Roll No ....

MCADD-803

M.C.A. (Integrated), VIII Semester

Examination, May 2022

Network Security

Time : Three Hours

Maximum Marks : 70

Note : i) Attempt any five questions.

ii) All questions carry equal marks.

1. a) Explain the terms Authentication, confidentiality, Integrity, Non-repudiation. Also give the difference between steganography and cryptography.

    b) Describe the model of Network Security.

2. a) Explain Data Encryption Standard (DES) in detail.

    b) Explain Diffie-Hallman key exchange algorithm.

3. a) What is Triple DES? How do two key and three key triple DES differ?

    b) What is the purpose of S-Boxes in DES?

4. a) What is digital signature? What are its requirements? Discuss arbitrated digital signature and direct digital signature.

    b) What do you understand by web security? What are various web security protocols? Explain any one.

5. a) Explain RSA.

b) Perform encryption and decryption using RSA algorithm for the following data

$p = 3, q = 11$ (p and q are Prime numbers)

$l = 7, m = 5$ (l- encryption, m- message)

6. a) Give a brief note on x.509 authentication services.

b) Describe IP security architecture.

7. a) Explain three classes of intruder.

b) What do you mean by intrusion? Explain types of IDS detection techniques.

8. Explain the following any two.

i) Trusted systems

ii) Secure socket layer

iii) Combining security associations

******

MCADD-803