

(3 hours)

Marks:[80]

N.B

1. Question No. 1 is compulsory.
2. Attempt any 3 out of remaining 5.

- Q.1 a) Explain the different software flaws with example. **05**
 b) Define goals of security and mechanism to achieve them. **05**
 c) Define the properties and applications of Hash function. **05**
 d) Explain handshake protocol in SSL. **05**
- Q.2 a) How is security achieved in Transport and Tunnel modes of IPSEC? **10**
 Explain the role of AH and ESP.
- b) How does PGP achieve confidentiality and authentication in emails? **10**
- Q.3 a) Why are digital certificates and signatures required? What is role of digital signature in digital certificates? Explain any one digital signature algorithm. **10**
- b) What are the different components of Intrusion Detection System? Compare signature based IDS to anomaly based IDS. **10**
- Q.4 a) Discuss DES with reference to following points **10**
- Block size and key size
 - need of expansion permutation
 - role of S-box
 - weak keys and semi weak keys
 - possible attacks on DES
- b) Explain Diffie Hellman key exchange algorithm. What types of attacks are possible on it explain with example. **10**
- Q.5 a) Explain briefly the following attacks with example **10**
- | | |
|-----------------------|----------------------|
| (I) Session hijacking | (II) Salami Attack |
| (III) SQL injection | (IV) Buffer overflow |
- b) What is Denial of Service attack? What are the different ways in which an attacker can mount a DOS attack on a system? **10**
- Q.6 a) Explain the working of Kerberos. **10**
- b) Elaborate the steps of key generation using RSA algorithm. In RSA system the public key (E, N) of user A is defined as (7,187). Calculate $\Phi(N)$ and private key 'D'. What is the cipher text for M=10 using the public key. **10**