10EC832

Eighth Semester B.E. Degree Examination, Jan./Feb. 2021
Network Security

Time: 3 hrs.   Max. Marks:100

Note: *Answer any FIVE full questions, selecting atleast TWO questions from each part.*

PART – A

1   a. Discuss the OSI Security Architecture focusing on security mechanism, services and attacks. **(12 Marks)**
    b. With a neat diagram, discuss the function of Network Security model. List the basic tasks of designing security model. **(08 Marks)**

2   a. Explain block cipher design principle. **(06 Marks)**
    b. With a neat diagram, explain the single round of DES encryption. **(08 Marks)**
    c. Discuss the evaluation criteria for Advanced Encryption Standard. **(06 Marks)**

3   a. Discuss with illustrations i) Prime curves defined over Zp   ii) Binary curves constructed over GF (2^n) iii) Elliptic Curve Encryption and decryption. **(12 Marks)**
    b. Describe RSA Algorithm and discuss the security of RSA. **(08 Marks)**

4   Write short notes on :
    a. Authentication function   b) Hash function
    c. Authentication protocols   d) Digital signature standard. **(20 Marks)**

PART – B

5   a. Explain SSL protocol stack with a neat diagram and define the different parameters used in session and states. **(10 Marks)**
    b. Explain in detail the transactions supported by SET protocol. **(10 Marks)**

6   a. Write short notes on :
       i) Statistical anomaly detection   ii) Rule based intrusion detection. **(10 Marks)**
    b. What are different techniques employed in choosing passwords? Compare their relative merits. **(10 Marks)**

7   a. Give the taxonomy of malicious programs. List the software threats and explain them. **(10 Marks)**
    b. Discuss the following : i) Email viruses   ii) Digital Immune Systems. **(10 Marks)**

8   a. What is a Firewall? Explain the various types of firewall configurations, with relevant diagrams. **(10 Marks)**
    b. With a neat diagram, explain the various working of a packet – filtering router. **(06 Marks)**
    c. With reference to the concept of trusted system. Explain
       i) Multilevel security requirements   ii) Reference monitor property. **(04 Marks)**

*****