RAJARATA UNIVERSITY OF SRI LANKA
FACULTY OF APPLIED SCIENCES

B.Sc. (General) Degree in Applied Sciences
Third Year - Semester I Examination – June/July 2018

COM 3204 – INFORMATION SECURITY

Time: Two (2) hours

Answer All questions

Q1. (a) What are the three components of the CIA triad? Briefly explain each of them. [9 Marks]

(b) Consider an automated teller machine (ATM) in which users insert a card and provide a personal identification number (PIN) for account access. Give an example for two of the CIA components associated with the system. [5 Marks]

(c) Distinguish between authenticity and accountability. [5 Marks]

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

i. Awareness and Training.

ii. Audit and Accountability. [6 Marks]

Q2. (a) Distinguish between vulnerability and threat. [6 marks]

(b) Explain the different categories of vulnerabilities of a computer system or network asset. [6 marks]

(c) What are the differences between passive and active security attacks? [4 marks]

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

i. Masquerade.

ii. Falsification.

iii. Repudiation. [9 marks]

Q3. (a) List the essential ingredients of a symmetric encryption scheme. [5 marks]

(b) What are the differences between a substitution cipher and a transposition cipher? [4 marks]

(c) Explain Caesar Cipher encryption algorithm with an example. [8 marks]

(d) Use Playfair cipher to encrypt the message "Rajarata" with the key "monarchy". [8 marks]

Q4. (a) Briefly explain the following DES modes.

i. Electronic Code Book (ECB).

ii. Cipher Block Chaining (CBC). [6 marks]

(b) What is the difference between *secure message format* and *open message format* in asymmetric encryption? [4 marks]

(c) Briefly explain the following components that are required for the operation of PKI.

i. Certificate Authorities.

ii. Registration Authorities. [6 marks]

(d) What is the difference between a digital signature and a digital certificate? [4 marks]

(e) Explain how Kerberos mitigate the security risks such as man-in-the-middle attacks. [5 marks]

END