Index No: ……...

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
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.
- **Calculators are not 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
TRUE
Copher Text = 11011011
Key = 11101010
Plain Text = 00110001

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

(02 marks)

ANSWER IN THIS BOX
False
A block cipher encrypts a group of plaintext symbols as one block. The Cesar cipher encrypts one
character at a time. Hence the Cesar cipher is an example a stream cipher.

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

(02 marks)

ANSWER IN THIS BOX
True
The AES algorithm uses 128,192 and 256 bit keys.

(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
True
PKCS5 padding inserts new dummy block when the plain text size equals to the block
size of the cipher algorithm. The block size of DES algorithm is 8 bytes.
Hence cipher text size will be 16 bytes when the plain text size equals to 8 bytes.

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

(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
False
For the private key x and public key X, we have the relation $X = g^x \bmod n$.
public key of A (X) = $5^3 \bmod 10$; X= 125 mod 10, X=5
public key of B (Y) = $5^5 \bmod 10$; Y= 3125 mod 10, Y=5
Session key $k = X^y \bmod n$: $k=5^5 \bmod 10$ k= 5 OR
Session key $k = Y^x \bmod n$: $k=5^5 \bmod 10$ k= 5

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

(02 marks)

ANSWER IN THIS BOX
True
Relatively prime numbers should not have common factors.

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

(02 marks)

ANSWER IN THIS BOX
True
GCD(455,324)
=GCD(324,131)
=GCD(131,62)
=GCD(62,7)
=GCD(7,6)
=GCD(6,1)

(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 is **M=2** equal to **29**.

(02 marks)

ANSWER IN THIS BOX
True
$S=P^d \bmod n$
$S=2^7 \bmod 33=128 \bmod 33=29$

(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
True
$C=P^e \bmod n$
$C=3^3 \bmod 33 =27 \bmod 33=27$

(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
False
The system as a whole has 2^{40} = 1099511627776 security keys.

(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
False
The hash size depends on the algorithm.
It does not depend on the length of the input message.
The Secure Hash Algorithm Version 1 (SHA1) generates 160 bit hash value.

(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
Fasle
Copyright gives the programmer exclusive right to make copies of the software and sell it to
the public.
The distinction between patents and copyrights is that patents were intended to apply
to the results of science, technology, and engineering, whereas copyrights were meant to
cover works in the arts, literature, and software.

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

(02 mark)

ANSWER IN THIS BOX
False
ISO security services supported by the Secure Socket Layer (SSL) protocol are:
authenticity, integrity and confidentiality.

(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
False
The characteristics of distributing the information from single plaintext letter over the entire
ciphertext is called diffusion.
Confusion: The interceptor should not be able to predict what changing one character in the plaintext
will do to the ciphertext.

(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
False
The Trusted Computer System Evaluation Criteria (TCSEC) defined criteria for six different
evaluation classes identified by their rating scale of C1, C2, B1, B2, B3, and A1.

(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
Fasle
Anomaly detection method uses the assumption that unexpected behaviour is evidence of an
Intrusion. Therefore signature based detection is only one method.

(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
False
Individual privacy can suffer from the data mining. Inference issues may occur when we
widely analyse the data available in social networks by using same kind of data mining
techniques.

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

(02 mark)

ANSWER IN THIS BOX
True
Kerberos is used for authentication between intelligent processes, such as client-to-server tasks, or a user's workstation to other hosts. Kerberos is based on the idea that a central server provides authenticated tokens, called tickets, to requesting applications. A ticket is an unforgeable, nonreplayable, authenticated object.

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

(02 mark)

ANSWER IN THIS BOX
False
A virus that can change its appearance is called a polymorphic virus. (Poly means "many" and morph means "form"). A worm is a program that spreads copies of itself through a network.

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)	X	
2. Advance Encryption Standard (AES)	X	
3. Ron Rives, Adi Shamir and Len Adleman(RSA)		X
4. Eliptic Curve (EC)		X
5. Diffie and Hellman(DH)		X

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

(04 mark)

ANSWER IN THIS BOX
A **vulnerability** is a weakness in the security system, for example,
in procedures, design, or implementation, that might be exploited to cause loss or harm.
A **threat** to a computing system is a set of circumstances that has
the potential to cause loss or harm.

