Index No: ……...

UNIVERSITY OF COLOMBO, SRI LANKA

UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY (EXTERNAL)
Academic Year 2014/2015 – 3rd Year Examination – Semester 5

IT5204: Information Systems Security

Structured Question Paper
07th March, 2015
(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 **13 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 allowed.**

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) **State whether each of the following statements is true or false and then briefly justify giving reasons for your answer.**

(a) The Vernam cipher decrypts cipher text C = **11011011** to the plain text P = **00110001**.
The security key K= **11101010**

(02 marks)

ANSWER IN THIS BOX

(b) The Ceasar Cipher is an example of a block cipher.

(02 marks)

ANSWER IN THIS BOX

(c) The Advanced Encryption Standard (AES) algorithm uses a **192** bit security key.

(02 marks)

ANSWER IN THIS BOX

(d) The Data Encryption Standard (DES) algorithm encrypts **eight (8)** bytes of a plain text message to the **sixteen (16)** bytes of a cipher text message when DES uses Electronic Code Book (ECB) mode and Public Key Cryptography Standard 5 (PKCS5) padding scheme.

(02 marks)

ANSWER IN THIS BOX

(e) An asymmetric key system with **five (5)** users requires **ten (10)** public and private key pairs and each user must track and remember a private key for each other user with whom he or she wants to securely communicate.

(02 marks)

ANSWER IN THIS BOX

(f) Suppose we want to use the Diffie-Hellman Key Agreement protocol between two end points A and B, and we have chosen the integer **g=5** and the integer **n=10**. If A generates the private key **x=3** and B generates the private key **y=5**, the session key **k** between A and B is **9**.

(02 marks)

ANSWER IN THIS BOX

(g) (18, 13), (15,14), (17,19) are relatively prime numbers.

(02 marks)

ANSWER IN THIS BOX

(h) The greatest common divisor of **455** and **324** is **1**.

(02 marks)

ANSWER IN THIS BOX

(i) Nimal has RSA public key **(n, e) = (33, 3)** and private key = **(n, d) = (33, 7)**. The digital signature (S) of the plain text message **M=2** equal to **29**.

(02 marks)

ANSWER IN THIS BOX

(j) Nimal has RSA public key **(n, e) = (33, 3)** and private key = **(n, d) = (33, 7)**. Suppose Kamala encrypts plain text message **M=3** to Nimal. Therefore, Cipher text (C) = **27**.

(02 marks)

ANSWER IN THIS BOX

(k) Suppose RC4 cryptographic algorithm uses a security key equal to **5** bytes. The system as a whole has **72057594037927900** security keys.

(02 marks)

ANSWER IN THIS BOX

(l) The Secure Hash Algorithm Version 1 (SHA1) generates **128** bit hash value when the input message length equals **eight (8)** bytes and generates **160** bit hash value when the input message length equals **sixteen (16)** bytes.

(02 marks)

ANSWER IN THIS BOX

(m) Patents gives the programmer exclusive right to make copies of his software and sell it to the public.

(02 marks)

ANSWER IN THIS BOX

(n) One of the ISO security service supported by the Secure Socket Layer (**SSL**) protocol is **non-repudiation**.

(02 mark)

ANSWER IN THIS BOX

(o) The mechanism of spreading information of a single plaintext letter over the entire ciphertext is known as **Confusion**.

(02 mark)

ANSWER IN THIS BOX

(p) The Trusted Computer System Evaluation Criteria (**TCSEC**) defines the criteria for **three (3)** different evaluation classes identified by their rating levels of PASS, FAILED and UNKNOWN.

(02 mark)

ANSWER IN THIS BOX

(q) Intrusion Detection Systems (**IDS**) can use only the known evidence (**signatures**) of an intrusion to detect any remote attacks.

(02 mark)

ANSWER IN THIS BOX

(r) Data mining is widely used to analyse system data, for example, audit logs, to identify any patterns related to attacks. The approach would not create any security problems with respect to the sensitivity of individual data items.

(02 mark)

ANSWER IN THIS BOX

(s) Kerberos is a system that supports authentication in distributed systems.

(02 mark)

ANSWER IN THIS BOX

(t) A virus that can change its appearance is called a worm.

(02 mark)

ANSWER IN THIS BOX

2) (a) Consider the following cryptographic algorithms. Classify these algorithms as **symmetric key cryptography** algorithms or **asymmetric key cryptography** algorithms by placing "X" mark in the relevant position.

(05 mark)

ANSWER IN THIS BOX

Cryptography Algorithms	**Symmetric Key**	**Asymmetric Key**
1. Data Encryption Standard(DES)		
2. Advance Encryption Standard (AES)		
3. Ron Rives, Adi Shamir and Len Adleman(RSA)		
4. liptic Curve (EC)		
5. Diffie and Hellman(DH)		

(b) Define the terms **vulnerability** and **threat** with respect to information system security.

(04 mark)

ANSWER IN THIS BOX

(c) Define the terms **confidentiality**, **integrity**, and **availability** with regard to information system security.

(06 mark)

ANSWER IN THIS BOX

(d) A digital signature is a protocol that produces the same effect as a real signature. It is a mark that only the sender can make where other people can easily recognize it as belonging to the sender. Propose a protocol to create a digital signature by using a hash algorithm and an asymmetric key algorithm.

(05 mark)

ANSWER IN THIS BOX

3) (a) List **five(5)** memory protection methods that can be used to prevent one program from affecting the data and programs in the shared memory space of other users, when executed on a computer.

(05 mark)

ANSWER IN THIS BOX

(b) A serious security problem for a Database Management System (DBM) is the possible blocking or the damaging of the computing system in the middle of a data modification cycle. Propose a simple solution to address this problem.

(06 mark)

ANSWER IN THIS BOX

(c) Security policies are used for several purposes or intents in an organization. Identify **four (4)** such purposes.

(04 mark)

ANSWER IN THIS BOX

(d) Briefly describe the term **trade secret** with respect to information protection.

(05 mark)

ANSWER IN THIS BOX

4) (a) List three (3) possible **controls,** each, to overcome the three (3) **network vulnerabilities** given in the following table.

(06 marks)

ANSWER IN THIS BOX	
Network vulnerability	**Possible controls**
1. Port scan	
2. Social engineering	
3. OS and application fingerprinting	

(b) List **four (4)** main security requirements of a secure e-mail system.

(04 marks)

ANSWER IN THIS BOX

(c) Nimal connects his office computer to the Internet via his mobile phone(WLAN) up it as wi-fi hub since local area network connection (LAN) in his office is really slow. He uses LAN connection to conduct his day to day activities and keeps the WLAN connection to browse the Internet. The latest version of a firewall protects the LAN network in his organization. Briefly discuss the security issues which might occur in his organization due to Nimal's action.

(05 marks)

ANSWER IN THIS BOX

(d) Briefly describe the concepts of "**Cold Site**" and "**Hot Site**" with regards to disaster recovery.

(05 marks)

ANSWER IN THIS BOX
Cold Site
Hot Site

****