

C

Reg. No. :

--	--	--	--	--	--	--	--	--	--

**Question Paper Code: 51P01**

M.E. DEGREE EXAMINATION, MAY 2018

Second Semester

Computer Science and Engineering

15PNE203 – NETWORK SECURITY

(Regulation 2015)

Duration: Three hours

Maximum: 100 Marks

Answer ALL Questions

PART - A (5 x 1= 5 Marks)

- DES is a \_\_\_\_\_ cipher. CO1- R  
(a) Block                      (b) Stream                      (c) Character                      (d) Byte
- Which of the following is suitable for creating a session key ? CO2 -R  
(a) DSA                      (b) RSA                      (c) DH                      (d) None of the above
- Each Security association has a unique \_\_\_\_\_ CO3- R  
(a) Security Parameter Index                      (b) Destination IP  
(c) Source IP                      (d) None of the above
- 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
- A proxy firewall filters at the \_\_\_\_\_ CO5- R  
(a) physical layer                      (b) application layer                      (c) data link layer                      (d) network layer

PART – B (5 x 3= 15Marks)

- |  |         |
|--|---------|
| 6. Define steganography.                                       | CO1-U   |
| 7. Show whether $E_{11}(1,2)$ is an elliptic curve.            | CO2-App |
| 8. How can IPSec be employed to protect the integrity of data? | CO3-U   |
| 9. Write short notes on dual signature.                        | CO4-U   |
| 10. Differentiate a worm and virus.                            | CO5-U   |

PART – C (5 x 16= 80Marks)

- |  |         |      |
|--|---------|------|
| 11. (a) Explain different modes of operations of a block cipher with neat diagrams.  | CO1- U  | (16) |
| Or   |         |      |
| (b) Explain AES algorithm with neat diagrams.  | CO1- U  | (16) |
| 12. (a) Explain Diffie Hellman algorithm with example.   | CO2- U  | (16) |
| Or   |         |      |
| (b) Explain DSA algorithm with example.  | CO2- U  | (16) |
| 13. (a) A multinational company has off shore offices across the world with central office in India. Discuss the kinds of communication networks to be established between the offices. Explain the role of security associations for secured communications between them. | 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 SET protocol in detail with various components.  | CO4 -U  | (16) |

Or

(b) A customer visits an online store and places order for an item and performs online payment with a debit card. Evaluate the security requirements for various entities and describe how the SET protocol facilitates the same. CO4 -U (16)

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

Or

(b) Explain different types of Intrusion detection systems. CO5-U (16)

