Index No: ……..

UNIVERSITY OF COLOMBO, SRI LANKA

UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY (EXTERNAL)
Academic Year 2016 – 3rd Year Examination – Semester 5

IT5205: Information Systems Security

Structured Question Paper
14 May , 2016
(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 **15 pages**.
- **Answer all 4 questions**.
- **Question 1 and 2 carry** 30% marks each **and other questions carry** 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. [×]) 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 giving reasons for your answer.**

(a) The Vernam cipher encrypts plain text P = **1001 10001** to the cipher text C = **1111 00100**. The security key K= **1110 10101**

(02 marks)

ANSWER IN THIS BOX
FALSE
Plain Text = 1001 10001
Key = 1110 10101
Cipher Text = 0111 00100

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

(02 marks)

ANSWER IN THIS BOX
False
A block cipher encrypts a group of plaintext symbols as one block.
Hence the AES cipher is an example a block cipher.

(c) The Advanced Encryption Standard (AES) algorithm encrypts **sixteen (16)** bytes of a plain text message to **sixteen (16)** bytes of a cipher text message under Electronic Code Book (ECB) mode and Public Key Cryptography Standard 5 (PKCS5) padding scheme.

(02 marks)

ANSWER IN THIS BOX
False
PKCS5 padding inserts new dummy block when the plain text size equals to the block
size of the cipher algorithm. The block size of AES algorithm is 16 bytes.
Hence cipher text size will be 32 bytes when the plain text size equals to 16 bytes.

(d) 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=2** and the integer **n=10**. If A generates the private key **x=2** and B generates the private key **y=3**, the session key **k** between A and B is **5**.

(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) = $2^2 \bmod 10$; X= 4 mod 10, X=4
public key of B (Y) = $2^3 \bmod 10$; Y= 8 mod 10, Y=8
Session key k = $X^y \bmod n$: k=$4^3 \bmod 10$ k= 4 OR
Session key k = $Y^x \bmod n$: k=$8^2 \bmod 10$ k= 4

(e) Nimal has RSA public key **(n, e) = (33, 3)** and private key = **(n, d) = (33, 7)**. Suppose Kamal encrypts plain text message **M=2** to Nimal. Nimal receives cipher test (C)=**8**.

(02 marks)

ANSWER IN THIS BOX
True
$C=P^d \bmod n$
$C=2^3 \bmod 33=8 \bmod 33=8$

(f) Suppose DES cryptographic algorithm uses a security key of length 56 bits. The system as a whole has **72057594037927900** possible security keys.

(02 marks)

ANSWER IN THIS BOX
True
The system as a whole has 2^{56} = 72057594037927900 security keys.

(g) The MD5 hash algorithm generates a **128** bit hash value when the input message length is equal **eight (8)** bytes and SHA1 hash algorithm generates a **160** bit hash value when the input message length is equal **sixteen (16)** bytes.

(02 marks)

ANSWER IN THIS BOX
True
The hash size depends on the algorithm.
It does not depend on the length of the input message.
The MD5 generates 128 bit hash values and SHA1 generates 160 bit hash value.

(h) The **SSL** protocol uses both the symmetric key and the asymmetric key cryptographic algorithms.

(02 marks)

ANSWER IN THIS BOX
True
One of the most important advantages of the SSL protocol is mixing
the better of two encryption key techniques symmetric and asymmetric.

(i) One of the ISO security service supports by the Secure Shell (**SSH**) protocol is **non-repudiation**.

(02 marks)

ANSWER IN THIS BOX
False
ISO security services supported by the SSH protocol are:
authenticity, integrity and confidentiality.

(j) An ATM card provides two-factor authentication.

(02 marks)

ANSWER IN THIS BOX
True
In the ATM card system, user needs to present the card and enters
the PIN so it provides two factor authentication.

(k) A network-based Intrusion Detection Systems (IDS) typically runs on a single workstation or client or host, to protect that host.

(02 marks)

ANSWER IN THIS BOX
False
A network-based IDS is a stand-alone device attached to the network
to monitor traffic throughout that network;
a host-based IDS runs on a single workstation or client or host, to protect that one host.

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

(02 marks)

ANSWER IN THIS BOX
False
Anomaly detection method uses the assumption that unexpected
behaviour is evidence of an Intrusion.
Therefore signature based detection is only one method.

(m) The fundamental data structures of IPSec protocol are the AH (authentication header) and the IP header.

(02 marks)

ANSWER IN THIS BOX
False
The fundamental data structures of IPSec are the AH (authentication header)
and the ESP (encapsulated security payload).

(n) Web sites use cookies to avoid a customer having to authenticate in each successive visit to a site.

(02 marks)

ANSWER IN THIS BOX
True
A cookie is a text file stored on the user's computer and passed by the user's browser
to the web site when the user goes to that site. So it can be used
to maintain the authentication sessions.

(o) A Hardware Security Module (HSM) is a device that keeps certain types of network traffic out of a private network.

(02 marks)

ANSWER IN THIS BOX
False
A firewall filters incoming and outgoing network traffic, thus keeping
certain kinds of network traffic out of a private network.

