RAJARATA UNIVERSITY OF SRI LANKA
FACULTY OF APPLIED SCIENCES

B.Sc. (Information and Communication Technology) Degree
Third Year - Semester I Examination – September/October 2019

ICT 3303 – INFORMATION SYSTEMS SECURITY

Time: Three (3) hours

Answer **ALL** the questions

1. a) Briefly explain the three security objectives for information and information systems. [6 Marks]

b) Consider an online internet banking system in which users provide a password and account number for account access. Give examples for two of the three security objectives associated with the system. [4 Marks]

c) Distinguish between data integrity and system integrity. [4 Marks]

d) Briefly explain the following functional requirements of information security.

i. Configuration Management.

ii. Contingency Planning.

iii. Incident Response. [6 Marks]

2. a) What is the difference between a threat and a threat agent? Give an example. [5 marks]

b) "Employees are one of the greatest threats to information security in an organization". Do you agree with this statement? Justify your answer. [5 marks]

c) What are the threats to the availability of software assets in an information system? [4 marks]

d) Briefly explain the following threat actions that cause disruption threat consequences.

i. Incapacitation.

ii. Corruption.

iii. Obstruction. [6 marks]

3. a) Distinguish between cryptography and steganography. [4 marks]

b) What are the differences between an unconditionally secure cipher and a computationally secure cipher? [4 marks]

c) What is a monoalphabetic substitution cipher? Give an example to illustrate a monoalphabetic substitution cipher. [6 marks]

d) Using the Vigenère cipher, encrypt the word "mechanical" using the key "hat". [6 marks]

4. a) What are the roles of the public key and the private key of a public-key cryptosystem? [4 marks]

b) In the context of public-key cryptography, briefly explain the following terms.

i. Secure message format.

ii. Digital signature. [4 marks]

c) Explain how authentication and integrity are provided by a public-key cryptosystem. [6 marks]

d) What is the purpose of Diffie-Hellman algorithm? Explain how it works using an example. [6 marks]

5. a) Parity bits are used in protocols to detect modifications in streams of bits as they are passed from one computer to another, but they can usually detect only unintentional modifications. Explain why parity bits cannot identify intentional modifications in a message. [4 marks]

b) Briefly explain the following terms:

i. Message digest.
ii. One-way hash.
iii. Message authentication. [6 marks]

c) List the steps involved in a hashing process that can be used to verify data integrity. [6 marks]

d) Does HMAC provide confidentially and non-repudiation? Explain your answer. [4 marks]

--- END ---