MASTER OF SCIENCE (COMPUTER SCIENCE) (CBCS-2018 COURSE)
M.Sc. (Computer Science) Sem-II :SUMMER- 2022
SUBJECT : NETWORK SECURITY

Day : Tuesday
Date : 12/7/2022

S-20047-2022

Time : 03:00 PM-06:00 PM
Max. Marks : 60

N.B.:

1) All questions are **COMPULSORY.**
2) Figures to the **RIGHT** indicate full marks.
3) Draw neat labeled diagrams **WHEREVER** necessary.

Q1. What is meant by Public key Cryptography? Explain. Also explain in detail security uses of Public key Cryptography. **(15)**

OR

Explain in detail International Data Encryption Algorithm(IDEA) **(15)**

Q2. **A)** Answer **ANY ONE** of the following: **(08)**

i) Explain the concept of Cipher Block Chaining and also explain in detail threats faced by it.

ii) Explain modular arithmetic with respect to the following points:
a) Modular addition b) Modular multiplication c) Modular exponentiation

B) Answer **ANY ONE** of the following: **(07)**

i) Explain the concept of on-line password guessing and off-line password guessing.

ii) Explain the security services for electronic mail.

Q3. Answer **ANY THREE** of the following: **(15)**

a) Explain the concept of viruses, worms and Trojan horses.

b) What is TCP, IP and UDP? Explain.

c) Explain the basic structure of Data Encryption Standard.

d) Explain the concept of Key Distribution Centre(KDC).

e) Describe the concept of elliptic curve cryptography.

Q4. Write short notes on **ANY THREE** of the following: **(15)**

a) Address-based authentication

b) NetwareV3

c) Active and passive attacks

d) Multiple encryption DES

e) Privacy Enhanced Mail(PEM)

****