Index No: ……..

UNIVERSITY OF COLOMBO, SRI LANKA

UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY (EXTERNAL)

Academic Year 2018 – 3rd Year Examination – Semester 5

IT5205: Information Systems Security

Structured Question Paper

19th May, 2018

(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 **16 pages**.
- **Answer all 4 questions**. (all questions **do not** carry equal marks)
- **Question 1 and 2 (**30% marks each**) 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. [×]) 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:					

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

(a) Suppose we know an efficient algorithm to factorise extremely large numbers. This will make it possible to break RSA encryption.

(02 marks)

ANSWER IN THIS BOX
True
The strength of RSA algorithm depends on the factorization of extremely large numbers.

(b) "The security of an encryption scheme must depend strongly on the secrecy of the algorithm" is an example of security through obscurity.

(02 marks)

ANSWER IN THIS BOX
True
Security through obscurity refers to security that relies on secret information,
design or implementation details to prevent attack.

(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 when AES uses Electronic Code Book (ECB) mode and the 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 parties, A and B, and we have chosen the integer **g=5** and the integer **n=100**. 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 **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) = $5^2 \bmod 100$; X= 25 mod 100, X=25
public key of B (Y) = $5^3 \bmod 100$; Y= 125 mod 100, Y=25
Session key k = $X^y \bmod n$: k=$25^3 \bmod 100$, 15625 mod 100 k= 25 OR
Session key k = $Y^x \bmod n$: k=$25^2 \bmod 100$, k= 25

(e) Nimal has RSA public key **(n, e) = (33, 3)** and private key = **(n, d) = (33, 7)**. Kamal has RSA public key **(n, e) = (91, 11)** and private key = **(n, d) = (91, 59)**. Suppose Kamal encrypts plain text message **M=2** to Nimal. Nimal receives cipher text message C = **8**.

(02 marks)

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

(f) Suppose we have nodes A, B, C, D, E and F in a network. We have to generate a total of nine (9) keys to let each node communicate with every other node in a bidirectional secure way using the AES encryption algorithm.

(02 marks)

ANSWER IN THIS BOX
False
Number of keys = number of node * (number of nodes - 1)/2
Number of keys = 6*5/2=15

(g) The MD5 hash algorithm generates a **128** bit hash value and the SHA256 hash algorithm generates a **256** bit hash with an input message of **eight (8)** bytes.

(02 marks)

ANSWER IN THIS BOX
True
The hash size only depends on the algorithm.
It does not depend on the length of the input message.
The MD5 always generates 128 bit hash values and SHA256 generates
256 bit hash values irrespective of the message length.

(h) The **PGP** standard is an example of a hybrid encryption standard.

(02 marks)

ANSWER IN THIS BOX
True
One of the most important advantages of the PGP standard is mixing
the better of two encryption key techniques symmetric and asymmetric.
Therefore it is an example of a hybrid standard.

(i) One of the ISO security services supported by the **SSL protocol** is **non-repudiation**.

(02 marks)

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

(j) A One Time Password (OTP) protocol which sends a random password via SMS to your mobile phone provides two-factor authentication.

(02 marks)

ANSWER IN THIS BOX
True
In using a this protocol, a user needs to access his mobile phone and enter the OTP.
Thus it provides two factor authentication.

(k) A "**Qualitative Risk Assessment**" is best suited for evaluating the strength of a server backup to the cloud.

(02 marks)

ANSWER IN THIS BOX
False
As numeric data regarding impact and probability of occurrence is available,
quantitative risk assessment is the best option here.

(l) An application level firewall looks at each IP packet entering or leaving the network and accepts or rejects it based on user-defined rules.

(02 marks)

ANSWER IN THIS BOX
False
Packet filtering firewall looks at each IP packet entering or leaving the network and
accepts or rejects it based on user-defined rules.
Application level firewall applies security mechanisms to specific applications,
such as HTP and FTP servers.

(m) The domain of security Controls may be categorised into **Physical**, **Technical**, and **Administrative** controls. **Antivirus software** is an example of **Administrative** control.

(02 marks)

ANSWER IN THIS BOX
False
Technical Controls involves the use of safeguards incorporated in applications
software and related devices.
Administrative Controls consists of management constraints,
operational procedures and accountability procedures.
Thus Antivirus software is an example of Technical Control.

