7E7032

Roll No. [Total No. of Pages : 2]

7E7032

B.Tech. VII - Sem. (Main/Back) Examination, Nov. - 2019
Computer Science And Engineering
7CS2A Information System Security
Common For CS, IT

Time : 3 Hours **Maximum Marks : 80**
Min. Passing Marks : 26

Instructions to Candidates:

*Attempt any **five** questions, selecting **one** question from **each 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.*

UNIT - I

1. Explain differential and linear cryptanalysis of DES. **(16)**

OR

1. a) What is Shannon's theory of confusion and diffusion? Explain fiestel structure of Block ciphers. **(10)**

   b) Write short note on triple DES. **(6)**

UNIT - II

2. a) Write and explain the design criterian of S - Box in detail. **(10)**

   b) Explain Construction of Balanced function for S - Box. **(6)**

OR

2. a) Explain RC.6 algorithm for information system security. **(8)**

   b) Write short note on propagation and non linearity of S - Box. **(8)**

UNIT - III

3. a) Discuss security analysis of RSA algorithm along with its application. **(8)**

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

OR

[Contd....

3. a) Explain Public key cryptosystems along with its principles. **(10)**
   b) Write short note on X.509. **(6)**

UNIT - IV

4. Explain following in detail.
   a) SHA **(8)**
   b) MD5 **(8)**

OR

4. a) Explain symmetric and Asymmetric Authentication. **(10)**
   b) Explain authentication protocols for digital signatures. **(6)**

UNIT - V

5. a) Explain the architecture of IP security in detail. **(10)**
   b) Write short note on Encrypted key exchange. **(6)**

OR

5. Explain following in detail.
   a) Encapsulation security payload in transport and Tunnel mode with multiple Security Association. **(10)**
   b) Lamport's Hash. **(6)**