M. SC. (Computer Science) SEM – II (CBCS 2018 Course) : SUMMER - 2019

SUBJECT – NETWORK SECURITY

Day: **Saturday**
Date: **20/04/2019**

S-2019-1239

Date: 03.00 PM TO 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. Explain Data Encryption Standard(DES) with respect to following points: i) Basic structure of DES ii) DES Round iii) Mangler function iv) Weak and semi-weak keys **(15)**

OR

Explain RSA algorithm. Also explain how RSA can be used for authentication purpose. **(15)**

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

i) What is cryptography? Explain the concept of breaking an encryption scheme.

ii) Write in detail about following trusted intermediataries:

a) Key distribution centre

b) Certification authorities

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

i) Explain the concept of Hash algorithms and password hashing

ii) Explain Euclid's algorithm.

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

a) How privacy is achieved in electronic mail? Explain in brief.

b) Explain how protection can be obtained against evasdropping and server database reading.

c) What is firewall? With neat diagram explain application level gateway.

d) Explain the broad level steps in PEM.

e) Explain the concept of Secret Key cryptography.

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

a) Pretty Good Privacy(PGP)

b) Elliptic curves

c) Netware V3

d) Multiple encryption DES

e) S/MIME

****