Printed Pages – 3 Roll No. : .....

322755(22)

APR-MAY

B. E. (Seventh Semester) Examination, 2020

(Old Scheme)

(CSE, IT Engg. Branch)

CRYPTOGRAPHY & NETWORK SECURITY

Time Allowed : Three hours

Maximum Marks : 80

Minimum Pass Marks : 28

Note : *All questions are compulsory and carries equal marks. Attempt any* ***two*** *parts from each question.*

Unit-I

1. (a) Explain the design principle used to design Block Ciphers. 8

   (b) Explain OFB and CFB modes of operations of DES. 8

(c) Use playfair cipher to encode the message. "must see you over cadogan west. Coming at once." with the key : 8

M	F	H	I / J	K
U	N	O	P	Q
Z	V	W	X	Y
E	L	A	R	G
D	S	T	B	C

Unit-II

2. (a) Explain CAST-128 block cipher. 8

(b) Explain Blum Blum Shub pseudonumber generator. 8

(c) Explain AES in detail. 8

Unit-III

3. (a) Explain RIPEMD-160 in detail. 8

(b) Explain Diffie Hellman key exchange algorithm in detail. 8

(c) Explain Chinese remainder theorem with an example. 8

Unit-IV

4. (a) Explain Kerberos in detail. 8

(b) Write notes on : 8

(i) PGP

(ii) SSL and TLS

(c) Explain DSA in detail. 8

Unit-V

5. (a) What do you mean by malicious program? Explain taxonomy of malicious program. 8

(b) Explain SET in detail. 8

(c) Write notes on : 8

(i) Digi cash

(ii) Smart card based systems