Exam.Code:0923
Sub. Code: 6848

1129

B.E. (Information Technology)

Fifth Semester

ITE-503: 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. Attempt the following:-

a) Define message integrity.

b) What is a stream cipher?

c) What is confusion?

d) What is diffusion?

e) What is a brute force attack?

f) What is message digest?

g) Define Distributed Denial of Service Attack.

h) Compute 5^{10} mod 17.

i) What is differential cryptanalysis?

j) Name the services provided by Kerberos. (10x1)

UNIT – I

II. a) What is the concept of Digital Envelope? How Symmetric key is exchanged using public key cryptography for implementing confidentiality?

b) Compare symmetric and asymmetric models of encryption. (2x5)

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

b) Design a mailing system for UIET. The proposed system should have confidentiality and integrity of messages exchanged. (2x5)

IV. What do mean by Triple DBS? Explain working of Triple DBS in detail. (10)

UNIT – II

V. a) Why Diffie-Hellman Key Exchange algorithm fails for establishing shared key between communication parties in absence of public key certificates?

P.T.O.

b) What do you mean by digital signature? How non-repudiation can be achieved in communication over Internet? (2x5)

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

b) Perform encryption and decryption on letter 'b' using RSA with the help of following parameters: p=31, q=23. (2x5)

VII. a) What are control access techniques?

b) Discuss various types of firewalls. (2x5)

x-x-x