(n) To determine if a threat poses a risk, the risk management team must determine the impact and probability of the risk.

(02 marks)

ANSWER IN THIS BOX
True
The probability of occurrence along with the impact gives an indication
of the threat posed by a risk.

(o) A **security policy** provides a way to establish a cost model for information security activities.

(02 marks)

ANSWER IN THIS BOX
False
A security policy provides a way to identify and clarify security goals and objectives.

2) **For each of the questions, select the correct answer, and then say why it is correct, <u>in at most one sentence</u>.**

a) Which one of the following security controls can be used to increase the authentication strength of an access control system?

(i) Key-pad door lock

(ii) Two Factor dongle

(iii) PIN number

(iv) Password

(02 marks)

ANSWER IN THIS BOX
(ii) CORRECT: Using two of the three factors
(something you know, something you have, and something you are)
increase the strength of authentication.

b) A '**worm**' most frequently spreads via,

(i) User misuse of resources

(ii) Software vulnerabilities

(iii) Mobile code attacks

(iv) Infected wireless access points

(02 marks)

ANSWER IN THIS BOX
(ii) CORRECT: Vulnerabilities in software is the most frequent
cause of spread of computer worms from system to system.

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

(i) To protect networks from each other

(ii) To prevent local IP traffic from going out of the network

(iii) To block ICMP and UDP traffic

(iv) To monitor network traffic

(02 marks)

ANSWER IN THIS BOX
(i) CORRECT: The primary objective of a firewall is the protection of
those assets that reside behind it

d) An advantage of **asymmetric** key cryptography is that

(i) It is relatively easy to distribute keys

(ii) Encryption and decryption keys are the same

(iii) It can be efficiently implemented in hardware

(iv) Its execution is very fast

(02 marks)

ANSWER IN THIS BOX
(i) CORRECT: one of the greatest uses of asymmetric key cryptography is to negotiate
or distribute symmetric keys and the ease of distributing the public keys of the users.

e) Which principle recommends the division of responsibilities to prevent a person from committing a fraud?

(i) Least privilege

(ii) Need to know

(iii) Mutual exclusion

(iv) Separation of duties

(02 marks)

ANSWER IN THIS BOX
(iv) CORRECT: The principle of 'separation of duties' recommends that the
responsibilities of critical activities be split to prevent fraud.

f) What principle is applicable when granting users, only those rights necessary for them to perform their work?

(i) Equality & fairness

(ii) Mandatory Access

(iii) Least Privilege

(iv) Separation of Duties

(02 marks)

ANSWER IN THIS BOX
(iii) CORRECT: Least Privilege is the security principle that requires the users
and processes in a system to have the least number of privileges.

g) A one-way encrypted file (a HASH file) is frequently used to store;

(i) User passwords within a computer system

(ii) Customer's names and addresses within a database

(iii) Software authentication keys

(iv) Usernames within a computer system

(02 marks)

ANSWER IN THIS BOX
(i) CORRECT: A one way encrypted file is computationally infeasible
to reverse engineer and therefore is used to store passwords within a computer system

h) Which best describes **qualitative risk analysis**?

(i) A probabilistic method for risk assessment

(ii) A method used to assign severity levels to potential loss, probability of loss, and risks

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

(iv) A method that uses opinions of individuals and a rating system to gauge the severity level of different threats and the benefits of specific countermeasures.

(02 marks)

ANSWER IN THIS BOX
(iv) CORRECT: A qualitative analysis uses opinions of individuals and a rating
system to gauge the severity level of different threats and the benefits
of specific countermeasures.

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

(i) Demonstrate adherence to a standard disaster recovery process

(ii) Agree on the goals and objectives of the plan

(iii) Identify applications to be run during a disaster

(iv) Determine the site to be used during a disaster

(02 marks)

ANSWER IN THIS BOX
(ii) CORRECT: Agree on the goals and objectives of the plan is a critical component
of all project management techniques.

j) Which of the following factors **need not** be considered when qualifying the value of data or an information system to an organization.

(i) The regulations or legislations governing the system

(ii) The number of people that require access to the system or data

(iii) The sensitivity of the data or system and risks associated with data disclosure

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

(02 marks)

ANSWER IN THIS BOX
(ii) 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

k) What activity should an organization conduct in order to gain a common understanding of functions that are critical to its survival, prior to defining a '**Business Continuity Plan (BCP)**'?

