Duration: 3hrs **[Max Marks: 80]**

N.B. : (1) Question No 1 is Compulsory.
(2) Attempt any three questions out of the remaining five.
(3) All questions carry equal marks.
(4) Assume suitable data, if required and state it clearly.

1 Attempt any FOUR [20]
a Explain the relationship between Security Services and Mechanisms in detail.
b Explain ECB and CBC modes of block cipher.
c Define non-repudiation and authentication. Show with example how it can be achieved.
d Explain challenge response-based authentication tokens.
e Explain buffer overflow attack.

2 a Elaborate the steps of key generation using the RSA algorithm. In RSA system the public key (E, N) of user A is defined as (7,187). Calculate Φ(N) and private key 'D'. What is the cipher text for M=10 using the public key. [10]

b Discuss DES with reference to following points [10]
1. Block size and key size
2. Need of expansion permutation
3. Role of S-box
4. Weak keys and semi weak keys
5. Possible attacks on DES

3 a What goals are served using a message digest? Explain using MD5. [10]
b What is DDOS attack? Explain how is it launched. [10]

4 a Why are digital certificates and signatures required? What is the role of digital signature in digital certificates? Explain any one digital signature algorithm. [10]
b How does PGP achieve confidentiality and authentication in emails? [10]

5 a State the rules for finding Euler's phi function. Calculate [10]
a. φ(11)
b. φ(49)
c. φ(240)
b Explain Kerberos. Why is it called as SSO? [10]

6 a Enlist the various functions of the different protocols of SSL. Explain the phases of handshake protocol. [10]
b How is security achieved in Transport and Tunnel modes of IPSEC? Explain the role of AH and ESP. [10]