1. Explain the following attacks:
   a) Reflection attack
      Tricking the challenger to respond to her own challenge by establishing a parallel session. Ways to avoid: 1) ensure that the initiator responds first 2) initiator / responder should choose challenges from different spaces (for example only even numbers for initiator and only odd numbers for responder)
   b) Man-in-the-middle attack
      Attacks that can be carried out by an attacker physically placed between the endpoints. When asymmetric primitives are used for mutual authentication the man in the middle can misrepresent public keys of the sender and the receiver. Should use public key certificates.
   c) Replay attack:
      Replaying an old packet. To overcome such attacks we need to use timestamps.

Briefly describe measures to overcome the 3 attacks

2. What are forward and reverse certificates? Why are they required?
   Forward certificates are certificates issued by parent to child. Or the parent signs the public key of the child. In reverse certificates the child signs the public key of the parent.
   All forward certificates starting from the root CA are required to verify the public key of an entity. Reverse certificates are used to convey the public key of the root CA to all entities (as entities trust only their immediate parents)

3. Explain why revocation is a difficult problem in PKI, but is trivially accomplished in Kerberos.
   The revocation certificates need to be physically delivered to every end entity in PKI. If A is not made aware of the fact that B has been revoked, A will entertain B's public key.
   In Kerberos the server is actively involved in every interaction (at least once a day). Revoked entities will not be issued tickets.

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
   A looks at the owner trust (OT) values for the records corresponding to B, C and D
   A copies the three OT value as signature trusts (ST) for their respective signatures of A's public key
   The three ST values are used together to compute the key legitimacy (KL) value for A's public key.

5. Consider a scenario where A sends an encrypted message to B (encrypted with the public key of B), 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.
   The desirable order is sign, compress and encrypt.
   Encryption has to be done after compression as we cannot compress encrypted data well. The question now is if we should sign the original data or the compressed and encrypted data. It is preferable to sign the original data due to two reasons. 1) the receiver does not need to store the session key (used for encryption) to demonstrate the validity of the data at a later time 2) the receiver does not have to specify which compression scheme was used by the sender.

6. State T/F
   a) Kerberos is susceptible to man-in-the-middle attacks: (F)
   b) In Kerberos all servers share a secret with the authentication server (F) – only clients and TGS shares a secret with the AS
   c) The purpose of the authenticator in Kerberos is to avoid replay attacks (T)
   d) Kerberos requires time synchronization of all clients and servers (T) – to use time stamps
   e) Reverse certificates are used for revocation of X.509 certificates (F)
   f) In Kerberos the ticket granting server shares a secret with the authentication server. (T)
   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. (F)
   h) PGP requires an hierarchical certificate authority (F) No CA needed
   i) The Key ID of a PGP key is the last 64 bits of the private key. (F) last 64 bits of the public key
   j) In the PGP private key ring of Joe, Joe's RSA private key is stored encrypted using the corresponding public key. (F) encrypted using Joe's password.