Index No: ………………...

UNIVERSITY OF COLOMBO, SRI LANKA

UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY (EXTERNAL)

Academic Year 2021 – 3rd Year Examination – Semester 5

IT5205: Information Systems Security

Structured Question Paper

(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 **16 pages**.
- **Answer all 4 questions**. (all questions **do not** carry equal marks)
- **Question 1 and 2** carry 30 marks each **and other two 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 is true or false, and then briefly justify your answer.**

(a) In password protection, the name of a random string of data used to modify a password hash is called a Dongle.

(02 marks)

ANSWER IN THIS BOX

False

The name of a random string of data used to modify a password hash is called Salt.

(b) Suppose we have nodes A, B, C, D and E in a network. We have to generate a total of ten (10) key pairs to let every node communicate with every other node in a bidirectional secure way using the RSA encryption algorithm.

(02 marks)

ANSWER IN THIS BOX

False

Number of key pairs = 5 (one pair for each user)

(c) The Advanced Encryption Standard (AES) algorithm encrypts **thirty two (32)** bytes of a plain text message to **thirty two (32)** bytes of a cipher text message when it uses Electronic Code Book (ECB) mode and the Public Key Cryptography Standard 5 (PKCS5) padding scheme.

(02 marks)

ANSWER IN THIS BOX

False

The block size of AES algorithm is 16 bytes. If plain text is multiplication of a block size,

additional block will be added.

(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=11**. 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 4.

(02 marks)

ANSWER IN THIS BOX

True

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 mod 11; X= 25 mod 11, X=3

public key of B (Y) = 5^3 mod 11; Y= 125 mod 11, Y=4

Session key k = X^y mod n: k=3^3 mod 11, 27 mod 11 k= 5 OR

Session key k = Y^x mod n: k=4^2 mod 11, 16 mod 11 k= 5

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

(02 marks)

ANSWER IN THIS BOX

True

C=P^e mod n

C=2^3 mod 33=8 mod 33=8

(f) **Cyberstalking** is a type of cybercrime in which a person (or victim) is being followed continuously by another person or group of several people through electronic means to harass the victim.

(02 marks)

ANSWER IN THIS BOX

True

In general, Cyberstalking refers to continuous surveillance on the target (or person) done

by a group of people or by the individual person.

(g) The **SHA-512** hash algorithm generates a **128** bit hash from an input message of **sixty four (64)** bits.

(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 SHA-512 always generates 512 bit hash values irrespective of the message length.

(h) A **Directory Server** is a trusted entity that issues digital certificates.

(02 marks)

ANSWER IN THIS BOX

False

A Certification Authority (CA) is a trusted entity that issues digital certificates.

(i) In a **dictionary-attack**, malicious actors use trial-and-error methods to decrypt encrypted data.

(02 marks)

ANSWER IN THIS BOX

false

In a brute-force attack, malicious actors use trial-and-error methods to decode encrypted data.

(j) A **10 bit** plain message will be encrypted to **10 bit** cybertext by a stream cipher.

(02 marks)

ANSWER IN THIS BOX

True

With a stream cipher, binary digits in a message are encrypted one bit at a time,

meaning each plaintext digit equals one ciphertext digit.

Therefore, an encrypted 10-bit message would be 10 bits long.

(k) **Access Control** refers to a security violation, if the system is no more accessible.

(02 marks)

ANSWER IN THIS BOX

False

Availability refers to the security violation, if the system is no more accessible.

(l) In Wi-Fi Security, the **WEP** is one of the most widely used protocols because it offers a more secure encryption algorithm compared to the **WPA**.

(02 marks)

ANSWER IN THIS BOX

False

The WPA2 is one of the most widely used protocol which uses AES.

(m) A **Firewall** is a software device installed at the boundary of a network to protect it against the unauthorized access.

(02 marks)

ANSWER IN THIS BOX

True

A firewall can be the type of either a software.

It can be considered as a device installed at the boundary of a network.

(n) Suppose an employee demands root access to a UNIX system, where you are the administrator; that right or access should not be given to the employee unless that employee has work that requires certain rights and privileges. It can be considered as a perfect example of **least privileges principle** of information security.

(02 marks)

ANSWER IN THIS BOX

True

The least privileges principle of cyber security states that no rights,

access to the system should be given to any of the employees

of the organization unless he/she needs those particular rights,

access in order to complete the given task.

(o) A Virtual Private Network (VPN) is usually based on the IPsec (IP Security) or TLS (Transport Layer Security) protocols.

(02 marks)

ANSWER IN THIS BOX

True

IPSec and TLS protocols provides authentication and encryption in between

two network end points. Thus these protocols can be used to implement VPNs.

