C 80818 **(Pages : 2)**

Name..............................

Reg. No...........................

SIXTH SEMESTER B.TECH. (ENGINEERING) [09 SCHEME] DEGREE EXAMINATION, APRIL 2015

CS/PTCS 09 L01—INFORMATION SECURITY

Time : Three Hours Maximum : 70 Marks

Part A

Answer **all** *questions.*

1. Distinguish between a substitution cipher and a transposition cipher.
2. List the attacks that threaten the integrity of information.
3. What are the types of firewall ?
4. Mention the purpose of Alert protocols.
5. Write any *two* software based attacks.

(5 × 2 = 10 marks)

Part B

Answer any **four** *questions.*

6. Let the prime numbers be $p = 11$ and $q = 13$, public key $e = 11$ and plain text $M = 7$. Perform encryption and decryption using RSA algorithm.
7. How will you find a message digest using MD5 Algorithm ?
8. What is access control ? How is it different from availability ?
9. What are the positive and negative effects of firewall ?
10. What problem was Kerberos designed to address ?
11. Write a note on software flaws.

(4 × 5 = 20 marks)

Part C

Answer the following.

12. (a) Describe man-in-the-middle attack on the Diffie hellman key exchange protocol.

Or

(b) Name the main components of the public key cryptosystem and formulate the security requirements. Discuss the use of the system for secrecy and authenticity.

13. (a) What are the approaches for achieving Single Sign On (SSO) ? Explain in detail.

Or

(b) Why is confidentiality an important principle of security ? How will you achieve the same ? Discuss the reasons behind the significance of authentication. Find out simple mechanisms of authentication.

14. (a) When a session is returned with a new connection, SSL does not require the full handshaking process. Show the messages that need to be exchanged in partial handshaking.

Or

(b) Describe authentication protocols in detail.

15. (a) Mention the security features provided by Windows Operating system. Explain in detail.

Or

(b) Bring out the significance of software recovery engineering.

(4 × 10 = 40 marks)