

等 別：三等一般警察人員考試

類 科 別：警察資訊管理人員

科 目：網路安全與資訊倫理

考試時間：2 小時

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。

一、Salt value 經常被使用於 UNIX 電腦的使用者認證系統中，來產生使用者密碼的雜湊值。

(一)列出這個認證系統收到使用者以帳號和密碼登入後之驗證步驟。(10 分)

(二)此認證系統之密碼檔中，加入 Salt value 的三個主要目的為何？(15 分)

二、電子郵件安全協定 (Secure/Multipurpose Internet Mail Extension, S/MIME) 提供 MIME 協定的安全性延伸：

(一) S/MIME 與 MIME 相較，多提供那四個安全性的功能？(20 分)

(二)寫出 Alice 透過 S/MIME 寄信給 Bob 且需滿足下列兩個要求之步驟：(10 分)

1. Bob 需確定信件來源是 Alice。

2. Alice 需確定只有 Bob 可看到信件內容。

三、防火牆常用於過濾網路封包來進行存取控制，依照其管制之方式主要可分為四種控制，請列出並解釋這四種控制方式。(25 分)

四、列出並說明安全評估共通準則規範 (Common Criteria specification) 中，所定義一個可信任的系統之隱私保護所應包含的四個特性。(20 分)