103年公務人員特種考試司法人員、法務部調查局調查人員、國家安全局國家安全情報人員、海岸巡防人員及移民行政人員考試試題　代號：21060　全一頁

考 試 別：調查人員
等　　別：三等考試
類 科 組：資訊科學組
科　　目：資訊安全實務
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、美國科技媒體網站（Ars Technica）2013 年發表文章引述我學者論文指出，自然人憑證有弱金鑰問題，恐影響憑證安全性。請問何謂弱金鑰？主要發生原因為何？（20 分）

二、一些駭客會透過偽造 DNS（Domain Name System,網域名稱系統）伺服器將使用者引向錯誤網站，以達到竊取使用者隱私訊息的目的。為解決此一問題，網際網路工程任務組（IETF）提出域名系統安全擴展（DNSSEC, Domain Name System Security Extensions），請說明 DNSSEC 之做法。（20 分）

三、數位鑑識（digital forensics）主要在針對數位裝置中的內容進行調查與復原，試舉例說明一般典型的數位鑑識程序。（20 分）

四、資訊安全監控中心（Security Operations Center, SOC）目的在於整合並管理組織各種不同環境下的資安訊息，並且對安全事件做出對應的機制。試舉出五種常見的 SOC 服務項目，並說明其內容。（20 分）

五、網路安全演練是一個評估團體是否準備好應對網路危機、技術失誤及關鍵資訊基礎設施事故的重要工具。一些國際知名的網路安全演練，如美國國土安全部主辦的 Cyber Storm 國際網路安全演練，提供網路安全演練的參考性指標。試舉例從演練範圍、演練情境與情境細節說明網路安全演練的知識與經驗，並說明其可強化公共與私人部門的網路防護。（20 分）