是否有存取資源的權限

(B) MAC是一種存取控制機制，其中存取權限由系統中的政策決定，不允許使用者或擁有者更改

(C) DAC允許資源的擁有者或使用者決定誰可以存取該資源，提供較大的靈活性

(D) RoBAC將存取控制權限分配給特定使用者，由存取控制規則決定

管理 113-2 答案D

(RoBAC將存取控制權限分配給特定群組，由存取控制規則決定)

47. 行動裝置常被作為雙因子認證（Two-Factor Authentication, TFA）的認證因子之一，請問下列何項「不」是行動裝置常用的認證開機方式？

(A) 人臉辨識

(B) 指紋辨識

(C) RFID辨識

(D) 圖形辨識

技術 113-2 答案C

9. 一個要導入 ISO 27001的組織，為了降低組織資產未經授權或誤用的機會，下列何種措施較 「 無法 」 避免？

(A) 職務區隔

(B) 職務輪調

(C) 資產清冊 (主要用於追蹤與管理組織的資產，例如硬體、軟體、資料等。雖然它有助於識別哪些資產需要保護，但**單靠資產清冊本身，並不能直接防止未經授權的存取或誤用**，因為它**不會限制存取權限或規範使用者行為**)

(D) 存取控制政策

規劃 113-1 答案C

10. 針對資安防護機制配置，下列何種說明較符合縱深防禦（Defense in Depth）的概念？

(A) 購買符合公司規格流量的防火牆

(B) 定期更新防毒軟體的病毒碼

(C) 針對內部系統、網路、軟體進行多層次的安全控制

(D) 全程使用加密的資料傳輸

防護 113-1 答案C

(縱深防禦 (Defense in Depth) 的概念：

**多層次 (Multiple Layers)：** 在不同層面部署安全控制，例如：網路、主機、應用程式、資料等。

**多樣性 (Diversity)：** 使用不同的安全技術和產品，例如：防火牆、入侵偵測系統、防毒軟體、身分驗證等。

**分段隔離 (Segmentation)：** 將網路和系統劃分成不同的區域，限制攻擊者在網路內的橫向移動。)

11. 關於「資料」存取的控制方法，「不」包括下列何者？

(A) 強制存取控制（Mandatory Access Control，MAC）

(B) 存取控制清單（Access Control List，ACL）

(C) 隨機存取控制（Randomly Access Control，RAC） (這個詞彙並非標準的資訊安全存取控制方法)

(D) 角色基準存取控制（Role-based Access Control，RBAC）

規劃 113-1 答案C

20. 規劃系統安全架構時可採取之控制措施，下列敘述哪些「有誤」？

(A) 使用單一的帳號名稱及密碼 (每個系統應該使用唯一的帳號和強密碼應該使用獨立帳號與強密碼，並考慮多因素驗證（MFA），避免帳號被駭導致整個系統淪陷。使用相同帳號名稱與密碼會提高憑證洩露風險)

(B) 無須定期檢視防火牆規則 (防火牆規則需要定期檢視和更新，以確保其仍然有效且符合當前的安全需求)

(C) 定期執行漏洞掃描並修補漏洞

(D) 開放不必要的伺服器連接埠 (每個開放的連接埠都是一個潛在的攻擊入口。應該只開放必要的連接埠，並關閉所有不必要的連接埠，以減少受攻擊面。)

規劃 113-1 答案A、B、D

20. 為提供資通訊系統可以安全進行遠端維護，請問下列何項措施「不」是必要的管理模式？

(A) 設定網路火牆管理遠端連線機制及限制存取的主機位置

(B) 建立 SSO（Single sign-on）單一簽入作業，統一連線帳密管理 (主要目的是提升使用者體驗與管理便利性，但它並不是遠端維護安全的必要措施)

(C) 使用多因子認證，確保連線使用者的身份

(D) 建立 VPN機制，僅限制維護作業人員可以進行遠端安全連線作業

防護 113-1 答案B

26. 若採行多因素身分驗證，除了原本的帳號密碼之外，下列何項的內容可以當成第二階段認證的方式？ （請選擇最佳的組合）

(A) 個別員工之IC識別證 、傳輸至個人手機的隨機驗證碼 (知+物+物)

(B) 身份證字號 、傳輸至個人手機的隨機驗證碼 (知+知+物)

(C) 身份證字號 、出生年月日 (知+知+知)

(D) 出生年月日 、個別員工之 IC識別證 (知+知+物)

管理 113-1 答案A

(A選項組合了"所持之物"(IC卡和手機)，比起其他選項使用"所知之事"(身份證號、生日)來說更安全，因為"所知之事"容易被猜測或洩漏。)

27. 關於存取控制的基本管理敘述，下列何者錯誤？

(A) 「責任分擔」是避免高機密資訊由某人完整的持有

(B) 「最低權限」要求每個人都只能擁有完成任務的最低權限

(C) 「知的必要性」是指對於負責的業務需求性有「知的權利」

(D) 「資訊分類」使用者必須完整掌握其權限以外的對應系統與資料

管理 113-1 答案D

(使用者不應該知道權限以外的系統資訊，這違反了最小權限原則和知的必要性原則，所以(D)是錯的)

28. 關於身份認證技術的敘述，下列何者正確？

(A) 採用生物資訊認證技術需考量錯誤接受率（FAR）與錯誤拒絕率（FRR）

(B) 指紋屬於所持之物（Something you have） (所具之形)

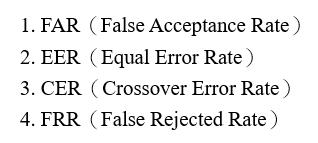
(C) 一次性密碼（OTP）屬於所知之事（Something you know） (所持之物)

(D) 申辦時提供雙證件確認屬多因子認證（MFA）(物+物為單因子)

管理 113-1 答案A

(生物辨識技術確實需要考慮FAR(誤放非法使用者)和FRR(誤拒合法使用者)的平衡，這是評估其可靠性的重要指標。)

30. 如附圖所示，採用生物識別作為身分認證機制時，生物特徵識別系統的辨識精確度會有其誤差值的存在，請問附圖中哪些是「最」常用以評估誤差值的種類？



(A) 1、 2、 3

(B) 1、 2

(C) 2、 4

(D) 1、 4

管理 113-1 答案D

(生物識別系統主要用FAR(假接受率)和FRR(假拒絕率)評估系統精確度，故選D。)

35. 關於僅知原則（Need to Know）、最小權限原則 （Principle of Least Privilege）、僅用原則（Need to Use）的描述，下列何者最「不」適切？

(A) 僅知原則強調只有當成員需要特定資訊來完成其職務時，才應該給予存取該資訊的權限

(B) 最小權限原則要求給予成員執行其工作所需的最少權限

(C) 僅用原則指出應該限制成員對系統資源的存取，以防止資訊洩漏和不當使用

(D) 僅知原則、僅用原則及最小權限原則也可應用在資料加密之理論基礎

管理 113-1 答案D

(因為這三個原則主要用於存取控制領域，並不適用於資料加密的理論基礎，故選D)

9. 如要實施多層次防禦，下列何種措施最為合適？

(A) 在個人電腦安裝防毒軟體

(B) 運用不同網路區段，隔離不同用途的設備，並分別進行相關流量過濾措施 (這是一種典型的縱深防禦策略。透過網路分段，可以將不同安全層級的設備隔離開來，例如將伺服器、工作站和無線網路分開。並在不同網段間設定防火牆規則，過濾流量，限制不同網段之間的通訊，這樣即使某個網段受到攻擊，也能阻止攻擊擴散到其他網段。這有效提高了整體安全性。)

