03

RAJARATA UNIVERSITY OF SRI LANKA

FACULTY OF APPLIED SCIENCES

Department of Physical Sciences

B.Sc. (General) Degree

Third Year – Semester II Examination

COM 3204 – INFORMATION SECURITY

Time allowed: 3 hours

September 2013

INSTRUCTIONS TO CANDIDATES

- This paper consists of six (06) questions on 4 pages including this page.
- Answer **ANY FIVE (05)** questions.
- This examination accounts for 60% of the module 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.

Q1 (a) "Information security can be defined in terms of **C**, **I** and **A**". What does this statement mean?

Note: In your answer, you first need to define the terms referred to by C, I and A, and then provide the meaning of the statement.

[1x3 + 4 marks]

(b) Not all computer programs are secure. What kind of a computer program is considered to be a secure program? Explain with examples.

[8 marks]

(c) Explain the principle of "least privilege". Use an organisational application as an example in your explanation.

[5 marks]

Q2 (a) With respect to information security, what is a "risk"? Briefly explain.

[3 marks]

(b) In an organisation, who are the people responsible for information security?

Note: Using the administrative structure of an organisation of your choice, explain your answer.

[8 marks]

(c) Discuss the similarities and differences between an "information security standard" and an "information security policy of an organisation".

[9 marks]

Q3 (a) What is the difference between a substitution cipher and a transposition cipher?

[3 marks]

(b) What is the difference between a mono-alphabetic cipher and a poly-alphabetic cipher?

[3 marks]

This question continues in the next page

(c) The algebraic representation of Vigenere Cipher can be stated as:

Encryption: $C_i = (P_i + K_i) \bmod 26$

Decryption: $P_i = (C_i - K_i) \bmod 26$

C, P and K have their usual meanings: cipher text, plain text and key.

Explain how a string of characters can be encrypted using Vigenere cipher.

Hint: Consider how Vigenere Cipher is practically implemented..

[14 marks]

Q4 **(a)** What are the differences between symmetric crypto systems and asymmetric crypto systems?

Note: use labelled diagrams to illustrate the operation of both crypto systems in order to show the differences.

[6 marks]

(b) Explain the following:

i. block cipher

ii. stream cipher

[2x4 marks]

(c) What is "hybrid encryption"? Briefly explain.

[4 marks]

(d) What is the purpose of using hybrid encryption?

[2 marks]

Q5 **(a)** Outline the DES algorithm.

Note: you may use block diagrams. It is not necessary to explain the details. Only the operational aspects need to be outlined.

[8 marks]

(b) Argue for or against the statement: "Triple-DES is a stronger encryption scheme than DES".

Hint: outline the operation of Triple-DES in order to argue.

[6 marks]

(c) Why do we consider a hash function to be a "non reversible" or a "one way" function?

[6 marks]

Q6 (a) What is a "digital signature"?

[3 marks]

(b) Explain how public key infrastructure (PKI) is used for secure information exchange.

Note: in your explanation, briefly explain the components of PKI. Use diagrams where necessary.

[10 marks]

(c) Outline the operation of Kerberos authentication protocol.

Note: you need to highlight only the main points and components. No details are required. Use diagrams where necessary.

[7 marks]