

A-820

Total Pages : 3

Roll No.

MIT (CS)-204

(MSCCS)

(Cryptography and Network Security)

2nd Semester Examination, 2024 (June)

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. What is Firewall ? What are the basic components of firewall ? Explain the types of firewall.
2. Explain the following components of encryption algorithm :
 - (i) Plain text
 - (ii) Network Security
 - (iii) Encryption Algorithm
 - (iv) Secret Key
 - (v) Decryption Algorithm
 - (vi) Cipher text
3. What is Secure Socket Layer (SSL) ? Describe the Secure Socket Layer (SSL) Architecture in detail.
4. Explain the various types of transposition cryptography in detail.
5. Explain the RSA algorithm and explain the RSA with $P = 7$, $q = 11$, $e = 17$, $M = 8$. Discuss its merit.

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 IP Security ? What are the Applications and Benefits of IPsec ?
2. Differentiate between monoalphabetic and Polyalphabetic cipher with example.
3. Describe Chinese Remainder Theorem and explain its application.
4. Differentiate between public key and private key cryptosystem.
5. What is Symmetric and Asymmetric cryptography ? Explain with an example.
6. Explain the principles of stream ciphers and block ciphers.
7. How does PGP provide confidentiality and authentication service for e-mail and file storage applications ?
8. Write and explain the digital signature algorithm.
