Exam.Code:1006
Sub. Code: 7362

2063

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.

x-x-x

Q1	Distinguish between the following:	
a)	Monoalphabetic and Homophonic Substitution Cipher.	2
b)	MAC and Hash	2
c)	Public and Private Key	2
d)	Digital Signature Standard (DSS) and RSA	2
e)	Integrity and Authentication.	2
	SECTION A	
Q2	a) Consider the following: Plaintext: "TRANSPOSITION" Secret key: 43152 What is the corresponding cipher text using transposition cipher method? b) What are threats? Explain the different categories of Threats with suitable examples.	5+5
Q3	a) Explain ECE and CBC Operation Modes for Block Cipher with their advantages and disadvantages. b) Discuss the following terms with respect to Cryptography: i. Symmetric ii. Asymmetric iii. Hash c) What are different approaches to Public-key Management?	5+3+2
Q4	a) How Triple DES works? Explain in detail. Is Triple DES being compatible with double DES? b) What are the principles of public key cryptosystems? Discuss the different components of Cryptosystem.	5+5
	SECTION B	
Q5	a) What s the usage of authentication protocol? Explain the requirements defined by Kerberos and its working. b) Discuss the steps that are performed by an entity that generated the digital signature (intended signatory).	5+5
Q6	a) With suitable diagram discuss the importance of Transport Layer Security (TLS) and Secure Socket Layer(SSL). b) What are the important points to be considered for web security? c) What is a Firewall? Explain its design principles and types with example.	4+3+3
Q7	a) How Encapsulating Security Payload (ESP) provides confidentiality and authentication? b) Explain the importance of knapsack algorithm c) What are the capabilities and limitations of Firewalls.	5+3+2

x-x-x