

108 年特種考試地方政府公務人員考試試題

等 別：三等考試
類 科：資訊處理
科 目：資通網路

一、在交換式的區域網路 (Switched Local Area Network) 上，VLAN 是常見的網路架構，請說明：
(每小題5分，共20分)

- (一) 什麼是 VLAN？
- (二) 建置 VLAN 之目的？
- (三) 同一 VLAN 如何跨兩個或多個交換器？
- (四) 不同 VLAN 上之使用者如何互送資料？

【解題關鍵】

《考題難易》：★★

《破題關鍵》：VLAN 原理與實作，可參考講義 P591-592 與 97 警察二等考古題解出。

【擬答】：

- (一) 這是一種建構於區域網路交換技術的網路管理技術，網管人員可以藉此透過控制交換機有效分派出入區域網路的封包到正確的出入埠，達到對不同實體區域網中的設備進行邏輯分群 (Grouping) 管理，並降低區域網內大量資料流通時，因無用封包過多導致壅塞的問題，以及提昇區域網的資訊安全保障。
- (二) VLAN 發展目的
 - 1. 支援虛擬組織需求
 - 2. 簡化網路管理
 - 3. 提昇網路資源效率
 - 4. 加強網路安全
- (三) 同一 VLAN 下不同交換機的機器可以藉由 trunk (中繼技術) 即可實現互通，在完成組態設定 (Configuration) 後需要將虛擬區域網路成員的資訊傳播到所有的橋接器或路由器，使每一個橋接器或路由器都能辨識訊框屬於哪一個虛擬區域網路，交換機就會根據這些資訊訂出輸入、轉送、輸出規則。進行轉送訊框時，交換機接著就可以根據這些規則傳送。
- (四) 不同 VLAN 間互送資料則需要藉助 L3 switch 的路由技術達成。

二、以下為無線網路與通訊中常見之術語，請列出它們之英文全名，並試述其用意。(每小題4分，共20分)

- (一) QPSK
- (二) 3GPP
- (三) MANET
- (四) FHSS
- (五) MIMO

【解題關鍵】

《考題難易》：★★

《破題關鍵》：解釋名詞，參考講義後附名詞解釋解答。

【擬答】：

- (一) 四位元相位偏移調變 (Quadrature Phase-Shift Keying)，PSK 是一種利用相位差異的訊號來傳送資料的調變方式。該傳送訊號必須為正交訊號，其基底更須為單位化訊號。QPSK 在坐標圖上看是圓上四個對稱的點。通過四個相位，QPSK 可以編碼 2 位元符號。
- (二) 第三代合作夥伴計劃 (3rd Generation Partnership Project，即 3GPP) 是一個成立於 1998 年 12 月的標準化機構。3GPP 的目標是在國際電信聯盟的 IMT-2000 計劃範圍內製訂和實現全

公職王歷屆試題 (108 地方特考)

球性的（第三代）行動電話系統規範。它致力於 GSM 到 UMTS（W-CDMA）的演化，雖然 GSM 到 W-CDMA 空中介面差別很大，但是其核心網採用了 GPRS 的框架，因此仍然保持一定的延續性。

(三)隨建即連網路（mobile ad hoc network，縮寫為 MANET，mobile mesh network），又譯為行動隨意網路、移動臨時網路，它是一種以行動裝置，通過無線連結，自我組態所形成的網路，屬於無線隨意網路的一種。在 MANET 之中的每個行動裝置都可以自由移動，隨時改變無線連結。每個行動裝置節點都必須協助轉發網路封包，即使這個封包是跟這個裝置無關的。因此，每個節點都扮演了路由器的角色。

(四)跳頻展頻（Frequency-hopping spread spectrum, FHSS）是展頻技術的一種；經由載波快速在不同頻率中切換，並在接收與發射端使用一種偽隨機的過程。

