103年公務人員特種考試警察人員考試
103年公務人員特種考試一般警察人員考試　　代號：20160　全一頁
103年特種考試交通事業鐵路人員考試試題

等　　別：二等一般警察人員考試
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、密碼學（Cryptography）廣泛應用在資訊與網路安全上，請問：
㈠私密金鑰（Private key）和公開金鑰（Public key）兩種密碼系統的特點及優缺點為何？請說明之。（10 分）
㈡使用公開金鑰密碼系統時需由 CA（Certificate Authority）提供一個憑證（Certificate），請問該憑證的主要內容為何？CA 在此扮演的角色為何？（10 分）

二、Bell LaPadula model 是應用來確保多階層資訊安全（Multi-level information security）。請問：
㈠何謂多階層資訊安全？（5 分）
㈡請詳細說明此 model 中兩個重要特性的意義：*1.* The Simple Security property 以及 *2.* The ★-property （10 分）
㈢此 model 所保障的資訊安全和另一種著名的 Biba model 有何不同？（5 分）

三、IPsec 是實現在 IP 層的複雜安全協定，可用於 VPN 的實現上。請問：
㈠「IPsec 可操作於 Transport mode 或者 Tunnel mode」，請問這句話代表的意義為何？請說明之。（10 分）
㈡ IPsec 提供 Authentication Header（AH）和 Encapsulating Security Payload（ESP）兩種基本協定，請說明這兩種協定的功能。（10 分）

四、WiFi 無線網路的使用愈來愈普遍，其安全性也日益受到重視，請問：
㈠ IEEE 802.1X 可用於 Access Point（AP）的存取控制上，請說明其工作原理？（10 分）
㈡ WPA（Wi-Fi Protected Access）安全標準應用於何處？其較 WEP（Wired Equivalent Privacy）標準主要做了那些改進？（10 分）

五、根據統計，緩衝區溢位（Buffer overflow）攻擊占惡意程式攻擊的大部分，請問：
㈠何謂緩衝區溢位攻擊？請詳細說明其攻擊原理。（10 分）
㈡從程式設計師的觀點來看，防制緩衝區溢位攻擊和防制 SQL-Injection 攻擊的方法有何異同？（10 分）