Exam.Code:1006
Sub. Code: 7697

2072

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 Section.*

1. Distinguish between the following:
   a) Threat Vs Attack 2
   b) Message Integrity Vs Entity Authentication 2
   c) Countermeasure Vs Vulnerability 2
   d) SET vs 3D Secure 2
   e) Strong Collision resistance Vs Weak Collision resistance 2

Section-A

2. Distinguish between DES and AES cipher. Explain working of DES with emphasis on substitution and transposition steps to achieve strength in encryption process. 4+6=10

3. How public and private keys are generated in ELGamal Crypto scheme and RSA Crypto scheme? Write rationales about Why both schemes are successful in achieving confidentiality? 6+2+2 =10

4. Design a mutual authentication system so that no masquerading be possible in communication and replay attacks are also avoided as for as possible. Enlist your assumptions and terminology to be used. 10

Section-B

5. What do you mean by security parameter negotiation in SSL? Explain Handshake protocol in detail with lucid diagram(s). 2+8 =10

6. Why IPSec is required to achieve secure communication? Explain various modes of using IPSec. Write header details of AH and ESP. 2+2+6 =10

7. What is the concept of dual signature? How is it practically used in SET to achieve specific business requirements of online purchase? Explain with lusid diagram(s). 2+8=10

x-x-x