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

(06 mark)

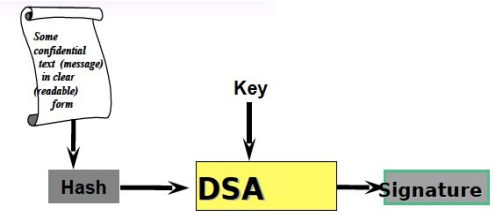
ANSWER IN THIS BOX
Confidentiality ensures that computer-related assets are accessed only by authorized parties.
Integrity means that assets can be modified only by authorized parties or only in authorized
Ways. In this context, modification includes writing, changing, changing status, deleting, and
creating.
Availability means that assets are accessible to authorized parties at appropriate times.
In other words, if some person or system has legitimate access to a particular set of objects,
that access should not be prevented.

(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

Student should describe a protocol by using the following diagram.



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

Fence, Relocation, Base/bounds register, Segmentation and Paging are the memory protection Methods that can be used to prevent one program from affecting the data and programs in the memory space of other users.

(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
Two phase update is the simple solution to the above problem. During the first phase, called the intent phase, the DBM gathers the resources it needs to perform the update. It does everything to prepare for the update, but it makes no changes to the database. The first phase is repeatable an unlimited number of times because it takes no permanent action. The last event of the first phase, called committing, involves the writing of a commit flag to the database. The commit flag means that the DBM has passed the point of no return: After committing, the DBM begins making permanent changes.
The second phase makes the permanent changes. During the second phase, no actions from before the commit can be repeated, but the update activities of phase two can also be repeated as often as needed. If the system fails during the second phase, the database may contain incomplete data, but the system can repair these data by performing all activities of the second phase.

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

(04 mark)

ANSWER IN THIS BOX
1. Recognizing sensitive information assets
2. Clarifying security responsibilities
3. Promoting awareness for existing employees
4. Guiding new employees

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

(05 mark)

ANSWER IN THIS BOX
The distinguishing characteristic of a trade secret is that it must always be kept secret.
The owner must take precautions to protect the secret, such as storing it in a safe,
encrypting it in a computer file, or making employees sign a statement that they will not
disclose the secret.

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	Firewall
	Intrusion detection system
	Running as few services as possible
2. Social engineering	Education
	user awareness
	Policies and procedures
3. OS and application fingerprinting	Firewall
	"Hardened" (self-defensive) applications
	Programs that reply with only what is necessary
	Intrusion detection system

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

(04 marks)

ANSWER IN THIS BOX
1. Message confidentiality (the message is not exposed en route to the receiver)
2. Message integrity (what the receiver sees is what was sent)
3. Sender authenticity (the receiver is confident who the sender was)
4. Nonrepudiation (the sender cannot deny having sent the message)

(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
Firewalls can protect an environment only if the firewalls control the entire perimeter.
That is, firewalls are effective only if **no unmediated** connections breach the perimeter.
If even one inside host connects to an outside address, by a mobile device for example, the
entire inside net is vulnerable through the mobile device and its host.

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

(05 marks)

ANSWER IN THIS BOX
Cold Site
A cold site or shell is a facility with power and cooling available, in which a computing
system can be installed to begin immediate operation. Some companies maintain their own
cold sites, and other cold sites can be leased from disaster recovery companies. These sites
usually come with cabling, fire prevention equipment, separate office space, telephone access,
and other features. Typically, a computing center can have equipment installed and
resume operation from a cold site within a week of a disaster.
Hot Site
If the application is more critical or if the equipment needs are more specialized,
a hot site may be more appropriate. A hot site is a computer facility
with an installed and ready-to-run computing system.
The system has peripherals, telecommunications lines, power supply, and
even personnel ready to operate on short notice.
Some companies maintain their own;
other companies subscribe to a service that has available one or
more locations with installed and running computers.

****