(五)多輸入多輸出系統（Multi-input Multi-output；MIMO）是一種用來描述多天線無線通訊系統的抽象數學模型，能利用發射端的多個天線各自獨立發送訊號，同時在接收端用多個天線接收並恢復原資訊。

三、(一)何謂HTTP串流（Streaming）？（5分）

(二) HTTP 串流有那些優點？（5分）

(三)試說明 HTTP 串流之運作方式。（10分）

【解題關鍵】

《考題難易》：★★★★

《破題關鍵》：串流技術概念題，參考講義 P587 與 100 資訊技師類似題作答。

【擬答】：

HTTP串流就是利用HTTP/TCP傳輸串流媒體。

(一)優點如下：

1. 利用 HTTP 協定可以讓串流媒體得以穿過防火牆的阻隔
2. 將串流媒體放在 WWW 上可以讓使用者方便的取得這些內容
3. 只要使用一般的網頁伺服器，並不需要再另外建置專屬的串流伺服器。

(二)在使用 HTTP streaming 前，多媒體資料必須先包裝成符合網頁伺服器的特定格式，像 RealPlayer 所使用的 Real Media Format(.rm)格式或 Window Media Player 所使用的 Advanced Streaming Format(.asf)格式。接著並不需要再另外建置專屬的串流伺服器，只要將這些檔案先放置於網頁，接著就像一般的網頁一樣，經過網際網路分段傳送資料，在網路上即時傳輸影音，並不將多媒體資料實際拷貝一份存放在本機端，而是利用客戶端緩衝記憶體(Buffer)的概念，將資料不經實體儲存而直接由緩衝記憶體讀取播放後丟棄，可節省本機端磁碟儲存空間，因此應用於線上教學、視訊會議、線上廣告、隨選視訊(VoD)、即時線上轉播、網路電視以及網路電台(NetRadio)等各種網路多媒體應用。

四、區塊加密（Block Cipher）是一類常用的對稱加密方式，但它在處理長串之訊息時有些缺點，因此加密區塊連結（Cipher Block Chaining）技術被用來改善區塊加密。

(一)請說明區塊加密之缺點。（8分）

(二)加密區塊連結技術如何運作以改善區塊加密之缺點？（12分）

【解題關鍵】

《考題難易》：★★★★

《破題關鍵》：區塊加密與加密區塊連結技術概念題，107 調查局特考電腦網路相似題。

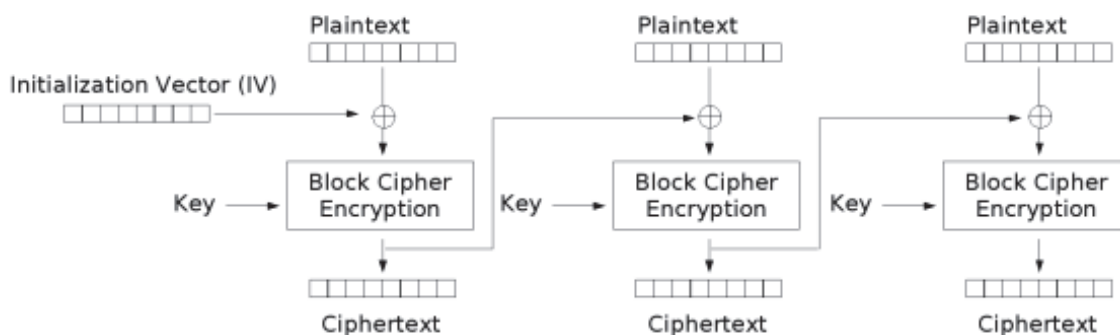
【擬答】：

block ciphers 只用同一份key，把加密文件一次用一個block文字進行加密，利用換位（位置交換）、替換（文字替換）…等方式，讓相似內容的明文，可以產出差異極大的密文（訊息獨立）。

(一)區塊加密之缺點

公職王歷屆試題 (108 地方特考)

