

B.Sc. Semester-VI Examination, 2022-23**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 answers in their own words as far as practicable.***Answer all the questions.****UNIT-I**

1. Answer any **five** of the following questions:

 $1 \times 5 = 5$

- a) What is steganography?
- b) What do you mean by impersonation attack?
- c) What is watermarking?
- d) What is the main difference between substitution cipher and transposition cipher?
- e) What is traffic padding?
- f) What do you mean by product cipher?
- g) What is the basic difference between Feistel cipher and non-Feistel cipher?
- h) What is proxy firewall?

[Turn Over]

UNIT-II

2. Answer any **two** of the following questions:

$$5 \times 2 = 10$$

- a) Explain the concepts of Confusion and Diffusion.
- b) Explain the working principle of Feistel Cipher.
- c) Explain in brief the concepts of replay attack and repudiation. Which security goal is threatened by these two attacks? $(2+2)+1=5$
- d) What is meant by IP spoofing? What is fishing?

$$2\frac{1}{2} + 2\frac{1}{2} = 5$$

UNIT-III

3. Answer any **one** of the following questions:

$$10 \times 1 = 10$$

- a) Describe HMAC algorithm. How does HMAC is different from other cryptographic Hash functions? $6+4=10$
- b) What is firewall? Briefly explain possible attacks and countermeasures on a packet filtering firewall. $3+7=10$