(2 ½ Hours.) **[Total Marks: 75]**

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 labelled diagrams** wherever **necessary**.
(6) Use of **non-programmable** calculators is **allowed**.

1. Attempt any four of the following: **20**

a. What is CIA Triad? Explain in detail.
b. Define Security attacks. Explain with its types.
c. List and explain different categories of security services.
d. Write an overview of DES algorithm.
e. Explain ECB and CBC mode of operation of cipher.
f. Describe play-fair Ciphering technique in detail.

2. Attempt any four of the following: **20**

a. Discuss Diffie Hellman key exchange process.
b. Write a short note on Kerberos.
c. Differentiate between stream cipher and block cipher.
d. Describe RSA algorithm in detail.
e. Explain the format of X.509 certificate.
f. Explain public key infrastructure. Explain its key elements.

3. Attempt any four of the following: **20**

a. Discuss SSL handshaking protocol in detail.
b. Define malicious software. Explain different types of viruses.
c. What are Honeypots? State its significance.
d. Write a short note on firewalls.
e. Explain PGP with different services offered by it.
f. Define Intrusion. Explain different approaches of Intrusion detection.

4. Attempt any five of the following: **20**

a. Explain lifecycle of virus.
b. Describe Man in middle attack.
c. Explain IPSec Protocol in detail.
d. Write a short note on MAC.
e. Describe rail-fence Cipher with suitable example.
f. Briefly explain Digital Signature process.

XSAGARDADMINY381F40XSAGARDADMINY381F40