K–984

MIT(CS)–204

MSCCS IInd Semester Examination Dec., 2023

CRYPTOGRAPHY & NETWORK SECURITY

Time : 2 Hours]   [**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 there in. ***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.

K–984   (1)   P.T.O.

1. What is Network Security ? Explain the Different Types of Security.

2. What is Cryptography ? What are the Network Security Applications ? Explain.

3. Explain key generation, encryption and decryption of the RSA algorithm.

4. Explain the various types of transposition cryptography.

5. What are the different modes of operation in DES ? Explain.

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. Differentiate passive attack from active attack with an example.

2. Discuss about the Chinese Remainder Theorem and algorithms.

3. What is the difference between public key and private key cryptosystem ?

4. What is Symmetric and Asymmetric cryptography ? Explain with an example.

K–984

5. Explain the principles of stream ciphers and block ciphers.

6. Explain RSA algorithm.

7. What is Firewall ? Explain the types of firewall in detail.

8. Explain the following terms :

(i) Data Integrity

(ii) Digital Signature

(iii) Security attacks

(iv) Plain text and Cipher feat

****

K–984 (3)