Exam.Code:0923
Sub. Code: 6504

2122

B.E. (Information Technology)

Fifth Semester

PCIT-501: Network Security and Cryptography

Time allowed: 3 Hours

Max. Marks: 50

NOTE: *Attempt five questions in all, including Question No. I which is compulsory and selecting two questions from each Unit.*

x-x-x

I. Distinguish between the following:-

a) Threat Vs Attack with example

b) Substitution Vs Transposition cipher with example

c) KDC Vs CA

d) Transport Vs Tunnel Mode with layered diagrams

e) Hash Vs MAC

(5x2)

UNIT - I

II. a) What do you mean by KDC? How Symmetric key is exchanged using KDC for implementing confidentiality? What are the limitations of this method to exchange the key? How needham schroeder protocol eliminates these limitations and help to exchange symmetric key?

(4+3)

b) Compare symmetric and asymmetric cryptography. (3)

III. a) What do you mean by a hash function? What are the essential requirements of a hash function? Justify all these requirements.

b) Design a mailing system for UIET. The proposed system should have confidentiality, integrity and authentication.

(2x5)

IV. What do you mean by AES? Explain working of AES in detail. (10)

UNIT - II

V. a) What do you mean by digital signature? How non-repudiation can be achieved in communication over Internet?

b) Write header details of AH and ESP.

(2x5)

P.T.O.

VI. a) Why RSA works for achieving confidentiality? Give its mathematical proof.

b) What are threats to secure web access? Explain architecture of SSL. (2x5)

VII. a) What is Single Sign in? Why is it required? Explain working of Kerberos system with diagram(s).

b) Discuss various types of firewalls. (8,2)

x-x-x