Before answering the question paper the candidate should ensure that they have been supplied the correct question paper. Complaints in this regard, if any, shall not be entertained after the examination.

Note: Question No. 1 is Compulsory and attempts any two questions from each section. All questions carry equal marks.

1. (a) Which of the modes of operation of block Ciphers are suitable for General-purpose stream oriented transmission and why? (5)
   (b) What is the purpose of S-boxes and P-boxes in DES? (5)
   (c) What is the difference between a message authentication code and a one-way hash function? (5)
   (d) What is a honey pot? Explain it. (5)

SECTION A

2. What is the difference between passive and active security threats? Explain these security threats. (20)

3. If \( p = 5, q = 11, e = 3, M = 9 \) perform encryption & decryption by using RSA approach. (20)

4. (a) what is feistel cipher? Why is it important to study? (10)
   (b) What is the difference between differential and linear cryptanalysis? (10)

SECTION B

5. (a) What services are provided by IPSec? Describe the various services in detail. (10)
   (b) What is a replay attack? Illustrate it with suitable example known to you. (10)

6. (a) List and briefly define three classes of intruders. What are the ways to detect them? (10)
   (b) What is a dual signature and what is its purpose? Explain in detail. (10)

7. What is a fire wall? What are various types of firewall? List and explain four techniques used by firewalls to control access and enforce a security policy.