Printed Pages – 4 Roll No. : ......................................

# 328840(28)

## B. E. (Eighth Semester) Examination, April-May 2021

**(New Scheme)**

**(ET&T Engg. Branch)**

## CRYPTOGRAPHY & SECURE COMMUNICATION

**(Elective)**

***Time Allowed : Three hours***

***Maximum Marks : 80***

***Minimum Pass Marks : 28***

***Note :*** *Attempt all the five questions. Part (a) of each question is compulsory. Attempt any two parts from parts (b), (c) and (d) of each question.*

### Unit-I

**1.** (a) State and define Fermat's little theorem. 2

(b) Explain in detail about square and multiply method of fast exponentiation with proper example and its equations. 7

(c) Write Euclidean algorithm to obtain the greatest common divisor and extended Euclidean algorithm to obtain the multiplicative inverse with example. 7

(d) Write Euler's theorem first version and second version. Also find the result of : 7

(i) $6^{24}$ Mod 34

(ii) $20^{62}$ Mod 77

## Unit-II

2. (a) Write difference between transposition technique and substitution technique. 2

(b) Explain in detail about RSA algorithm along with suitable example with its advantages and disadvantages. 7

(c) Describe the working of data encryption standard along with its block diagram in detail. 7

(d) What do you mean by diffie-hellman key exchange algorithm also write valid reason why this algorithm is insecure against a Man-in-the middle attack. 7

## Unit-III

3. (a) Write / Define the term MD as wel as hash function. 2

(b) Briefly explain along with algorithm what do you understand by term digital signature? 7

(c) Explain in detail about the basic uses of message authentication code (MAC). 7

(d) Elaborate the working principle of SHA-512 algorithm. 7

## Unit-IV

4. (a) Define the term IP Security. 2

(b) What do you understand by term computer virus? Name any two phases of lifetime of computer virus. Also list atleast 4 different types of virus and also mention its effect of web security. 7

(c) Mention in detail about the services provided by IP sec in detail. 7

(d) Illustrate three common firewall configurations with their block diagram. 7

## Unit-V

5. (a) What is the purpose of dual signature? 2

(b) Briefly describe operations of SSL record protocol with SSL record format. 7

(c) Explain different types of threats involved in network security. 7

(d) Explain principle categories of SET participants. 7