Exam.Code:1006
Sub. Code: 7362

2054

M.E. (Information Technology)

Second Semester

MEIT-2101: 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

1. a) Define Cryptography

   b) Define Availability.

   c) What is a block cipher?

   d) What is need of random number in security?

   e) What is a Vulnerability?

   f) What is Intrusion Detection System?

   g) Define Distributed Denial of Service Attack.

   h) Define Message Integrity.

   i) What is cryptanalysis?

   j) What is dictionary attack? (10x1)

UNIT - I

2. a) What do you mean by attack? Enlist and explain various types of attacks possible on a typical information system. 5

   b) What do you mean by cipher? Differentiate between substitution and transposition ciphers. 5

3. a) Compare block and stream ciphers. 5

   b) What do mean by Public Key Certificates? What are their typical contents? 5

4. What do mean by AES? Explain working of AES in detail. 10

UNIT - II

5. a) Draw suitable diagram for implementation of Diffie-Hellman Key Exchange algorithm for establishing secrete key between communication parties? 5

   b) Prove that Diffie-Hellman Key Exchange algorithm is vulnerable to woman-in-the-middle attack. 5

P.T.O.

6. a) Explain RSA algorithm. 5

   b) Perform encryption and decryption on letter 'e' using RSA with the help of following parameters: p=11, q=13, e=11. 5

7. What is Single Sign-on? Explain Kerberos System with block diagram for implementing Single-Sign-on. 10

x-x-x