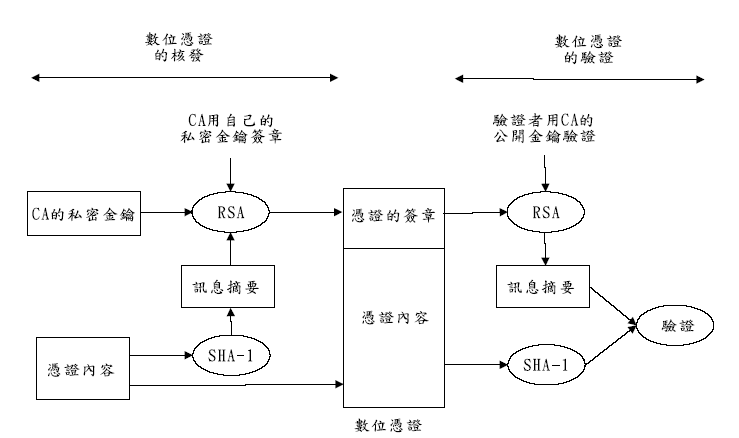
1. 請說明註銷的目錄(Certificate Revocation List，CRL)的功能，及其實際運作的困難點為何。
2. 下圖為數位憑證的核發與驗證過程，用文字說明CA(Certificate Authority)如何產生數位憑證。
3. 下圖為PGP協定的郵件傳遞流程，圖中說明使用者A對信件內容加密並簽章後傳送與使用者B，請用文字詳細描述此流程。



1. 在電子商務安全該章節中，我們介紹了不同的折價券分類方法。其中有種分類法將折價券分為商店折價券與製造商折價券。請以日常生活經驗舉例說明。
2. 電子商務安全該章節介紹了SET，請說明SET中的雙重簽章的運作方式，並說明SET的優缺點為何。
3. 請詳細說明盲簽章的運作方式。
4. IPSec主要包含兩種協定，(1)確認性標頭協定(Authentication Header, AH)與(2)安全資料封裝協定(Encapsulating Security Payload, ESP)。請說明為何僅有AH有提供「確保來源認證性」。
5. 請說明單向雜湊函數的三種特性。
6. 文件訊息鑑別碼(Message Authentication Code，MAC)可用來驗證文件訊息是否為約定好通訊的雙方所傳送，並可驗證文件訊息在傳遞過程中是否遭到篡改。請舉例如何利用單向雜湊函數H(.)與雙方事先共享的秘密金鑰K對訊息M計算並產生其對應的MAC。
7. 混合式加密同時採用對稱式密碼機制及公開金鑰密碼機制的加密系統，截長補短，使得它可以同時擁有這兩種密碼機制的優點。請舉例說明數位信封的運作方式。
8. 請說明何謂「(*t*,*n*)門檻機密分享技術」，只需說明精神不需說明方法。
9. 請說明Diffie-Hellman的金鑰協議與交換機制。