2) Select the correct answer, and then explain your selection, in at most one sentence.

a) The **three primary** methods for authentication of a user to a system or network are reflected by

a) Passwords, tokens and biometrics.

b) Authorization, identification and tokens.

c) Passwords, encryption and identification.

d) Identification, encryption and authorization.

(02 marks)

ANSWER IN THIS BOX
a) Correct – These are the tools used in the three primary methods of authentication, what you know, what you have and what you are.

b) An access system that grants users only those rights necessary for them to perform their work, is operating on the security principle of

a) Discretionary Access.

b) Least Privilege.

c) Mandatory Access.

d) Separation of Duties.

(02 marks)

ANSWER IN THIS BOX

b) Correct – Least Privilege is the security principle that requires the users and processes in a system to have the least number of privileges – and

for the shortest amount of time – needed to do their work.

c) Why do vendors publish SHA1 hash values when they provide software patches for their customers to be downloaded from the Internet?

a) Recipients can verify the software's integrity after downloading.

b) Recipients can confirm the authenticity of the site.

c) Recipients can request future updates to the software by using the assigned hash value.

d) Recipients need the hash value to successfully activate the new software.

(02 marks)

ANSWER IN THIS BOX

a) Correct – Comparing the hash value helps detect alterations.

d) A worm most frequently spreads via

a) User misuse.

b) Exploitation of vulnerabilities in software.

c) Mobile code attacks.

d) Infected USB drives and wireless access points.

(02 marks)

ANSWER IN THIS BOX

b) Correct – A worm usually spreads through a vulnerability in server or systems software.

e) What is the FIRST step to be performed in establishing a Disaster Recovery Plan?

a) Demonstrate adherence to a standard disaster recovery process.

b) Agree on the goals and objectives of the plan.

c) Identify applications to be run during a disaster.

d) Determine the site to be used during a disaster.

(02 marks)

ANSWER IN THIS BOX

b) Correct – This is a critical component of all project management techniques including disaster recovery projects

f) What is the BEST method of storing user passwords for a system?

a) Password-protected file.

b) File restricted to one individual.

c) One-way encrypted file.

d) Two-way encrypted file.

(02 marks)

ANSWER IN THIS BOX

c) Correct – A one way encrypted file is computationally infeasible to reverse engineer and thereby obtain a listing of the original passwords

g) Why does fiber optic communication technology have a significant security advantage over other transmission technologies such as copper or radio.

a) Higher data rates can be archived

b) Interception of data traffic is made more difficult

c) Traffic analysis is prevented by multiplexing multiple streams

d) Only single and double-bit errors are more likely to occur on fiber

(02 marks)

ANSWER IN THIS BOX

b) Correct – Fiber is resistant to tapping

h) Computer security is the responsibility of

a) Everyone in the organization.

b) The corporate management only.

c) The corporate security staff only.

d) Everyone with computer access.

(02 marks)

ANSWER IN THIS BOX

a) Correct – Everyone in the organization (including contractors and cleaning personnel under contract) need to be aware of the requirements of computer security.

i) What is the proper way to dispose of confidential computer printouts?

a) Have them collected and destroyed by cleaning staff.

b) Place them with other printouts for collection by a document removal service.

c) Store them securely until removed and destroyed by authorized personnel only.

d) Place them in a recycling bin for pickup and removal.

(02 marks)

ANSWER IN THIS BOX

c) Correct – Usually they are kept in a locked box until removed for shredding

j) A timely review of system access audit records would be an example of which basic security function in an organization?

a) Avoidance of unauthorized activities

b) Deterrence of unauthorized activities

c) Prevention of unauthorized activities

d) Detection of unauthorized activities

(02 marks)

ANSWER IN THIS BOX

d) Correct – Review of audit records can detect unauthorized activity.

k) Which one of the following is the PRIMARY objective of a firewall?

a) To protect networks from each other

b) To prevent IP traffic from going out of the user network

c) To block incoming and outgoing ICMP and UDP traffic

d) To monitor network traffic usage

(02 marks)

ANSWER IN THIS BOX

a) Correct- The primary objective of a firewall is the protection of those assets that reside behind it

l) Who should ideally provide access authorization to computerized information in an organization?

a) Database administrator

b) Security administrator

c) Data owner

d) Network administrator

(02 marks)

ANSWER IN THIS BOX

c) Correct - The data owner is responsible for accurate use of the information and

should normally provide written authorization for users to gain access to computerized information.

m) At what stage of the application development process should the information security department first become involved?

a) Prior to the installation of the software

b) Prior to user acceptance testing

c) During unit testing

d) During requirements development

(02 marks)

ANSWER IN THIS BOX

d) Correct – Because Security Dept. should be involved at the beginning of the project. It is much easier than adding it later and much harder, more costly to do.

n) The value of data or the access to an information system of an organization should consider all of the following factors EXCEPT?

a) The requirements of regulations or legislation

b) The number of people that require access to the systems or data

c) The sensitivity of the data or systems and risks associated with disclosure

d) Whether access to the data or system is critical to business functions

(02 marks)

ANSWER IN THIS BOX

b) Correct – while this is a factor in determining the value especially in relation to the cost of downtime of the system, it is not as direct a valuation as the other choices

o) Which of the following best describes a quantitative risk analysis?

a) Scenario-based analysis to research different security threats

b) A method used to apply severity levels to potential loss, probability of loss, and risks

c) A method that assigns monetary values to components in the risk assessment

d) A method that is based on gut feelings and opinions

(02 marks)

ANSWER IN THIS BOX

c) Correct - A quantitative risk analysis assigns monetary values and percentages to the different components within the assessment.