1. 包含同樣資訊的區塊會被加密成同樣的密文，使得 Diffusion 不足（無法保障密文與明文間的複雜）。
 2. 容易被**重放攻擊**，即因為每一個區塊都有獨立的訊息，即使攻擊者不知道加密方式與金鑰，只要攻擊者知道區塊的功能後也只需要重複傳遞該區塊，接收端便會誤認接收了多次相同的訊息，比方說其中一個區塊是匯款給他人，那麼攻擊者可以透過不斷傳遞該區塊的方式把使用者的餘額給提領光。
- (二) 在 CBC 模式中，每區塊的明文會先跟前一個密文區塊進行 XOR 運算後再加密同時，為了保證每條訊息的唯一性，在第一個區塊中需要使用初始向量 (IV)。因為此時每個區塊的加密都會使用到前面所有區塊的參數，因此只要中間其中一個區塊被更改過，那麼便會輕易地被發現。



Cipher Block Chaining (CBC) mode encryption

五、網頁瀏覽已經是現代生活之一部分，而瀏覽器大多必須透過網域名稱系統 (Domain Name System; DNS) 來運作，請問：

- (一) DNS 的任務是什麼？(5 分)
- (二) 針對一個使用者請求，DNS 如何運作？(6 分)
- (三) DNS 伺服器分成三大類，試說明之。(9 分)

【解題關鍵】

《考題難易》：★★

《破題關鍵》：DNS 概念題，參考講義 P579-580 作答。

【擬答】：

- (一) DNS 系統可在領域名稱與 IP 地址之間進行轉換。由於 IP 地址太難記憶，因此將之對應成一個類似地址的名稱，就是所謂的領域名稱，各領域名稱與 IP 地址的對應由各地的領域名稱伺服器 (Domain name server) 負責維護，由各領域自行控制其下的領域的命名。
- (二) 主機向本地域名伺服器的查詢一般都是採用遞歸查詢。如果主機所詢問的本地域名伺服器不知道被查詢域名的 IP 地址，那麼本地域名伺服器就以 DNS 客戶的身份，向其他根伺服器繼續發出查詢請求報文。本地域名伺服器向根伺服器的查詢通常是採用反覆運算查詢。當根伺服器收到本地域名伺服器的反覆運算查詢請求報文時，要麼給出所要查詢的 IP 地址，要麼告訴本地域名伺服器：“你下一步應當向哪一個域名伺服器進行查詢”。然後讓本地域名伺服器進行後續的查詢。
- (三) DNS 伺服器類型

1. 根伺服器

根伺服器是最重要的域名伺服器。所有的根伺服器都知道所有的頂級域名伺服器的域名和 IP 地址。不管是哪一個本地域名伺服器，若要對網際網路上任何一個域名進行解析，只要自己無法解析，就首先求助於根伺服器。在網際網路上共有 13 個不同 IP 位址的根伺服器，它們的名字是用一個英文字母命名，從 a 一直到 m（前 13 個字母）。根伺服器並不直接把域名直接轉換成 IP 地址。在使用反覆運算查詢時，根伺服器把下一步應當找的頂級域名伺服器的 IP 地址告訴本地域名伺服器。

2. 頂層網域名伺服器

這些域名伺服器負責管理在該頂級域名伺服器註冊的所有二級域名。當收到 DNS 查詢請求時，就給出相應的回答（可能是最後的結果，也可能是下一步應當找的域名伺服器的 IP 地址）

3. 權威域名伺服器(Authoritative name server)

負責一個區的域名伺服器。當一個權威域名伺服器還不能給出最後的查詢回答時，就會告訴發出查詢請求的 DNS 客戶，下一步應當找哪一個權威域名伺服器。

4. 本地域名伺服器

本地域名伺服器對網域名稱系統非常重要。當一個主機發出 DNS 查詢請求時，這個查詢請求報文就發送給本地域名伺服器。每一個網際網路服務提供者 ISP 都可以擁有一個本地域名伺服器，這種域名伺服器有時也稱為默認域名伺服器。

公
職
王