

6E1553

Total No. of Questions : 14

Total No. of Pages : 04

Roll No. :

6E1553

B.Tech. VI-Sem. (Back) Exam. - 2024

COMPUTER SCIENCE AND ENGG.

6CS4-03 Information Security System

CS, IT

Time : 2 Hours

Maximum Marks : 80

Note : Attempt all 5 questions from Part-A, 04 questions out of 06 questions from Part-B and 02 questions out of 03 questions 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)

1.

2.

ersahilkagyan.com

PART-A

[5×2=10]

(Answer should be given up to 25 words only)

All questions are compulsory

Q.1. What is Cryptography?

- Q.2. Explain the three Security Principles.
- Q.3. Define Security. What are the multiple layers of security?
- Q.4. What are the function of Information Security?
- Q.5. List down different Modes of operation.

PART-B

[4×10=40]

(Analytical/Problem solving questions)

Answers should be given up to 100 words only

Attempt any four questions

- Q.1. What are the basic difference between Passive and Active attacks?
- Q.2. Explain the concept of MAC and its function.
- Q.3. Explain Symmetric and Asymmetric authentication.
- Q.4. Write short notes on the following:
- (a) IP Security Architecture
 - (b) Authentication Header
- Q.5. Why is SSL important?
- Q.6. What is MD5?

PART-C

[2×15=30]

(Descriptive/Analytical/Problem Solving/Design Questions)

Attempt any two questions

- Q.1. What is Digital Signature? List the security provided by Digital Signature. Explain its uses with help of an example.

Q.2. Explain the principal of RSA Algorithms. In an RSA system it is given that

$p = 4, q = 12, e = 8, M = 5$. Find Cipher-text C and M from decryption.

Q.3. What is Cryptanalysis? Explain the Substitution and Transposition Cryptographic Techniques.