代號：30570
頁次：2－1

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：三等考試
類 科 別：警察資訊管理人員
科　　目：網路安全與資訊倫理
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、假設考試成績最低為 0 分，最高 100 分。某位考生的成績為 x 分，為了保密，教師隨機從 0 到 100 之中選擇一個整數 k，並將這位考生的成績 x 加密為 y = (x+k) mod 101，就是將原成績 x 加上 k，再除以 101 取餘數，其結果 y 當作密文。

㈠假設 k 的選法是每個從 0 到 100 之中的整數被選到的機率是一樣的。證明即使攻擊者有無限多的計算資源，也無法從密文 y 推算得明文 x。（10 分）

㈡假設班上有 n 位同學，n > 1。每位同學均以相同方式，相同的 k 值加密。這樣的加密系統是否仍是安全的？（10 分）

二、通行碼是最常被使用的身分識別方法。但是通行碼的設定必須不容易被惡意者猜中，否則就不安全。㈠說明至少三類容易被猜中的通行碼（也就是一般使用者常犯的錯誤）。㈡設計一個選擇通行碼的具體可行的方法，使得所選取的通行碼不容易被惡意者猜中，且使用者容易記憶。（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蒐集到的個人資料。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 k-匿名（k-anonymity）之定義，並說明至少 2 種最常用之處理方式，使公布之資料可達到 k-匿名。（20 分）

四、防火牆是一種用來控制網路存取的設備。但是安裝了防火牆並非表示就可防止網路的攻擊。列出至少四項防火牆做不到，但是會影響網路、系統或資訊安全的項目。（20 分）

五、依照我國現行之個人資料保護法規定，當事人就其被蒐集之個人資料，可行使那些權利？蒐集這些個人資料之機關可否因為作業方便，或給予當事人更多優惠，在獲得當事人書面同意之後，要求當事人放棄這些權利？（20 分）