Reg. No. : | | | | | | | | | | |

Question Paper Code: 22042

M.E. DEGREE EXAMINATION, MAY 2014.

Second Semester

Computer Science and Engineering (with Specialization in Networks)

01PNE203 - NETWORK SECURITY

(Regulation 2013)

Duration: Three hours Maximum: 100 Marks

Answer ALL Questions.

PART A - (10 x 2 = 20 Marks)

1. Why network need security?
2. Define steganography.
3. What are the roles of public and private keys?
4. What is message authentication?
5. Specify the IP security services.
6. List out the basic tasks in Public Key Encryption in key distribution.
7. Draw the SSL Record format.
8. What is digital signature?
9. Give few examples for worms.
10. Define trusted system.

PART - B (5 x 14 = 70 Marks)

11. (a) (i) Explain a single round of DES algorithm with neat diagram. (10)

(ii) Use a Hill cipher to encipher the message "we live in a insecure world". Use the key . (4)

Or

(b) (i) Discuss in detail about active and passive attacks. (6)

(ii) Explain about the Block cipher modes of operation. (8)

12. (a) Using elliptic curve cryptography, explain how secret keys are exchanged and messages are encrypted. (14)

Or

(b) Explain the MD5 message digest algorithm by giving suitable diagrams for message digest generation and message processing of 512 bit block and MD 5 operation. (14)

13. (a) (i) Draw the IP security authentication header and explain the functions of each field. (7)

(ii) What are transport mode and tunnel mode authentication in IP? Explain how ESP is applied to both these modes? (7)

Or

(b) Discuss about encapsulating security payload of IP. (14)

14. (a) Explain Secure Electronic transaction with neat diagram. (14)

Or

(b) Discuss about SSL architecture and SSL record protocol. (14)

15. (a) Enumerate the need for using firewalls to provide system security and explain the types of firewalls with neat sketch. (14)

Or

(b) (i) Write short notes on Password selection strategies and their significance. (7)

(ii) Define virus. Explain it in detail. (7)

PART - C (1 x 10 = 10 Marks)

16. (a) Users A and B want to establish a secret key using Diffie - Hellman key exchange protocol using a common prime q = 353, a primitive root $\alpha = 3$, A's secret key XA = 97 and B's secret key XB = 233. Compute the public and common secret keys of A and B. (10)

Or

(b) Perform encryption and decryption using the RSA algorithm with p = 5; q = 11, e = 3; M = 9. (10)