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

True
Justification:

The cipher text C= "khoor elw vwxghqwv" is equal to the plain text P = "Hello bit students" as Cesar Cipher: C(i)=P(i)+3

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

(02 marks)

ANSWER IN THIS BOX

False
Justification: A block cipher encrypts a group of plaintext symbols as one block, hence AES is an example of a Block cipher.

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

(02 marks)

ANSWER IN THIS BOX

False
Justification: The DES algorithm uses 64 bit data blocks

(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

False
Justification: 7 users require 7*(7-1)/2=21 keys as a symmetric key system with n users requires n * (n - 1)/2 keys.

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

(02 marks)

ANSWER IN THIS BOX

True
Justification:
Following the HMAC standard, one can convert any hash algorithm to MAC. Thus SHA can also be used as a MAC according to the HMAC standard.

(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

False
Justification: According to Shannon theory, errors in ciphering should not propagate and cause corruption of further information in the message.

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

(02 marks)

ANSWER IN THIS BOX

True
Justification: One of the most important advantages of the SET protocol is mixing the better of two encryption key techniques symmetric and asymmetric. Thus it is a hybrid protocol.

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

(02 marks)

ANSWER IN THIS BOX

False
Justification: Cipher Feedback Mode or Output Feedback Mode converts a block cipher into a stream cipher.

(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

False
Justification: In military security policy, data items are associated with a particular security level while in a commercial security policy, data items are associated by a set of programs permitted to manipulate it.

(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

False

Justification: A honeypot is a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems.

(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

False
Justification:
A computer virus is a malicious computer program that can copy itself and infect a computer without the permission or knowledge of the owner and a trapdoor is a secret undocumented entry point into a computer program.

(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

False
Justification: 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.

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

(02 marks)

ANSWER IN THIS BOX

False
Justification:

GCD(46,68)
GCD(68,46)
GCD(46,22)
GCD(22,2)
GCD = 2

gcd(46,68) =2

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

(02 marks)

ANSWER IN THIS BOX

False
Justification: An Attribute Authority (AA) trusted by one or more users is to create and sign attribute certificate and Certificate Authority (CA) trusted by one or more users is to create and sign digital certificates.

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

(02 marks)

ANSWER IN THIS BOX

True
Justification: Relatively prime numbers should not have common factors.

(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

False
Justification: The system as a whole has $26^1 + 26^2 + 26^3 + 26^4 = 475254$ passwords.

(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

True
Justification:
For the private key x and public key X, we have the relation $X = g^x \bmod n$.
public key of A (X) = $3^5 \bmod 13$; X= 243 mod 13, X=9
Thus session key (k) = $X^y \bmod n$. = $9^7 \bmod 13$ = 4782969 mod 13 =9

(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

False
Justification: Bell-La Padula model which is a multilevel security model, is a process which can only read objects at its level or higher or can only write objects at its level or higher.

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

(02 marks)

ANSWER IN THIS BOX

False
Justification: Database integrity ensures that data entered into the database is accurate, valid, and consistent.

(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

False
Justification: Inference is a way to infer or derive sensitive data from non-sensitive data. A direct attack, a user tries to determine values of sensitive fields by seeking them directly with queries.

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

(05 Marks)

ANSWER IN THIS BOX

Confusion: The interceptor should not be able to predict what changing one character in the plaintext will do to the ciphertext

Diffusion: The characteristics of distributing the information from single plaintext letter over the entire ciphertext is called diffusion

(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

Symmetric key cryptography algorithms: Data Encryption Standard – DES, Advance Encryption Standard - AES

Asymmetric key cryptography algorithms: Ron Rives, Adi Shamir and Len Adleman – RSA , Diffie and Hellman - DH

Hashing algorithms: Secure Hash Algorithm – SHA, Message Digest Algorithm Version 5 - MD5

(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

Cipher Block Channing Mode destroys properties and patterns in the plain text. Thus it is suitable to encrypt an image file. Some sections of the image will appear in the cipher text in different colour, if we use a mode such as Electronic Code Book (ECB).

(d) Nimal has 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

Signing

$S=M^d \bmod n$

$M=3$, $e=7$ and $n=33$, so that $3^7 \bmod 33$; $S=9$

Then he encrypts it to Kamal

$C=S^e \bmod n$

$S=9$, $e=7$ and $n=55$, so that $9^7 \bmod 55$; $C=4$

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

(03 Marks)

ANSWER IN THIS BOX

1. Authentication
2. Integrity
3. Confidentiality

(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

Private key will be saved to privkey.pem file and self-signed certificate will be saved to host.pem file.

(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

This command will generate RSA Private and Public key pair and store it in the key database called "UCSC"

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

(03 Marks)

ANSWER IN THIS BOX

1. Flat model
2. Hierarchy model
3. Web of trust model

(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

When a certificate authority (CA) generates a certificate, that certificate is valid for a specific amount of time. A certificate can be revoked before it has expired if:

- an employee leaves a company
- moves to a new position in the same company
- private key has been compromised
- private key has been lost

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

(05 Marks)

ANSWER IN THIS BOX

- Authentication
- Integrity
- Access control
- Confidentiality
- Replay protection (Partial)

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

(05 Marks)

ANSWER IN THIS BOX

With mandatory access control, users do not have the ability to override the security policy and, for example, grant access to files that would otherwise be restricted. By contrast, discretionary access control, which also governs the ability of subjects to access objects, allows users the ability to make policy decisions and/or assign security attributes.

(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

	File1	File2	Program1	Program2
U1	W		X	
U2		R,W		
U3	R			X
U4	R	R	X	X

R -Read; W- Write; X- Execute

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

(05 Marks)

ANSWER IN THIS BOX

Copyright gives the author/programmer exclusive right to make copies of the expression and sell them to the public. That is, only the author can sell copies of the author's book or software.

Patents are unlike copyrights in that they protect inventions, not works of the mind. 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.

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.

****