

105年公務人員特種考試外交領事人員及外交行政人員、
民航人員、國際經濟商務人員及原住民族考試試題

代號：20250

全一張
(正面)

考試別：外交人員特考

等別：四等考試

類科組：外交行政人員資訊組

科目：資訊安全與網路管理概要

考試時間：1小時30分

座號：_____

※注意：禁止使用電子計算器。

甲、申論題部分：(50分)

(一)不必抄題，作答時請將試題題號及答案依照順序寫在申論試卷上，於本試題上作答者，不予計分。

(二)請以黑色鋼筆或原子筆在申論試卷上作答。

一、請說明下列名詞的意涵：(每小題5分，共20分)

(一)魚叉式釣魚攻擊 (Spear phishing attack)

(二)內容傳遞網路 (Content Delivery Network, CDN)

(三)服務層級協議 (Service Level Agreement, SLA)

(四)公眾交換資料網路 (Public Switched Data Network, PSDN)

二、防火牆 (Firewall) 是一般組織最常見的安全防護工具，而現代防火牆多採用 Stateful Packet Inspection (SPI) 技術，請詳細回答下列問題：

(一)何謂 SPI？為何要使用此技術？(10分)

(二)Packet-filtering Firewall 和 Web Application Firewall (WAF) 有何不同？(10分)

三、無線區域網路 (Wireless LAN) 已是目前非常普遍的網路技術，請問：

(一)為何無線區域網路在實體層要使用展頻 (Spread spectrum) 技術？(5分)

(二)Evil Twins Access Point 攻擊會對 WLAN 造成何種安全危害？請說明之。(5分)

乙、測驗題部分：(50分)

代號：5202

(一)本測驗試題為單一選擇題，請選出一個正確或最適當的答案，複選作答者，該題不予計分。

(二)共25題，每題2分，須用2B鉛筆在試卡上依題號清楚劃記，於本試題或申論試卷上作答者，不予計分。

1 ECDSA (Elliptic Curve Digital Signature Algorithm) 技術無法提供的安全功能為何？

(A)鑑別性 (authentication)

(B)機密性 (confidentiality)

(C)完整性 (integrity)

(D)不可否認性 (non-repudiation)

2 有關 spam 之敘述何者錯誤？

(A)不請自來的大量廣告行銷電子郵件為 spam 之一種

(B)公務用的個人電子郵件信箱僅用於公務，私人網購或是訂閱免費電子報使用免費電子郵件服務如 gmail 之措施可以有效降低公務用的個人電子郵件信箱收到 spam

(C)使用過濾識別黑名單機制無法改善 spam 的干擾

(D)永遠不要回覆 spam，有機會降低 spam 的量

3 下列技術何者最適合通訊雙方用來建立會議密鑰 (session key)？

(A)AES

(B)DES

(C)DSA

(D)RSA

4 下列區塊加解密模式何者在兼顧安全之前提下，有最適合網路高速傳輸之條件？

(A)CTR mode

(B)CFB mode

(C)CBC mode

(D)ECB mode

5 保護資料私密性目前大部分都不採取單一 DES 的最主要原因為何？

(A)核心功能已被破解而不安全

(B)受專利保護應用成本相對偏高

(C)核心技術不夠公開透明有疑慮

(D)密鑰長度太短容易受暴力攻擊

6 Diffie-Hellman Key Exchange 技術潛存何種攻擊之威脅？

(A)DDOS attack

(B)Phishing attack

(C)Man-in-the-middle attack

(D)Meet-in-the-middle attack

(請接背面)