(C) 依照各別使用者，建立各自的電腦帳號

(D) 於作業系統中啟用檔案存取記錄，保留資料存取的相關記錄

規劃 112-2 答案B

10. 關於身分識別與存取管理（ Identity and Access Management

IAM）的敘述，下列何者正確？

(A) 管理網路防火牆的設定

(B) 控制使用者對系統或資源的存取權限

(C) 監控網路流量與入侵偵測

(D) 保護敏感資料的傳輸

規劃 112-2 答案B

11. 關於職務區隔（ Segregation of Duties SOD）的說明，下列

何者正確？

(A) 可以促進內部員工合作和溝通

(B) 可以確保資訊系統的可用性

(C) 可以減少內部詐欺行為或誤用之風險

(D) 可以簡化組織的工作流程

規劃 112-2 答案C

12. 關於權限管理的說明，下列哪些正確？（複選）

(A) 一旦使用者通過身份驗證後，系統會根據其授權層級與角色來分配相應的權限

(B) 可以確保每個使用者僅能存取其需要的資源或功能

(C) 能夠防止越權存取

(D) 可以透過以角色為基礎的存取控制（ Role-based access control RBAC）實作

規劃 112-2 答案A、B、C、D

30. 關於存取控制的基本管理敘述，下列何者錯誤？

(A) 「責任分擔」是避免高機密資訊由某人完整的持有

(B) 「最低權限」要求每個人都只能擁有完成任務的最低權限

(C) 「知的必要性」是指對於負責的業務需求性有「知的權利」

(D) 「資訊分類」使用者必須完整掌握其權限以外的對應系統與資料

管理 112-2 答案D

(資訊分類原則下，使用者只能掌握其權限內的系統和資料，而非權限以外的，故D錯誤。)

31. 指紋等生物特徵認證，屬於密碼學身分認證中的何種認證因

素？

(A) 所知之事（something you know）

(B) 所持之物（something you have）

(C) 所具之形（something you are）

(D) 所分享之物（Something you share）

管理 112-2 答案C

(生物特徵認證屬於"所具之形"(something you are)，因為是用個人與生俱來的身體特徵來進行身分認證，故選C。)

32. 如附圖所示，為有效強化身分認證機制，常會使用多因子（Multi-factor authentication, MFA）認證機制，下列哪些應用組合屬於多因子認證類型？

1. 聲紋辨識+帳號密碼（Password） (形+知)
2. 指紋辨識+圖形驗證碼（Captcha）(形+沒有)
3. 臉型辨識+指靜脈辨識+虹膜 (形+形+形)
4. 帳號密碼+自然人憑證IC卡 (知+物)
5. 帳號密碼+虹膜+自然人憑證IC卡 (知+形+物)
6. 帳號密碼+指紋辨識+圖形驗證碼（Captcha）(知+形+沒有)

(A) 1、 2、 3、 5

(B) 1、 4、 5、 6

(C) 1、 2、 3

(D) 2、 3、 5

管理 112-2 答案B

33. 下列何者「不」屬於存取控制認證技術型式一：你所知道的事物（Something you know）？

(A) 密碼

(B) 你喜歡的數字

(C) 通行語

(D) 指紋

112-2 答案D

(指紋屬於"所具之形"(something you are)而非"所知之事"，故選D。)

35. 資訊系統存取權限管理 ，下列何項較「不」正確？

(A) 提供臨時人員暫時存取權限

(B) 更新職務已異動者之存取權限

(C) 拒絕職務代理需求之暫時存取權限

(D) 撤銷已離職員工之存取權限

管理 112-2 答案C

(職務代理是合理的工作需求，不應拒絕其暫時存取權限，因此C選項較不正確)

15. 身分驗證機制是利用帳戶密碼進行作為識別使用者的機制，是多數資訊 系統驗證使用者身分的基礎。關於身分驗證機制的敘述，下列哪些正確？（複選）

(A) 設定「最小密碼長度」的原則主要是要產生更多的密碼組合，提高被破解的難度。美國國家標準暨技術研究院（National Institute of Standards and Technology, NIST）建議最小長度為 8個字元

(B) 設定「密碼歷程記錄」的原則為了方便使用者自己找到以前使用過的密碼 (「密碼歷程記錄」的主要目的是防止使用者重複使用近期的密碼，以提高密碼的安全性。)

(C) 設定「密碼最短使用效期」的原則是指該密碼必須使用一段時間後才能再次進行變更，通常是配合密碼歷程機制啟用 (「密碼最短使用效期」（Minimum Password Age）確保使用者在更改密碼後，必須至少使用該密碼一段時間（例如 1 天）後，才能再次變更密碼。這通常與密碼歷程機制一起使用，以防止使用者通過頻繁更改密碼來繞過密碼歷程限制。)

(D) 「圖形驗證碼」是設計一組對人類能夠輕易回答而對電腦是困難的題目，以作為區分執行動作的是電腦還是人類的行為

防護 112-1 答案A、C、D

26. 關於存取控制（Access control）的描述，下列何者錯誤？

(A) 存取者向受保護資源進行存取操作的控制管理

(B) 未被授權者，可透過系統管理員，取得未被授權的資源 (未經授權者不應該透過系統管理員取得未授權的資源，這違反資訊安全基本原則)

(C) 存取控制包含了認證、授權以及稽核

(D) 現實生活中門禁系統也是一種存取控制的表現

管理 112-1 答案B

27. 在自由決定存取控制（Discretionary Access Control, DAC）環境中，以下哪個角色被授權向其他人授予資訊存取權限？

(A) 資安經理

(B) 部門經理

(C) 資料擁有者 (DAC模型中，資料的存取權限由資料擁有者自行決定並授予他人)

(D) 執行長（CEO）

管理 112-1 答案C

28. 最常見的身分驗證方式是「帳號密碼」的驗證，請問下列措施中何者無法提升安全性？

(A) 要求定期修改密碼

(B) 採用動態密碼

(C) 規範高強度密碼長度與複雜度

(D) 密碼統一並共用 (密碼不應統一共用，這會增加密碼洩露風險且無法追蹤個人責任)

管理 112-1 答案D

29. 在存取控制（Access Control）中，提到存取控制系統能夠達到的AAA機制，請問這3個A「不」包含下列何者？

(A) Availability (AAA機制包含Authentication(認證)、Authorization(授權)和Accounting(稽核)，不包含Availability(可用性))

(B) Accounting

(C) Authentication

(D) Authorization

管理 112-1 答案A

30. 下列關於存取控制的作法，何者較「不」正確？

(A) 應訂定資訊存取控制政策，並文件化公告

(B) 存取控制規範，需符合資料保護法令與契約規定

(C) 為了能快速進行除錯，存取記錄應開放給所有工程人員存取 (存取記錄不應開放給所有工程人員，這違反最小權限原則且可能導致安全風險)

(D) 資訊存取控制規範，應依照人員的工作與職務分別訂定

管理 112-1 答案C

31. 為避免職務及責任範圍衝突，應採取下列何者控制措施？

(A) 強化密碼管理

(B) 日誌管理

(C) 資訊之分級

(D) 職責區隔 (為避免職務與責任範圍衝突，應採取職責區隔的控制措施)

