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

## Question Paper Code: 42203

M.E. DEGREE EXAMINATION, MAY 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 the above

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. In anonymous e-money _____ factor is used to encrypt the random number.
   (a) blinded (b) prince (c) prime (d) anonymity

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. Differentiate worm and virus.

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) (i) Explain the implementation of a Rivest – Shamir – Adleman algorithm. (12)

(ii) Assume the RSA public key is given by (n,e) = (527, 11). Determine the corresponding RSA private key and compute the encryption of the message m = 3. (4)

Or

(b) (i) Explain RSA algorithm with an example. (10)

(ii) Discuss the security of RSA algorithm. (6)

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

Or

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

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

Or

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

15. (a) (i) Explain digital immune system with a neat diagram. (10)

(ii) Explain the different types of viruses. (6)

Or

(b) (i) List and briefly define three classes of intruder. (4)

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

(iii) Write short notes on viruses. (4)

———————