長庚大學114學年度碩士班考試招生筆試試題

系所：資訊管理學系碩士班　　考試科目：資訊安全概論

注意：請詳細閱讀下列試題，並請標明題號依試題順序將答案書寫於答案卷上。　　本試題共 二 頁：第 / 頁

資訊安全碩士班研究所考題

一、選擇題(每題 4 分，共 80 分)

1. 以下關於不可否認性的敘述哪個為真? (A)　防止通訊的雙方否認曾經傳送或接收訊息 (B)　接收端能夠證明發送端事實上已送出訊息 (C) 發送端能夠證明接收端已經收到送出的訊息 (D) 以上皆是
2. 有一種攻擊是利用三向交握的弱點，攻擊者一直送出連線要求的封包，當伺服器回送的訊息時，卻不回應確認(ACK)封包，造成連線無法建立，而且連線要求會一直佔據伺服器的佇列，佇列被佔滿之後，伺服器就無法再接受其他的連線要求了，是屬於哪種攻擊? (A) TCP SYN Flood 攻擊 (B) Land Attack (C) UDP Flood 的攻擊 (D) Smurf 攻擊
3. 偽裝成可被伺服器信任(Trusted)的 IP 位址，再發動攻擊，是屬於哪種攻擊? (A) TCP SYN Flood 攻擊 (B) Land Attack (C) UDP Flood 的攻擊 (D) Smurf 攻擊
4. Ping 到死攻擊是屬於哪種通訊協定為基礎的攻擊手法? (A) TCP (B) UDP (C) IPSec　(D) ICMP
5. 以下何者為非? (A) 有別於用自然語言寫成的紙本合約，智慧合約的智慧之處在於藉由編寫程式碼，達成資產交換自動化，但不是所有程式都可以交給以太坊執行，只有用以太坊專屬的程式語言（例如 Solidity）才可以。(B) 利用大量封包傳送，癱瘓受害者的電腦、伺服器；或是篡改傳送中的封包資料；或是傳送假的訊息給另一具有利益關係的受害者，造成其財務上或精神上的損失，是屬於 passive attack。(C) RSA 是非對稱式的加密方法。(D) DES 是對稱式的加密方法。
6. 利用加密技術，讓非授權者因無法取得金鑰而無法解開通訊中的祕密訊息，是為了符合資安的哪個基本需求? (A)完整性 (B) 不可否認性　(C)可用性　　(D) 機密性
7. 可以利用數位簽章及公開金鑰基礎架構(Public Key Infrastructure, PKI)對使用者身份及訊息來源做身份驗證及資料來源驗證之後，對於傳送方或接收方，都不能事後否認之前曾進行資料傳輸或接收，是為了符合資安的哪個基本需求? (A)完整性　(B) 不可否認性　(C)可用性　　(D) 機密性
8. 確保資訊與系統持續運轉無誤，以防止惡意行為導致資訊系統毀壞，當合法使用者要求使用資訊系統時，收/送電子郵件、遠端存取資訊等，使用者均可在適當的時間內獲得回應，並完成服務需求，是為了符合資安的哪個基本需求? (A)完整性　(B) 不可否認性　(C)可用性　　(D) 機密性
9. 確保資料內容僅能被合法授權者所更改，不能被未經授權者所篡改或偽造，是為了符合資安的哪個基本需求? (A)完整性 (B) 不可否認性　(C)可用性　　(D) 機密性
10. 要能確認資料訊息之傳輸來源，以避免有惡意的傳送者假冒原始傳送者傳送不安全的訊息內容(包括身份驗證及資料來源驗證)，是為了符合資安的哪個基本需求? (A)完整性 (B) 不可否認性 (C)可用性　　(D) 認證性
11. 在智能合約中，倘若總金額是 100 元，透過以下兩行程式碼
    winner.transfer(address(this).balance / 10 * 7);
    owner.transfer(address(this).balance);
    這兩行程式是代表 winner 及 owner 分別拿多少錢?(A)winner 拿 90 元、owner 拿 10 元 (B)winner 拿 60 元、owner 拿 40 元　　(C) winner 拿 70 元、owner 拿 30 元　　(D) winner 拿 80 元、owner 拿 20 元

12. 加密後的內容不能完全都打不開來，而是要有一把鑰匙能打開，這就是數學上所說的什麼? (A)one-way trap-door function (B)one-way hash function (C)Symmetry encryption technique (D) 以上皆是
13. DoS 是屬於違反資訊安全的哪個特性? (A) Authentication. (B) Availability (C) Confidentiality (D) Integrity
14. 利用 SHA 雜湊演算法計算出雜湊值，若收方及送方的雜湊值皆相同，必須文件在傳送途中沒有遭竄改或傳送錯誤，是符合資安的什麼特性? (A) Authenticity (B) Availability (C) Integrity (D) Confidentiality
15. 竊取是屬於違反資訊安全的哪個特性? (A) Authentication. (B) Availability (C) Confidentiality (D) Integrity
16. 入侵者將封包的來源 IP 位址設定成某台內部的主機 ，藉此躲過防火牆的安全檢查，是指哪種封包過濾器的攻擊? (A) IP Spoofing (B) 來源路徑攻擊法 (C) 細微區段攻擊法 (D)ARP Spoofing
17. 下列惡意軟體不需宿主程式? (A)Worms (B)Trapdoors (C) Logic Bombs (D) Viruses
18. 下列何者不是 active attack 的攻擊方式? (A) Denial of Service (B) 修改內容 (C) Masquerade (D) 竊取機密
19. 下面哪個非 Visual Cryptography 的特性? (A)運算量低 (B)快速解碼 (C)不需要 key (D)利用對稱式加密系統
20. 以下敘述哪個為假? (A) 連接導向(Connection-oriented)的完整性服務保證收到的訊息如寄送端所送出的內容 (B)連接導向可以指出包括訊息串流的修改和阻絕服務 (C)非連接導向(Connectionless)提供完整性服務 (D) 非連接導向(Connectionless)不僅能提供預防訊息修改的保護並可指出阻絕服務

二、問答題 (每小題 5 分，共 20 分)

以下範例操演一次 El-Gamal 加密演算法的過程，我們假設 Alice 要傳送明文訊息 M = 3 給 Bob，請回答以下的 1~4 題，求出 C_1、C_2、Y 及解回的 M 過程，並求出值。

Note1: 公開選定的數(任意) g = 4，大質數 p = 7，每次傳送隨機選一個數字(任意) r = 5，首先 Bob 要利用 g 值和另一個自選的值 X = 4

Alice 發送端運算密文的方法：

1. $Y = g^X \bmod p =$ _____

2. $C_1 = g^r \bmod p =$ _____

3. $C_2 = M*(Y)^r \bmod p =$ _____

Alice 傳送 C1, C2 給 Bob

Bob 解密的方法：

4. $M= (C_1^X)^{-1} * C_2 \bmod p =$ _____