計算機網絡安全技術・期末考

2022 秋　考題回憶版　by BoxWorld

一、單項選擇題

1. 在 Enigma 中，除了三個轉輪，還加上了一個反射器，其作用是（）。

   A. 和轉輪一樣，增加了密碼的強度

   B. 使解碼過程和編碼過程完全一樣，提升了使用的簡潔性

   C. 和連線設置一起工作，加強了密碼強度

2. 3-DES、Blowfish、RC5、AES 算法中，只有（）不是典型的 Feistel 密碼結構。

   A. 3-DES

   B. Blowfish

   C. RC5

   D. AES

3. Shannon 引入混淆和擴散來刻畫任何密碼系統，（）是盡可能地使密文和密鑰間的統計關係更複雜。

   A. 混淆

   B. 擴展

   C. 擴散

   D. AES

4. 網絡安全目標 CIA 的含義是：（）、（）和（）。

   A. 保密性、繼承性、可用性

   B. 保密性、完整性、可用性

   C. 機密性、繼承性、完整性

   D. 機密性、完整性、公證性

5. 安全性攻擊可以簡單地分成（）攻擊和（）攻擊，通過竊聽進行傳輸流量分析，屬於（）攻擊。

   A. 主動、被動、被動

   B. 主動、被動、主動

   C. 普通、特定、特定

   D. 普通、特定、普通

6. 蠻力破解、中間人攻擊、拒絕服務攻擊等屬於詐騙地下黑色產業鏈的第幾層?

   A. 最高層：漏動挖掘

   B. 第四層：代碼編寫

   C. 第三層：信息竊取

   D. 最低層：社會工程學

7. 在網絡環境中的（）等行為屬於消息認證範疇。

   A. 內容修改、順序修改、計時修改

   B. 發送方否認、接收方否認

   C. 泄密、傳輸分析

8. 認證即（），消息認證就是驗證所收到的消息來自真正的發送方且（）。

   A. 比較、未被修改

   B. 比較、順序正確

   C. 加密、未被修改

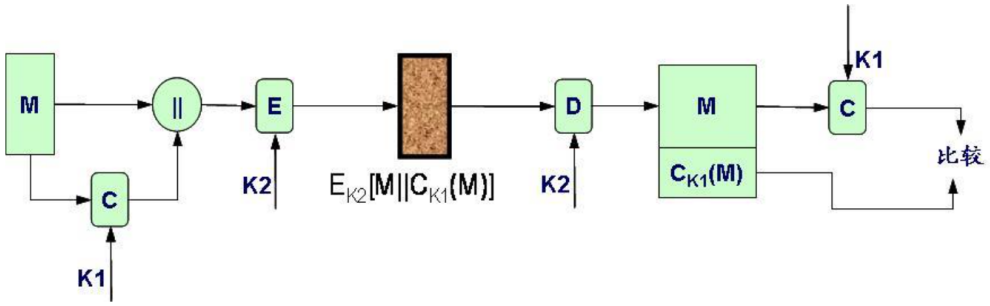
9. 任何消息在功能上可以看做兩層：下面是可以產生（）的函數，上面協議可以驗證消息的真實性。

   A. 消息認證符

   B. 哈希碼

   C. 校驗和

10. 如下圖所示，密鑰 K1 的作用是（），密鑰 K2 的作用是（）。



   A. 計算哈希碼的密鑰、對稱加密的密鑰

   B. 非對稱加密的密鑰、計算 MAC 的密鑰

   C. 計算 MAC 的密鑰、對稱加密的密鑰

   D. 非對稱加密的密鑰、計算哈希碼的密鑰

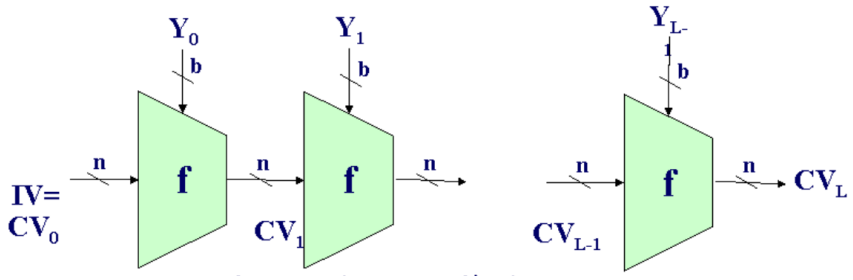
11. 將題 10 圖中的方法定為 A；如果先用 K2 加密 M，再用 K1 計算認證碼，定為方法 B；哪個方法更加安全?

