UNIVERSITY OF SRI JAYEWARDENEPURA

Faculty of Technology

Bachelor of Information and Communication Technology

Year III Semester II Examination – February/March 2020

ITC 3093 – Principles of Computer Security

Time allowed: **THREE (3)** hours

Answer **ALL** questions

1 a. What is meant by *computer security*? **[5 marks]**

b. Write short explanations for the following topics. **[5 marks]**

i. Threat

ii. Vulnerability

iii. Attack

iv. Risk

c. Differentiate between amateur criminals, crackers, and career criminals. **[5 marks]**

d. Do you think attempting to break into (that is to, obtain access or use of) a computing system without authorization should be illegal? Why or why not? **[5 marks]**

2 a. Why is data encryption important in data communications? **[5 marks]**

b. Distinguish the following topics. **[5 marks]**

i. Cryptography vs. Cryptology

ii. Active vs. Passive Attacks

c. List down five major objectives of information security. **[5 marks]**

d. What weaknesses of private key encryption can be addressed by public key encryption? **[5 marks]**

3 a. What is the difference between stream cipher and block cipher? [5 marks]

b. Calculate the number of private keys needed if six (6) users are communicating with each other. [5 marks]

c. Explain the public key encryption process with the support of a suitable diagram. [5 marks]

d. *Digital signature is an important entity in public key cryptography.* Do you agree with this statement? Justify your answer. [5 marks]

4. a. List down four major characteristics of a Hash function. [5 marks]

b. Explain the process of challenge response authentication. [5 marks]

c. Explain how a user (Alice) starts a secure communication with another user (Bob) with the support of a Key Distribution Center (KDC). [5 marks]

d. What are the good practices of selecting a password for an electronic mail account access through the Internet? [5 marks]

5. a. Compare *viruses* and *worms* in the context of computer security. [5 marks]

b. What measures can be taken to protect your computer from malware and attacks? [5 marks]

c. *Some encryption algorithms are theoretically breakable but practically unbreakable.* Do you agree with this statement? Justify your answer. [5 marks]

d. What are the disadvantages of using pirated operating systems in terms of computer security? [5 marks]

--- End of the paper ---