

328752(28)

APR-MAY

B. E. (Seventh Semester) Examination, 2020

(Old Scheme)

(Et & T Engg. Branch)

CRYPTOGRAPHY & SECURE COMMUNICATION

Time Allowed : Three hours

Maximum Marks : 80

Minimum Pass Marks : 28

Note : Part (a) of each question is compulsory.

Attempt any two out of (b), (c) and (d).

Unit-I

1. (a) What is the difference between public key and private key? 2

[2]

- (b) Write the statement for Fermat's and Euler's theorem. 7
- (c) Draw the block diagram of public key cryptosystem and explain it. 7
- (d) Explain RSA algorithm in detail. 7

Unit-II

- 2. (a) What is Brute Force Attack? 2
- (b) Explain basic uses of Hash with the help of diagrams. 7
- (c) What are the basic uses of MAC? Explain with proper diagrams. 7
- (d) Explain Brute force attack in detail. 7

Unit-III

- 3. (a) What is Digital Signature? 2
- (b) Describe MD5 message digest algorithm in detail. 7
- (c) Explain SHA-I algorithm along with the difference between MD-5 and SHA-I. 7
- (d) What are the types of digital signature standard? Explain any one. 7

[3]

Unit-IV

- 4. (a) What is Firewall? 2
- (b) What are the Web Security threats? Explain each of them in detail. 7
- (c) Draw AH, Authentication Header Protocol and explain it. 7
- (d) Draw IP Sec architecture and explain it. 7

Unit-V

- 5. (a) What is the difference between cryptography and steganography? 2
- (b) With the difference in deterministic and indeterministic model. Explain any one of them. 7
- (c) Draw the simplified model of steganography. 7
- (d) How security is achieved using deterministic model of information theory? 7