Printed Pages – 4 Roll No. : .....

328840(28)

APR-MAY

B. E. (Eighth Semester) Examination, 2020

(New Scheme)

(ET&T Engg. Branch)

CRYPTOGRAPHY & SECURE COMMUNICATION

Time Allowed : Three hours

Maximum Marks : 80

Minimum Pass Marks : 28

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

Unit-I

1. (a) Define finite group and order of group.

(b) Explain Euler's theorem with example.

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

(d) State and explain Fermat's theorem with example.

Unit-II

2. (a) Define Block cipher and Stream Cipher.

(b) Briefly describe the working of Data Encryption Standard (DES).

(c) Explain RSA algorithm with example in detail along with its advantages and disadvantages.

(d) Explain Diffie-Hellman key exchange algorithm and show how this algorithm is insecure against a Man-in-the-middle attack.

Unit-III

3. (a) Define Hash function.

(b) Briefly describe the MD5 algorithm with the working steps in it.

(c) Explain Digital signature with its advantages and disadvantages.

(d) Describe the basic usage of Message Authentication Code (MAC).

Unit-IV

4. (a) Define Virus and Firewall.

(b) Explain the services provided by IPSec in detail.

(c) Mention, how the most significant types of viruses can be categorized.

(d) Describe firewall configurations in brief.

Unit-V

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

(b) Briefly describe the overall operation of SSL Record protocol with SSL Record format.

(c) Draw a table of comparison of threats, their consequences and counter measures.

(d) What is Secure Electronic Transaction (SET)? Give an overview of SET along with its key features.