**Exercise 7**

**Student ID: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Student Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. What does Kerberos model include?

2. In Kerberos, a client sends an authenticator to the server for authentication. Who generates the authenticator?

3. In Kerberos, a client sends a ticket to the server for authentication. Who generates the ticket?

4. In Kerberos, which server keeps all client secret keys?

5. In Kerberos, which server keeps all server secret keys?

6. What is the man-in-the-middle attack?

7. What are the two main applications of public keys?

8. In PKI, there are three types of entities. What are them?

9. What is Certificate Authority?

10. What is Object identifier (OID) of RSA encryption algorithm?

11. Describe the simplified Kerberos protocol with a diagram.

12. In PKI, Alice has a public key certificate issued by a Certificate Authority CA1. Bob does not know CA1’s public key, but know a Certificate Authority CA2’s public key. How can Bob authenticate the public key certificate of Alice?