(3 Hours) **[Total Marks: 100]**

N. B.: (1) **All** questions are **compulsory**.
(2) Make **suitable assumptions** wherever necessary and **state the assumptions** made.
(3) Answers to the **same question** must be **written together**.
(4) Numbers to the **right** indicate **marks**.
(5) Draw **neat labeled diagrams** wherever **necessary**.
(6) Use of **Non-programmable** calculators is **allowed**.

1. **Attempt *any two* of the following:** **10**

a. Write a short note on Cryptanalysis.
b. Explain EIGamal signature scheme. What are their limitations?
c. Explain model for Network security.
d. What are benefits of IPSec?

2. **Attempt *any three* of the following:**

a. Explain Euclidean algorithm.
b. Explain Huffman Encodings with example.
c. Explain working of the Vigenere Cipher with an example.
d. What are various mode of operation in DES? Explain any one in detail.
e. Explain RSA Algorithm?
f. Describe AES with example.

3. **Attempt *any three* of the following:** **15**

a. What do you mean by Undeniable signature?
b. Explain working of time stamping with application.
c. Describe Hash function.
d. Write a short note on Blom's scheme.
e. Explain MTI key agreement protocol.
f. Explain in detail Diffie – Hellman key exchange algorithm.

4. **Attempt *any three* of the following:** **15**

a. Write as short note on security trends.
b. What is OSI security architecture?
c. Explain various categories of security services.
d. Explain Active attacks & Passive attacks.
e. What are categories of Security mechanism?
f. Define & Explain Computer security concept.

5. **Attempt *any three* of the following:** **15**

a What are the various web security protocols?
b Explain public key infrastructure. Also write its components?
c Explain x.509 authentication service?
d Write short note on Kerberos?
e What is S/MIME?
f What are principal services provided by PGP?

[Turn Over]

6. Attempt *any three* of the following: **15**

a. Explain various services provided by IPSec.
b. Explain ESP packet format.
c. What are the advantages of IP security?
d. Write difference between SSL connection and SSL session.
e. What is concept of Handshake protocol in secure socket layer?
f. Explain the objectives of Set protocol.

7. Attempt *any three* of the following: **15**

a. List and explain component of viruses.
b. Explain advantages of packet filters.
c. Explain the role of intruders.
d. What are limitations of Firewall? 5marks
e. What are circuit level gateways? Also write it's advantages.
f. How to protect computer against Virus.