**Exam.Code:0924**
**Sub. Code: 6852**

**1059**

B.E. (Information Technology)
Sixth Semester
ITE-643/672: Network Security and Cryptography

Time allowed: 3 Hours Max. Marks: 50

***NOTE:*** *Attempt five questions in all, including Question No. 1 which is compulsory and selecting two questions from each Unit.*

*x-x-x*

I. Distinguish between the following:-

a) Hash Function Vs Message Authentication Code (MAC)

b) SET Vs 3D-Secure

c) Transport Vs Tunnel Mode with layered diagrams

d) Digital Signature Vs Conventional Signature

e) Cipher Text Analysis Vs Brute Force Attack (5x2)

## UNIT – I

II. a) What are Monoalphabetic and Polyalphabetic ciphers. Explain their types with examples.
b) What is the concept of Digital Envelope ? How Symmetric key is exchanged using public key cryptography for implementing confidentiality? (2x5)

III. Distinguish between DES and AES. Explain the working of AES with suitable diagrams. (3+7)

IV. a) Perform encryption and decryption on letter 'e' using RSA with the following parameters:
p = 11, q = 13, e=11 (2x5)
b) How dual signature is constructed? Explain how merchant verifies the dual signature. (2x5)

## UNIT – II

V. a) What do you mean by an IP Tunnel ? How IP tunnel successfully implement security ? Explain with suitable diagrams. (2+4)

b) Write header details of ESP and explain its fields. (4)

VI. You are to implement secure web access in your institute. Which protocol will you use for the purpose ? Explain secure connection establishment in details with suitable diagrams. (10)

VII. What is MD5? Explain working of MD5 in detail. (10)

*x-x-x*