72

RAJARATA UNIVERSITY OF SRI LANKA

FACULTY OF APPLIED SCIENCES

B.Sc. (General) Degree

Third Year Semester II Examination, September/October 2014

COM 3204 – INFORMATION SECURITY

Time allowed: 2 hours

INSTRUCTIONS TO CANDIDATES

- This paper consists of five (05) questions on 3 pages including this page.
- Answer **ANY FOUR (04)** questions.
- This examination accounts for 60% of the module 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)** Security level that should be provided by an information system depends on the type of information it processes, stores and communicates. It is stated that "the security level of an information system depends on how far the information system is capable of achieving CIA".

   Explain what mechanisms should be integrated in to an information system to ensure achieving CIA. In your answer, you need to consider the aspects of CIA and how they relate to the aspects such as processing, storing and communicating. You may take an information system of your choice as an example to elaborate your answer.

   [12 marks]

   (b) What role should a server administrator play in ensuring the security of an information system? Think of the activities that a server administrator should carry out and how an operating system of a server need to be maintained.

   [8 marks]

2. **(a)** Discuss why an IT security policy prepared for the purpose of general staff of an organisation may not be adequate to be followed by the staff of the IT Division of that organisation. In you discussion, you need to consider the security controls that may be enforced in an IT security policy.

   [8 marks]

   (b) Prepare an IT security policy outline for the IT Division of a bank. Your outline should be well structured with necessary sub-sections.

   [12 marks]

3. **(a)** Using Vigenere cipher as an example, show how the concepts used in a weak mono-alphabetic cipher can be improved to have a stronger encryption.

   [8 marks]

   (b) Using block diagrams to illustrate necessary steps, outline the operation of DES. Necessary transformations and other operations need to be indicated in the diagram.

   [8 marks]

   (c) What is Cipher Block Chaining? Use diagrams to explain your answer.

   [4 marks]

4. **(a)** Briefly explain four (04) components that are required for the operation of PKI.
[8 marks]

(b) Consider a web-based e-commerce application that requires secure information processing and transfer. Explain how PKI can be used to ensure the authenticity and confidentiality of transactions that take place in such an application. Consider a real-life example to illustrate your answer.
[12 marks]

5. **(a)** Outline the operation of Kerberos authentication protocol, highlighting the important aspects of the protocol and the components required for the Kerberos implementation.
[8 marks]

(b) Time is an important factor for the operation of Kerberos. Explain why. Consider Kerberos protocol steps where current time, life-time of tickets, etc., are used.
[6 marks]

(c) While Kerberos, PKI, etc., need a trusted third party, PGP follows a different trust model. Explain how PGP can be used to make e-mail communications trustworthy in a distributed commercial organisational environment.
[6 marks]