



**RAJARATA UNIVERSITY OF SRI LANKA
FACULTY OF APPLIED SCIENCES**

**B.Sc. (General) Degree
Third Year - Semester I Examination - Nov./Dec. 2016**

COM 3204 - INFORMATION SECURITY

Time: Two (02) hours

- 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 80. 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) Describe why people are considered the weakest link in security. [5 mark]
- b) Explain why the following statement is true.
"Perfect security does not exist." [6 marks]
- c) Briefly explain the following security principles.
 - Secure the Weakest Link
 - Fail Securely
 - Be reluctant to trust
 [3x3 marks]
2. a) "A cryptosystem can be created to work only using asymmetric algorithms (without using any symmetric algorithms)."

What is your opinion about the above statement and its practicality? [5 marks]
- b) Assume that you are working for an IT company which is developing a proprietary software product that needs to be secure. The source code of the software should be a secret and you need to protect your product against any internal threats. You sell your product and service through the Internet.

Describe how you would achieve **CIA** in the above scenario. [5x3 marks]
3. a) Compare and contrast "Block Ciphers" with "Stream Ciphers". [6 marks]
- b) Briefly explain the weakness of the original DES algorithm. [4 marks]
- c) Briefly explain the role of "Symmetric Key Algorithms" in "Public Key Cryptosystems". Discuss what happens if the "Symmetric Key Algorithm" is weak. [2+2 marks]
- d) Briefly explain the concept of "Non-Repudiation" with its relationship to the modern digital world. [6 marks]
4. a) Describe why "Monopoly Model" in PKI is difficult to be used widely in the World Wide Web. [6 marks]
- b) Compare and contrast CA's and RA's in PKI. [4 marks]

This question continues in the next page...

- c) Explain why Kerberos protocol uses “time” in the “Authenticator” in the “Ticket”.
[3 marks]
 - d) Describe the differences between Public and Private Keys in a cryptosystem.
[4 marks]
 - e) Describe the use of a “Certificate Revocation List” used by CA’s.
[3 marks]
5. a) Describe how employee privacy will affect the “Internet Usage Policy” of an organization.
[5 marks]
- b) Assume that the organization has undergone a cyber-attack that requires the help of the criminal justice system. What would be the responsibilities of the internal Incident Response Team in this situation?
[5 marks]
 - c) Describe the importance of the “Follow-up Stage” in the Incident Response Procedures.
[5 marks]
 - d) Describe two (02) weaknesses in “Firewalls”.
[5 marks]

END