Roll No .....

IT-801

B.E. VIII Semester

Examination June, 2013

Information Security

Time : Three Hours

Maximum Marks : 100 ***Minimum Pass Marks :35***

Note : All questions carry equal marks. Attempt any question from internal choice.

Unit - I

1. a) What is the difference between passive and active security threats? 10

   b) How many keys are required for two people to communicate via a cipher? 10

OR

2. a) Write a program that can encrypt and decrypt using general caesar cipher also known as additive cipher. 10

   b) Which parameters and design choices determine the actual algorithm of a feistel cipher? What is the purpose of the s-boxes in DES? 10

Unit - II

3. a) What is the difference between modular arithmetic and ordinary arithmetic? List three classes of polynomial arithmetic. 10

   b) What are the broad categories of applications of public-key crypto systems? 10

OR

4. a) What is an elliptic curve and what is zero point on elliptic curve? 10

   b) Explain Digital signature standards in brief. 10

Unit - III

5. a) What are the problems associated with clean text passwords? 10

   b) How does one prevent the misuse of another user's certificate in certificate based authentication? 10

OR

6. a) Explain the Security handshake pitfalls? 10

   b) What is Kerberos? How does Kerberos work? 10

Unit - IV

7. a) Explain SQL injection. Why is this for Web attack only? 10

   b) How is a circuit gateway different from application gate way. 10

OR

8. a) What is phishing ? How to avoid phishing attacks? 10

   b) What are the Firewalls? How Firewall guards corporate networks? 10

Unit - V

9. a) What are the Hardware and software requirements? Classify them into various cryptographic services. 10

   b) Give difference among viruses, worms and malwares. 10

OR

10. a) Why would leased line as a better approach than VPM? 10

    b) List the characteristics of a good firewall implementation. 10

******