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

Day : Wednesday — Time : 10:00 AM-01:00 PM

Date : 4/1/2023 — **W-20047-2022** — Max. Marks : 60

N.B.

1) All questions are **COMPULSORY.**
2) Figures to the right indicate **FULL** marks.
3) Draw diagrams **WHEREVER** necessary.

Q.1 Explain password-based authentication, address based authentication and cryptographic authentication protocols. **(15)**

OR

a) Explain international Data Encryptions Algorithm (IDEA) with respect to the following points: **(08)**
- i) Basic structure
- ii) Key expansion
- iii) Odd and even rounds

b) Explain the security services for electronic mail. **(07)**

Q.2 A) Answer **ANY ONE** of the following: **(08)**

a) Explain RSA algorithm. Also explain how RSA can be used for authentications.

b) What is meant by public key cryptography? Explain the security uses of public key cryptography.

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

a) Explain Data Encryption Standard (DES) with respect to
- i) Basic structure of DES
- ii) DES round
- iii) The mangler function

b) Explain modular arithmetic with respect to the following points:
i)Modular additions ii) Modular multiplication
iii) Modular exponentiations.

Q.3 Answer **ANY THREE** of the following: **(15)**

a) Explain the basic concept of Diffie-Hallman algorithm.

b) What is meant by cryptography? Explain the security uses of secret key cryptography.

c) How is authentications of people carrier out in authentication system? Explain.

d) Explain the basic structure of Advanced Encryption Standard (AES).

e) Explain in brief different types of malicious software.

Q.4 Write Short notes on **ANY THREE** of the following: **(15)**

a) Preety and good privacy (PGP)

b) Firewalls

c) Security handshake pitfalls

d) Hash algorithms

e) Cipher Block Chaining (CBC)

* * * *