UNIVERSITY OF COLOMBO, SRI LANKA

UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY (EXTERNAL)
Academic Year 2010/2011 – 3rd Year Examination – Semester 5

IT5203: Security of Information Systems

Structured Question Paper
12th March, 2011
(TWO HOURS)

To be completed by the candidate

BIT Examination Index No: ....

Important Instructions:

- The duration of the paper is **2 (Two) hours**.
- The medium of instruction and questions is English.
- This paper has **4 questions** and **12 pages**.
- **Answer all 4 questions.** (all questions **do not** carry equal marks)
- **Question 1 (**40% marks**) and other questions (**20% marks**).**
- **Write your answers** in English using the space provided **in this question paper**.
- Do not tear off any part of this answer book.
- Under no circumstances may this book, used or unused, be removed from the Examination Hall by a candidate.
- Note that questions appear on both sides of the paper.
  If a page is not printed, please inform the supervisor immediately.
- **Non-programmable Calculators may be used**

Questions Answered

Indicate by a cross (×), (e.g. ☒) the numbers of the questions answered.

	Question numbers				
To be completed by the candidate by marking a cross (×).	1	2	3	4	
To be completed by the examiners:					

Index No: ………………..

1) **Answer each question as true or false, and then justify your answers with at most one sentence.**

(a) Vernam cipher is immune to most cryptanalytic attacks.

(02 marks)

ANSWER IN THIS BOX

(b) According to Shannon, the implementation of the encryption process should be as complex as possible.

(02 marks)

ANSWER IN THIS BOX

(c) The columnar transposition and other transposition ciphers are examples of block ciphers.

(02 marks)

ANSWER IN THIS BOX

(d) The triple DES procedure is defined as C = E(k1, E(k2, D(k1,m))). That is, you encrypt with one key, decrypt with the second and encrypt again with the first key.

(02 marks)

ANSWER IN THIS BOX

(e) The AES algorithm as defined can use 56 or 128 bits keys.

(02 marks)

ANSWER IN THIS BOX

(f) A symmetric key system with six (6) users requires 15 keys and each user must track and remember a key for each other user with which he or she wants to communicate.

(02 marks)

ANSWER IN THIS BOX

(g) A public key and a user's identity are bound together with a private key which is issued by an entity called a certificate authority.

(02 marks)

ANSWER IN THIS BOX

(h) The Euclidean algorithm is a procedure for computing the Hash value of a message.

(02 marks)

ANSWER IN THIS BOX

(i) A logic bomb is a class of malicious code that "detonates" or goes off when a specified condition occurs.

(02 marks)

ANSWER IN THIS BOX

(j) A virus spreads copies of itself as a stand-alone program, whereas a worm spreads copies of itself as a program that attaches to or embeds in other programs.

(02 marks)

ANSWER IN THIS BOX

(k) An access control matrix is a table in which each row represents a subject and each column represents an object.

(02 marks)

ANSWER IN THIS BOX

(l) A “security model” is a statement of the security we expect the system to enforce.

(02 marks)

ANSWER IN THIS BOX

(m) Web sites use cookies to avoid a customer having to log in on each visit to a site; these cookies may contain the user's ID and password.

(02 marks)

ANSWER IN THIS BOX

(n) “Integrity” refers to a way to infer or derive sensitive data from non-sensitive data.

(02 mark)

ANSWER IN THIS BOX

(o) Lampson constructed a security model for preventing inappropriate modification of data.

(02 mark)

ANSWER IN THIS BOX

(p) RSA algorithm can be used for signing and encryption.

(02 mark)

ANSWER IN THIS BOX

(q) A packet filtering firewall maintains state information on each packet in the input stream.

(02 mark)

ANSWER IN THIS BOX

(r) An Intrusion Detection System (IDS) can be network based or host based.

(02 mark)

ANSWER IN THIS BOX

(s) The principal difference between Secure Multipurpose Internet Mail Extensions (S/MIME) and Pretty Good Privacy(PGP) is the method of key exchange.

(02 mark)

ANSWER IN THIS BOX

(t) The fundamental data structures of IPSec are the virtual private network header and the virtual private network payload.

(02 mark)

ANSWER IN THIS BOX

2) (a) Determine the greatest common divisor of 123309 and 9315?

(05 mark)

ANSWER IN THIS BOX

(b) Identify pairs of relatively prime numbers from among the following list.
(18,17), (27, 81), (13,39), (8,3), (16, 21)

(05 mark)

ANSWER IN THIS BOX

(c) Suppose we want to use the Diffie-Hellman Key Agreement protocol between two end points, A and B and have chosen the integer 3 as g and the integer 10 as the n. where g and n are as defined in the protocol. For the private key x and public key X, we have the relation

$$X = g^x \text{ mod } n.$$

If A generates the private key x=5 and B generates the private key y=6, what is the session key k between A and B?

(05 mark)

ANSWER IN THIS BOX

(d) Nimal and Kamal use the RSA algorithm to communicate. Nimal's public key = (n, e) = (33, 3) and private key = (n, d) = (33, 7). Nimal received an encrypted message C=26. What is the corresponding plain text M?

(05 mark)

ANSWER IN THIS BOX

3) (a) Using a schematic diagram, describe a symmetric key block cipher encryption mode that can produce a stream cipher.

(06 mark)

ANSWER IN THIS BOX

(b) Describe the two (2) problems associated with the one-time pad encryption method.

(04 mark)

ANSWER IN THIS BOX

.

(c) Authentication mechanisms use three(3) basic principles to confirm a user's identity. Briefly describe these three(3) basic principles.

(06 mark)

ANSWER IN THIS BOX

(d) List four (4) key features of a trusted operating system.

(04 mark)

ANSWER IN THIS BOX

4) (a) List five (5) fundamental user requirements for database security.

(05 marks)

ANSWER IN THIS BOX

(b) Briefly describe a typical "Host to Security Gateway" IPSec configuration method referring to an example.

(05 marks)

ANSWER IN THIS BOX

(c) Compare and contrast the issues of copyright, patent and trade secrets which are intended to provide protection by law, to data and programs.

(05 marks)

ANSWER IN THIS BOX

(d) Write down the steps that are necessary in order to create and execute a **signed** Java applet?

(05 marks)

ANSWER IN THIS BOX

****