管理 112-1 答案D

32. 下列何者為使用持有物（Something You Have）進行身分驗證（Authentication）？

(A) 密碼 （所知之事 Something You Know）

(B) 指紋 （所具之形 Something You Are）

(C) 個人識別證

(D) 簽名 （所具之形 Something You Are）

管理 112-1 答案C

34. 為了防止非授權的存取，企業應根據存取控管政策對使用者（包括內、外部使用者）存取權限進行管理，下列何者最相關？

(A) 定期變更密碼

(B) 定期審查使用者存取權限 (定期審查使用者存取權限能確保權限符合當前職務需求，避免非授權存取)

(C) 保留存取紀錄

(D) 資料備份

管理 112-1 答案B

38. 關於雙重要素驗證（Two-factor authentication, 2FA）的敘述，下列何者錯誤？

(A) 指的是登入帳戶時需要提供多個驗證因素，通常是三個或更多。除了密碼外，其他驗證因素可能包括短信驗證碼、生物識別、硬體安全鑰匙、安全問題、行為分析等 (雙重要素驗證(2FA)顧名思義只需要兩個驗證因素而非三個或更多)

(B) 郵件釣魚攻擊，攻擊者可以進行釣魚攻擊，試圖騙取您的2FA代碼，以進入您的帳戶

(C) 使用安全性低的第三方服務來實現2FA可能會導致安全漏洞，讓攻擊者入侵您的帳戶

(D) 當使用第三方應用程式進行2FA驗證時，攻擊者可能通過偽造應用程式來竊取您的2FA代碼，以進入您的帳戶

管理 112-1 答案A

39. 密碼學身分認證的三個因素：所知之事（something you know）、所持之物（something you have）、所具之形（something you are）。下列何項為所持之物認證因素？

(A) 指紋（所具之形 Something You Are）

(B) 晶片卡

(C) 密碼（所知之事 Something You Know）

(D) 臉型（所具之形 Something You Are）

管理 112-1 答案B

14. 關於雙因子認證（Two-Factor Authentication）的敘述 ，下列何者錯誤？

(A) 雙因子指的是「你知／ Something you know」「你有／ Something you have」「你是／Something you are」任兩者

(B) 兩重的密碼認證，不算雙因子認證方式

(C) 可以有效防禦資料隱碼攻擊

(D) 可以有效防禦中間人攻擊

技術 111-2 答案C、D皆給分

(C選項錯誤：資料隱碼攻擊需要透過輸入驗證、參數化查詢、Web 應用防火牆（WAF）等防禦，而非 2FA，  
D選項錯誤：若僅是一般的簡訊 OTP，仍可能遭遇 MITM (釣魚 + 轉發) 攻擊)

30. 以現行科技發展而言，下列何種生物特性較「不」適合拿來作為身份鑑別使用？

(A) 指紋

(B) 虹膜

(C) 臉部特徵

(D) 身高

管理 111-2 答案D

(身高不是常見的身分證別方式，尤其身高可能會重複)

31. 關於生物辨識錯誤型態的敘述，下列何者正確？

(A) 錯誤接受（False Acceptance）發生時，會拒絕正確使用者進入 (會接受錯誤的人進入)

(B) 交叉錯誤率（Crossover Error Rate, CER）發生時為第一型錯誤率等於第二型錯誤率 (CER 是 FAR（錯誤接受率）= FRR（錯誤拒絕率）的交叉點)

(C) 對存取控制來說第一型錯誤發生時比第二型錯誤嚴重 (第二型錯誤為接受錯誤的人進入比第一型嚴重)

(D) 視網膜與虹膜辨識的CER 最高 (CER越高表示準確率越不准，臉部辨識比CER更高)

管理 111-2 答案B

35. 公司的簽到系統是採用動態行為特徵「簽名辨識」（在電子筆上加裝感應器），但某日員工Alex 因為慣用右手受傷，改用左手簽名，卻一樣可以通過辨識簽到系統，請問安全管理人員得知此狀況後，該如何處理？

(A) 將簽到系統的敏感度調高，以降低錯誤拒絕率（False Rejection Rate）

(B) 將簽到系統的敏感度調低，以提高錯誤拒絕率（False Rejection Rate）

(C) 將簽到系統的敏感度調高，以降低錯誤接受率（False Acceptance Rate）

(D) 將簽到系統的敏感度調低，以提高錯誤接受率（False Acceptance Rate）

管理 111-2 答案C

(敏感度調高會讓錯誤拒絕率(誤殺)上升，以降低錯誤接受率(誤放))

5. 下列何項安全實作原則是為了預防僅因個人行為而造成可能的舞弊情

形發生？

(A) 強制休假（ Mandatory vacation）

(B) 僅知原則（ Need to know basis）

(C) 最小權限（ Least privilege）

(D) 職責分離（ Separation of duties）

規劃 111-1 答案D

(職責分離（Separation of duties） 的核心目的是透過將關鍵任務或權限分散給不同人員，避免單一角色擁有過度集中的控制權，從而降低因個人行為導致舞弊的可能性)

11. 使用指紋或是掌紋來辨識身份，屬於下列何種身份認證方式？

(A) 所知之事

(B) 所持之物

(C) 所具之形－靜態特徵

(D) 所具之形－動態特徵

管理 111-1 答案C

(指紋或是掌紋是靜態特徵、走路身形和簽名是動態特徵)

15. 「 某網站伺服器經常有大量的使用者來進行異動，且常會定義不同的使用者身份，例如會員、非會員或系統管理者。」關於網站存取控制

模型之選擇，下列何者管理效率較高？

(A) 存取控制清單（Access Control List）

(B) 強制存取控制（Mandatory Access Control）

(C) 自主性存取控制（Discretionary Access Control）

(D) 以角色為基礎的存取控制（Role Based Access Control）

規劃 111-1 答案D

(以角色為基礎的存取控制 RBAC 是管理效率最高的模型)

28. 關於系統安全性中，IETF（Internet Engineering Task Force）制定的AAA協定，下列何者定義主要說明認證機制？

(A) Applicability

(B) Authentication (認證)

(C) Authorization (授權)

(D) Accounting (紀錄)

管理 111-1 答案B

31. 為強化身份認證機制，我們常會使用雙因素認證機制，下列何種組合並「不」屬於雙因素認證的定義？

(A) 密碼（Password）+RFID 感應卡（如悠遊卡） (知+物)

(B) RFID 感應卡+自然人憑證IC卡 (物+物)

(C) 自然人憑證IC 卡+指紋 (物+形)

(D) 指紋+密碼 (形+知)

