(3 Hours) **[Total Marks: 80]**

N.B.: (1) Question No. **1** is **compulsory.**
(2) Solve any **three** questions out of remaining **five.**
(3) Figures to **right** indicate **full** marks.
(4)Assume suitable **data** where **necessary.**

1. a) Explain Biometric authentication. [5]
   b) Explain Vulnerability, Threat and Attack. [5]
   c) What is Distributed Denial of Service Attack? [5]
   d) Describe TCP Syn Flood attack. [5]

2. a) Explain different types of Firewalls that can be used to secure a network. [10]
   b) Explain RSA algorithm for public key encryption. Given modulus N = 143 and public key = 7, find the values of p, q, phi(n), and pivate key d. Can we choose value of e = 5? Justify. [10]

3. a) What is Digital Signature? Explain how it is created by sender and verified by receiver. [10]

   b) What is session hijacking? Give two ways to prevent a session hijacking attack. [10]

4. a) What are the different approaches to Software Reverse Engineering? [10]
   b) Explain the need of Intrusion Detection System (IDS)? Differentiate between signature based and anomaly based IDS. [10]

5. a) What are the file system vulnerabilities for a Linux system? [10]
   b) What is SSO? Explain the working of Kerberos Authentication Protocol (KAP) [10]

6. Write short notes on: (Any Four)
   a) Honey Pots [5]
   b) Secure email [5]
   c) Federated Identity Management [5]
   d) CIA Security goals [5]
   e) Incomplete Mediation [5]