(i) A Risk Assessment

(ii) A Business Assessment

(iii) A Disaster Recovery Plan

(iv) A Business Impact Analysis

(02 marks)

ANSWER IN THIS BOX
(iv) CORRECT: A Business Impact Analysis (BIA) is an assessment of an organization's
business functions to develop an understanding of their criticality, recovery time objectives,
and resources needed. By going through a Business Impact Analysis, the organization
will gain a common understanding of functions that are critical to its survival.

l) When a communication link is subject to monitoring, what advantage does **end-to-end** encryption have over link encryption?

(i) Clear text is only available to the sending and receiving processes

(ii) Routing information is included in the message transmission protocol

(iii) Routing information is encrypted by the originator

(iv) Each message has a unique encryption key

(02 marks)

ANSWER IN THIS BOX
(i) CORRECT: Clear text is only available to the sending and receiving processes since
in end-to-end encryption the transmitted information is encrypted at the originating point
and not decrypted until at the terminating point. With link encryption - usually used only
in semi-trusted or trusted networks, the information may be decrypted and re-encrypted at several nodes along the way

m) The overall objective of risk management in Information Security is to;

(i) Eliminate all vulnerabilities, if possible.

(ii) Determine the best way to transfer risk.

(iii) Manage risk to an acceptable level.

(iv) Implement effective countermeasures.

(02 marks)

ANSWER IN THIS BOX
(iii) CORRECT: Risk management is the process of reducing risk to an acceptable level

n) When should security concerns become involved in the systems development life cycle?

(i) Prior to implementation

(ii) Prior to all audits

(iii) During requirements specification

(iv) During goal development

(02 marks)

ANSWER IN THIS BOX
(iii) CORRECT: Security must be considered during requirements specification.

o) What are the three objectives of **information security**?

(i) Prevent, detect, respond to security breaches

(ii) Integrity, authenticity, and completeness of data

(iii) Confidentiality, integrity, and availability of data

(iv) Identification, authentication, nonrepudiation of data

(02 marks)

ANSWER IN THIS BOX
(iii) CORRECT: Standard definition of Information Security

3) (a) Over a communication link, suppose **User A** generates a **cipher text C** for a certain plaintext P by using a **symmetric key S1** and encrypts the **symmetric key S1** with **A's public key K1**. Then the User A sends cipher text C and encrypted symmetric key to the **User B**.

(i) Can the User B retrieve the plain text P? If your answer is "YES", describe the decryption scheme. If your answer is "NO", describe the correct encryption scheme.

(05 marks)

ANSWER IN THIS BOX
User B **cannot** retrieve plain text.
Correct Process:
1. User A generates a **cipher text C** by using a **symmetric key S1.**
2. User A encrypts the **symmetric key S1** with **User B's public key**.
3. User A sends cipher text C and encrypted symmetric key to the **User B.**

(ii) Suppose **User A** requires to confirm the **authenticity** of the **symmetric key S1** to **User B**. Propose a suitable method to authenticate the symmetric key S1.

(05 marks)

ANSWER IN THIS BOX
Process:
1. User A encrypts (signs) the **symmetric key S1** with his **private key**.
2. User A encrypts the signed **symmetric key S1** with **User B's public key**.
3. User A sends double encrypted symmetric key to the **User B.**

(c) Suppose User A generates a cipher text C = EK1[DK1[EK2[P]]] where K1 and K2 are symmetric keys. Can User B retrieve the plain text P= DK2[EK3[DK3[C]]] where K2 and K3 are symmetric keys. Justify your answer.

(05 marks)

ANSWER IN THIS BOX

User B can retrieves the plain text.

User A generates a cipher text C = EK1[DK1[EK2[P]]] where K1 and K2 are symmetric keys.

This is equal to C= EK2[P]

User B retrieve the plain text P= DK2[EK3[DK3[C]]] where K2 and K3 are symmetric keys.

This is equal to P= DK2[C]

(d) Compare and contrast a computer **virus** and **bot**.