A. 方法 A 更安全，認證碼也被加密保護了

B. 方法 B 更安全，明文首先被加密保護了

C. 方法 A 和 B 一樣安全

12. 在下圖中，n 表示（）；b 表示（）；因為 b>n，所以 f 被稱為（）。



A. 哈希碼長度、輸入分組長度、複雜函數

B. 輸入分組長度、哈希碼長度、複雜函數

C. 哈希碼長度、輸入分組長度、壓縮函數

D. 輸入分組長度、哈希碼長度、壓縮函數

13. 網站的用戶認證模塊是基於 Basic 認證的，客戶端將自己的賬號口令（U, P）進行 Base64 編碼後發送到 Web 服務器端，是否可以保障賬號密碼安全?

A. 可以保障，Base64 編碼具有不可讀性

B. 可以保障，Base64 編碼是二進制到字符的轉換，可以傳輸較長的信息

C. 不能保障安全，Base64 編碼不是加解密技術

D. 不能保障安全，Base64 編碼傳輸的是明文

14. 為了解決賬號口令明文傳輸可能被監聽盜取的問題，基於 Basic 認證在改進方案中使用了（）技術和（）技術。

A. 表單驗證、Session

B. 加解密、消息認證

C. 加解密、表單驗證

15. 1971 年，夏威夷大學實現的 ALOHA Net 是第一個使用（）技術代替點到點連接線路作為通信設施的計算機系統，無線網絡正式誕生。

A. 無線電通信

B. 移動蜂窩

C. 載波

D. 摩斯電碼

16. 有線等效保密協議 WEP（Wired Equivalent Privacy）目的是為無線局域網提供與有線網絡相同級別的安全保護。WEP 使用（），保證無線局域網的數據傳輸安全性；使用了（），只能檢測消息中的隨機錯誤，不能進行消息認證。

A. 非對稱加密算法，CRC-32 算法

B. 非對稱加密算法，校驗和算法

C. 對稱加密算法，CRC-32 算法

D. 對稱加密算法，校驗和算法

17. 虛擬專用網 VPN 的目的是在不安全的互聯網環境中，建立一條仿真的點到點私有連接。在歷史上，出現過（）VPN 技術。

A. 物理層和數據鏈路層

B. 網絡層和應用層

C. 數據鏈路層和傳輸層

D. 數據鏈路層、網絡層和傳輸層

18. 虛擬專用網 VPN 的安全功能包括：數據機密性保護、數據完整性保護、（）和（）。

A. 消息認證、接收方否認

B. 數據源身份認證、接收方否認

C. 消息認證、重放攻擊保護

D. 數據源身份認證、重放攻擊保護

19. IPSec 協議工作在（）和（）之間，其工作原理在於可以在（）加密或認證所有流量。

A. 網絡層、傳輸層、網絡層

B. 網絡層、傳輸層、傳輸層

C. 傳輸層、應用層、網絡層

D. 傳輸層、應用層、傳輸層

20. IPSec 協議的交檔包括七個部分，除了認證 AH 及其認證算法、封裝安全載荷 ESP 及其加密算法、還有用於相互聯繫的一些參數值集合的（）和用於（）的 IKE。

A. 安全關聯 SA、密鑰管理

B. 安全關聯 SA、錯誤預警

C. 解釋域 DOI、密鑰管理

D. 解釋域 DOI、錯誤預警

21. IPSec 協議具有兩個不同的報頭格式，只提供認證的是，可以提高加密和認證的是（）。

A. AH、ESP

B. AH、ISAKMP

C. ESP、ISAKMP

22. 安全關聯 SA 是 IPSec 通信雙方之間對某些安全信息參數的一種協商，是收發方之間的（）關係；一個安全關聯 SA 可以由三個參數唯一確定，包括安全參數索引 SPI、IP 目的地址和（）。

