Printed Pages – 3 Roll No. : .....

322734(22)

B. E. (Seventh Semester) Examination, April-May 2020/ NOV-DEC 2020

(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 containing 2 marks. Attempt* ***two*** *part from (b), (c) and (d) each part carry 7 marks*

1. (a) What is Cryptanalysis? 2

(b) Explain the types of security attacks in detail. 7

(c) Differentiate between symmetric and asymmetric key cryptography. 7

(d) Explain working principle of DES. 7

2. (a) Define group and ring. 2

(b) Explain RC 4 with diagram. 7

(c) Explain the operation of pseudo random number generator. 7

(d) Explain Euclid's algorithm with suitable example. 7

3. (a) State fermat's theorem. 2

(b) Explain RSA algorithm with example. 7

(c) Explain Elliptic curve cryptography. 7

(d) Explain the steps in MD 5. 7

4. (a) Define hash function. 2

(b) Write the requirements and properties of a digital signature. 7

(c) Explain various authentication protocols. 7

(d) Write short notes on : 7

(i) MAC

(ii) HMAC

(iii) CMAC

5. (a) What is firewall? 2

(b) What are the various types of virus? Explain the phases of a virus during its life time. 7

(c) Explain kerberos message authentication scheme. 7

(d) Explain SSL and TLS architecture with suitable diagram. 7