No. of Questions	5
No. of Pages	3

UNIVERSITY OF SRI JAYEWARDENEPURA

Faculty of Technology

Bachelor of Information and Communication Technology Honours Degree

Academic Year 2021/2022

Third Year Second Semester Examination - April 2024

ITC3093 Computer Security

Duration: Three (3) Hours

Read and follow the instructions given below:

- This paper contains five (5) questions in three (3) pages.
- **"Index number"** should be written on top of each page of the answer script, and pages must be **numbered appropriately**.

Question 1 **[20 Marks]**

a) Define Information Security and briefly explain its primary objectives. [5 Marks]

b) Enumerate and explain the three main pillars of Information Security. Provide an example for each. [5 Marks]

c) Differentiate between a threat and vulnerability in the context of Information Security. Provide an example for each. [5 Marks]

d) What countermeasures can be taken to protect your computer from malware and attacks? Explain with examples. [5 Marks]

Question 2 **[20 Marks]**

a) Briefly explain the difference between stream cipher and block cipher? [5 Marks]

b) Distinguish the following with examples [5 Marks]

I. Cryptography vs. Cryptanalysis
II. Intrusion Detection System (IDS) vs. Intrusion Prevention System (IPS)

c) Do you think attempting to break into (that is to, obtain access or use of) a computing system without authorization should be illegal? Defend your answer. [5 Marks]

d) Discuss the security challenges of using pirated operating systems in terms of computer security? [5 marks]

Question 3 **[20 Marks]**

a) Differentiate between Active Attacks and Passive Attacks in computer systems with illustrations. [4 Marks]

b) What are the 3 factors that come under multi-factor authentication and provide examples for each. [6 Marks]

c) Differentiate between Symmetric and Asymmetric encryption algorithms. Provide an example for each. [4 Marks]

d) Briefly explain how each of the following characteristics is achieved using digital signature. [6 marks]

- Authenticity
- Integrity
- Non-repudiation

Question 4 **[20 Marks]**

a) "Hash function is used to protect the information in a computer system". Briefly explain how hash functions protect information by ensuring integrity in brief. [6 Marks]

b) Answer the following questions about Digital Certificates (DC). [5 Marks]

I. Illustrate and explain the method of generating a digital certificate with the CA and RA.

II. List down and explain the challenges of using digital certificates.

c) Examine the role of a Certificate Authority (CA) and Registration Authority (RA) in securing information. [4 Marks]

d) "Some encryption algorithms are theoretically breakable but practically unbreakable". [5 Marks]

I. Do you agree with this statement?

II. Justify your answer with an example.

Question 5 **[20 Marks]**

a) Using the shift (or caesar) Cipher, encrypt the text "ATTACKATONCE" using the shift value 7. [5 Marks]

b) Illustrate the working principle of transposition Cipher. with an example. [5 Marks]

c) Encrypt the message "CRYPTOLOGY" using the Vigenère cipher with the keyword "KEY" and provide the cipher text. Show your calculation. [5 Marks]

d) Define phishing attacks and discuss common indicators that can help identify phishing attempts. [5 marks]

*****End of the Question Paper*****