RAJARATA UNIVERSITY OF SRI LANKA
FACULTY OF APPLIED SCIENCES

Bachelor of Science in Applied Sciences
Third Year - Semester I Examination – July / August 2023

COM 3204 – INFORMATION SECURITY

Time: Two (02) hours

Instructions

- Answer <u>**ALL**</u> questions.
- This paper contains **four (04)** questions in **two (02)** pages.

1. a) "The NIST definition of Computer Security introduces three key objectives, which should be guaranteed in any kind of secure system." Briefly explain them.

(6 marks)

b) Distinguish between authenticity and accountability.

(5 marks)

c) "Computer security is essentially a battle of wits between a perpetrator who tries to find holes and the designer/administrator who tries to close them." Do you agree with this statement? Explain.

(5 marks)

d) Briefly explain the following functional requirement areas that primarily involve management controls and procedures to reduce vulnerabilities and to deal with threats to system assets in information systems.

i. Contingency planning.

ii. Physical and environmental protection.

iii. Personnel security.

(9 marks)

96

2. a) List four (04) possible security failures reflected by the vulnerabilities in sending a message from a sender to a recipient through a transmission medium.

(4 marks)

b) Comment on the followings with respect to cryptosystems:

i. Cleartext and ciphertext.

ii. Authentication and authorization.

(6 marks)

c) Find the Vigenère cipher of the following plain text using only the uppercase letters of the English alphabet and the given key.

Plain text: Information Security

Key: Computer

(9 marks)

d) Briefly explain Triple-DES and its four (04) modes of operation.

(6 marks)

3. a) Name and briefly explain the essential ingredients of an asymmetric-key encryption scheme.

(6 marks)

b) Explain the use of public key cryptosystems if confidentiality is the most important security service to a sender.

(5 marks)

c) What requirements must a public key cryptosystem fulfill to be a secure algorithm? Give at least four (04) requirements.

(8 marks)

d) Briefly explain the main purpose of the following asymmetric algorithms:

i. Diffie-Hellman algorithm.

ii. RSA algorithm.

(6 marks)

4. a) What is a one-way hash function? List four (04) basic requirements for a strong cryptographic hash function.

(6 marks)

b) Explain a possible attack against one-way hash functions.

(4 marks)

c) What are the steps involved in a hashing process that can be used to verify data integrity?

(7 marks)

d) What is message authentication code (MAC)? Briefly explain the steps involved in Cipher Block Chaining MAC.

(8 marks)

--- End ---