Riara University

UNIVERSITY EXAMINATIONS

EXAMINATION FOR SEPTEMBER/DECEMBER 2019/2020 FOR BACHELOR OF SCIENCE IN COMPUTER SCIENCE

COURSE CODE: **RCS 402** COURSE TITLE: **CRYPTOGRAPHY AND INFORMATION SECURITY**

DATE: ____________________ TIME: 2 HOURS

GENERAL INSTRUCTIONS:

Students are NOT permitted to write on the examination paper during examination time.

This is a closed book examination. Text book/Reference books/notes are not permitted.

SPECIAL INSTRUCTIONS:

This examination paper consists Questions in Section A followed by section B.

Answer **Question 1 and any Other Two** questions.

QUESTIONS in ALL Sections should be answered in answer booklet(s).

1. **PLEASE start the answer to EACH question on a NEW PAGE.**
2. **Keep your phone(s) switched off at the front of the examination room.**
3. **Keep ALL bags and caps at the front of the examination room and DO NOT refer to ANY unauthorized material before or during the course of the examination.**
4. **ALWAYS show your working.**
5. **Marks indicated in parenthesis i.e. ( ) will be awarded for clear and logical answers.**
6. **Write your REGISTRATION No. clearly on the answer booklet(s).**
7. **For the Questions, write the number of the question on the answer booklet(s) in the order you answered them.**
8. **DO NOT use your PHONE as a CALCULATOR.**
9. **YOU are ONLY ALLOWED to leave the exam room 30minutes to the end of the Exam.**
10. **DO NOT write on the QUESTION PAPER. Use the back of your BOOKLET for any calculations or rough work.**

QUESTION ONE (30 Marks)

a) Define the following terms **(3 Marks)**
   i) Work factor
   ii) Cryptography
   iii) Initialization vector

b) Most emerging threats to computer systems are categorized into two distinct categories: Passive and Active. Briefly describe their differences and cite examples. **(4 Marks)**

c) Discuss the goals of cryptography **(6 Marks)**

d) Secure Hash function is a collision-resistant, one way function. Explain. **(4 Marks)**

e) Discuss the following intrusion Detection mechanisms **(6 Marks)**
   i) NIDS
   ii) HIDS
   iii) Signature based

f) Let p = 17 and q = 11. Find the encryption and decryption keys. Choose your encryption key to be at least 5. Show the encryption and decryption for Plaintext 6 **(7 Marks)**

QUESTION TWO (15 Marks)

a) Security best practices are security guidelines and policies aimed at enhancing system security. Briefly explain **FIVE** components of a good security policy for protecting an organization’s technology and information assets. **(10 Marks)**

b) Discuss a Sampled Model of Symmetric Encryption. **(5 Marks)**

QUESTION THREE (15 Marks)

a) What is PKI? Why is it so important in information security? **(3 Marks)**

b) Define a digital signature in information security systems and explain how it is generated. **(8 marks)**

c) Differentiate between stream cipher and block cipher stating example for each **(4 marks)**

QUESTION FOUR (15 Marks)

a) Discuss THREE ways under which ciphers can be classified **(6 Marks)**

b) Describe TWO reasons why an effective intrusion detection system is needed in a company **(4 Marks)**

c) Sketch a simple diagram to illustrate how smurf attack is propagated. **(5 Marks)**

QUESTION FIVE (15 Marks)

a) Discuss the basic components of cryptography. **(5 Marks)**

b) Explain the main characteristics of the Kerberos authentication scheme **(5 Marks)**

c) With aid of a diagram, describe how bastion router is used to provide security and explain how it is different from a firewall. **(5 Marks)**