Roll No. _____

6E1553

6E1553

B.Tech. VI Sem. (Main/Back) Examination, June - 2022
Information Technology
6IT4-03 Information Security System

Time : 2 Hours **Maximum Marks : 80**
Min. Passing Marks : 28

Instructions to Candidates:

*Attempt **all five** questions from **Part A**, **four** questions out of **six** questions from **Part B** and **two** questions out of **three** from **Part C**.*

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)

Part - A

(Answer should be given up to **25** words only)

All questions are **compulsory** **(5×2=10)**

1. What is encryption?
2. Define Cryptanalysis.
3. What is digital signtaure?
4. Write down the name of five web security threats.
5. Define block ciphers.

Part - B

(Analytical/Problem solving questions)

Attempt any **four** questions **(4×10=40)**

1. What are security attacks? Explain substitution ciphers and transposition ciphers.
2. Explain Data Encryption standard with the help of an example.
3. Explain the design principles of block cipher in detail.
4. What are public key cryptosystams? Explain its requirements and cryptanalysis in detail also explain RSA cryptosystem.

5. Explain the concept of hash functions along with its requirement and security also describe secure hash algorithm (SHA).

6. Explain following in detail.

   a. HTTPS and SSH.

   b. SSL architecture and protocol.

Part - C

(Descriptive/Analytical/Problem Solving/Design Questions)

Attempt any **two** questions **(2×15=30)**

1. Explain Rabin Cryptosystem, Elgamal cryptosystem and Elliptic curve cryptosystem in detail.

2. What are Message Authentication codes. Explain MACs based on Hash functions and MACs based on Block ciphers in detail.

3. What is Symmetric key distribution? How it can be achieved using symmetric and Asymmetric encryptions also explain concept of public key infrastructure.