Total No. of Questions : 10] [Total No. of Printed Pages : 3

Roll No. .....

IT–801

B. E. (Eighth Semester) EXAMINATION, June, 2012

(Information Technology Engg. Branch)

INFORMATION SECURITY

(IT – 801)

Time : Three Hours

Maximum Marks : 100

Minimum Pass Marks : 35

Note : Attempt any *one* question from each Unit. Draw neat diagrams. Differentiate columnwise on the basis of properties specified separately.

Unit – I

1. (a) Write algorithm, draw flowchart and also write a program in C++ for one time pad cipher. 10

   (b) Explain DES algorithm with the help of diagrams. 10

Or

2. (a) Explain such Block cipher modes of operation which use encryption and decryption. Draw complete and clear diagrams of each. 10

   (b) Differentiate between the following : 10

   (i) Block cipher and stream cipher

   (ii) Diffusion and confusion

P. T. O.

Unit – II

3. (a) Write short notes on any *two* of the following : 10

   (i) Hash value

   (ii) Birthday attack

   (iii) Meet-in-the-middle attacks

   (b) Explain Euclidean algorithm and solve the following using above algorithm : 10

   (i) determine gcd (1970, 1066)

   (ii) determine gcd (24140, 16762)

Or

4. (a) What characteristics are needed in a secure hash function ? 10

   (b) Explain R and A algorithm and using this algorithm encrypt the following : 10

   (i) P = 3, q = 11, e = 7, M = 5

   (ii) P = 7, q = 11, e = 17, M = 8

Unit – III

5. (a) What are the principal differences between version 4 and version 5 of kerberos ?

   (b) List and briefly define the parameters that define an SSL session state. 10

Or

6. (a) What is the difference between tunnel mode and transport mode ? 10

   (b) What services are provided by IPsec ? 10

Unit – IV

7. (a) Draw generic transmission diagram in PGP and explain in brief. 10

   (b) How does a worm propagate ? 10

Or

8. (a) What sort of testing can be performed in order to guard against possible CSS attacks ? 10

   (b) What is the role of compression in the operation of a virus ? 10

Unit – V

9. (a) What are *three* benefits that can be provided by an intrusion detection system ? 10

   (b) What are the weaknesses of a pocket filtering router ? Discuss its solution. 10

Or

10. (a) Explain the working of application level gateway. 10

    (b) Specify and explain classes of intruders. 10