# A-0863

**Total Pages : 4** **Roll No. -------------**

# MIT (CS)-204

## Cryptography and Network Security

**(MSCCS)**

2nd Semester Examination 2024(Dec.)

Time: 2:00 hrs Max. Marks: 70

Note : This paper is of Seventy (70) marks divided into Two (02) Section 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.

P.T.O.

## 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.

[2x19=38]

Q.1. Solve the following:

a. Compute the modular exponentiation $\chi = (5^3 \bmod 13)$.

b. Explain the relevance of modular arithmetic in cryptography.

Q.2. Explain the Data Encryption Standard (DES). Discuss the DES round structure and evaluate its strength and weaknesses.

Q.3. What is IP Security (IPsec)? Explain its architecture, benefits, and applications in securing communications.

Q.4. Describe the working of Elgamal Cryptosystem. Explain its encryption and decryption process with an example.

Q.5. Discuss the Need for Security in Networks. Why is network security crucial in today's digital environment? Explain the common cyber threats faced by modern networks and the strategies used to safeguard them.

## 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.

[4x8=32]

Q.1. Differentiate between symmetric and asymmetric cryptography with examples.

P.T.O.

Q.2. Explain Chinese Remainder Theorem and its application in cryptography.

Q.3. Write and explain the Digital Signature Algorithm (DSA).

Q.4. Explain the principles of block cipher modes: CBC, ECB, and OFB.

Q.5. What are the benefits and applications of IP Security (IPsec)?

Q.6. Describe the structure of CMAC and its cryptographic significance.

Q.7. Differentiate between public key and private key cryptosystems.

Q.8. What is WLAN? Explain its topologies and the role of 802.11 MAC in securing wireless communication.

*********************