考試別：外交人員特考

等別：四等考試

類科組：外交行政人員資訊組

科目：資訊安全與網路管理概要

- 7 數位憑證之應用與下列資訊安全技術之關聯性何者最直接？
(A)AES (B)Triple DES (C)RC6 (D)RSA
- 8 數位憑證的最主要功能為何？
(A)提供公鑰與驗證其正確之資訊 (B)儲存並提供私鑰之資訊
(C)證明數位簽章的正確性 (D)保護資料的隱私性
- 9 有一數位影像傳送前須經下列三處理程序以確保資訊安全與傳輸效率，處理程序在傳送端之先後順序，何者最理想？
①壓縮 ②加密 ③數位簽章
(A)③①② (B)②①③ (C)③②① (D)②③①
- 10 下列技術，何者包含鑑別鏈結伺服器身分之功能？
(A)RC6 (B)SHA512 (C)TLS (D)DES
- 11 攻擊者寄出假冒官方來源之電子郵件，使收信者誤認信件來源正常，並進而回應個人隱私資料或連結信件提供的超連結網站之攻擊方式與下列攻擊模式何者最接近？
(A)XSS attack (B)DDoS attack (C)Phishing attack (D)Trojans attack
- 12 下列何種技術可用在電子商務系統的交易中，作為確認交易存在及後續有交易糾紛時釐清權責之根據？
(A)AES (B)DES (C)DSA (D)SHA512
- 13 UDP 封包表頭的檢查碼 (Checksum) 如果設定為 0，下列敘述何者正確？
(A)檢查碼是 0 (B)檢查碼功能不使用 (C)封包有錯 (D)封包太大
- 14 關於網頁代理伺服器 (HTTP Proxy) 的運作，下列敘述何者錯誤？
(A)使用 TCP 協定 (B)可提供快取 (Cache) 功能，加速瀏覽網頁效能
(C)可提供資料加密功能，提昇瀏覽網頁安全 (D)可解析網址 (DNS name resolution)，便利瀏覽網頁
- 15 IPv4 封包 (IP datagram) 最多可被路由器 (Router) 轉送 (Forward) 幾次？
(A)15 (B)31 (C)127 (D)254
- 16 如果電腦開機後，網路介面的 IP 是 169.254.0.181，是下列何者網路協定出問題？
(A)DNS (B)DHCP (C)SMTP (D)SNMP
- 17 如果將一台家裏個人使用的電腦的 IP 設定為 74.200.13.235，子網路遮罩 (netmask) 設定為 255.0.0.0，則當此電腦要連線至 www.google.com (IP：74.125.23.106) 時，會出現下列何者結果？
(A)正常連線，可以看見網頁 (B)正常連線，連線速度很慢
(C)無法正常連線，憑證錯誤 (D)無法連線
- 18 如果一台電腦要使用 RIP 路由協定與相鄰網路設備交換路由表，有關這台電腦的防火牆設定，下列敘述何者正確？
(A)允許 UDP Port 520 (B)允許 TCP Port 520 (C)允許 IP 224.0.0.5 (D)允許 TCP Port 179
- 19 關於 HTTP (Hyper Text Transfer Protocol) 網路協定的運作，下列敘述何者正確？
(A)封包有加密功能 (B)基本認證 (Basic Authentication) 有加密功能
(C)是無狀態協定 (Stateless) (D)預設通訊埠 (Port) 是 8080
- 20 關於網頁第三方 Cookies (Third-Party Cookies) 的敘述，下列何者正確？
(A)可以增加網頁瀏覽的速度 (B)可以提昇網頁瀏覽的安全
(C)會洩漏網頁瀏覽的隱私 (D)會無法瀏覽 HTTPS 的網站
- 21 關於 SSH (Secure Shell) 網路協定的運作，下列何者錯誤？
(A)封包有加密功能 (B)有主機驗證 (host-based authentication) 功能
(C)有金鑰的安全驗證 (public key-based authentication) 功能
(D)有憑證的安全驗證 (X.509 certificate-based authentication) 功能
- 22 電腦網路探測工具 traceroute 是利用下列何者網路協定的功能來探測封包路徑？
(A)ICMP Echo Reply (B)ICMP Echo Request (C)ICMP Time Exceeded (D)ICMP Redirection
- 23 一個 IPv4 的封包在轉送途中如果被分段 (Fragmentation)，會在那裏被還原組合 (Reassembly)？
(A)下個路由器 (Router) (B)目的主機 (Host) (C)目的交換器 (Switch) (D)不用還原組合
- 24 一台手機的 IP 位址是 10.67.99.18，可以正常連線至 Internet，主要是靠下列何者網路協定？
(A)NAT (B)ICMP (C)SNMP (D)IGMP
- 25 下列何者網路攻擊不是中間人攻擊 (Man-In-The-Middle Attack)？
(A)ARP poisoning (B)ICMP redirect (C)DNS spoofing (D)IP address spoofing

測驗式試題標準答案

考試名稱：105年公務人員特種考試外交領事人員及外交行政人員、民航人員、國際經濟商務人員及原住民族考試

類科名稱：外交行政人員資訊組

科目名稱：資訊安全與網路管理概要（試題代號：5202）

單選題數：25題 單選每題配分：2.00分

複選題數： 複選每題配分：

標準答案：

題號	第1題	第2題	第3題	第4題	第5題	第6題	第7題	第8題	第9題	第10題
答案	B	C	D	A	D	C	D	A	A	C

題號	第11題	第12題	第13題	第14題	第15題	第16題	第17題	第18題	第19題	第20題
答案	C	C	B	C	D	B	D	A	C	C

題號	第21題	第22題	第23題	第24題	第25題	第26題	第27題	第28題	第29題	第30題
答案	D	C	B	A	D					

題號	第31題	第32題	第33題	第34題	第35題	第36題	第37題	第38題	第39題	第40題
答案										

題號	第41題	第42題	第43題	第44題	第45題	第46題	第47題	第48題	第49題	第50題
答案										

題號	第51題	第52題	第53題	第54題	第55題	第56題	第57題	第58題	第59題	第60題
答案										

題號	第61題	第62題	第63題	第64題	第65題	第66題	第67題	第68題	第69題	第70題
答案										

題號	第71題	第72題	第73題	第74題	第75題	第76題	第77題	第78題	第79題	第80題
答案										

題號	第81題	第82題	第83題	第84題	第85題	第86題	第87題	第88題	第89題	第90題
答案										

題號	第91題	第92題	第93題	第94題	第95題	第96題	第97題	第98題	第99題	第100題
答案										

備註：