C 41290 (Pages 2) Name.....

Reg. No.....

SIXTH SEMESTER B.TECH. (ENGINEERING) DEGREE EXAMINATION, MAY 2013

CS/PTCS 09 L 01—INFORMATION SECURITY

(2009 Admission onwards)

Time : Three Hours Maximum : 70 Marks

Part A

Short Answer Questions (one/two sentences).
Answer **all** *questions.*

1. What is the difference between subject of an attack and object of an attack ?
2. What are the multiple layers of security in the organization ?
3. What is the difference between macro virus and boot virus ?
4. What are the services provided by PGP services ?
5. What is Software flaws ?

(5 × 2 = 10 marks)

Part B

Analytical/Problem solving questions.
Answer any **four** *questions.*

6. What is meet-in-the-middle attack ?
7. User A and B exchange the key using Diffie Hellman alg. Assume $a = 5$ $q = 11$ XA = 2 XB = 3. Find YA, YB, K.
8. List the design goals of firewalls ?
9. What is meant by SET ? What are the features of SET ?
10. What is a Screened Subnet Firewall ?
11. Discuss software recovery engineering.

(4 × 5 = 20 marks)

Part C

Descriptive/Analytical/Problem solving questions.

12. (a) Explain about the various key management techniques.

Or

(b) Explain RSA algorithm and state approaches for attacking RSA algorithm.

Turn over

13. (a) Explain with suitable diagrams how authentication and confidentiality is provided in Electronic Mail.

Or

(b) Explain the Firewall Design Principles.

14. (a) Explain any *one* of approach and algorithm for Digital Signatures.

Or

(b) Explain Authentication protocols.

15. (a) Describe next generation secure computing.

Or

(b) Write a note on :

(i) Technical hardware failures or errors.

(ii) Technical software failures or errors.

(4 × 10 = 40 marks)