UNIVERSITY OF COLOMBO, SRI LANKA

UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY (EXTERNAL)

Academic Year 2019 – 3rd Year Examination – Semester 5

IT5205: Information Systems Security

Structured Question Paper

6th July, 2019

(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** on **15 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 your answer.**

(a) Suppose users in two offices would like to access each other’s file servers over the Internet. Digital signature security control could provide confidentiality for such communication.

(02 marks)

ANSWER IN THIS BOX

False

Virtual private network (VPN) security control would provide

confidentiality for those communications.

(b) Suppose the university network begins to experience symptoms of slowness. Upon investigation, it is realized that the network is being bombarded with TCP SYN packets. This is because the obscurity principle of information security is being violated.

(02 marks)

ANSWER IN THIS BOX

False

Security through obscurity refers to security that relies on secret information,

design or implementation details to prevent attack.

Availability principle of information security is being violated.

(c) The Advanced Encryption Standard (AES) algorithm encrypts **twenty three (23)** bytes of a plain text message to **thirty two (32)** 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

True

The block size of AES algorithm is 16 bytes.

Hence cipher text size will be 32 bytes when the plain text size equals to 23 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=10**. If A generates the private key **x=3** and B generates the private key **y=2**, the session key **k** between A and B is **5**.

(02 marks)

ANSWER IN THIS BOX

True

For the private key x and public key X, we have the relation X = g^x mod n.

public key of A (X) = 5^3 mod 10; X= 625 mod 10, X=5

public key of B (Y) = 5^2 mod 100; Y= 25 mod 100, Y=5

Session key k = X^y mod n: k=5^3 mod 10, 625 mod 10 k= 5 OR

Session key k = Y^x mod n: k=5^2 mod 10, k= 5

(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=3** to Nimal. Nimal receives cipher text message C = **27**.

(02 marks)

ANSWER IN THIS BOX

True

C=P^e mod n

C=3^3 mod 33=27 mod 33=27

(f) 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 Nimal signs a plain text message **M=3**. Nimal's signature will be S = **9**.

(02 marks)

ANSWER IN THIS BOX

True

C=P^d mod n

C=3^7 mod 33=2187 mod 33=9

(g) The SHA1 hash algorithm generates a **256** bit hash from an input message of **eight (8)** bytes.

(02 marks)

ANSWER IN THIS BOX

False

The hash size only depends on the algorithm.

It does not depend on the length of the input message.

The SHA1 always generates 160 bit hash values

irrespective of the message length.

(h) The **S/MIME** standard is an example of a hybrid encryption standard.

(02 marks)

ANSWER IN THIS BOX

True

One of the most important advantages of the S/MIME 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 **PGP standard** is **non-repudiation**.

(02 marks)

ANSWER IN THIS BOX

True

ISO security services supported by the PGP standard are:

authenticity, integrity, confidentiality and non-repudiation.

(j) Vendors publish MD5 hash values when they provide software patches for their customers in order to verify vendor authentication.

(02 marks)

ANSWER IN THIS BOX

False

Vendors publish MD5 hash values when they provide software patches

for their customers to verify software integrity.

(k) The final step of a **Qualitative Risk Analysis** is to conduct a cost/benefit analysis to determine whether the organization should implement proposed countermeasure(s).

(02 marks)

ANSWER IN THIS BOX

False

The final step of a **quantitative risk analysis** is conducting a cost/benefit analysis to

determine whether the organization should implement proposed countermeasure(s).

As numeric data regarding impact and probability of occurrence is available,

quantitative risk assessment is the best option here.

(l) A worm most frequently spreads via infected USB drives.

(02 marks)

ANSWER IN THIS BOX

False

A worm most frequently spreads via exploitation of vulnerabilities in software.

(m) The domain of security **Controls** may be categorised into **Physical**, **Technical**, and **Administrative** controls. A **Firewalls** 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 Firewall is an example of Technical Control.

(n) Mike recently implemented an intrusion prevention system designed to block common network attacks from affecting his organization. This is an example of **Risk Avoidance**.
(02 marks)

ANSWER IN THIS BOX

False

Risk mitigation strategies attempt to lower the probability and/or impact of a risk occurring.

Intrusion prevention systems attempt to reduce the probability of a successful attack

and are, therefore, examples of risk mitigation.

