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

**Question Paper Code: 52941**

M.E. DEGREE EXAMINATION, DECEMBER 2015

Elective

Computer Science and Engineering (With Specialization in Networks)

15PNE517 - INFORMATION SECURITY

(Regulation 2015)

Duration: Three hours Maximum: 100 Marks

Answer ALL Questions

PART A - (5 x 1 = 5 Marks)

1. _____ attack is a passive attack

   (a) Denial of Service attack (b) Eavesdropping
   (c) Masquerading (d) Modification of messages

2. The generation of $2^{m/2}$ variations of valid message by the opponent with same meaning is known as _____.

   (a) brute force attack (b) timing attack
   (c) birthday attack (d) replay attack

3. The computational infeasibility of finding the message*(x)* from hash function *H(x)* is known as _____ property

   (a) one-way (b) strong collision resistance
   (c) weak collision resistance (d) two-way

4. The principle state that a subject should be given only those privileges that it needs in order to complete the task

   (a) Principle of least privilege (b) Principle of complete mediation
   (c) Principle of open design (d) Principle of fail-safe defaults

5. _____ is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

(a) Trojan (b) Logic bomb (c) Worm (d) Virus

PART - B (5 x 3 = 15 Marks)

6. Compare brute force attack with cryptanalytic attacks.

7. How do you counter the timing attacks?

8. Find the GCD (158, 46) using Euclid's algorithm.

9. Write the possible ways to avoid buffer overflow vulnerabilities.

10. What are the environmental shortcomings of Kerberos version 4?

PART - C (5 x 16 = 80 Marks)

11. (a) (i) Describe the various security services that are used to satisfy the various security requirements. (10)

(ii) What are the possible kinds of security attacks that are used to attack the information stored in an educational institution? Explain them in detail. (6)

Or

(b) (i) Explain the various ways of implementing the security services to protect the information from different kinds of attacks. (8)

(ii) How does the access control matrix provide security to the information stored in an organization? Explain. (8)

12. (a) (i) How do you use the DES algorithm in different ways? Explain. (8)

(ii) Explain the AES design criteria. (8)

Or

(b) Analyze the strengths and weaknesses of the DES algorithm. (16)

13. (a) (i) Prove that $Z_{19}$ is a field. (8)

(ii) Test whether 123 is a prime number or not using Miller-Rabin test. (8)

Or

(b) Given the message $M = 13$, prime numbers $P = 11$, $Q = 13$ and the sender's private key $e = 7$. Calculate the sender's public key, encrypt the message and decrypt the message using RSA algorithm. (16)

14. (a) Explain in detail the three types of security policies (EISP, ISSP and sysSP). (16)

Or

(b) What is information security blue print? Explain its salient features. (16)

15. (a) How do you secure an organization's emails using PGP? Explain with neat block diagrams. (16)

Or

(b) Explain the different protocols that are used to provide security to user data at the transport layer level. (16)