18-

Exam.Code:1005
Sub. Code: 7696

1128

M.E. (Biotechnology) First Semester
MEIT-105/MEIT-115: Information Security

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. Answer the following questions with suitable examples:

a) What is Cryptanalysis and Cryptology?

b) Differentiate between threat and attack?

c) What is the difference between block cipher and stream cipher?

d) Perform encryption and decryption using RSA algorithm given: *P*=7, q=l 1, e=17, M=8

e) What is the difference between MAC and Hash? (5x2)

UNIT – I

II. a) Encrypt the word "Semester Result" with the keyword "Examination" using Playfair Cipher. List the rules used.

b) Explain ECE and CBC Operation Modes for Block ciphers (5,5)

III. a) Explain how triple DES works. Is Triple DES compatible with double DES which uses 2 keys for two encryptions?

b) What is differential cryptanalysis?'Discuss the cryptanalysis of DES algorithm. (5,5)

IV. a) Define a trapdoor one way function and explain its use in asymmetric key cryptography. With a neat diagram discuss the ingredients of a Public Key Cryptosystem.

b) Write short notes on: Knapsack Systems, Polyalphabetic Substitution Cipher. (5,5)

P.T.O.

UNIT – II

V. a) Why cryptographic hash functions are used? Explain the MD5 hash algorithm in brief and also discuss its limitations.

b) What is Kerberos? Explain the requirements defined by Kerberos and its working. (5,5)

VI. a) List the security services provided by digital signatures. Explain the Digital Signature Standard.

b) Draw the IP security authentication header and describe the functions of each field. (5,5)

VII. a) How 'Encapsulating Security Payload (ESP) provides confidentiality and authentication.

b) How is a security gateway different from application gateway? Discuss about any two firewalls available in the market today that are used in organizations to prevent attacks. (5,5)

x-x-x