P-855

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

MIT(CS)-204

Cryptography and Network Security

M.SC. Cyber Security (MSCCS)

2nd Semester Examination, 2023 (June)

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 therein. Candidates should limit their answer to the questions on the given answer sheet. No additional (B) answer sheet will be issued.

SECTION–A
(Long Answer Type Questions)

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.

(2×19=38)

1. Explain classical encryption techniques with symmetric cipher and hill cipher model.

2. What do mean by AES? Diagrammatically illustrate the structure of AES and describe the steps in AES encryption process with example.

3. Explain IP security architecture. Show how ESP works in transport and tunnel mode.

4. (a) Discuss WLAN Topologies (i) Independent basic service sets (IBSSs) (ii) Basic service sets (BSSs) (iii) Extended service sets (ESSs)

(b) Describe Message Authentication Code (MAC).

5. How does PGP create a secure network? Also explain PGP.

SECTION–B

(Short Answer Type Questions)

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. (4×8=32)

1. What is Chinese Remainder theorem? Determine the numbers that leave remainders 2, 3 and 2 when divided by 3, 5 and 7 respectively.

2. What GCD Recursion theorem?

3. Explain active attack and passive attack with supportable and real-life examples.

4. Explain data encryption standard (DES) and its operational architecture with supportable diagram.

5. Describe ElGamal Cryptosystem and its process.

6. Briefly describe the role of IP security to enhance the security over wireless network.

7. List down the advantages of MD5 and SHA algorithms.

8. Cite examples from real life, where the following security objectives are needed.

(a) Authentication.

(b) Access control.

(c) Non-repudiation.

Suggest suitable security mechanism to achieve them.