(o) Securing information is the responsibility of system administrators.
(02 marks)

ANSWER IN THIS BOX

False

Information security is the responsibility of everyone in the organisation.

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) Why would a hacker use a proxy server?

(i) To create a stronger connection with the target.

(ii) To create a ghost server on the network.

(iii) To obtain a remote access connection.

(iv) To hide malicious activity on the network.

(02 marks)

ANSWER IN THIS BOX

(iv) CORRECT: Hacker hide their IP address by connecting though a proxy server.

b) A substitution cipher substitutes a given symbol with

(i) A Key

(ii) Another symbol

(iii) Multiple other symbols

(iv) Multiple Keys

(02 marks)

ANSWER IN THIS BOX

(ii) CORRECT: A substitution cipher replace one symbol at a time according to a security key.

c) A man-in-the-middle attack can endanger the security of Diffie-Hellman method if the two parties have not

(i) Authenticated

(ii) Joined

(iii) Submitted their keys

(iv) Separated

(02 marks)

ANSWER IN THIS BOX

(i) CORRECT: If two parties are not authenticated, an attack can replace the Diffie-Hellman public keys. Thus they can execute man-in-the-middle attack.

d) Suppose your supervisor is very busy and asks you to log into the Mail Server using his/her user name and password to retrieve some of his e-mails. What should you do?

(i) He/she is your supervisor, so it's okay to do this.

(ii) Ignore the request and hope he/she forgets.

(iii) Decline the request and remind your supervisor that it is against the security policy.

(iv) Since you are also busy, ask your friend to do it.

(02 marks)

ANSWER IN THIS BOX

(iii) CORRECT: User names and passwords must not be shared.

e) The mouse pointer on your computer screen starts to move around on its own and click on things on your desktop. What should you do?

(i) Disconnect your computer from the network

(ii) Unplug your mouse

(iii) Turn your computer off

(iv) All of the above

(02 marks)

ANSWER IN THIS BOX

(i) CORRECT: It seems possible that someone is controlling the computer remotely,

it is best if you can disconnect the computer from the network

(and turn off wireless if you have it) until help arrives.

f) Which is **not** an objective of a network security policy?

(i) Authentication

(ii) Access control

(iii) Identification

(iv) Shoulder surfing

(02 marks)

ANSWER IN THIS BOX

(iv) CORRECT: The Identification, Authentication and Access control are

the objectives of network security. Shoulder surfing is password guessing method.

g) Which of the following is **not** a proper method of maintaining information confidentiality?

(i) Biometric verification

(ii) Password based verification

(iii) Two-factor authentication

(iv) Switching off the computer

(02 marks)

ANSWER IN THIS BOX

(iv) CORRECT: Switching off the computer in the fear of preserving the confidentiality of data is not a proper solution for data confidentiality.

h) Which of the bellow is an example of **physical** hacking?

(i) Inserting a malware loaded USB to a system

(ii) A DDoS (Distributed Denial of Service) attack

(iii) SQL Injection on SQL vulnerable site

(iv) Remote access attempt

(02 marks)

ANSWER IN THIS BOX

(i) CORRECT: If a suspicious gain access to server room or into any confidential area with a malicious pen-drive loaded with malware which will get triggered automatically once inserted to USB port of any PC; such attacks come under physical hacking.

i) Which among the following is the **least** strong wireless encryption standard?

(i) WEP

(ii) WPA

(iii) WPA2

(iv) WPA3

(02 marks)

ANSWER IN THIS BOX

(i) CORRECT: The most widespread types of wireless security standard are Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2 and WPA3.

WEP is weak encryption standard which uses RC4 cipher.

j) Which of the following is **not** an example of a block cipher?

(i) DES

(ii) AES

(iii) Caesar cipher

(iv) Twofish

(02 marks)

ANSWER IN THIS BOX

(iii) CORRECT: A block cipher, encrypts a plain text data block to a cipher-text block. Examples of block ciphers are DES, IDEA and Twofish.

Caesar cipher is an example of a stream cipher.

k) A firewall can protect which of the following attacks?

(i) Phishing

(ii) Dumpster diving

(iii) Denial of Service (DoS)

(iv) Shoulder surfing

(02 marks)

ANSWER IN THIS BOX

(iii) CORRECT: Firewalls are used to protect the computer network and restricts illicit traffic. Denial of Service (DoS) attack is one such automated attack which a firewall can resist and stop from getting executed.

l) Which of the following is **not** a secured mail transferring methodology?

