《資訊安全實務》

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）

試題評析	可由「RSA」非對稱加密演算法與「PKI」思考。
考點命中	《高點資訊管理與資通安全講義》第三回，張又中編撰，頁 3-8、13~14。

【擬答】

1.自然人憑證採 RSA 非對稱加密法，民國 99 年 12 月 31 日以前核發其金鑰長度爲 1024 Bits，由於金鑰產生過程中質數非隨機產生且有跡可尋，研究發現有 103 張自然人憑證共享 119 個質數，因此攻擊者可於數小時內破解金鑰。

2.因此，內政部與中華電信全面檢視所有 220 餘萬張自然人憑證，發現有 163 張屬於弱金鑰，故於 101 年 7 月主動更換金鑰長度 2048 Bits 的新憑證給弱金鑰持卡民眾，以確保自然人憑證應用之安全。

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）

試題評析	可由數位簽章、雜湊函數思考。
考點命中	《高點資訊管理與資通安全講義》第三回，張又中編撰，頁 3-10~12、15。

【擬答】

由於 DNS 的查詢與回應封包並未加密，因此駭客可於其中僞造，將使用者導向錯誤的主機，或是進行 DNS 放大攻擊。因此，DNSSEC 利用公開加密演算法與雜湊函數來提供：

(一)資料完整性(Data Integrity)

DNS 伺服器使用數位簽章將每筆資源紀錄(Resource Record, RR)產生資源紀錄簽章(Resource Record Signature, RRSIG)，用戶端可用 DNS 伺服器的公開金鑰(DNSKEY)與 RRSIG 驗證。

(二)來源可驗證性(Origin Authentication of DNS Data)

DNS 伺服器必須將其 DNSKEY 做數位簽章後放在 Parent Zone Server，此資料紀錄稱爲 DS(Delegation Signer)，可由 Parent Zone 的 DS 紀錄驗證 Child Zone 之 DNSKEY 正確且未經竄改。

(三)可驗證之不存在性(Authenticated Denial of Existence)

攻擊者可能假造回應不存在之封包，因此，DNSSEC 將所有 DNS 紀錄依字母排序，在每個網址間加上一筆 NSEC 紀錄並做電子簽章，可比對 NSEC 紀錄中前後對應的字母來驗證。

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）

試題評析	本題爲近年常考之「數位鑑識」，可由講義內容切入。
考點命中	《高點資訊管理與資通安全講義》第一回，張又中編撰，頁 1-6~9。

【擬答】

數位鑑識程序如下：

(一)蒐集

從犯罪現場找出所有可能成爲證據的數位資訊設備及儲存媒體，爲提出訴訟的第一步。需檢視證據是否充足，以及採證過程是否完備。

蒐集證據的過程中，如果是原告自行蒐集，可能會在法庭上受到被告質疑數位證據遭到竄改。因此，需透過公正第三方的採證或鑑識，以確保所蒐集的數位證據具證據能力。

(二)檢驗

檢驗涉及存取並擷取輸出與案情相關的資訊。

(三)分析

針對資料進行分析、交叉檢驗及推論案情。實務上數位鑑識人員必須與案件承辦人溝通，瞭解案情的重點所在。

(四)報告

將分析的結果及結論，以清楚明瞭的方式呈現以供參考。

(五)呈現

相關數位證據與報告呈現於法庭，作爲認定事實，適用法律之基礎。並視案情需要出庭作證。

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）

試題評析	可由「SOC」之觀念思考。
考點命中	《高點資訊管理與資通安全講義》第三回，上課補充。

【擬答】

SOC 爲一集中式的安全管理平台及維運機制，可記錄多種資安設備及伺服器所產生的資安事件，並以系統化的方式收集、分析、儲存。透過 SOC 管理平台進行 7×24 之監控服務、事件通報與處理，以提升企業組織之資訊安全並確保資訊資產安全。SOC 主要服務項目有：

(一)資安警訊管理

每日蒐集最新的資安警訊，判斷其是否會對系統造成風險，並對新發現的弱點進行修補。

(二)資安弱點管理

常見的稽核方式爲弱點掃描及滲透測試，必須定期執行，並對發現的弱點進行修補。

(三)資安設備管理

如定期更新防毒軟體病毒碼、定期審定防火牆規則、定期檢視 IDS 與 IPS 的 Log。

(四)資安事件監看

7×24 監看系統，由 SOC 平台進行初步的資料過濾，再由專業的資安技術人員分析，於資安事件發生時立即處理。

(五)資安事故處理

進行資安事故的後續處理與改善，事故處理的方式端視系統重要性與關鍵性，如重要性較低的主機可以逕行重新安裝作業系統的方式解決。

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）

試題評析	爲資訊安全趨勢，可由行政院國家資通安全會報技術服務中心之公開資料切入。
考點命中	上課補充筆記。

【擬答】

Cyber Storm 爲由美國國土安全部主辦的國際網路安全演練，2006 年起每兩年舉辦一次，提供大規模政府供應商網路安全演練的框架。基於真實資安事件的經驗教訓，讓參與者面臨更複雜、更具挑戰性的演練，以強化公/私部門的網路防護，可用來評估國家抵抗數位間諜活動的防禦能力。Cyber Storm 的參與者會進行下列活動：

(一)檢查組織面對網路攻擊潛在影響之準備、保護及應變能力。

(二)依照國家層級的政策和程序，練習戰略決策與事件應變之協調。

(三)驗證資訊分享關係及收集和傳播網路事件的態勢、應變及復原的通訊途徑。

(四)檢查透過通訊途徑分享跨邊界與部門敏感資訊的方法與流程，不影響其自身或國家安全利益。

	Cyber Storm I	Cyber Storm II	Cyber Storm III
演練範圍	11個聯邦政府部門 3個州政府 30多家民間企業 4個盟國	18個聯邦政府部門 9個州政府 40多家民間企業 4個盟國 10個資料處理中心	國土安全部 6個聯邦政府部門 11個州政府 60多家民間企業 12個盟國
演練情境	能源、IT、交通及電信等關鍵基礎建置遭到大規模網路攻擊	IT、通信、化工及交通等關鍵基礎建置遭到網路攻擊，看國內、外合作夥伴的應變、協調能力	針對DNS與CAs進行攻擊
情境方向	1. 用網路攻擊擾亂關鍵基礎建置 2. 阻礙政府應對網絡攻擊的能力 3. 破壞民眾對政府提供/保護服務能力的信心	1. 網路中斷 2. 通訊中斷 3. 控制系統問題	1. Compromise服務更新 2. Compromise EMS 3. 化工與運輸、4.聯邦、5.國際、6.DoD/LE/I、7.PA及8.美國情境聯繫

參考資料：”Cyber Storm 簡介”，谷威函，財團法人資訊工業策進會與行政院國家資通安全會報檢測技術中心。