1. Explain the following terms (15 points)
   (a) Man-in-the-middle attack
   (b) Meet-in-the-middle attack
   (c) Reflection Attack

2. Justify the following statement (5 points)
   “Even while adding redundancy to encrypted data facilitates brute force attacks, such redundancies are desirable...”

3. What is the purpose of the “Authenticator” in Kerberos? (3 points)
4. Explain the need for a hierarchical PKI infrastructure. Why is it more desirable than a “flat” KPI? Are there any disadvantages in using a hierarchical KPI? (7 points)

5. What are forward and reverse certificates? In the KPI hierarchy depicted below explain how an authenticated exchange between nodes A and B would take place (what forward / reverse certificates need to be exchanged and / or used for verification of each others public keys) (10 points)