A. 雙向、IP 源地址

B. 雙向、安全協議標識

C. 單向、IP 源地址

D. 單向、安全協議標識

23. 負責存儲、維護安全關聯的數據庫是（）；負責將 IP 流量與特定 SA 相關聯的是（）。如果所需要的 SA 不存在，則（）負責去和對方進行協商。

A. SADB、SPDB、IPSec

B. SPDB、SADB、IPSec

C. SADB、SPDB、IKE

D. SPDB、SADB、IKE

24. 在 AH 和 ESP 的報頭中，（）域是用於防範重放攻擊的，（）域是用於消息認證的。

A. Sequence Number、Authentication Data

B. Sequence Number、Padding

C. Security Parameters Index、Authentication Data

D. Security Parameters Index、Padding

25. 使用 IPSec 協議在兩台主機之間進行端對端的加密和認證，要求一個隧道 SA 中有一個傳輸 SA，加密前認證。應該是下面哪種數據格式：

A. 【新 IPv4 頭 | AH 頭 | 原 IPv4 報頭 | ESP 頭 | TCP 報頭 | 數據 | ESP 尾】

B. 【新 IPv4 頭 | ESP 頭 | 原 IPv4 報頭 | AH 頭 | TCP 報頭 | 數據 | ESP 尾】

C. 【新 IPv4 頭 | ESP 頭 | AH 頭 | 原 IPv4 報頭 | TCP 報頭 | 數據 | ESP 尾】

D. 【新 IPv4 頭 | AH 頭 | ESP 頭 | 原 IPv4 報頭 | TCP 報頭 | 數據 | ESP 尾】

26. 作為互聯網的密鑰交換協議，IKE 協議解決了在不安全的網络環境中安全地建立或更新共享密鑰的問題；IKE 的精髓在於（）。

A. 通過雙方原有的共享密鑰，傳遞新的共享密鑰

B. 永遠不在不安全的網絡上直接傳送密鑰

C. 通過數據交換，各自計算出密鑰，並相互驗證

27. IKE 使用了兩個階段的 ISAKMP 框架，第一階段，協商創建一個通信信道（），第二個階段是使用使用已建立的通信信道建立（）。

A. IKE SA、IPSec SA

B. IPSec SA、IKE SA

C. 主模式、快速模式

D. 快速模式、主模式

28. SSL 協議為端到端的應用提供保密性、完整性、身份認證等安全服務，它可以保護正常運行於（）之上的任何應用層協議、與（）協議無關。

A. TCP、網絡層

B. UDP、網絡層

C. TCP、應用層

D. UDP、應用層

29. 在 SSL 中，（）定義了報文格式，（）負責協商參數。

A. SSL 記錄協議、SSL 握手協議

B. SSL 握手協議、SSL 記錄協議

C. SSL 記錄協議、SSL 告警協議

D. SSL 握手協議、SSL 告警協議

30. HTTPS = （） + （）。

A. HTTP、SSL

B. HTTP、IPSec

C. HTML、SSL

D. HTML、IPSec

31. HTTPS（）阻止 ARP 欺騙或者報文篡改，但是因為傳輸的是（），所以可以保護賬號密碼等敏感信息。

A. 可以、密文

B. 不可以、密文

C. 可以、明文

D. 不可以、明文

32. 雙簽名機制的目的是為了連接兩個發送給不用接收者的報文，在 SET 的支付處理過程中使用了雙簽名機制，下面觀點錯誤的是（）。

A. 商家和持卡人須分開加密和簽名，以保護用戶隱私不被泄露。

B. PIMD 和 OIMD 拼接後再次進行消息認證（計算 Hash 碼），得到的 POMD 就是雙簽名。

C. 在雙簽名機制中，商家既可以看到客戶的訂單信息，也可以看到客戶的銀行賬戶信息。

D. 在雙簽名機制中，銀行只能看到客戶訂單需要支付的總費用，並判定客戶賬戶是否可以支付。

二、計算題

- 下面所有題目均要求列出必要的計算步驟，只有最終結果不得分。

1. 【古典密碼計算題】

首先，使用 Hill 密碼加密，密鑰為 $K=\begin{bmatrix}1 & 7\\ 0 & 3\end{bmatrix}$，試對明文「BEST」加密，得到密文 ①。

之後，對密文 ① 使用 Caesar 密碼加密，c=(m+5) mod 26，得到密文 ②。

最後，將密文 ① 和密文 ② 簡單串接在一起，作為 Playfair 密碼算法中的密鑰詞，字母矩陣是 5×5 的矩陣（I 和 J 使用同一位置）。請對明文「TSINGHUA」用此 Playfair 密碼加密，得到密文 ③。

請依次求出密文 ①、密文 ②、密文 ③。

2. 【近現代密碼計算題】

Alice 和 Bob 是一個安全工作組成員。某日上班伊始，Alice 計算自己的 RSA 密鑰（已知 p=3，q=11，e=7），公佈了自己的公鑰。Bob 也公佈了自己的公鑰。

之後，Alice 和 Bob 使用 Diffie-Hellman 密鑰交換算法（已知公用素數 q=11，a=2 是 q 的一個本原根，Alice 公佈的 YA=9，Bob 公佈的 YB=3）得到 S-DES 算法的會話密鑰 Ks。

【*2.1*】請計算出 Alice 的公鑰和私鑰，以及 Alice 和 Bob 所使用的會話密鑰。

這時，Alice 接到命令，要將二進制明文（0000 1001）安全送給 Bob。 Alice 首先用 RSA 算法進行數字簽名，之後用 S-DES 算法進行信息加密發送給 Bob。

【*2.2*】請計算出 Bob 收到的密文。