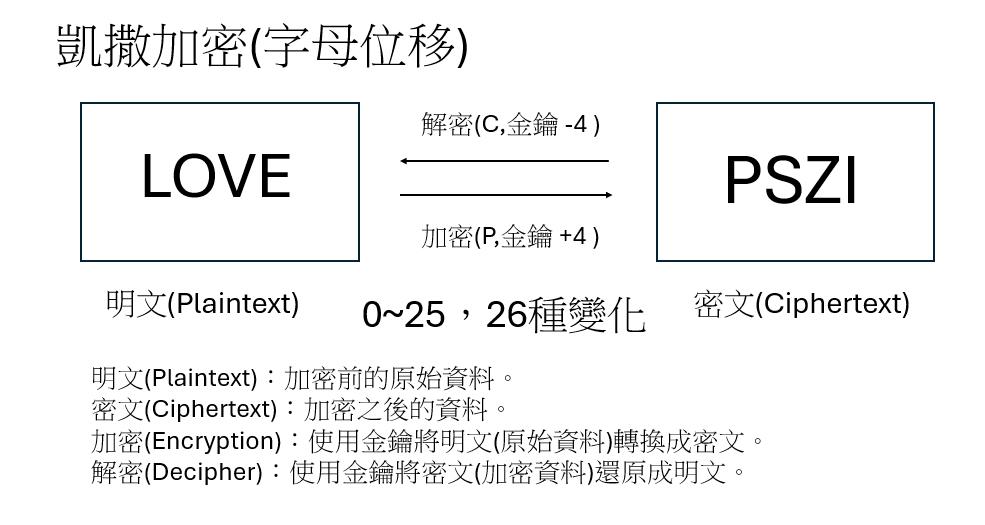
管理 111-1 答案B

密碼學原理和數位安全機制

**科克霍夫原則 (Kerckhoffs's Principle)**

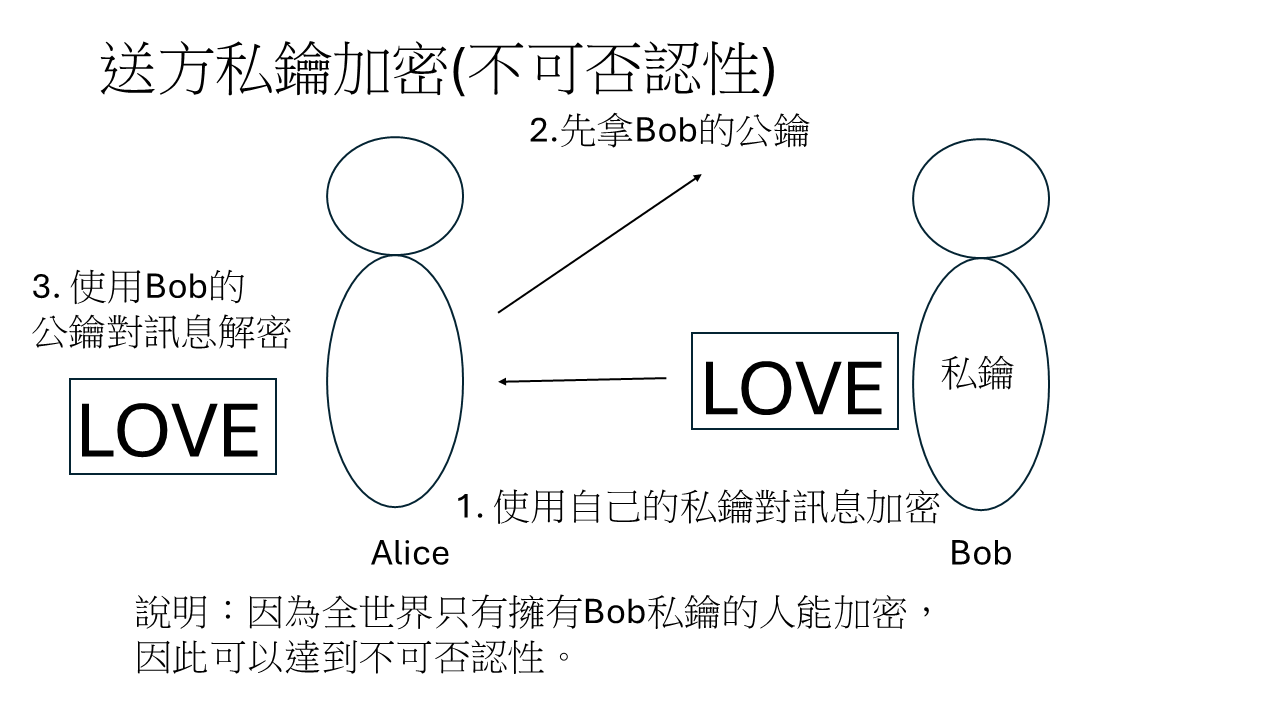
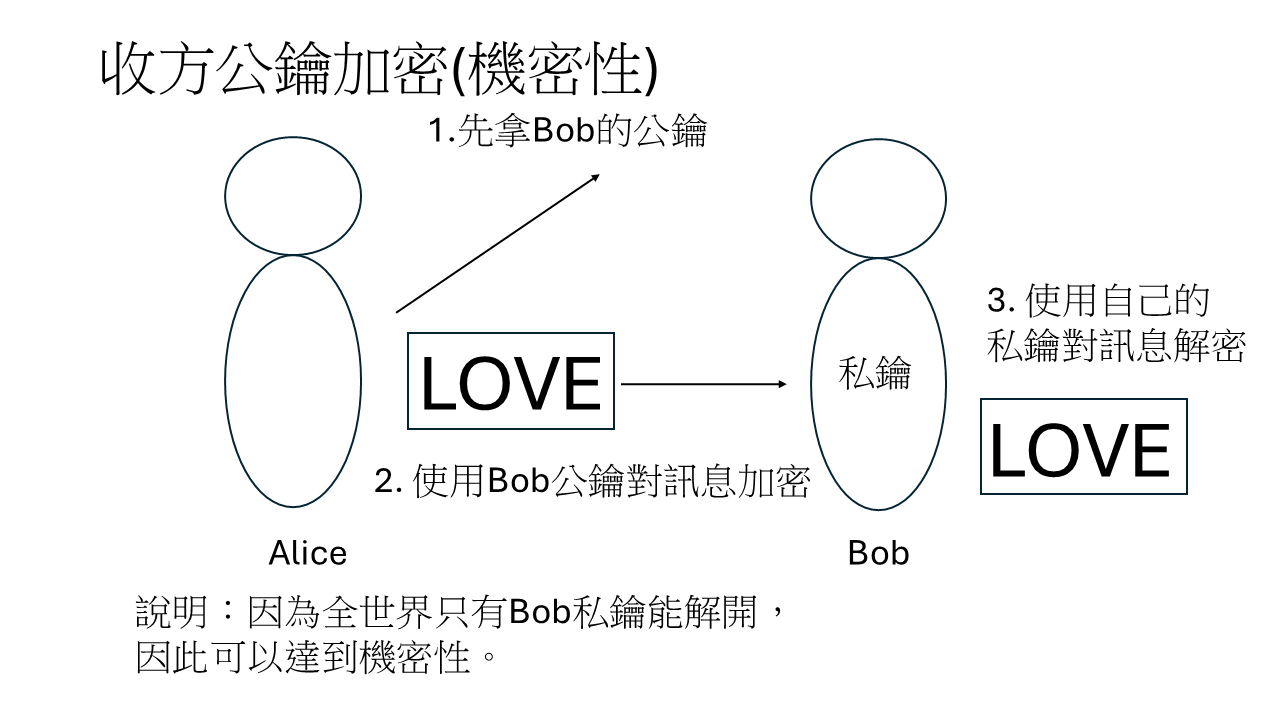
* 加密系統的安全性應該僅依賴於密鑰的保密性，而不是算法的保密性。
* 即使加密算法是公開的，只要密鑰足夠保密且難以破解，系統仍然是安全的。
* 現代密碼學的核心思想：公開算法接受廣泛分析與驗證，而不依賴「安全性通過隱秘性」。

