1. Introduction

- What is CIA Triad ? Explain.
- List any 5 challenges of computer security.
- What is OSI Security Architecture ? Explain
- What are Security Attacks ? Explain the various types of Passive attacks.
- List and explain Security Services as per the OSI Security Architecture.
- List and explain the Security Mechanisms as per the OSI Security Architecture.
- Explain a typical model for network security.

2. Key Management & Distribution

- List 4 different ways to share a key.
- Explain a simple key distribution scenario under the presence of a KDC.
- Explain a scenario where Symmetric Key is distributed using symmetric encryption.
- Explain a scenario where Symmetric Key is distributed using asymmetric encryption.
- Explain a MITM attack scenario
- Explain 4 different ways of distribution of public keys.
- Draw X.509 certificate's architecture.
- List and explain the elements of a PKIX Architectural Model.
- List and explain any 5 PKIX Management Functions.

3. User Authentication Protocols

- List the steps involved in authentication process.
- Four general means of authenticating a user's identity.
- List 4 different types of Replay Attacks.
- Explain the process of Mutual Authentication for authenticating a Remote user using symmetric encryption.
- What is a Kerberos Realm ?
- Explain the secure authentication dialogue in Kerberos v4.
- Summarize the message exchanges of Kerberos v4.
- Summarize the message exchanges of Kerberos v5.
- Explain the overview of Kerberos version 4 using appropriate diagram.
- Explain how a client request for service in another kerberos realm.
- List 6 environmental shortcomings in the Kerberos v4.
- List 4 technical deficiencies in the Kerberos v4.
- Explain the process of Mutual Authentication for authenticating a Remote user using Asymmetric Encryption.
- What is Identity Management ? List the 9 principal elements of an identity management system.
- Explain the Generic Identity Management Architecture.
- What is Identity Federation ? Illustrate the entities and data flows in a generic federated identity management architecture.