Exam.Code:1000
Sub. Code: 7309

2014

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 (Section-A) which is compulsory and selecting two questions each from Section B-C.

x-x-x

SECTION-A

1 a) What are different security attacks?
b) What is the stream cipher structure?
c) What are applications of hash functions?
d) What is the role of security associations in IP Security?
e) How does IPS can be deployed in campus-networks? 10

SECTION -B

2 a) How does the play-fair achieve secrecy? What are the challenges associated with using the play-fair Cipher? 5
b) How the Diffie-Hellman generates key pair? Explain its algorithm? 5

3. a) How does the Triple-DES algorithm work? What is its significance? 5
b) Explain Digitally Signing process in RSA algorithm with example. 5

4. a) With the help of flow-chart, explain in detail working of MD5 algorithm? 6
b) What are the different methods available for distribution of public-keys? 4

SECTION-C

5. With the help of a diagram, explain Digital Signature Standard (DSS) format and how it generates digital signatures with the help of SHA? 10

6. Explain IP Security architecture. Also draw and explain the packet format of Authentication Header and Encapsulation Security Payload. 10

7. Write short notes on:
a) Different types of firewalls
b) HTTPS 10

x-x-x