UNIVERSITY OF COLOMBO, SRI LANKA

UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY (EXTERNAL)
Academic Year 2013/2014 – 3rd Year Examination – Semester 5

IT5204: Information Systems Security

Structured Question Paper
08th March, 2014
(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 **11 pages**.
- **Answer all 4 questions**. (All questions **do not** carry equal marks).
- **Question 1 (**40% marks**) and other questions (**20% marks each**)**.
- **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. [X]) 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) State whether each of the following statements are **true** or **false**, and then briefly justify your answer.

(a) The plain text P= "hello bit student" will be encrypted to the cipher text C = "khoor elw vwxghqwv" by the Cesar cipher.

(02 marks)

ANSWER IN THIS BOX

(b) The Advance Encryption Standard (AES) is an example of a stream cipher.

(02 marks)

ANSWER IN THIS BOX

(c) The Data Encryption Standard (DES) algorithm uses 128 bit data blocks.

(02 marks)

ANSWER IN THIS BOX

(d) A symmetric key with seven (7) users requires 7 keys and user must track and remember a key for each other user with whom he or she wants to communicate.

(02 marks)

ANSWER IN THIS BOX

(e) The Secure Hash Algorithm (SHA) can be used to implement a Message Authentication Code (MAC).

(02 marks)

ANSWER IN THIS BOX

(f) According to Kerckhoffs's principle, errors in ciphering should not propagate and cause corruption of further information in the message.

(02 marks)

ANSWER IN THIS BOX

(g) The Secure Electronic Transaction (SET) protocol is an example of a hybrid encryption protocol.

(02 marks)

ANSWER IN THIS BOX

(h) Electronic Code Book Mode converts a block cipher into a stream cipher.

(02 marks)

ANSWER IN THIS BOX

(i) In commercial security policy, data items are associated with a particular security level; while in a military security policy data items are associated by a set of programs permitted to manipulate it.

(02 marks)

ANSWER IN THIS BOX

(j) A zombie is a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems.

(02 marks)

ANSWER IN THIS BOX

(k) A trapdoor is a malicious computer program that can copy itself and infect a computer without the permission or knowledge of the owner.

(02 marks)

ANSWER IN THIS BOX

(l) A honey token is a memory protection method that can be used to prevent one program from affecting the data and programs in the memory space of other users.

(02 marks)

ANSWER IN THIS BOX

(m) The greatest common divisor of 46 and 68 is 1.

(02 marks)

ANSWER IN THIS BOX

(n) An Attribute Authority trusted by one or more users is to create and sign digital certificates.

(02 marks)

ANSWER IN THIS BOX

(o) (18, 7), (8, 5), (16, 3) are relatively prime numbers.

(02 marks)

ANSWER IN THIS BOX

(p) In a given information system, a password consist of uppercase characters of the English Alphabet and is of variable length from 1 to 4 characters. The system as a whole has 456976 passwords.

(02 marks)

ANSWER IN THIS BOX

(q) Suppose we want to use the Diffie-Hellman Key Agreement protocol between two end points, A and B, and we have chosen the integer 3 as g and the integer 13 as n. If A generates the private key x=5 and B generates the private key y=7, the session key k between A and B is 9.

(02 marks)

ANSWER IN THIS BOX

(r) Biba model is a multilevel security model, where a process can only read objects at its level or higher or can only write objects at its level or higher.

(02 marks)

ANSWER IN THIS BOX

(s) Database views ensure that data entered into the database is accurate, valid, and consistent.

(02 marks)

ANSWER IN THIS BOX

(t) In an inference attack, a user tries to determine values of sensitive fields in a database by seeking them directly through queries.

(02 marks)

ANSWER IN THIS BOX

2) (a) State what is meant by **Confusion** and **Diffusion** with respect to cryptographic algorithms.

(05 Marks)

ANSWER IN THIS BOX

(b) List two (2) symmetric key cryptography algorithms, two (2) asymmetric key cryptography algorithms and two (2) hashing algorithms.

(03 Marks)

ANSWER IN THIS BOX

(c) Which mode of operation of the Advanced Encryption Standard (AES) block cipher would you use to protect an image file which is in the BMP format? Give a brief justification for your answer.

(05 Marks)

ANSWER IN THIS BOX

(d) Nimal hss RSA public key (n, e) = (33, 3) and private key = (n, d) = (33, 7). Kamal has RSA public key (n, e) = (55, 7) and private key = (n, d) = (55, 23). Suppose Nimal signs the plain text M=3 and then encrypts it and sends C to Kamal. Determine the final cipher text C.

(07 Marks)

ANSWER IN THIS BOX

3) (a) List three (3) ISO security services supported by Secure Socket Layer (SSL) protocols.

(03 Marks)

ANSWER IN THIS BOX

(b) Which files will be created as the result of the following command:

openssl req -new -x509 -out host.pem

(05 Marks)

ANSWER IN THIS BOX

(c) What is the purpose of the following command with regard to Java key management?

keytool -genkey -keyalg RSA -keystore UCSC

(05 Marks)

ANSWER IN THIS BOX

(d) List three (3) certification infrastructure models available in the context of public key distribution.

(03 Marks)

ANSWER IN THIS BOX

(e) In certain situations, a user has to revoke a digital certificate. What are the reasons for such revocations?

(04 Marks)

ANSWER IN THIS BOX

4) (a) List five (5) security services supported by IPSec protocols.

(05 Marks)

ANSWER IN THIS BOX

(b) What is the main difference between mandatory access control and discretionary access control?

(05 Marks)

ANSWER IN THIS BOX

(c) Draw an access control matrix to represent the following conditions.

1. Subjects are U1, U2, U3 and U4
2. Objects are File1, File2, Program1 and Program2
3. U1 can write File1 and execute Program1
4. U2 can read and write File2
5. U3 can read File 1 and execute Program 2
6. U4 can read File 1 and File 2 and execute Program 1 and Program 2

(05 Marks)

ANSWER IN THIS BOX

(d) Briefly describe copyright, patent and trade secret with respect to information protection.

(05 Marks)

ANSWER IN THIS BOX

****