C **Reg. No. :** | | | | | | | | | | |

Question Paper Code: 52R05

M.E. DEGREE EXAMINATION, APRIL 2019

Second Semester

Computer Science and Engineering

15PCS205 – NETWORK SECURITY

(Regulation 2015)

Duration: Three hours Maximum: 100 Marks

Answer ALL Questions

PART - A (5 x 1= 5 Marks)

1. __________ is generally used in ECB,CBC, or CFB mode CO1- R

   (a) DES (b) AES (c) IDEA (d) RSA

2. On an average an attacker has to generate ______ number of fraudulent messages for birthday attack CO2 -R

   (a) 2m (b) 2^m (c) $2^{m/2}$ (d) $2^{m/2 -1}$

3. Which authentication method ensures authentication using a secret shared key? CO3- R

   (a) Windows Authentication (b) Preshared keys

   (c) Kerberos v5 (d) Kerberos v5

4. Who will be responsible for processing the payment from the customer's account to the merchant account? CO4 -R

   (a) Acquirer (b) Merchant (c) Issuer (d) Payment gateway

5. In _______, the virus places an identical copy of itself into other programs or into certain system areas on the disk. CO5- R

   (a) Dormant phase (b) Propagation phase (c) Triggering phase (d) Execution phase

PART – B (5 x 3= 15Marks)

6. Differentiate block cipher and stream cipher . CO1-U

7. Find whether 5 is a primitive root of 7. CO2-App

8. Define a Security Association. What the parameters of SA? CO3-U

9. Differentiate SSL connection and session. CO4-U

10. List the 3 classes of intruders. CO5-U

PART – C (5 x 16= 80Marks)

11. (a) Demonstrate the operations of any block cipher along with key generation with neat diagrams. CO1- U (16)

Or

(b) Show the results of encryption in the first round of DES encryption. Expand the data by padding 0s to the left. Assume suitable values for S-box data. CO1- U (16)

12. (a) Explain RSA algorithm with example. CO2- U (16)

Or

(b) Explain DSA algorithm with example. CO2- U (16)

13. (a) An organization requires authentication, integrity and confidentiality services for transfer of data. Illustrate the use of IPSec in realizing the services with neat diagrams. Analyze the appropriateness of IPsec protocols for the same. CO3-Ana (16)

Or

(b) A bank has 100 branches across India. Discuss the key management practices suitable for secured communications between them. Explain how automated key management protocols of IPSec can be used in the above scenario. CO3-Ana (16)

14. (a) Explain SSL protocol with neat diagrams. CO4 -U (16)

Or

(b) Explain SET protocol in detail with various components. CO4 -U (16)

15. (a) Explain different types of firewall configurations in detail. CO5-U (16)

Or

(b) Explain the role of trusted systems in improving system security. CO5-U (16)