科目：計算機應用　學習單　範圍：單元八　電子商務

班級：＿＿＿＿＿　座號：＿＿　姓名：＿＿＿＿＿＿

1.電子商務(Electronic Commerce, EC)：(P.248)

利用網路進行交易活動和相關服務活動，例如：產品廣告行銷、網路購物...等。

2.電子商務的特性：(P.248)

(1)全年無休、(2)全球化市場、(3)線上即時回應、(4)經營成本降低、

(5)資訊密集且公開、(6)多樣化的多媒體內容。

3.電子商務的基本類型：(P.248)

(1) 企業對消費者 B2C，Business to Consumer

(2) 消費者對消費者 C2C，Consumer to Consumer

(3) 消費者對企業 C2B，Consumer to Business

(4) 企業對企業 B2B，Business to Business

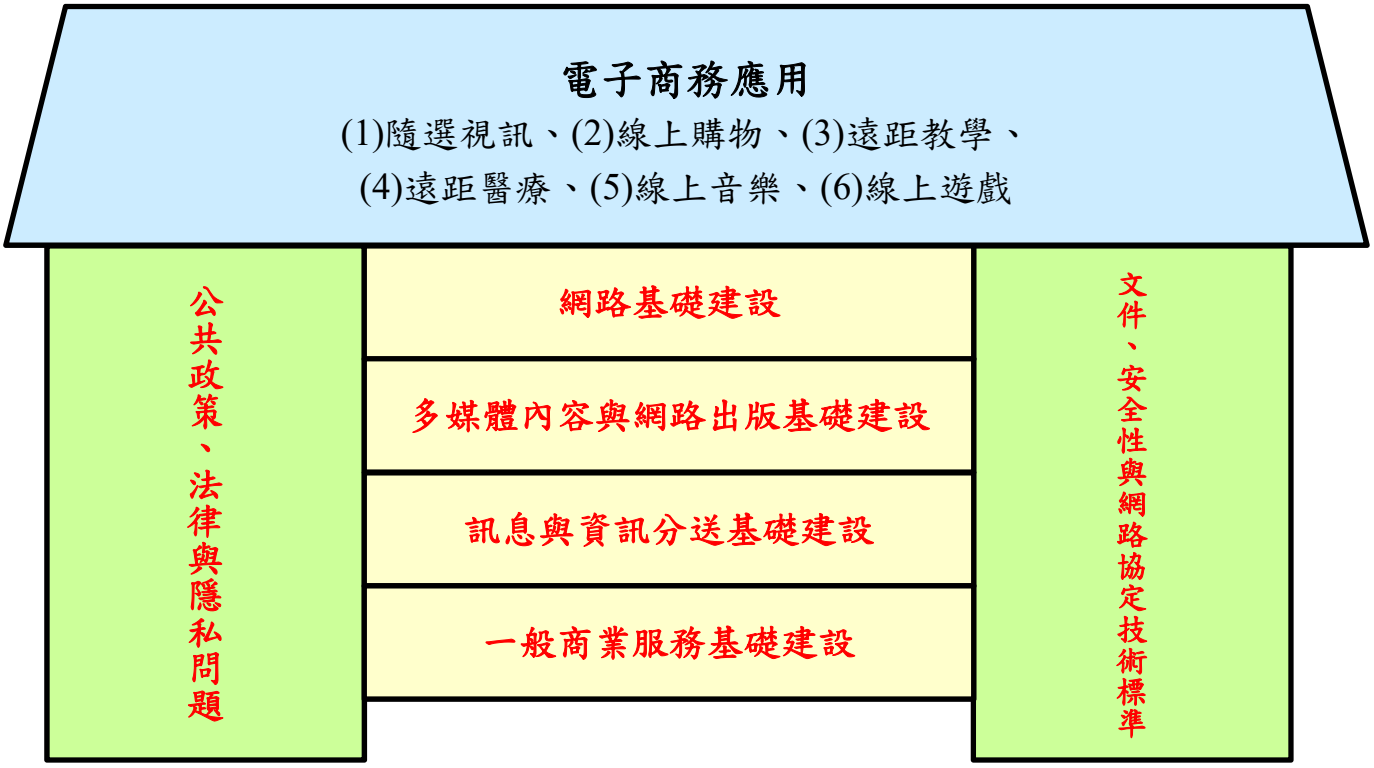
(5) 政府對人民 G2C，Government to Citizen

(6) 政府對企業 G2B，Government to Business

(7) 政府對政府 G2G，Government to Government

(8) 企業對政府 B2G，Business to Government

4.電子商務的架構：(P.253)　根據 Frontiers of Electronic Commerce (Kalakota & Whinston, 1996) 書中的定義，架構內容如下圖。



