1. Explain the following attacks:
   a) Reflection attack
   b) Man-in-the-middle attack
   c) Replay attack
   Briefly describe measures to overcome the 3 attacks

2. What are forward and reverse certificates? Why are they required?

3. Explain why revocation is a difficult problem in PKI, but is trivially accomplished in Kerberos.

4. Consider the scenario where the public key ring of Joe has an entry for a public key of A. The public key of A has been signed by B, C and D. Briefly describe the process employed by Joe for computing the legitimacy of A’s public key.

5. Consider a scenario where A wished to send an encrypted message to B (encrypted with the public key of B) and signed by A. In addition A and B desire to use some lossless compression (for example Lempel Ziv) scheme for saving bandwidth. Explain the desirable order of the three operations: encryption, signature and lossless compression.

6. State T/F
   a) Kerberos is susceptible to man-in-the-middle attacks
   b) In Kerberos all servers share a secret with the authentication server
   c) The purpose of the authenticator in Kerberos is to avoid replay attacks
   d) Kerberos requires time synchronization of all clients and servers
   e) Reverse certificates are used for revocation of X.509 certificates
   f) In Kerberos the ticket granting server shares a secret with the authentication server.
   g) During the process of registration every entity who wishes to obtain a certificate from the CA should provide a copy of their private keys to the CA.
   h) PGP requires an hierarchical certificate authority
   i) The Key ID of a PGP key is the last 64 bits of the private key.
   j) In the PGP private key ring of Joe, Joe’s RSA private key is stored encrypted using the corresponding public key.