99年公務人員特種考試警察人員考試及
99年特種考試交通事業鐵路人員考試試題　　代號：20140　　全一頁

等　　別：二等考試
類　　科：刑事警察人員數位鑑識組
科　　目：網路與資訊安全（包括資訊安全技術與應用、資安事件處理）
考試時間：2 小時　　座號：＿＿＿＿＿＿＿＿

※注意：㈠禁止使用電子計算器。
㈡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、ITU-T 定義出 OSI 之安全架構（Security Architecture for OSI），內容焦點在安全攻擊（Security attack）、安全機制（Security mechanism）及安全服務（Security service）這三個面向。請就安全服務這一項，說明其將安全服務分成那幾大項，各大項下特定細目安全服務有那些？（15 分）

二、在架設有防火牆（Firewall）之網路時：
㈠試說明有那三種運作型態或功能之防火牆（Types of Firewalls）及其運作方式為何？（10 分）
㈡三種基本有防火牆之網路架構（Firewall configurations）為何，並請在其中說明在該架構中，使用何種型態或功能之防火牆？（10 分）

三、有關 IPSec（IP Security）：
㈠何謂 IPSec？其與 SSL（Secure Socket Layer）差異為何？（10 分）
㈡ IPSec 使用那兩種協定？另其內涵為何？（10 分）

四、有關公鑰系統之運作基礎：
㈠何謂數位憑證（Digital certificate），使用者 A 與 B 如何使用數位憑證作互相認證？（5 分）
㈡數位憑證格式或內容，應包含那些項目？（5 分）
㈢憑證授權中心（Certificate authority）角色及其服務項目為何？（5 分）
㈣公鑰基礎架構（Public-Key Infrastructure）之內涵為何？（5 分）

五、試說明下列名詞之意義及內涵：（每小題 5 分，共 25 分）
㈠ DSA（Digital Signature Algorithm）
㈡ HMAC（Hashed Message Authentication Code）
㈢ DH（Diffie-Hellman）key exchange
㈣ MD5（Message-Digest algorithm 5）
㈤ Kerberos protocol