5.電子商務的四流：(P.255)

(1) 金流(Money Flow) ：指買賣雙方之間的資金轉移及支付方式，常見的方式有信用卡付費、ATM轉帳、郵政劃撥、便利商店付款、貨到付款、電子錢包。

(2) 物流(Logistic Flow) ：指商品從生產者到消費者的流通過程，常見的物流業務有郵局、貨運公司、快遞、宅配、便利商店取貨。

(3) 資訊流(Information Flow) ：是指透過網路技術來傳遞廠商與消費者之間的各種溝通資訊，例如：採購訊息、商品訂購及會員註冊等相關資訊。

(4) 商流(Busicess Flow) ：是商品所有權轉移的方式或過程，為無形的權利移轉。

6.電子商務的經營類型：(P.258)

(1)入口網站、(2)線上內容提供者、(3)線上零售商、(4)線上仲介商、

(5)線上市場創造者、(6)線上社群提供者。

7.加密技術原理：(P.260)

(1)明文：加密之前的原始資料，未經過任何處理的資訊。

(2)金鑰(Key)：進行加密及解密所需的資料，是一組數字或符號字串所組成的，金鑰的長度愈長，代表用此金鑰加密的資料愈難被破解。

(3)加密演算法：用來對明文資料進行加密編碼動作的演算法，必須配合金鑰一起使用。

(4)密文：明文經加密處理後的結果，內容如同一堆亂碼所組成，若不了解資料解密的方法就無法解讀其中的內容。

(5)解密演算法：利用金鑰對密文資料進行解密動作的演算法，能將密文資料還原成明文。

(6)對稱加密：不論是加密或解密的過程，都是使用同一把金鑰來處理。

(7)非對稱加密：又稱公開金鑰加密法(Public Key Encryption)，金鑰生成時會產生公開金鑰(Public Key)放於網路上供人使用，私密金鑰(Private Key)由使用者自行保管。例如傳送者會將資料以「接收者的公鑰」進行加密，接著在接收者收到資料後，使用「接收者的私鑰」進行解密。

8.數位簽章原理：(P.261) 用來確認發送者身分及內容，可用來驗證數位資訊來源。

9.加密技術的應用：(P.261)

(1)**數位簽章**：為電子簽章的一種，用來確認發送者身分及內容，可用來驗證數位資訊來源。

(2)安全通道層/傳輸層保全（**SSL/TLS**）：提供用戶端(Client)與伺服器端(Server)間在資料傳送時的加密與解密，避免重要資訊被竊取或竄改。使用 SSL/TLS 機制的網頁會在網址列呈現「**https**」開頭的網址，並在視窗上出現「**鎖**」的圖案作為提示。

(3)**安全電子交易標準（SET）**：由 **MasterCard** 和 **Visa** 等公司共同制定的電子交易標準，為了解決消費者、商家與銀行間，**線上信用卡交易**問題。

(4)**虛擬私有網路（VPN）**：利用加密技術將資料加密，並在網際網路中的虛擬通道(Tunnel)傳送，經過通道的資料都必須進行驗證，檢查資料是否遭到修改。

10.電子交易的安全事項：(P.262)

(1)**隱私性**：Privacy，保護個人隱私資料不會外流出去的機制，即使有心人士竊取資料，也無法解讀其中的內容。

(2)**認證性**：Authentication，需透過驗證機制確認交易雙方身分，當身分確認無誤時才能進行交易。

(3)**完整性**： Integrity，檢查資料送出和收到的內容是否一致，確保交易資料在傳輸過程中沒有遭到竄改。

(4)**不可否認性**：Non-repudiation)，使用機制驗證雙方是否有收到或發出訊息，避免交易雙方否認已送出或已接收到的資料。

(5)**存取控制**：Access Control，規範使用者存取網路資源的權利與限制，避免資料被不符合權限的人士竊取或濫用。

11.不同安全機制所符合的安全事項：(P.263)

安全機制 / 安全事項	防火牆	入侵偵測系統	數位簽章	SSL/TLS	SET	VPN
隱私性				✓	✓	✓
認證性	✓		✓	✓	✓	✓
完整性			✓	✓	✓	✓
不可否認性			✓		✓	✓
存取控制	✓	✓				✓