B.Sc. Semester -VI Examination, 2023-24

COMPUTER SCIENCE (Honours)

Course ID : 61516 Course Code : SH/CSC/603/DSE-3

Course Title : Information Security

Time: 1 Hour 15 minutes Full Marks : 25

The figures in the right-hand margin indicate marks.

Candidates are required to give their answer in their own words as far as practicable

Answer all the questions.

Unit – I

1. Answer any five (5) of the following questions: 1×5 = 5

a) Write two critical characteristic of information.

b) What do you mean by decryption?

c) What is firewall?

d) Write a difference between virus and worm.

e) What is spoofing?

f) Define digital signature

g) What is phishing attack?

h) What is residual risk?

Unit – II

2. Answer any two (2) of the following questions: 5×2 = 10

a) Explain goals of using Information Security. What is MAC? 4 + 1

b) The decryption key in a transposition cipher is (6,2,1,5,3,4). Find the encryption key. Explain the rail

fence cipher with suitable example. 2 + 3=5

c) Write two differences between symmetric key and asymmetric key encryption algorithm. With suitable diagram explain the key generation process of DES encryption algorithm (no table is required). 2+3=5

d) Distinguish between DoS and DDoS attack. For a multiplicative cipher encryption key is 11. Find out the decryption key. What do you mean by cryptanalysis? 2+1+2=5

Unit – III

3. Answer any one of the following questions: 10×1=10

a) Describe HMAC algorithm. Comment on the security of HMAC. 4 + 6

b) Distinguish between a modern and a traditional symmetric key cipher. Define a P-Box. Explain its three variations with suitable example. Which variation is invertible? 3 + 2 + 3 + 2