**傳統加密驗算法**

****

**加密**

* 確保機密性，分成對稱加密和非對稱加密。
* 對稱加密
  + 特性：加密和解密使用相同金鑰，資源少，運算速度快。
  + 明文->對稱演算法+金鑰->密文；  
    密文->對稱演算法+金鑰->明文。
  + 範例：
    - 安全算法：AES。
    - 不安全算法：DES、3DES、RC4。
  + 優點：
    - 運算速度快，適合大規模資料加密。
  + 缺點：
    - 密鑰交換困難。
    - 金鑰數量增長迅速，為 。
* 非對稱加密
  + 特性：使用公鑰加密，私鑰解密；使用私鑰加密，公鑰解密，金鑰成對存在，公鑰可以隨意給任何人，私鑰則需要永遠保留在自己手上。
  + 範例：
    - 安全算法：RSA、ECC(資源消耗更少)。
  + 優點：
    - 無需共享私密金鑰，解決對稱加密密鑰分發問題。
  + 缺點：
    - 運算資源消耗大，物聯網設備難以應用。



**註解：**

此處所謂的「不可否認性」，是指**鑰匙層級**的不可否認性（即僅有該私鑰能產生此加密結果）。

若要進一步達成**身分層級**的不可否認性（能確認發送者為某特定實體），則通常需搭配數位簽章和數位憑證（CA）等機制。

**雜湊**

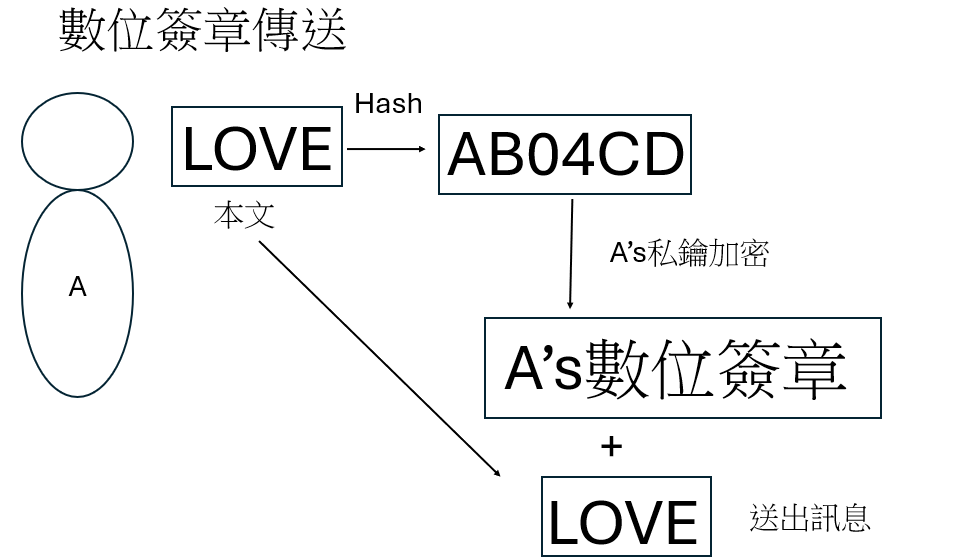
* 特性：確保完整性，不可逆，每次輸出的摘要長度固定。
* 應用：密碼儲存、資料完整性校驗。
* 安全算法：SHA-2 家族。
* 不安全算法：SHA-1、MD5 (因已發現碰撞) 。
* 密碼儲存防破解方法：
  + 使用加鹽 (Salt) 存儲密碼，抵禦彩虹表攻擊。

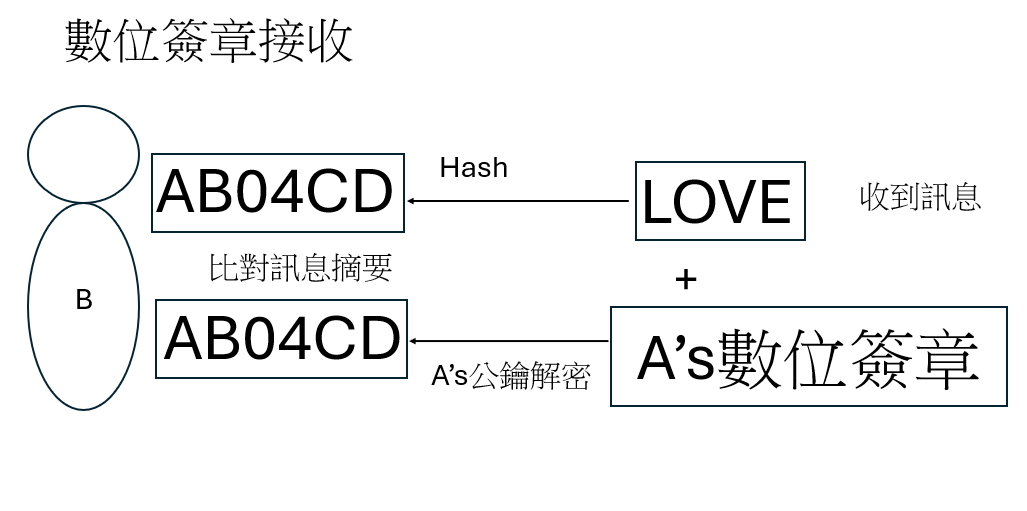
**編碼**

* 特性：可逆，無機密性。
* 用途：將資料轉換為方便網路傳輸的格式。
* 常見算法：Base64，使用 = 填充**：** Base64 編碼經常在結尾使用 = 字符進行填充，以確保輸出長度是 4 的倍數。給定字串中出現 == 是 Base64 的強烈指標。