(i) POP3

(ii) PGP

(iii) S/MIME

(iv) SSMTP

(02 marks)

ANSWER IN THIS BOX

(i) CORRECT: POP (Post Office Protocol) is a simple protocol which fetches mail.

S/MIME (Secure/Multipurpose Internet Mail Extensions), SSMTP (Secure-Simple Mail Transfer Protocol), and PGP (Pretty Good Privacy) are examples of protocols for secure mailing.

m) Which of the following is **not** a typical way of web application hacking?

(i) XSS

(ii) CSRF

(iii) SQLi

(iv) Brute-force

(02 marks)

ANSWER IN THIS BOX

(iv) CORRECT: The mistreatment of web applications that uses

HTTP or HTTPS can be done by manipulating the web application through

its graphical web interface. Such popular hacking methods are XSS, CSRF, SQLi.

n) Which of the following is **not** an appropriate solution for preserving user **privacy**?

(i) Install Antivirus

(ii) Use privacy-focussed Social Networks

(iii) Disable cookies

(iv) Use private Browser-window

(02 marks)

ANSWER IN THIS BOX

(i) CORRECT: Preserving data privacy can be archived

by using privacy-focussed search engines, using private browser window and

by disabling cookies.

o) Which of the following is **not** an example of an approach for maintaining **anonymity**?

(i) Use of VPNs

(ii) Use of Tor Browser

(iii) Use of Proxy servers

(iv) Use of Antivirus

(02 marks)

ANSWER IN THIS BOX

(iv) CORRECT:

An anonymity network allows users to block the trackers or agents

which track the identity online. Use of VPNs, Tor Browser, proxy servers

are examples of approaches usually taken by online users for maintaining anonymity.

3) (a) What is the main purpose of a Public Key Infrastructure (PKI)?

(05 marks)

ANSWER IN THIS BOX

The Public key infrastructure (PKI) is the set of hardware, software, policies, processes, and procedures required to create, manage, distribute, use, store, and revoke digital certificates.

(b) List three(3) types of Public Key Infrastructure models available for public key management.

(03 marks)

ANSWER IN THIS BOX

Flat model

Hierarchical Model

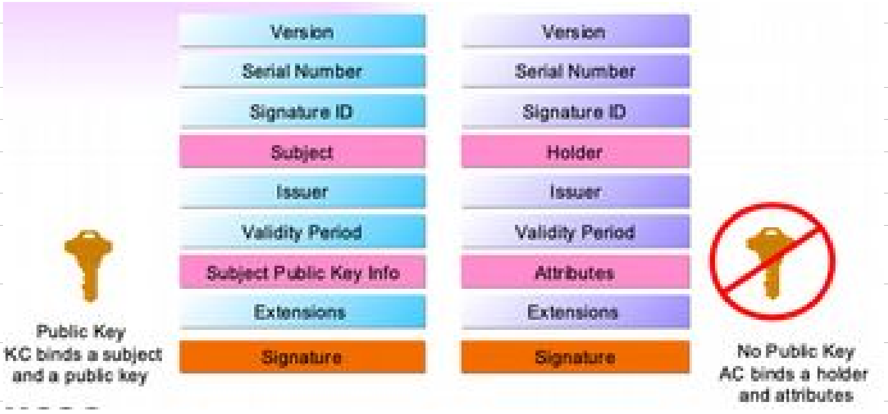
Web of Trust model

(c) Discuss the difference between a Public Key Certificate (PKC) and an Attribute Certificate (AC).

(05 marks)

