CH08

是非題

(○) 1. 資料機密性通常透過資料加密來達成。

(○) 2. 對稱式加密演算法的執行效率，一般而言，較非對稱式加密演算法來得好。

(×) 3. 在密碼長度相同的情況下，非對稱式的加密演算法較對稱式加密演算法來得安全。

(○) 4. 使用非對稱式金鑰演算法進行加密，只有擁有私密金鑰的使用者，可以順利地進行解密。

(×) 5. 網站的網址只要是使用 https 的協定傳輸，就一定是安全無虞的。

(×) 6. 手機所使用的 A5 演算法，是一種對稱式的區塊加密演算法。

(○) 7. RSA 演算法是基於因數分解的困難度設計而成的。

(×) 8. 只要不知道密碼，就永遠都無法得知被加密保護的密文。

(○) 9. 憑證（certificate）的目的是用以證明公開金鑰的擁有者以及其背書者是否正確。

(×) 10. 雜湊函數的輸出與輸入內容的長度成比例。

選擇題

(A) 1. 下列何種對稱式演算法是美國國家標準技術局自 2001 年起採用的加密標準?

(A)AES (B)BES (C)CES (D)DES

(C) 2. 若要在公開場合交換密碼,我們可使用下列何種演算法進行交換?

(A)RSA (B)ElGamal (C)Diffie-Hellman (D)BlowFish

(B) 3. 阻斷服務攻擊(DoS)的進階版 DDoS,其字首 D 的意義為何?

(A)Daniel (B)Distributed (C)Denial (D)Distributor

(D) 4. 下列何者不是常見的無線網路傳輸相關的加密機制?

(A)WEP (B)TKIP (C)WPA (D)WAP

(C) 5. 下列哪種應用和非對稱式加解密演算法無關?

(A)RSA (B)DSA (C)DES (D)ElGamal

(B) 6. RSA 演算法是基於計算何種問題的困難度設計而成?

(A)離散對數 (B)因數分解 (C)二次剩餘 (D)橢圓曲線

填充題

1. 基於效率考量，數位簽章通常不直接對內容進行簽章，而是針對內容的 雜湊值 進行簽章。

2. 我們可以使用 雜湊函數 來檢查資料是否遭到修改。

3. 駭客自製介面精美的偽冒網站，以吸引使用者提供其帳號密碼等個人資訊。這種攻擊我們稱為 （網路）釣魚 。

4. 表面上沒有惡意，卻暗地裡在電腦主機上開啟後門的程式，我們常常稱其為 特洛伊木馬（Trojan horse） 。

5. 我們可以透過 加密 的方式，避免資料在網路傳輸時遭到監聽。

6. 目前常見的無線網路連線常用的安全加密機制為 WEP 以及 WPA 。

簡答題

1. 請列舉 3 種常見的對稱式金鑰加密演算法。

【詳解】

DES、AES、IDEA、RC5 等。

2. 區塊加密的對稱式加密演算法常常需要配合操作模式如 CBC、CTR 等運作，其主要原因為何？

【詳解】

其主要原因是避免使用相同的密碼與相同的演算法，對相同的資料進行 加密時，產生相同的密文。透過初始向量（IV）、密文以及加密資料的 XOR 運算，可以提升加密資料安全性。

3. 請列舉 2 種常見的雜湊演算法。

【詳解】

MD5、SHA1、SHA256 等。

4. 我們在建置高可用性的系統時，常常使用「心跳」（heartbeat）機制。請簡述心跳機制的做法。

【詳解】

心跳機制讓二個系統之間，互相偵測另一個系統是否還是在正常運作中。簡單的說，心跳機制就是讓二台主機之間定期交換一個特定的探測訊息。如果其中一方發現另一個系統沒有回應時，就可以判斷系統異常而啟動備援，接手工作的機制。