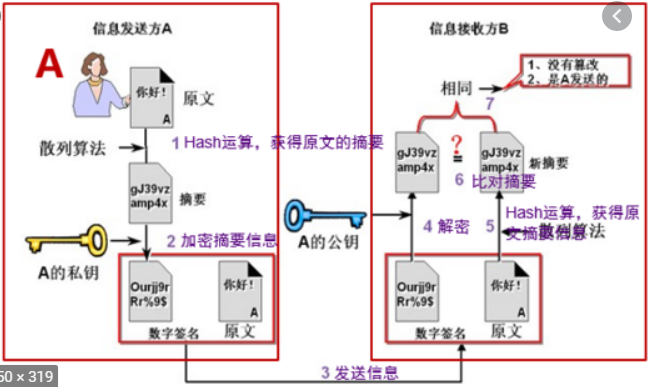
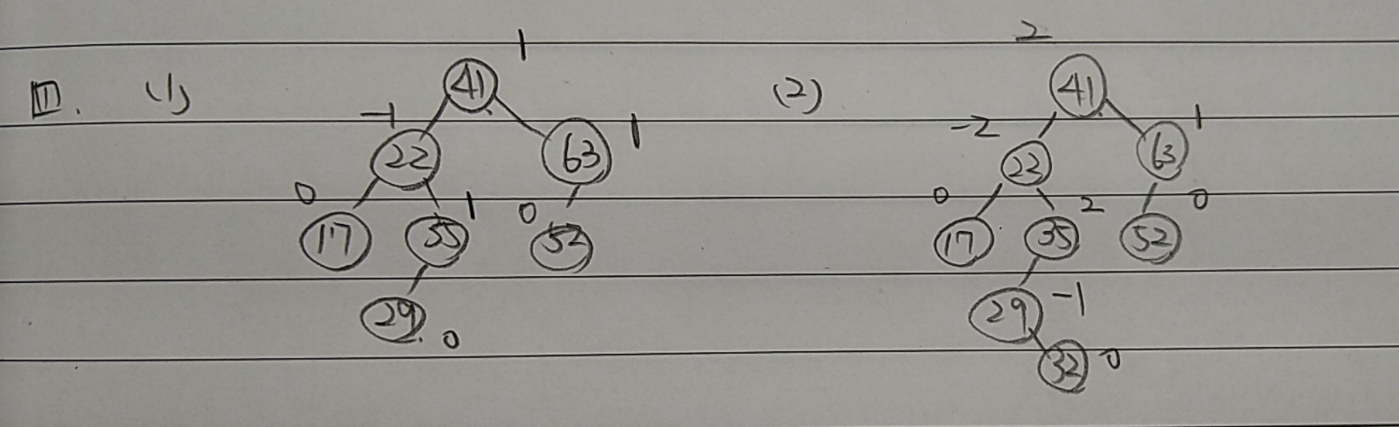
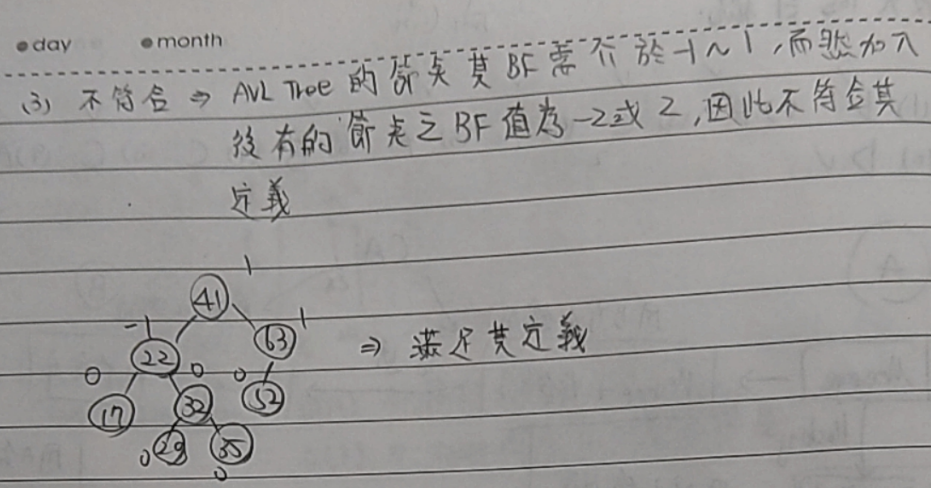
1. PKI
2. 
3. 身分驗證 : 藉由項第三方機構CA提出憑證申請，證明該公鑰擁有者的身分後，頒發使用憑證進行簽章加密
4. 交易不可否認性 : 訊息摘要使用送出方經由的私鑰進行簽章，再用送出方的CA認證公鑰加密送出內容與簽章，非送出方無法解密
5. 資料完整性 : 運用hash演算法計算訊息摘要後與原有內容一起送給收方，收方再用相同的hash方法計算收到的訊息，比較與收到的訊息摘要是否相同，hash演算法的特性只要有內容遭到更改就會產生不同的值，因此可以確保資料完整性
6. 隱密性 : 藉由RSA等非對稱式加密法，非收方無法解密其內容
7. C語言 - buffer overflow
8. buffer overflow
9. 指標對程式設計缺陷，向程式輸入緩衝區寫入使之溢位的內容（通常是超過緩衝區能儲存的最大資料量的資料），從而破壞程式執行、趁著中斷之際並取得程式乃至系統的控制權
10. 加上輸入值與緩衝區長度檢查機制
11. AVL Tree





1. 網路IP配置