ANSWER IN THIS BOX

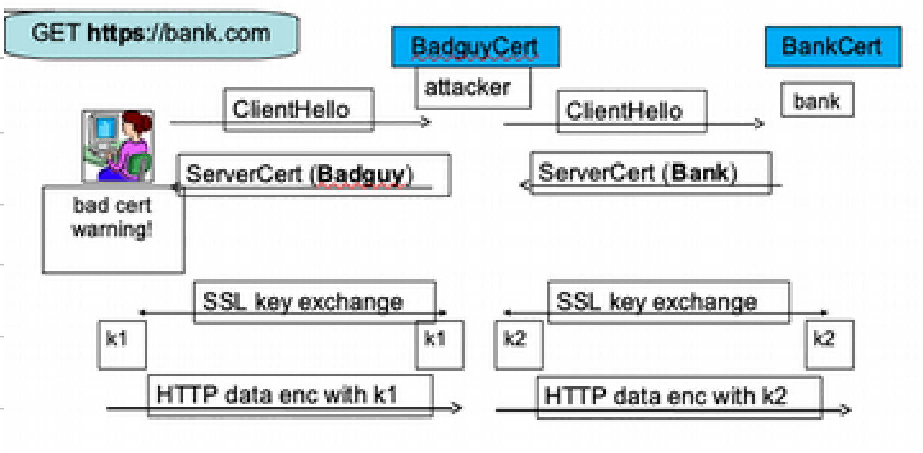
Student should discuss the bellow diagram.



(d) Describe how a man-in-the-middle attack may be performed on a TLS connection.

(07 marks)

ANSWER IN THIS BOX



As shown in the above figure, attacker's proxy server establishes TLS session with a user.

It also establishes a TLS session with the server.

Then attacker's proxy sever decrypts the data from the user, save it and encrypts it back to the server.

4) a) Copyright, Patent and Trade Secrets are three common methods used to provide protections by law to software. Discuss the suitability of each method to protect software.

(06 marks)

ANSWER IN THIS BOX

Copyrights are designed to protect the expression of ideas.

The algorithm is the idea, and the statements of the programming language

are the expression of the idea.

Therefore, copyrights protection is allowed for the program statements themselves,

but not for the design.

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

Thus it is not encouraged to patent the software.

Trade secret protection applies very well to computer software.

Trade secret protection allows distribution of the result of

a secret (the executable program) while still keeping the program design hidden.

b) List two(2) types of IPSec connection modes.

(04 marks)

ANSWER IN THIS BOX

Transport Mode

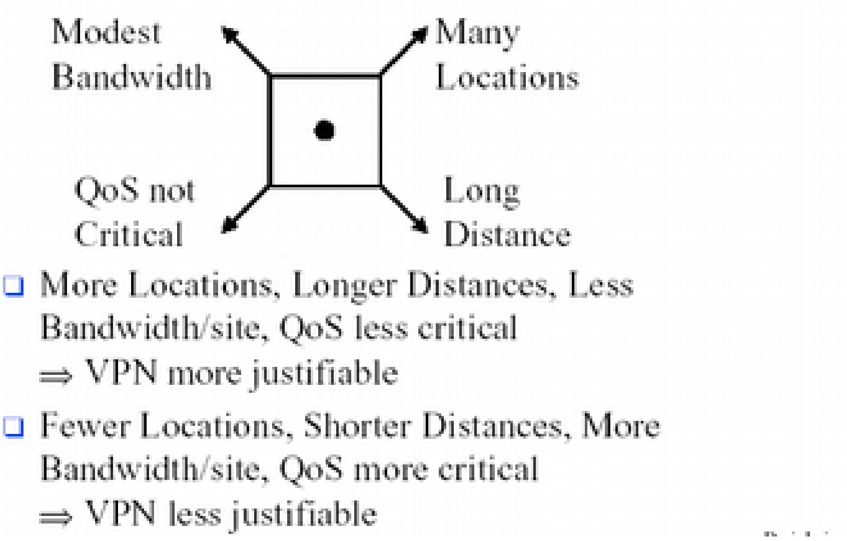
Tunnelling Mode

c) Provision of a Virtual Private Network (VPN) is not always justifiable in interconnecting branches of an organization. Briefly explain the deciding factors for using a VPN.

(04 marks)

ANSWER IN THIS BOX

The student should explain the following factors.



- ❑ More Locations, Longer Distances, Less Bandwidth/site, QoS less critical ⇒ VPN more justifiable
- ❑ Fewer Locations, Shorter Distances, More Bandwidth/site, QoS more critical ⇒ VPN less justifiable

d) You have received an email from your bank informing you, there is a problem with your bank account. The email provides instructions and a web link so you can log in to your bank account and fix the problem on-line. What should you do? Justify your answer.

(06 marks)

ANSWER IN THIS BOX

We should delete the email and report it as spam or phishing.

Any unsolicited email or phone call asking us to enter our account information,

disclose our password, financial account information or the other

private information is suspicious – even if it appears to be from

a company we are familiar with. These e-mails are called phishing e-mails.

****