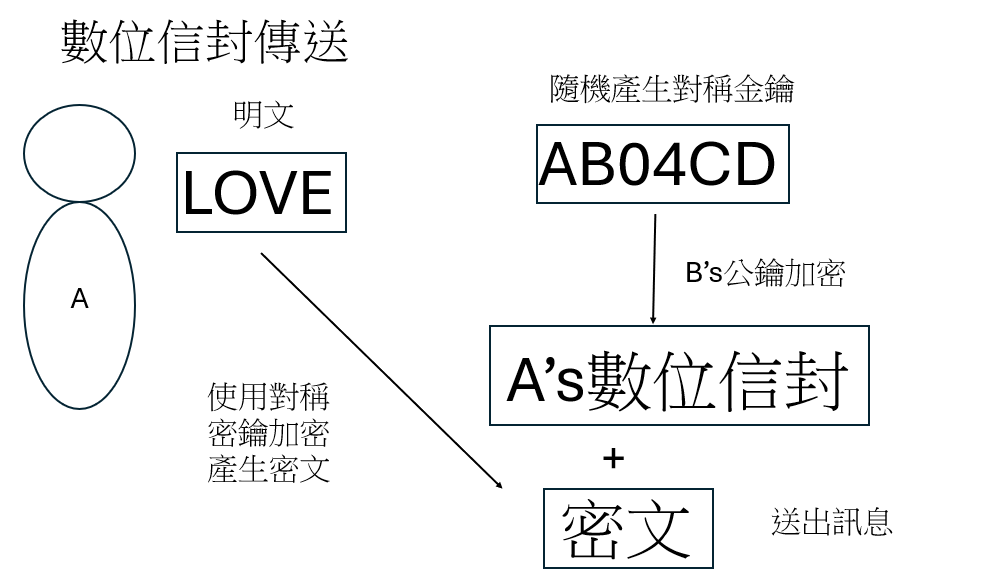
**數位安全機制**

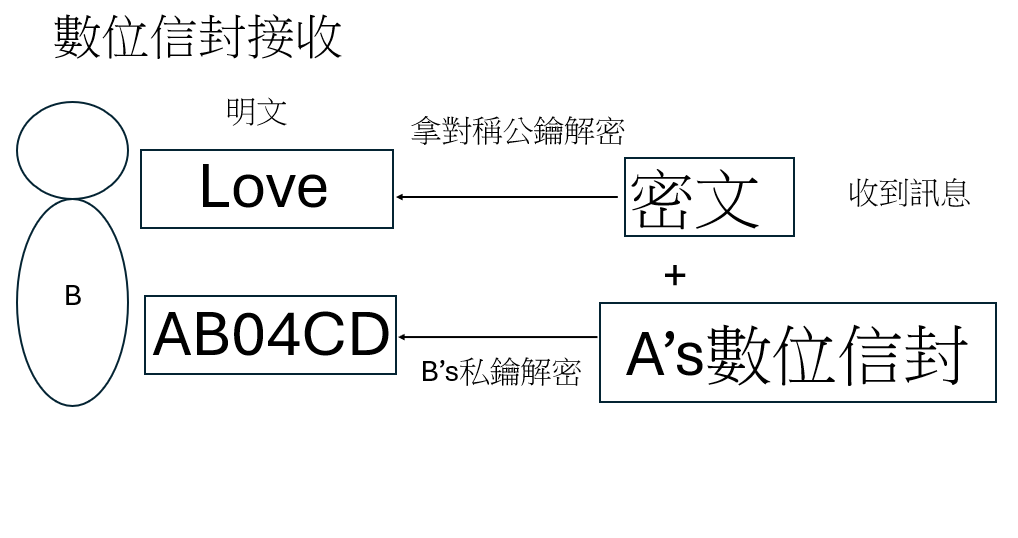
* 數位簽章 (Digital Signature)
* 特性：
  + 在實務應用中，數位簽章通常會與 PKI 及其數位憑證結合使用，以確保簽署者的真實身份和不可否認性，考試也是這樣考的，但是還是要分辨清楚。
  + 完整性：可驗證資料是否遭到竄改。
  + 真實性：能確認「某把私鑰」確實簽了這份文件，且傳輸的資料沒有被竄改，需搭配 PKI 及其數位憑證才能達到真實身分確認。
  + 不可否認性：只有「持有私鑰」的人才能產生該簽章，需搭配 PKI 及其數位憑證才能達到真實身分確認。
* 運作原理：
  + 先對文件做雜湊產生訊息摘要 (message digest)。
  + 以「簽署者的私鑰」加密訊息摘要，形成數位簽章。
  + 接收方用「簽署者的公鑰」解密數位簽章並比對訊息摘要，若一致則表示內容未被竄改。
* 效能考量：
  + 只對雜湊值 (非整份文件) 做私鑰加密，運算量小、速度較快。
* 缺點：
  + 不提供機密性：必須搭配「數位信封」才能保護訊息內容不被竊視。
  + 若無「數位憑證 (PKI)」，就無法在法律或實務層面證明「私鑰持有人」的真實身分，因而難以達到真正的不可否認性。



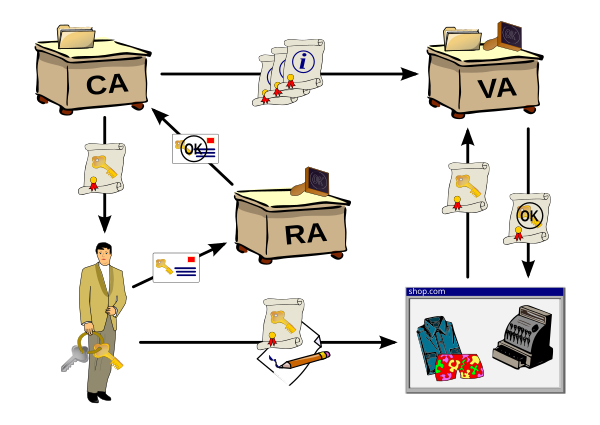


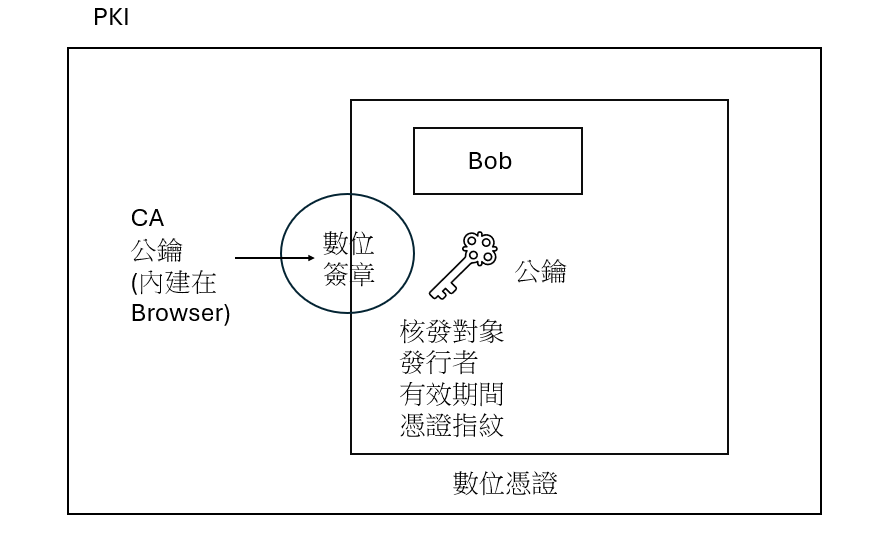
* 數位信封 (Digital Envelope)
* 特性：
  + 機密性：藉由對稱加密保護文件內容。
* 運作原理：
  + 先用「對稱式金鑰」加密整份文件（快速且適合大量資料）。
  + 再用接收方的「公鑰」加密這把對稱式金鑰，形成「數位信封」。
  + 接收方收到後，用自己的「私鑰」解開信封，取得對稱式金鑰，便能解密文件內容。
* 效能考量：
  + 大量資料用對稱式加解密更高效，非對稱加密只用來傳遞金鑰，減少運算成本。
* 缺點：
  + 不提供完整性：無法保證內容是否被修改，需要搭配「數位簽章」。





* 數位憑證 (Digital Certificate)
* 特性：
  + 真實性與（法律層面的）不可否認性：透過「公開金鑰基礎建設 (PKI)」機制，將「公鑰」和「身分」綁定，並由可信任的第三方 (CA) 背書。
* 管理單位：
  + 註冊中心 (RA)：負責身分認證、申請審查。
  + 憑證機構 (CA)：負責簽發數位憑證、管理憑證生命週期，需要撤銷憑證就是找它。
  + 驗證中心 (VA)：提供憑證狀態驗證服務。
* 憑證鏈：
  + 根憑證 → 中繼憑證 → 使用者憑證。
  + 任一層憑證失效，整個憑證鏈都視為無效。
* 憑證狀態查詢：
  + 憑證撤銷清單 (CRL)：可下載完整撤銷清單查閱。
  + 線上憑證狀態協定 (OCSP)：可即時查詢單筆憑證狀態。



(資料來源：維基百科)





