Exam.Code:1000
Sub. Code: 7309

2063

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) How does the network security protocol stack ensure confidentiality of data in transit?
   b) What are some common vulnerabilities in the network security and how can they be mitigated?
   c) How does the network prevent network attacks such as DoS/DDoS?
   d) What are the main differences between TLS and SSL?
   e) How does SQL injection occur and what measures can be taken to prevent it?? 10

SECTION-B

2. a) Explain how does a symmetric encryption algorithm ensure confidentiality of data? 3
   b) How does differential cryptanalysis exploit the behaviour of the plaintext and ciphertext differences? 3
   c) How AES differs from DES? Give examples of real-world applications that utilize AES for encryption and data protection. 4
3. Explain the mathematical principles behind RSA encryption and decryption. Describe the process of generating RSA keys and selecting appropriate prime numbers. 10
4. a) Explain the concept of man-in-the-middle attacks and how they can be mitigated in Diffie-Hellman Key exchange algorithm? 5
   b) What basic arithmetical and logical functions are used in SHA? 5

SECTION-C

5. a) Explain how key management systems protect against insider threats and unauthorized access? 5
   b) How does the input message get processed in the SHA algorithm? 5
6. a) What is the role of the ESP Security Association (SA) in securing communication? 5
   b) How does SET integrate with payment gateways and financial institutions? 5
7. Explain the following:
   a) Security implications of using third-party libraries and components in web applications
   b) Passive and active IDS responses 10

x-x-x