RAJARATA UNIVERSITY OF SRI LANKA
FACULTY OF APPLIED SCIENCES

B.Sc. (General) Degree
Third Year Semester I Examination Oct./Nov. 2015

COM 3204 INFORMATION SECURITY

Time Allowed: 2 hours.

INSTRUCTIONS TO CANDIDATES

- This paper contains **FIVE** (05) questions on 3 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) Explain why it is difficult to say whether a program is secure.

[4 marks]

(b) How would you practice "defense in depth" in the following scenario.

Assume that you are the network administrator for a departmental network which is a part of a larger company network. Your access to the Internet and to the outside networks has to pass through the larger company network and its proxy servers.

[6 marks]

(c) Assume that you are hired as an outside consultant to write a security policy for a computer laboratory in a University. The policy is intended for the use of the technical officer and other technical staff who maintain the laboratory. Considering standards, baselines and guidelines, prepare the security policy for this computer laboratory.

[10 marks]

2 (a) In cryptographic algorithms it is emphasized that the "key" should be a random variable. Explain the importance of having a random key while considering the consequences if the key is not random.

[6 marks]

(b) Describe how "one time pad" works and why it has been the choice for highly confidential communications.

[4 marks]

(c) What do you understand by the term "Cryptanalysis"?

[2 marks]

(d) Describe why both symmetric and asymmetric cryptosystems are required for the communication of web based applications.

[8 marks]

3 (a) Briefly explain Triple-DES and its four modes of operation.

[6 marks]

(b) Describe how the Diffie-Hellman cryptosystem works using diagrams. Also explain why it is susceptible to man in the middle attacks.

[8 marks]

(c) Briefly describe what is a "digital signature", and how and why it is used.

[4 marks]

(d) Briefly describe what is a "Birthday attack" in relation to hash functions.

[2 marks]

4 (a) Briefly describe four (04) PKI trust models.

[8 marks]

(b) Explain how Kerberos mitigate the security risks such as man-in-the-middle attacks.

[4 marks]

(c) Explain the legal considerations of why a private organization such as a life insurance company which keeps private records of its clients' personal information should take "due care" of those information.

[4 marks]

(d) Describe why it is important to have an "incident response team" for an organization.

[4 marks]

5 (a) Explain why IPSec would not offer much protection against insider attacks.

[4 marks]

(b) Explain how Trapdoors are different from Logic Bombs.

[4 marks]

(c) Explain the use and purpose of a "PGP Key Ring".

[4 marks]

(d) Assume that you are a law enforcement investigator who is focused on stopping software piracy. Explain how you would use a honeypot for that purpose.

[4 marks]

(e) Describe how Audit records are important when detecting intruders.

[4 marks]