2) **For each of the questions, select the correct answer, and then briefly justify your answer.**

a) You are provided the plain text “KASUN”. You need to convert the given plain text into cipher text under the Caesar cipher encryption technique. Which of the following options is the correct cipher text for the given plain text if the key is 2?

i. WPEKL

ii. MCUWP

iii. NUSAK

iv. ZQEKM

(02 marks)

ANSWER IN THIS BOX

(iI) CORRECT:

E (P , K) = (P + K) mod 26

Therefore,

E (K , 2) = (11 + 2) mod 26 = 20 = M ; E (A , 2) = (1 + 2) mod 26 = 20 = C

E (S , 2) = (18 + 2) mod 26 = 20 = U; E (U , 2) = (20 + 2) mod 26 = 22 = W

E (N , 2) = (13 + 2) mod 26 = 15 = P

Hence, the cipher text is "MCUWP".

b) Which of the following ciphers is a block cipher?

i. Caesar cipher

ii. Vernam cipher

iii. AES cipher

iv. RC4 cipher

(02 marks)

ANSWER IN THIS BOX

(iii) CORRECT:

The AES cipher uses a block of plain text, each block containing 16 bytes.

c) Which one of the following modes of operation in AES is suitable for encrypting an image?

i. Cipher Feedback (CFB)

ii. Cipher Block chaining (CBC)

iii. Electronic code book (ECB)

iv. Output Feedback (OFB)

(02 marks)

ANSWER IN THIS BOX

(ii) CORRECT:

In ECB mode, repetitions in Plain Text lead to repetitions in Cipher Text.

CFB and OFB modes convert AES into stream cipher.

Thus some of the image properties may be visible in cipher text as well.

CBC is the suitable mode.

d) Among the following options, chose the strongest encryption algorithm?

i. DES (Data Encryption Standard)

ii. Double DES

iii. Triple DES

iv. AES (Advance Encryption Standard)

(02 marks)

ANSWER IN THIS BOX

(iv) CORRECT:

It has been proved that the AES (128, 192, or 256 keys) performs much better than the

all the other DES, whether it be single DES or series of DES.

e) Which of the following algorithms is used to create a message digest by a network security protocol?

i. RSA

ii. AES

iii. DES

iv. MD5

(02 marks)

ANSWER IN THIS BOX

(iv) CORRECT:

RSA: Basically, it is an algorithm used to encrypt and decrypt messages.

AES: Advanced Encryption Standard is a symmetric key encryption algorithm.

DES: Data Encryption Standard is a symmetric key encryption algorithm.

MD5: It is a widely used cryptographic hash function that produces a 128-bit hash value.

f) Amongst which of the following is a suitable application for Hashing,

i. Network Traffic Analysis
ii. Password protection
iii. File Encryption
iv. Intruder Prevention

(02 marks)

ANSWER IN THIS BOX

(ii) CORRECT:

Despite the fact that hashing is not encryption,

it is a type of cryptography that can be used for a save password.

g) Which of the following does **not** relate to stealing one's idea or invention of others and using it for their own benefits?

i. Piracy
ii. Plagiarism
iii. Intellectual property rights
iv. Digital Watermarking

(02 marks)

ANSWER IN THIS BOX

(iv) CORRECT:

The stealing ideas or the invention of others and using them for their own profits can also be

defined in several different ways, such as piracy, intellectual property rights, and plagiarism.

Digital watermarks is a technology to protect intellectual property rights.

h) Which of the following is **not** an anti-spam technique?

i. Signature-based content filtering

ii. DNS filtering

iii. Bayesian Content Filtering

iv. Collaborative content filtering

(02 marks)

ANSWER IN THIS BOX

(ii) CORRECT:

Anti-spamming techniques help in reducing the spamming of unwanted messages and emails.

Signature-based content filtering, Bayesian Content Filtering, and

collaborative content filtering are examples of anti-spam technique.

i) If you receive an e-mail with an attachment from someone you don't know, what should you do?

i. Forward it to the police immediately.

ii. Delete it without opening it.

iii. Open it and respond to them saying you don't know them.

iv. Reply and ask them for their personal information.

(02 marks)

ANSWER IN THIS BOX

(ii) CORRECT:

Replying or forwarding unknown email supports malware infections.

It may be a phishing email as well.

j) The man-in-the-middle attack can endanger the security of the **Diffie-Hellman** method if two parties are not

i. Mutually authenticated

ii. joined

iii. separated

iv. submitted their initial keys

(02 marks)

ANSWER IN THIS BOX

(i) CORRECT:

If two parities are authenticated, an attacker cannot establish a bogus session key.

k) Which of the following is a part of network identification?

i. UserID

ii. Password

iii. OTP

iv. Fingerprint

(02 marks)

ANSWER IN THIS BOX

(i) CORRECT:

UserID is a part of identification.

