|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |

**Reg. No. :**

**Question Paper Code: 42323**

M.E. DEGREE EXAMINATION, NOV 2017

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. 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. What is a session fixation attack?

10. Differentiate worm and virus.

PART - C (5 x 16 = 80 Marks)

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

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

Or

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

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, α=2, XA=4, XB=6*. (8)

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) Explain key management in IP Sec. (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) (i) Draw a neat diagram illustrating dual signature mechanism. (4)

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

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

Or

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