A–1282

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

MIT (CS)-204

Cryptography and Network Security

Examination February, 2026

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 in detail the various classical cryptographic techniques. Discuss substitution and transposition ciphers with suitable examples.

2. What is Firewall ? What are the basic components of firewall ? Explain the types of firewall. Explain its application in cryptography

3. Describe the working of the RSA public key cryptosystem. Using P = 5, Q = 19, E = 11, encrypt the message M = 7 and show the decryption process. State the advantages of RSA.

4. Describe the Data Encryption Standard (DES). Explain its encryption process and round structure, including the major steps and key schedule. Also discuss the strengths and limitations of DES in network security.

5. Explain key management in public-key cryptography and describe the Diffie-Hellman key exchange protocol. Also discuss ECC-based Diffie-Hellman, symmetric-key agreement, and the man-in-the-middle attack.

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 Digital Signature ? Explain its purpose and the role of the Digital Signature Standard (DSS).
2. What is IP Security (IPSec) ? Explain its basic purpose and components in brief.
3. What is SSL/TLS ? Briefly explain how it provides secure communication over the web ?
4. What is a Message Authentication Code (MAC) ? Explain its purpose and how HMAC enhances message authentication.
5. Explain the Chinese Remainder Theorem and describe its use in solving modular arithmetic problems.
6. What is a Digital Certificate ? Briefly explain its purpose and key components.
7. What are the different types of access control in security models ? Explain briefly.
8. Explain Euler's Theorem and Fermat's Little Theorem with their basic statements.

****