107年公務人員特種考試警察人員、一般警察人員考試及
107年特種考試交通事業鐵路人員考試試題　代號：20120　全一頁

考 試 別：一般警察人員考試
等　　別：二等考試
類 科 別：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。
㈢本科目除專門名詞或數理公式外，應使用本國文字作答。

一、Alice 將明文檔案切成大小相等的 N 個區塊（$P_1, P_2, \ldots, P_N$），她用對稱加密演算法，以 CBC（Cipher Block Chaining）mode 進行加密，得到輸出密文（$C_1, C_2, \ldots, C_N$）並傳送給 Bob。
㈠假如在加密前，P_1 有一個位元錯誤，則此錯誤會傳導影響到加密後的那些密文區塊？又，此錯誤會影響到 Bob 解密後的那些明文區塊？（15 分）
㈡假如在傳輸過程中，C_1 有一個位元錯誤，則 Bob 解密後會有那些明文區塊是錯誤的？（10 分）

二、HTTPS（Hypertext Transfer Protocol Secure）是常用於 client-server 架構的協定。
㈠ HTTPS 如何確保通訊安全？（10 分）
㈡詳細說明使用 HTTPS 時，瀏覽器（Web browser）與伺服器（Web server）之間有那些通訊內容會被加密？（15 分）

三、無線傳輸（wireless transmission）有那些主要的安全威脅（security threats）？對於這些安全威脅有什麼解決對策？（25 分）

四、在資安事件處理程序中，偵測階段（detection）的目的是找出潛在安全事件的跡象。
㈠那些資訊來源有助於偵測階段的工作？（15 分）
㈡如果事件的受害系統有整合外部提供的雲端服務，偵測工作可能會有那些問題？（10 分）