A–0807

Total Pages : 3 **Roll No. ....**

MIT (CS)-204

CRYPTOGRAPHY AND NETWORK SECURITY

Examination, June 2025

Time : 2:00 Hrs. Max. Marks : 70

Note :– This paper is of Seventy (70) marks divided into Two (02) Sections ‘A’ and ‘B’. Attempt the questions contained in these sections according to the detailed instructions given therein. ***Candidates should limit their answers to the questions on the given answer sheet. No additional (B) answer sheet will be issued.***

Section–A

Long Answer Type Questions 2×19=38

Note :– Section ‘A’ contains Five (05) Long-answer type questions of Nineteen (19) marks each. Learners are required to answer any *two* (02) questions only.

1. Explain the various types of transposition ciphers. Provide examples to illustrate their working.

2. Solve the following :

   (a) Compute x using the Chinese Remainder Theorem for the following system of congruences:

   $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 2 \pmod{7}$.

   (b) Explain its application in cryptography

3. Explain the RSA Algorithm in detail. Solve RSA with P = 7, Q = 11, E = 17, and M = 8. Discuss its merit.

4. Explain the principles of stream ciphers and block ciphers. Provide their differences with examples.

5. What is Advanced Encryption Standard (AES) ? Discuss its key scheduling process and modes of operation.

Section–B

Short Answer Type Questions 4×8=32

***Note* :–** Section 'B' contains Eight (08) Short-answer type questions of Eight (08) marks each. Learners are required to answer any *four* (04) questions only.

1. What is a firewall ? Explain its components and types.

2. Explain Euler's Theorem with a suitable example

3. Describe the architecture of Secure Socket Layer (SSL) and how it ensures secure communication.

4. Describe the structure of HMAC and its applications.

5. Differentiate between public key and private key cryptosystem.

6. What is the Diffie-Hellman key exchange algorithm ? Explain its steps with an example.

7. What are the different types of access control in security models ? Explain briefly.

8. What is PGP (Pretty Good Privacy) ? Explain its working in email security.

****