

等 級：佐級晉員級

類科(別)：技術類（選試資訊管理與資通安全概要）－公路

科 目：資訊管理與資通安全概要

考試時間：1 小時 30 分

座號：_____

※注意：(一)禁止使用電子計算器。

(二)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。

(三)本科目除專門名詞或數理公式外，應使用本國文字作答。

- 一、請說明數位憑證（Digital Certificate）、憑證中心（Certificate Authority, CA）、公鑰（Public Key）、私鑰（Private Key）、數位簽章（Digital Signature）及憑證廢止清單（Certificate Revocation List, CRL），並詳述其如何交互運作，以完成一份文件的數位簽章及驗證。（25 分）
- 二、企業內部使用的軟體，常因設計瑕疵而存在安全上的隱憂。確保軟體安全有些重要的原則，例如「設計簡單化」、「適度的權限劃分」等。請說明何謂「設計簡單化」與「適度的權限劃分」，並請再另外舉出三個確保軟體安全的重要原則。（25 分）
- 三、假設兩個體共同持有一把長期秘密金鑰（Long-Term Secret Key） k ，且沒有任何第三者知道 k ，試述如何利用對稱式密碼機制（Symmetric Cryptosystem）設計一個可重複執行之協定，使得每次執行此協定後，雙方可秘密地協議好一把隨機產生的會談金鑰（Session Key），且任何第三者不能仿冒任一方成功地執行完成此協定，並請詳述其安全特性。（25 分）
- 四、國家資通安全會報推行「建立我國通資訊基礎建設安全機制計畫」，要求與社會安定或國家安全相關的重要資訊系統必須建置資通安全監控中心（Security Operation Center, SOC），以增強其資安防護能力。請說明 SOC 必須包含那些重要功能？（25 分）