(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. What four requirements were defined for Kerberos?
b. Describe transport mode and tunnel mode.
c. What is Application Level Gateway? Explain its working
d. Explain the header format of MIME messages.

2. Attempt *any three* of the following:

a. Define the following:
(i)Cryptography (ii)Symmetric encipherment (iii) Asymmetric Encipherment
b. Explain the working of DES.
c. Define Cryptosystem. Explain it with suitable diagram.
d. What is shift cipher? Explain with simple example
e. List some of the components of modern block cipher.
f. Explain p-1 factoring algorithm.

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

a. Explain “ElGamal signature scheme”
b. Write a note on Digital signature
c. Explain Fail-stop signatures in detail.
d. Explain Blom's scheme of key distribution.
e. Write a short note on station-to-station protocol.
f. Explain Diffie-Hellman Key exchange algorithm.

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

a. Define Computer Security. Explain the necessity of computer security.
b. What are the problems of computer security mechanism?
c. Describe CIA Triad of computer security.
d. List & explain the categories of security mechanism of x.800.
e. Explain the following terms:
i)Authentication ii)Access Control iii)Non-Repudiation
f. What are active attacks? Discuss various passive attacks.

[Turn Over]

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

a Explain the general format of PGP message.

b What are three threats associated with user authentication over a network?

c Write short note on Kerberos.

d What are the various Web security protocols?

e What are the operational services of PGP? Explain any one.

f In S/MIME, explain how Bob and Alice exchange the secret key for encrypting messages.

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

a. What are the groups of IP security document?

b. What services are provides by IPsec?

c. Describe anti-relay attack.

d. Compare transport mode with tunnel mode of IP.

e. Describe ESP packet format.

f. What are the advantages of IP security?

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

a. What is DMZ? Explain the importance of DMZ.

b. What is the context of UNIX password scheme?

c. How viruses are different from worms and Trojan horses?

d. What are the typical phases of operation of virus or worm?

e. What are advantages and disadvantages of Application Level Gateway? How is it different from circuit level gateway and packet filter firewall?

f. What is DOS? How DOS is different from DDOS?

____