1. Briefly explain the following attacks: (6 points)
   - Reflection attack
   - Man-in-the-middle attack
   - Replay attack
   and suggest measures to overcome the attacks

Reflection Attack: In a challenge response protocol between a challenger C and a responder R the responder R tricks the challenger C into answering his own challenger by establishing a parallel channel and submitting the same challenge. This can be overcome if (for example) if challenger and responder are required to choose challenges from non overlapping sets (odd and even numbers)

Man-in-the-middle attack: Situated between two parties A and B the man in the middle can establishes a channel with A pretending to be B and establishes a channel with B pretending to be A. Both A and B are totally unaware of the presence of the man-in-the-middle. Man-in-the-middle can modify exchanges between A and B. This can be avoided by establishing a secure authenticated channel between A and B. If asymmetric cryptographic schemes are used, the certified public keys should be used.

Replay attack: Typically performed by replaying a packet at a later time. An encrypted packet can be replayed even by a listener who does not have access to the secret used for encrypting the packet. Can be avoided by time-stamping packets.

2. What are forward and reverse certificates? Why are they required? (4 points)

Forward certificates are issued by a CA at a higher level of hierarchy certifying the public key of a CA at a lower level of hierarchy.

Reverse certificates are issued by a CA at a lower level of hierarchy certifying the public key of a CA at a higher level of hierarchy.

Clients of the lower level CA may not even be aware of the existence of the higher level CA. Reverse certificates are thus essential to create certificate chains.

A--------B---------C

e f g        i j k

Assume that e,f, g have their public keys signed by CA A
Certificates represented as A<a>, A<b>, A<c> respectively.
Assume i,j,k have their public keys signed by C
Certificates represented as C<i>, C<j>, C<k> respectively.
A signs public key of B – certificate A<B>
B signs public key of A – certificate B<A>
B signs public key of C – certificate B<C>
C signs public key of B – certificate C<B>
To verify public key of j, f requires A<B> (reverse certificate), B<C>, C<j>
To verify public key of f, j requires C<B> (reverse certificate), B<A>, A<f>

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

Certificates are specified to be valid till some time t. Revoking a certificate is to render a certificate invalid before time t. An entity requiring his certificate to be invalidated contacts the CA and the CA should convey this information (that a certificate has been prematurely revoked) to all entities. In Kerberos (or any mechanism based on the Needham-Schroeder protocol) all communications are mediated by a trusted server. The trusted server can be easily informed to deny communications to/from revoked entities.
4. State T/F (7 points)
   1. Kerberos is susceptible to man-in-the-middle attacks (F)
   2. In Kerberos all servers share a secret with the authentication server (F - they share a secret with TGS)
   3. The purpose of the authenticator in Kerberos is to avoid replay attacks (T)
   4. Kerberos requires time synchronization of all clients and servers (T)
   5. Reverse certificates are used for revocation of X.509 certificates (F – nothing to do with revocation)
   6. In Kerberos the ticket granting server shares a secret with the authentication server (T)
   7. 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).