S-790

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

MIT(CS)-204

Cryptography and Network Security

M.S. Cyber Security (MSCCS)

2nd Semester, Examination 2022(Dec.)

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.

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 x 19 = 38]

P.T.O.

Q.1. Explain the Diffie-Hellman key exchange with algorithm.

Q.2. What are the principal elements of a public key cryptosystem? Explain in detail the three broad categories of application of public-key cryptosystems.

Q.3. What is RSA algorithm? Explain the generation of public and private keys and hence generation of CIPHER text through RSA with the help of example.

Q.4. (a) Discuss key management in cryptography? Also explain the two types of key management?

(b) Discuss modes of operation in cryptography?

Q.5. Discuss the role of digital signatures in modern communication. Also discuss the differences between digital certificates and digital signatures in authentication.

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 x 8 = 32]

Q.1. Compare substitution and transportation cipher techniques.

Q.2. State and prove Chinese Remainder theorem.

Q.3. Describe the security services to counterpart the security attacks in network security.

Q.4. Explain the role and functions of secure socket layers (SSL) in network security.

Q.5. Give a real-life example where both confidentiality and integrity are needed. Explain why encryption alone does not provide integrity of information.

P.T.O.

Q.6. Discuss how firewalls help in the establishing a security framework for an organization.

Q.7. Discuss in brief about IPsec architecture.

Q.8. What is Kerberos? How does it work?

****