(05 marks)

ANSWER IN THIS BOX

Virus is a program that gets into a computer system by means of hardware or software

without the knowledge of the computer user, and then attaches itself to a program file.

The virus then starts to replicate itself and do the damage it has been programmed to do.

Viruses and worms implant software robots, or "bots," into a computer.

They can be controlled remotely to perform tasks without the knowledge of computer owners.

Bots allow hackers into a computer's "back door" to seize control, and then turn into "zombies"

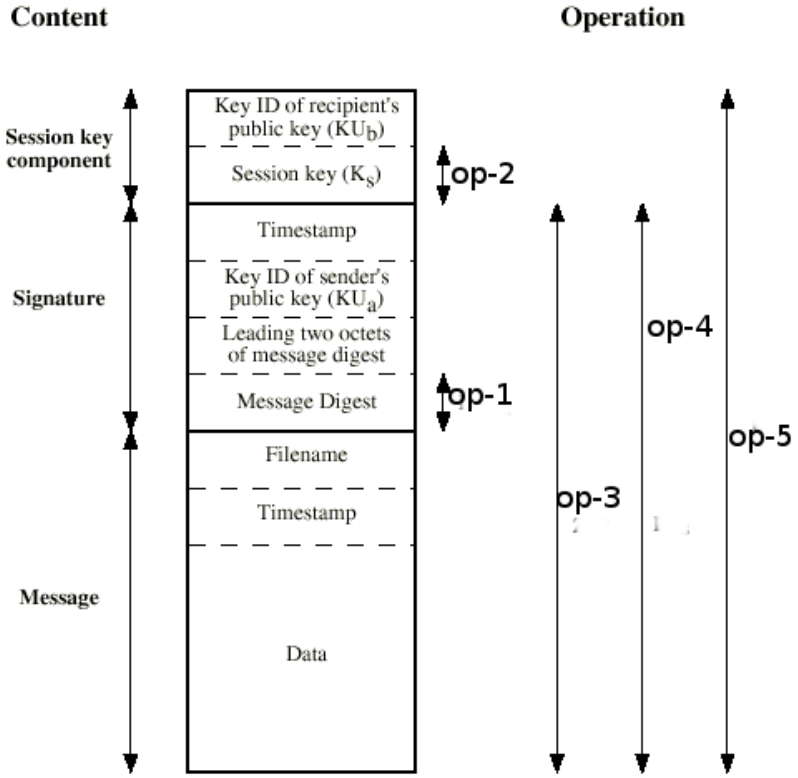
that send out spam or search for other vulnerable networks.

4) a) List three (3) ISO security services provided by the **Secure Socket Layer (SSL)** protocol.

(03 marks)

ANSWER IN THIS BOX
Authentication
Confidentiality
Integrity

b) The format of a PGP e-mail message is given below. Define the operations which are labelled as op-1, op-2, op-3, op-4 and op-5 in the diagram.



(05 marks)

ANSWER IN THIS BOX
op-1: signs the message
op-2: Encrypts the session key with the public key of recipient
op-3: Compress the message
op-4: Encrypt the compressed message with the session key
op-5: Encode the encrypted message

c) Briefly explain the role of the **human factor** in formulating an information system security policy.

(06 marks)

ANSWER IN THIS BOX

The student should describe his/her thought on the matter as an example given bellow:

There's a wide variety of security software available, including firewalls, intrusion detection systems, antivirus solutions etc. Each type of software is designed to perform very specific functions, and using such software will help protect a system. However, even using the very best software, which implements the most advanced technology and the most secure algorithms, cannot guarantee 100% s information security. This is because people are involved in the development and implementation of software, and people make mistakes.

Consequently people, who are a part of any system, are always going to be the weak point in a security system.

The human factor is the underlying reason why many attacks on computers and systems are successful.

d) **"The migration of web applications to the Cloud will introduce additional issues on the privacy of user's sensitive data"**. Elaborate on the above statement.

(06 marks)

ANSWER IN THIS BOX
In a cloud service, there are many questions needing to be addressed in order to determine the
risks to information privacy:
Who are the stakeholders involved in the operation?
What are their roles and responsibilities?
Where is the data kept?
How is the data replicated?
What are the relevant legal rules for data processing?
How will the service provider meet the expected level of security and privacy?
The student should elaborate his/her thought based on the above questions.

****