**考古題：**

19. 建置異地或遠距系統的安全連網機制時，請問下列何者通訊安全加密機制規劃較為適當？

(A) 採用對稱式加密機制來處理大量訊息，並使用非對稱式加密進行金鑰交換

(B) 採用對稱式加密機制來處理大量訊息，並使用數位簽章進行金鑰交換

(C) 採用非對稱式加密機制來處理大量訊息，並使用數位簽章進行金鑰交換

(D) 採用非對稱式加密機制來處理大量訊息，並使用對稱式加密進行金鑰交換

防護 113-2 答案A

(這是目前業界常用的安全通訊機制，例如 TLS/SSL 協議。

**大量訊息加密：** 使用對稱式加密 (例如 AES) 來加密實際傳輸的資料，因為它的速度快、效率高。

**金鑰交換：** 使用非對稱式加密 (例如 RSA、ECC) 來安全地交換對稱式加密的密鑰。利用非對稱加密的特性，可以安全地將對稱式金鑰傳送給對方，即使傳輸過程被攔截，攻擊者也無法解密金鑰。)

26. 當資料庫洩漏時，儲存在其中的使用者密碼，使用下列何種機制較「不」容易被輕易破解？

(A) 使用明文儲存密碼

(B) 使用對稱加密儲存密碼

(C) 使用加鹽式（Salt）雜湊函數後儲存密碼

(D) 使用Base64編碼儲存密碼

技術 113-2 答案C

(因為雜湊函數容易受到彩虹表攻擊，加鹽是常見作法)

36. 下列何者並非RSA金鑰機制的相關特性？

(A) 使用非對稱加密演算法

(B) 使用單一金鑰加解密

(C) 私密金鑰（private key）不可交給他人

(D) 公開金鑰（public key）可公開讓有需要之人取得

管理 113-2 答案B

(非對稱使用公鑰和私鑰)

37. 憑證管理中心（CA）所管理的憑證中，有部分憑證已有安全顧慮時，應運用下列何種處罝方式最為合適？

(A) 註銷憑證

(B) 憑證審核

(C) 發佈憑證

(D) 交互認證

管理 113-2 答案A

(如發現憑證有問題，需要註銷憑證)

39. 「生日攻擊法」（Birthday Attack）主要針對下列何種加密演算法進行攻擊？

(A) MD5 (雜湊)

(B) Rijndael (AES的基礎，是對稱加密算法)

(C) 3DES (對稱加密算法)

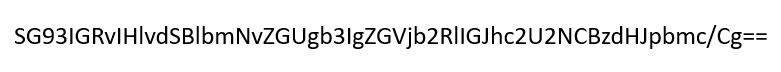
(D) RSA (非對稱加密算法)

管理 113-2 答案A

(「生日攻擊法」（Birthday Attack）主要利用生日悖論來尋找兩個不同的輸入產生相同的雜湊值，這種攻擊方法特別針對雜湊函數的碰撞（collision）進行攻擊。雜湊函數的安全性在很大程度上依賴於其抗碰撞性，因此生日攻擊法常用於測試和攻擊雜湊演算法。)

35. 如附圖所示，分析圖中非明文字串，所使用的加密、雜湊或編碼方

式，下列敘述何項正確？



(A) SHA3

(B) NetNTLMv2

(C) AES-128

(D) Base64

技術 113-1 答案D

(**使用 = 填充：** Base64 編碼經常在結尾使用 = 字符進行填充，以確保輸出長度是 4 的倍數。給定字串中出現 == 是 Base64 的強烈指標)

37. 關於對稱式加密（Symmetric Encryption）與非對稱式加密（Asymmetric Encryption）的敘述，下列何者錯誤？

(A) 非對稱式加密算法包括 DES、 3DES、 AES等，這些算法使用相同的密鑰對資料進行加密和解密

(B) 對稱式加密使用相同的密鑰（也稱為加密鑰）來加密和解密資料。在對稱式加密中，發送方和接收方必須共享相同的密鑰，並且使用該密鑰對資料進行加密和解密

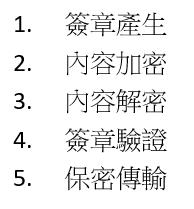
(C) 非對稱式加密是一種加密技術，使用一對密鑰（公鑰和私鑰）來加密和解密資料

(D) 對稱式加密需要發送方和接收方共享相同的密鑰，因此密鑰的管理和分發比較困難

管理 113-1 答案A

(DES、3DES、AES是對稱式加密算法而非非對稱式加密算法。非對稱式加密的代表算法是RSA、ECC等，故選A)

38. 數位簽章驗證程序 ，是執行附圖中的哪些作業行為



(A) 2、 4

(B) 1、 4

(C) 2、 3

(D) 1、 5

管理 113-1 答案B

(數位簽章驗證程序包括簽章的產生(1.簽章產生)和驗證(4.簽章驗證)這兩個步驟，數位簽章不保證機密性，故沒有內容加解密動作，傳輸加密主要是透過額外類似HTTPS方式達成的，故選B)

8. 當使用者利用帳號密碼登入系統時，密碼的儲存基本原則是不可以直接用明文方式存放於資料庫中，因此密碼通常利用加密（Encryption）或是雜湊（Hash）的方式進行編碼轉換。關於雜湊函數的敘述，下列何者錯誤？

(A) 雜湊原理是限制輸入長度為8 字元以上並透過雜湊函數進行計算，計算後會得到一樣長度的密文 (雜湊函數**不限制輸入長度**。無論輸入的字串是一個字元、一篇文章還是一個大型檔案，雜湊函數都可以處理，並且會產生固定長度的輸出（稱為雜湊值或摘要）。這個固定長度取決於所使用的特定雜湊函數（例如，MD5 產生 128 位元，)

(B) 常見的雜湊函數有MD5、SHA-1 及SHA-2 等

(C) 輸入的原始字串只差一個字元，透過雜湊函數得到的結果會差異很大 (雪崩效應（Avalanche Effect）)

(D) 雜湊函數具有不可逆的特性，無法利用雜湊值計算取得原始資料

防護 112-2 答案A

36. 關於對稱式密碼學（Symmetric cryptography）的敘述，下列何項錯誤？

(A) 加密（Encryption）與解密（Decryption）使用相同金鑰

(B) 通常加密速度相較於非對稱密碼學更快

(C) 通常運算成本相較於非對稱密碼學更高

(D) 缺點為金鑰交換須另外建立保護機制

管理 112-2 答案C

(對稱式密碼學的運算成本比非對稱式密碼學低(而非更高)，這也是為什麼對稱加密速度較快的原因，故C錯誤)

37. 關於HTTPS協議中所使用數位憑證（Digital Certification）的敘述，下列何項錯誤？

(A) 其為 X.509電腦網路標準，並使用 X.500資料模組定義屬性

(B) 用於驗證所代表之實體（Entity），例如：主機、組織或個人

(C) 可透過憑證確認其發行者的數位簽章（Digital Signature）

(D) 每張憑證僅能用於驗證一個網站（Website）

管理 112-2 答案D

(一張數位憑證可以用於驗證多個網站(如萬用憑證可以驗證多個子網域)，而不是僅能驗證一個網站，故D錯誤)

38. 下列何種密碼演算法，其加密與解密使用的金鑰不同？

(A) DES (對稱)

(B) 3DES (對稱)

(C) AES (對稱)

(D) RSA (非對稱)

管理 112-2 答案D

(RSA是非對稱加密算法，使用不同的公鑰和私鑰進行加解密，而DES、3DES、AES都是使用相同金鑰的對稱加密算法，故選D。)

