Exam. Code: 1000
Sub. Code: 34997

2056

M.E. (Computer Science and Engineering)
Second Semester
Elective - IV
CS-8207: Network Security

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

Q1
a) What is network security model?
b) What is the effect of DDoS attacks on network?
c) How are public keys distributed?
d) Differentiate between SSL and TLS.
e) What are high availability features in firewall? (10)

UNIT - I

Q2 What are substitution techniques? How they are different from transposition techniques. Compare all monoalphabetic and polyalphabetic substitution techniques in detail. (10)

Q3. What is the significance of the following:
a) Fermat's and Euler's theorem
b) Euclidean and Extended Euclidean algorithm
c) Triple-DES algorithm
d) Choosing two large numbers in RSA Algorithm (10)
e) HMAC technique

Q4. What are the requirements of authentication functions? With the help of flow-chart, explain in detail working of SHA-1 algorithm? (10)

UNIT - II

Q5. Explain with real time use cases the need of Digital Signature. Explain Digital Signature Standard format, its complete architecture and how it generates digital signatures? (10)

Q6. a) Draw and explain the architecture of Network based IDS operating in promiscuous mode. (10)
b) Explain signature-based and anomaly-based detection methods used in IDS/IPS systems.

Q7. Write short notes on:
a) IPSec
b) Different types of firewalls and their configuration (10)

x-x-x