RAJARATA UNIVERSITY OF SRI LANKA
FACULTY OF APPLIED SCIENCES

B.Sc. (General) Degree
Third Year Semester II Examination April/May 2016

COM 3204 - INFORMATION SECURITY

Time Allowed: 2 hours.

INSTRUCTIONS TO CANDIDATES

- This paper contains **FIVE (05)** questions on **three (03)** pages including this page.
- Answer ANY **FOUR (04)** questions.
- This examination accounts for 60% of the course assessment. The total maximum mark attainable is 100. The marks assigned for each question and section, thereof are indicated in square brackets.
- This is a closed book examination.
- Mobile phones or any other communication devices are not permitted.
- Clearly state the assumptions you make. If you have any doubts regarding the interpretation of the wording of a question, make your own decision, but clearly state it on the script.

1 (a) Explain why we have to make tradeoffs when considering security mechanisms for the following scenarios.

(i) Implementing a website for your faculty which would show news, announcements, notices, history of the faculty, achievements, etc.

(ii) Implementing an internal inventory management system for a shop. This system will not connect to the Internet.

[5x2 marks]

(b) Explain the term "Business Continuity Planning".

[3 marks]

(c) What is "vulnerability"? Explain.

[4 marks]

(d) Explain the difference between "Due Care" and "Due Diligence" with respect to security of information systems and explain their impact.

[6 marks]

(e) Explain why "Risk Management" is required for Information Security.

[2 marks]

2 (a) Write short definitions for the following terms.

(i) Cryptosystem
(ii) Key space
(iii) Cryptology
(iv) Cryptanalysis

[1.5x4 marks]

(b) Explain why "Polyalphabetic Ciphers" are better than "Monoalphabetic Ciphers".

[3 marks]

(c) Explain the difference between "Substitution Ciphers" and "Transposition Ciphers".

[3 marks]

(d) Explain the advantages and disadvantages of Asymmetric cryptosystems.

[4 marks]

(e) Explain the advantages and disadvantages of Symmetric cryptosystems.

[4 marks]

(f) Define and explain the effects of "Confusion" and "Diffusion".

[5 marks]

3 (a) Explain the operation and the features of a strong "Stream Cipher".

[6 marks]

(b) Explain the operation and the advantages of "Hybrid Encryption" over other cryptosystems.

[4 marks]

(c) Name and describe **three (03)** modes of operations of DES.

[3x3 marks]

(d) Describe what are "Hash Functions" and their significance to Information Security.

[6 marks]

4 (a) Explain how "Digital Signatures" will be used in a Asymmetric Cryptosystem. You may use diagrams.

[6 marks]

(b) Explain the steps involved in "PKI" using a diagram. Define the components which are involved in PKI (e.g.: RA's, CA's, etc.)

[12 marks]

(c) Discuss the advantages and disadvantages of "Kerberos".

[4 marks]

(d) Explain what a "Computer assisted crime" is.

[3 marks]

5 (a) Explain how the employees' privacy can be ensured when the employee is using company/organizational information systems.

[5 marks]

(b) Describe **two (02)** factors that need to be considered in Facility Selection.

[2x2 marks]

(c) Describe **four (04)** factors that need to be considered in Server Room construction.

[2x4 marks]

(d) Describe the steps and mechanisms that you would take to solve electrical power issues that may affect the facility that you are constructing.

[8 marks]