Printed Pages– 3 Roll No. .....

322734(22)

B. E. (Seventh Semester) Examination, April-May 2018

(New Scheme)

(CSE, IT Engg. Branch)

CRYPTOGRAPHY and NETWORK SECURITY

Time Allowed : Three hours

Maximum Marks : 80

Minimum Pass Marks : 28

Note : *Attempt all questions. Part (a) of each question is compulsory and carrying 2 marks each and attempt two parts from (b), (c) and (d) carrying 7 marks each.*

1. (a) Encrypt using caesar cipher "I Love Cryptography". 2

(b) Draw the model for network security and explain each in detail. 7

(c) Describe DES scheme and also the working of each block associated with it. 7

(d) Explain in detail the principle of security. Also discuss OSI security architecture. 7

2. (a) Define group, ring and field. 2

(b) Find gcd (1970, 1066) using euclidian algorithm. 7

(c) Develop modulae arithmetic tables for GF(5). 7

(d) Explain the steps in various rounds of AES. 7

3. (a) State Fermat's theoram. 2

(b) Differentiate between conventional and public key encription. 7

(c) Describe Diffie-Hellman key exchange algorithm with example. 7

(d) Encrypt message '88' using RSA algorithm explaining each step in detail. 7

4. (a) Define hash function. 2

(b) What are the various approaches of producing message authentication. Explain in detail. 7

(c) What is digital signature? Explain how to use public key infrastructure to provide digital signature. 7

(d) Explain birthday attack in detail. 7

5. (a) What is bastian host? 2

(b) What protocol comprises SSL and then explain the difference between SSL connection and SSL session. 7

(c) Name the four phases of lifetime of computer viruses, also list the different type of computer viruses. 7

(d) Explain different types of firewall alongwith its design goal. 7

http://www.csvtuonline.com

http://www.csvtuonline.com