Password, OTP, Fingerprint are part of authentication.

The answer is UserID.

l) In public key cryptography, a key that digitally signs the message is known as

i. Public key of sender

ii. Private key of sender

iii. Private key of recipient

iv. Public key of recipient

(02 marks)

ANSWER IN THIS BOX

(ii) CORRECT:

Public key cryptography has 2 keys.

They are private key and a public key.

The private key of sender signs the message.

m) Which of the following algorithms provides non-repudiation?

i. DES

ii. RSA

iii. 3DES

iv. AES

(02 marks)

ANSWER IN THIS BOX

(ii) CORRECT:

Asymmetric key cryptography algorithm is required to create digital signatures.

Thus correct answer is RSA.

n) Which of the following is **not** an example of a physical data leakage?

i. Phishing

ii. Dumpster diving

iii. Shoulder surfing

iv. Side channel attack

(02 marks)

ANSWER IN THIS BOX

(i) CORRECT:

Phishing is a type of social engineering where an attacker sends a

fraudulent message designed to trick a human victim into revealing sensitive information.

o) Which of the following is an independent malicious program that does not require any host program to run?

i. Trap door

ii. Trojan Horse

iii. Virus

iv. Worm

(02 marks)

ANSWER IN THIS BOX

(iv) CORRECT:

A computer worm is an independent malicious computer program that replicates itself

to spread to other computers. Often, it uses a computer network to spread,

relying on security failures on the target computer to gain access.

3) (a) A security service company is conducting an information security audit in several risk areas within a major corporation. Identify one (1) risk each of

- access to cloud storage devices.
- using social networking.
- access to removable media.

(06 marks)

ANSWER IN THIS BOX

Sensitive data lost through access to the cloud that has been compromised due to weak security settings

Data loss through access to personal or corporate instant messaging and social media sites

The unauthorized transfer of data containing valuable corporate information to a USB drive

(b) State two (2) common symptoms that may indicate that a personal computer is infected by malware.

(04 marks)

ANSWER IN THIS BOX

The computer gets increasingly slower to respond.

The computer freezes and requires reboots.

(c) List two (2) possible limitations of using a firewall in a network.

(04 marks)

ANSWER IN THIS BOX

A misconfigured firewall can create a single point of failure.

Network performance can slow down.

(d) Explain the **Transport Layer Security (TLS) Record** protocol by using a suitable diagram.

(06 marks)

ANSWER IN THIS BOX

The Record Protocol provides data confidentiality using symmetric key cryptography

and data integrity using a keyed Message Authentication Checksum (MAC).

The keys are generated uniquely for each session based on the security parameters

agreed during the TLS handshake.

4) a) List two (2) **disadvantages** of an Intrusion Detection System (IDS).

(04 marks)

ANSWER IN THIS BOX

The IDS does not stop malicious traffic.

The IDS requires other devices to respond to attacks.

b) Two geographically distinct corporations have completed a merger. The network engineer has been asked to connect the two corporate networks without the expense of leased lines. Propose a design for a cost effective security solution to connect these two corporate networks.

(06 marks)

ANSWER IN THIS BOX

The security gateway to security gateway VPN is an extension of a classic WAN network that provides a static interconnection of entire networks.

Frame Relay would be a better choice than leased lines, but would be more expensive than implementing gateway to security gateway VPNs.

The other options refer to remote access VPNs which are better suited for connecting users to the corporate network versus interconnecting two or more networks.

The student should propose an acceptable solution and justify it.

c) Compare and contrast the level of security of messaging using encrypted email (either PGP or SMIME) and end-to-end encrypted messaging apps (WhatsApp, Signal, or iMessage).

(04 marks)

ANSWER IN THIS BOX

When you use the Messages app to send end-to-end encrypted messages, all chats,

including their text and any files or media, are encrypted as the data travels between devices.

However it does not support digital signatures.

Since PGP or SMIME supports digital signatures, it provides,

authentication, integrity, confidentiality and non-repudiation security services.

d) An administrator is trying to develop a Bring Your Own Device (BYOD) security policy for employees who are bringing a wide range of devices to connect to the company network. List three (3) objectives of the BYOD security policy.

(06 marks)

ANSWER IN THIS BOX

Rights and activities permitted on the corporate network must be defined.

Safeguards must be put in place for any personal device being compromised.

The level of access of employees when connecting to the corporate network must be defined.

****