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

Question Paper Code: 42323

M.E. DEGREE EXAMINATION, NOV 2016

Second Semester

Computer Science and Engineering (With specialization in networks)

14PNE203 – NETWORK SECUTIRY

(Common to Computer Science and Engineering)

(Regulation 2014)

Duration: Three hours Maximum: 100 Marks

Answer ALL Questions.

PART A - (5 x 1 = 5 Marks)

1. The ---------- cipher is the simplest monoalphabetic cipher. It uses modular arithmetic with a modulus of 26
   (a) transposition (b) additive (c) shift (d) none of these

2. Which of the following anti-virus technique requires virus signature?
   (a) first generation (b) second generation
   (c) third generation (d) fourth generation

3. In ---------- mode, the authentication header is inserted immediately after the IP header.
   (a) tunnel (b) transport (c) authentication (d) both (a) and (b)

4. Merkle and hellman introduced the concept of
   (a) meet in middle attack (b) meet in attack
   (c) hijack (d) virus attacks

5. A firewall is installing at the point where the secure internal network and untrusted external network meet which is also known as
   (a) chock point (b) meeting point (c) firewall point (d) secure point

PART - B (5 x 3 = 15 Marks)

6. When an encryption algorithm is said to be computationally secure?

7. List the requirements of a hasing function.

8. What is a birthday attack?

9. What is a session fixation attack?

10. List out the limitation of firewall..

PART - C (5 x 16 = 80 Marks)

11. (a) Explain DES algorithm in detail. (16)

Or

(b) Write about any two classical cryptosystems (substitution and transposition) with suitable examples. (16)

12. (a) Explain the implementation of a Rivest-Shamir-Adleman algorithm. (16)

Or

(b) (i) Explain briefly about the elliptic curve cryptography. Can ECC be used with SSL and IPSec? (8)

(ii) Explain the implementation details about digital signature. (8)

13. (a) Differentiate the transport and tunnel mode operations of IP Sec for AH and ESP protocols. (16)

Or

(b) Define key management system. Explain about the public key authority and certificate. (16)

14. (a) Describe about secure electronic transaction. (16)

Or

(b) Explain SSL protocol with neat diagrams. (16)

15. (a) What is a firewall? Explain the various types of firewall configurations, with relevant diagrams. (16)

Or

(b) (i) With reference to the concept of trusted systems, explain multilevel security requirements and reference monitor property. (8)

(ii) Write short notes on viruses. (8)