24. 為確保應用程式中之資料安全，所需採取的安全措施，下列敘述何者錯誤？

(A) 演算法、協議與金鑰即時更新，並有適當金鑰管理機制

(B) 確保所有隱私資料於儲存時進行加密

(C) 總是使用雜湊函式來代替加密函式

(D) 不儲存不必要的隱私資料，或儘速清除

技術 112-1 答案C

(雜湊的特性就是資料不可逆，如果情境是需要還原原始資料，還是要選則加密函式使用)

36. 關於目前尚未被公開有碰撞攻擊（Collision attack）威脅之雜湊函式（Hash functions）類型，下列敘述何者正確？

(A) SHA-1

(B) SHA-2

(C) MD5

(D) CRC-32

管理 112-1 答案B

(SHA-2目前尚未被發現有效的碰撞攻擊，而SHA-1和MD5都已被發現碰撞攻擊的漏洞，CRC-32 主要用於錯誤檢測，並不適用於需要高安全性的應用，如數位簽章或加密驗證)

37. 關於非對稱式密碼學（Asymmetric cryptography）的敘述，下列何項錯誤？

(A) 私鑰（Private-key）僅能用於解密訊息

(B) 私鑰可用於產生數位簽章（Digital signatures）

(C) 公鑰（Public-key）可用於加密訊息

(D) 也稱作公鑰密碼學（Public-key cryptography）

管理 112-1 答案A

(私鑰不僅可以用於解密訊息，還可以用於生成數位簽章，故A選項錯誤)

40. 假設有兩金鑰，金鑰A用來將明文x變成密文y，而金鑰B用來將密文y變成明文x，當金鑰A與金鑰B是同一把金鑰時，請問他最有可能是下列何種加密演算法？

(A) AES (AES是對稱式加密，意味加密與解密使用相同金鑰)

(B) RSA (非對稱加密)

(C) ECC (非對稱加密)

(D) SHA (雜湊函數)

管理 112-1 答案A

12. 請問下列哪個 SSL Cipher Suite「 不 」 安全應停用？

(A) RC4

(B) AES256

(C) AES512

(D) AES128

技術 111-2 答案A

(RC4為非對稱演算法，且已不安全)

40. 下列何種機制「不」可用於加密及解密?

(A) AES（Advanced Encryption Standard） (對稱)

(B) DES（Data Encryption Standard）(對稱)

(C) RSA（Rivest–Shamir–Adleman）(非對稱)

(D) MD5（Message-digest algorithm）(雜湊)

管理 111-2 答案D

3. 下列選項何者作為金鑰分配（Key Distribution） 的安全性較佳？

(A) 3DES (對稱)

(B) MD5 (雜湊)

(C) Blowfish (對稱)

(D) ECC (非對稱)

規劃 111-1 答案D

(非對稱加密演算法（如ECC）能有效解決金鑰分配的核心問題，而對稱加密（3DES、Blowfish）需依賴其他機制傳輸金鑰，而雜湊函數（MD5）則完全不適用)

3. 下列何種密碼學演算法，對於不同大小的資料， 運算後產生的資料長度都一樣？

(A) RC5（Rivest Cipher 5） (對稱)

(B) RSA（Rivest, Shamir, Adleman） (非對稱)

(C) ECC（Elliptic Curve Cryptography） (非對稱)

(D) MD5（Message Digest Algorithm 5） (雜湊)

防護 111-1 答案D

(只有雜湊函數運算後的資料長度都一樣)

21. 關於自然人憑證，下列敘述何者「不」正確？

(A) 使用非對稱式演算法產生金鑰對

(B) 簽驗章和加解密是使用同一組金鑰對

(C) 目前自然人憑證設有有效期，但可以展延

(D) 透過自然人憑證進行簽章時，被簽章之資料無長度限制

管理 111-1 答案B

(自然人憑證非對稱式演算法產生金鑰對，因此金鑰非同一把)

22. 一般而言，公開公鑰會透過憑證管理中心發行公開憑證來傳遞，對於仍在有效期內，卻因為某些因素造成憑證廢止的情形，可以透過下列何項協定來查詢？

(A) Online Certificate Status Protocol（OCSP）

(B) Online Certificate Register Protocol（OCRP）

(C) Online Certificate Revoke Protocol（OCRP）

(D) Certificate Transmit Protocol（CTP）

管理 111-1 答案A

(OCSP可以透過瀏覽器即時查詢單筆憑證狀態)

28. 關於系統安全性中，IETF（Internet Engineering Task Force）制定的AAA協定，下列何者定義主要說明認證機制？

(A) Applicability

(B) Authentication (認證)

(C) Authorization (授權)

(D) Accounting (紀錄)

管理 111-1 答案B

45. 下列何者「不」是SSH所使用的密碼學技術？

(A) 對稱加密（Symmetric Encryption）

(B) 非對稱加密（Asymmetric Encryption）

(C) 金鑰雜湊訊息鑑別碼（Keyed-hash Message Authentication Code）(HMAC 全名為「基於雜湊的訊息認證碼」，主要用途在於確保資料傳輸過程中的完整性以及驗證訊息來源。簡單來說，它會用一組事先約定好的密鑰結合雜湊演算法（像是 SHA-256）來產生一段獨一無二的認證碼。這個認證碼就像是數位上的防偽標籤：

* **資料完整性保護**：傳送資料時，HMAC 會生成一個認證碼。如果資料在傳送過程中被竄改，重新計算出的認證碼就會不一樣，接收方就能發現異常。
* **驗證訊息來源**：由於只有雙方知道那個密鑰，所以只有合法的一方才能生成正確的 HMAC，這樣就能確認訊息的來源是可信的。)

(D) 三重資料加密演算法（3DES）

技術 111-1 答案D

(三重資料加密演算法（3DES） 雖然是對稱加密的一種，但由於其安全性較低（金鑰長度不足、易受特定攻擊）且效率不佳，現代SSH實現（如OpenSSH 7.0+）已預設禁用此算法，轉而使用更安全的AES或其他現代加密算法)

(SSH（Secure Shell）是一種用於遠端連線和資料傳輸的安全通訊協議，其主要流程大致可以分為以下幾個步驟：

1. **連線建立**客戶端向伺服器發起 TCP 連線，預設埠號為 22。
2. **版本交換**雙方互相傳送版本資訊，以確保彼此使用相容的 SSH 協議版本。
3. **密鑰交換與加密算法協商**
   * **密鑰交換**：雙方利用 Diffie-Hellman（或其他演算法）進行密鑰交換，生成用於對稱加密的共享秘密。
   * **算法協商**：同時協商使用的加密算法、雜湊函數與 HMAC 等驗證機制。
4. **伺服器認證**客戶端驗證伺服器所提供的主機金鑰，確保連線對象正確，以防範中間人攻擊。
5. **建立加密通道**利用密鑰交換所獲得的共享秘密，雙方建立起安全的加密通道，之後的所有通訊都會被加密。
6. **使用者認證**使用者需透過密碼、公鑰或其他認證方式向伺服器證明身份，認證成功後即可取得存取權限。
7. **資料傳輸與安全保護**在安全通道中，所有資料傳輸均經過加密，同時配合 HMAC 等訊息認證碼來驗證資料完整性與來源，防止資料被竄改或偽造。
8. **連線結束**傳輸完成或使用者主動結束連線時，雙方會安全地終止連線，釋放資源。

)