100年公務人員特種考試一般警察人員考試、
100年公務人員特種考試警察人員考試及 代號：20160　　全一頁
100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、請詳細說明下列專有名詞：（每小題 5 分，共 25 分）
㈠密碼學（Cryptology）
㈡區塊型密碼器（Block Cipher）
㈢雪崩效應（The Avalanche Effect）
㈣角色為基礎的允入控制（Role-Based Access Control, RBAC）
㈤非對稱式密碼器（Asymmetric Cipher）

二、公開金匙基礎建設（Public Key Infrastructure, PKI）：
㈠什麼是 PKI？PKI 如何運作？（10 分）
㈡憑證取消表（Certificate Revocation List, CRL）的功能為何？重要性為何？（5 分）
㈢列舉兩個 PKI 可能應用之範疇。在應用上還有那些問題可能要考慮？（10 分）

三、虛擬私有網路（Virtual Private Network, VPN）：
㈠什麼是 VPN？在那些情況下我們可以應用它？（10 分）
㈡VPN 應用隧道（Tunneling）機制，解釋什麼是隧道機制？（5 分）
㈢什麼是 IP-Sec（IP Security）VPN？簡單說明它的運作原理。（10 分）

四、風險管理（Risk Management）：
㈠什麼是風險？請定義。（5 分）
㈡什麼是風險分析（Risk Analysis）？風險鑑識（Risk Identification）主要有兩種方法，請說明之。（10 分）
㈢為什麼風險管理是資訊安全管理系統（Information Security Management System, ISMS）中很重要的一部分？（10 分）