8th Sem EC

USN | | | | | | | | | | |

10EC832

Eighth Semester B.E. Degree Examination, Dec.2015/Jan.2016
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. With a neat block diagram, discuss the functioning of network security model. List four basic tasks of designing security model. **(10 Marks)**

b. Encrypt the message "ELECTRONICS" using playfair cipher with a key "INDIA". Also, give the rules for encryption. **(10 Marks)**

2 a. Encrypt the plain text "HAND" using hill cipher with the key

$$\text{key} = \begin{vmatrix} 5 & 8 \\ 17 & 3 \end{vmatrix}$$

Also decrypt it and verify the encryption and decryption text. **(10 Marks)**

b. In S – DES, 10 – bit key is "1010000010". Find the sub keys k_1 and k_2. If

P_{10} = 3 5 2 7 4 10 1 9 8 6
P_8 = 6 3 7 4 8 5 10 9

(10 Marks)

3 a. In a RSA algorithm system, the cipher text received is C = 10 with a public key P_U = {5, 35}, deduce the plain text. Verify the answer by encryption process. **(10 Marks)**

b. Explain Diffie – Hellman key exchange algorithm. Also calculate the Y_A, Y_B and secret key (k) for q = 23, α = 07, X_A = 3 and X_B = 6. **(10 Marks)**

4 a. Write a short note on Hash function. **(05 Marks)**

b. Mention the requirements for a digital signature. **(05 Marks)**

c. Explain the signing and verifying functions of digital signature algorithm (DSA). **(10 Marks)**

PART – B

5 a. Explain the SSL architecture. **(10 Marks)**

b. Highlight the key features of SET. **(05 Marks)**

c. Explain in detail, the payment capture transaction supported by SET. **(05 Marks)**

6 a. Explain the architecture of a distributed intrusion detection system. Give the major issues in the design. **(10 Marks)**

b. Briefly explain the password selection strategies. **(10 Marks)**

7 a. Give the taxonomy of malicious programs and explain in brief. **(10 Marks)**

b. With a schematic, explain the typical step in digital immune system. **(10 Marks)**

8 a. With a neat diagram, explain the concept of trusted systems. **(10 Marks)**

b. What is firewall? Mention the capabilities and limitations of firewalls. **(10 Marks)**

* * * * *