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

Question Paper Code: 42243

M.E. DEGREE EXAMINATION, NOVEMBER 2015

Second Semester

Computer Science and Engineering (with specialization in networks)

14PNE203 – NETWORK SECURITY

(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. Identify the mono-alphabetic cipher
   (a) Caeser cipher (b) Hill cipher
   (c) Vigenere cipher (d) None of the 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. Digital signature envelope is decrypted by using _____
   (a) merchant private key (b) payment's private key
   (c) payment public key (d) merchant's public key

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. Define confusion.

7. List the requirements of a hasing function.

8. What is a birthday attack?

9. Encrypt 'word' using Hill cipher. Assume $n= 2$ and $M= [1\ 2; 3\ 4]$.

10. Differentiate worm and virus.

PART - C (5 x 16 = 80 Marks)

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

Or

(b) (i) Explain the conventional cryptographic model with a neat diagram. (8)

(ii) Explain poly alphabetic substitution with Plkayfair cipher. (8)

12. (a) (i) Explain Diffie-Hellman key exchange algorithm. (8)

(ii) Generate a secret key K using Diffie-Hellman algorithm for the following input $q=7$, $\alpha=2$, $X_A=4$, $X_B=6$. (8)

Or

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

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

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

Or

(b) Explain key management in IP Sec. (16)

14. (a) (i) Draw a neat diagram illustrating dual signature mechanism. (4)

(ii) Discuss the SET payment processing phase. (12)

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) Explain different types of firewalls with neat diagrams. (16)
