代號：20120
頁次：1－1

108年公務人員特種考試警察人員、一般警察人員考試及
108年特種考試交通事業鐵路人員、退除役軍人轉任公務人員考試試題

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本科目得以本國文字或英文作答。

一、*A* 和 *B* 時常需要使用電腦網路聯繫（開會），每次開會時希望可以將在網路傳送的訊息加密，以免洩漏機密資訊。

㈠假設 *A* 和 *B* 共享一個秘密金鑰 *k*。使用這個秘密金鑰 *k*，*A* 和 *B* 可在開會之前建立會議金鑰（session key）。但是秘密金鑰 *k* 可能會被偷竊、洩漏或破解。在此情況下，解釋向前保密（forward secrecy）之意義。（10 分）

㈡假設 *A* 和 *B* 使用 Diffie-Hellman 金鑰交換協定建立每次之會議金鑰。在何種形況下，可視為具有向前保密之性質？在何種形況下，就無法具有向前保密之性質？（10 分）

二、有些惡意網站會模仿真網站的顯示內容以騙取使用者的帳號和密碼。即使用了網站認證（website certificates）的技術，網頁還是容易被模仿。請設計一個簡單的方法來檢驗某個網站的真假。（20 分）

三、為提供研究或其他合法用途，政府機關或其他單位常會公開他們所收集到的個人資料。為了避免個人資料洩漏，在公布這些資料或提供查詢之前，必須先做去識別化的工作。解釋一個資料庫經去識別化之後達到 *l*-多樣（*l*-diversity）之意義。並解釋「不同 *l*-多樣」（distinct *l*-diversity），「熵 *l*-多樣」（entropy *l*-diversity），以及「遞歸（*c*, *l*）-多樣」（recursive（*c*, *l*）-diversity）。（20 分）

四、最近發現某類型的處理器（CPU）可能潛藏安全漏洞。請先解釋分支預測（branch prediction），再回答這些處理器為何會造成 spectre 安全漏洞。（20 分）

五、有人認為網路的安全問題之所以會發生，都是因為系統或應用程式撰寫不正確所造成的，所以只要程式沒有錯誤（bug）就可高枕無憂了。舉出至少三種事項說明即使所用的程式都沒有錯誤，也還會發生的問題與困擾。（20 分）