7E7032

Roll No. ________

Total No of Pages: 2

7E7032

B. Tech. VII - Sem. (Back) Exam., Feb.-March - 2021

Computer Science & Engineering

7CS2A Information System Security

CS, IT

Time: 2 Hours

Maximum Marks: 48
Min. Passing Marks: 15

Instructions to Candidates:

*Attempt **three questions**, selecting **one question each** from any three **unit**. All Questions carry **equal** marks. Schematic diagrams must be shown wherever necessary. Any data you feel missing suitably be assumed and stated clearly. Units of quantities used/ calculated must be stated clearly.*

Use of following supporting material is permitted during examination. (Mentioned in form No.205)

1. NIL ________ 2. NIL ________

UNIT- I

Q.1 (a) What is Cryptanalysis? Explain the Substitution and Transposition cryptographic technique. [8]

(b) What are the basic differences between passive and active attack? [8]

OR

Q.1 (a) Explain all block cipher modes of operation with suitable diagram. [8]

(b) Describe the Data Encryption Standard (DES) algorithm in detail. [8]

UNIT- II

Q.2 (a) What is AES? Explain the processing of plain text with suitable diagram. [8]

(b) What do you mean by bent function? Explain. [8]

OR

Q.2 (a) Explain RC6 in detail. [8]

(b) What is S-box? Explain the design criteria in the S-box structure. [8]

UNIT- III

Q.3 Discuss the Diffie-Hellman key exchange algorithm in detail. Also discuss the "Man in the middle attack" problem associated with the algorithm. [16]

OR

Q.3 (a) Explain the distribution of secret keys using Public Key Cryptosystem. [8]

(b) Explain the RSA algorithm with suitable example. [8]

UNIT- IV

Q.4 (a) Describe the MD5 message-digest algorithm in detail. [8]

(b) What is the Digital Signature? How authentication is accomplished using digital signature? [8]

OR

Q.4 (a) Explain the concept of MAC and its function. [8]

(b) Explain symmetric and Asymmetric authentication. [8]

UNIT- V

Q.5 (a) Explain Lamport's Hash protocol in detail. [8]

(b) Describe how PGP provides confidentiality and authentication services for e-mail application. [8]

OR

Q.5 Write short notes on- [2×8=16]

(a) IP Security Architecture

(b) Authentication Header