3) (a) In a cryptographic system, suppose the User A generates a cipher text C = EK1[DK1[EK2[P]]] where K1 and K2 are symmetric keys. Can the User B retrieve the plain text P= DK2[DK3[EK3[C]]] where K2 and K3 are symmetric keys. Justify your answer. (Note: E - DES encryption, D- DES decryption)

(06 marks)

ANSWER IN THIS BOX
Yes
User A: Plain text will be encrypted with K2.
Then it will be encrypted with K1 and decrypted with K1.
Therefore C = EK1[DK1[EK2[P]]] = EK2[P]
User B: Cipher text will be encrypted with K3 and decrypted back with K3. Then it will be decrypted with K2.
Therefore P=DK2[DK3[EK3[C]]]=DK2[C]

(b) In a cryptographic system, suppose the User A generates a cipher text C by using his public key K2. Can the User B retrieve the plain text P by using his private key K1. Justify your answer.

(06 marks)

ANSWER IN THIS BOX
No
Since User A generates a cipher text C by using his public key K2,
cipher text can be decrypted only with the private key of User A.
Thus User B cannot retrieve the plain text.

(c) Suppose one wants to authenticate and encrypt the IP packets (excluding the IP address) by using IPSec protocol. Explain the procedure by referring to the structure of a IPSec packet by using a suitable diagram.

(08 marks)

ANSWER IN THIS BOX

Student should explain the following digram.

Transport Mode

4) a) Briefly describe three (3) anti-phishing techniques.

(06 marks)

ANSWER IN THIS BOX

Student should explain any three of the following techniques:

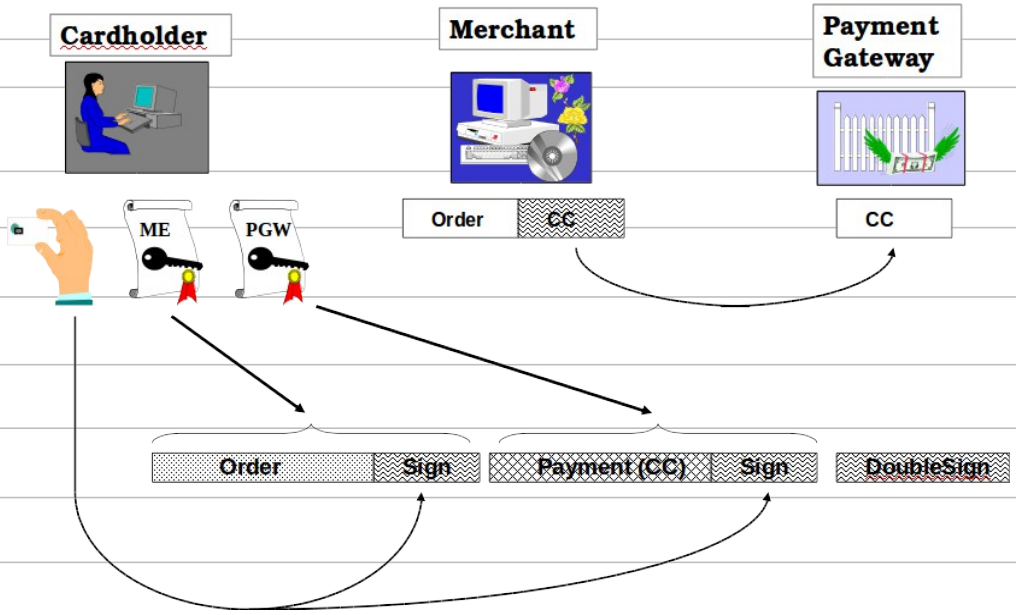
- Check the email Carefully.
- Do not click on links, download files or open attachments in emails from unknown senders.
- Never Enter Financial or Personal Information
- Protection through Software
- Never Send Personal Information through emails
- Never Download Files from Unreliable Sources

b) Briefly explain the **Payment Request Message** format with regard to the Secure Electronic Transaction (**SET**) protocol.

(06 marks)

ANSWER IN THIS BOX

Students should explain the following diagram.



c) **"Web applications security is not simply achieved by the Secure Socket Layer protocol alone"**, Discuss the above statement.

(08 marks)

ANSWER IN THIS BOX
SSL protocol provides confidentiality, integrity and Web server authentication.
User authentication is optional.
Even though we use it for credit card transactions, SSL cannot support digital signatures.
It cannot prevent any attacks caused due to vulnerable web applications.
Students should explain these facts in detail.

****