M. SC. (Computer Science) SEM – II (Choice Based Credit & Grade System) : WINTER - 2018

SUBJECT : NETWORK SECURITY

Day : Wednesday
Date : 10/10/2018

Time : 03.00 PM TO 06.00 PM
Max. Marks : 60

W-2018-1047

N.B.:

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

Q.1 **a)** Explain RSA algorithm. Also explain how RSA can be used for authentication purpose. **[07]**

b) Explain the basic structure of International Data Encryption algorithm (IDEA). How is the key expansion carried out in IDEA? **[08]**

OR

Explain Password-Based authentication, address based authentication and cryptographic authentication protocols. **[15]**

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

a) Explain the working of packet switching. Differentiate between active and passive attacks.

b) Explain modular arithmetic with example.

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

a) What is privacy in networking? How end to end privacy and privacy with distribution and list exploders carried out?

b) Explain Cipher block chaining.

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

a) What is cryptography? Explain secret key cryptography.

b) Explain the working of KDC. State its disadvantages.

c) Explain viruses, worms and Trojan horses.

d) Explain digital signatures in brief.

e) Explain the security services for electronic mail.

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

a) Structure of a PEM message

b) Netware V3

c) DES

d) Hashes and Message digests

e) Elliptic curves

* * * *