M. SC. (Computer Science) SEM – II (Choice Based Credit & Grade System) : SUMMER - 2019

SUBJECT : NETWORK SECURITY

Day : **Saturday** Time : 03.00 PM TO 06.00 PM

Date : **20/04/2019** **S-2019-1249** Max. Marks : 60

N.B.:

1) All questions are **COMPULSORY**.
2) Figures to the right indicate **FULL** marks.

Q.1 What is authentication system? Explain: **[15]**

a) Password-based authentication
b) Address-based authentication
c) Cryptographic authentication protocols

OR

Explain basic structure of International Data Encryption Algorithm (IDEA). How is the key expansion carried out in IDEA? **[15]**

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

a) Explain the structure, key establishment and certificate hierarchy of a PEM message.

b) Explain Cipher block chaining with its threats.

B) Answer **ANY ONE** of the following: **[07]**

a) What is a protocol? Explain IP, UDP and TCP.

b) Explain Euclids' algorithm with an example.

Q.3 Answer **ANY THREE** of the following: **[15]**

a) Explain modular addition, multiplication and exponentiation for modular arithmetic.

b) Explain Advanced Encryption Standard.

c) Explain active and passive attacks along with types of each.

d) Explain the working of hashes and message digests.

e) What is session key establishment? Explain.

Q.4 Write short notes on **ANY THREE** of the following: **[15]**

a) Diffie-Signature Standard

b) Elliptic curves

c) Security system for electronic mail

d) Public key cryptography

e) Firewalls

* * * *