Index No: ……...

UNIVERSITY OF COLOMBO, SRI LANKA

UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY (EXTERNAL)

Academic Year 2023 – 3rd Year Examination – Semester 5

IT5306: Principles of Information Security

Structured Question Paper

(TWO HOURS)

Important Instructions:

- The duration of the paper is **Two (2) hours**.
- The medium of instruction and questions is English.
- This paper has **4 questions** on **13 pages**.
- **Answer all 4 questions**. (all questions **do not** carry equal marks)
- **Questions 1 and 2** carry **20** marks each **and the other two questions 30** 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 (✕), 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 is true or false, and then briefly justify your answer.**

(a) A **transposition** cipher replaces one character with another character.

(02 marks)

ANSWER IN THIS BOX
False
A **substitution** cipher replaces one character with another character.

(b) Suppose we have nodes A, B, C, D. E and F in a network. We have to generate a total of ten (10) keys to let every 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 = n*(n-1)/2 = 6*5/2= 15

(c) The Data Encryption Standard (DES) algorithm encrypts **thirty (30)** 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
True
The block size of DES algorithm is 8 bytes.
The last block will be padded. Thus ciphertext size is 32 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=11**. If A generates the private key **x=7** and B generates the private key **y=5**, the session key **k** between A and B is 1.

(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) = $5^7 \bmod 11$; X= 78125 mod 11, X=3
public key of B (Y) = $5^5 \bmod 11$; Y= 3125 mod 11, Y=1
Session key k = $X^y \bmod n$: k=$3^5 \bmod 11$, 243 mod 11 k= 1 OR
Session key k = $Y^x \bmod n$: k=$1^7 \bmod 11$, 1 mod 11 k= 1

(e) Nimal generates two prime numbers **p=7** and **q=17** during the **RSA** key generation process. He selects his public key **e** as **5** together with **n=119**. His private key **d** is equal to **77** together with **n=119**.

(02 marks)

ANSWER IN THIS BOX
True
e*d mod (p-1)(q-1)=1
5*77 mod 6*16= 385 mod 96=1
Private key = (77,119)

(f) Nimal has an RSA public key **(e , n) = (7 , 33)** and a private key = **(d , n) = (3 , 33)**. Suppose Kamal encrypts a plain text message **M=2** to Nimal. Nimal receives cipher text message **C = 29**.

(02 marks)

ANSWER IN THIS BOX
True
$C=P^e \bmod n$
$C=2^7 \bmod 33$= 128 mod 33=29

(g) Nimal has an RSA public key **(e , n) = (7 , 33)** and a private key = **(d , n) = (3 , 33)**. Suppose

Nimal signs a plain text message **M=3** to Kamal. Kamal receives signature **S = 9**.

(02 marks)

ANSWER IN THIS BOX
True
$S=P^d \bmod n$
$C=3^3 \bmod 33= 9 \bmod 33=9$

(h) The **SHA1** 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 SHA1 hash algorithm generates a 160 bit hash value.

(i) Counter Mode (**CTR**) encrypts plaintext faster than Cipher Block Chaining (**CBC**) mode.

(02 marks)

ANSWER IN THIS BOX
True
Counter Mode (CTR) encrypts plaintext parallel thus it is faster than CBC.

(j) The Greatest Common Divisor (GCD) of **18** and **300** is equal to **6**.

(02 marks)

ANSWER IN THIS BOX
True

300= 16*18+ 12 => GCD(18,12)
18= 1*12 +6 => GCD(12,6)
12= 2*6+0 => GCD(6,0)
GCD(18,300)=GCD(300,18)=GCD(18,12)=GCD(12,6)=GCD(6,0)=6

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

a) Which of the following is **not** a type of **symmetric key cryptography** technique?

i. Caesar cipher
ii. Data Encryption Standard (DES)
iii. Diffie-Hellman cipher
iv. AES cipher

(02 marks)

ANSWER IN THIS BOX
(iii) CORRECT:
The Diffie-Hellman uses a pair of asymmetric keys for encryption and decryption processes.
All the rest mentioned cipher techniques use the same key for encryption as
well as decryption.

b) What function can be used to convert a hash function into a **MAC** function?

i. SHA1
ii. HMAC
iii. AES
iv. RC4

(02 marks)

ANSWER IN THIS BOX
(ii) CORRECT:
SHA1 is a hash function.

AES and RC4 are encryption algorithms.
Hash Mac (HMAC) converts hash into MAC.

c) Which of the following is **not a mode of operation** for the Block Ciphers in cryptography?

i. Cipher Feedback (CFB)
ii. Cipher Block chaining (CBC)
iii. Electronic code book (ECB)
iv. PKCS5

(02 marks)

ANSWER IN THIS BOX
(iv) CORRECT:
CFB, CBC and ECB are modes of operations of a block cipher.
PKCS5 is padding scheme. Thus the correct answer is iv.

d) Which of the following security services **cannot** be achieved using the **Hash** functions?

i. Password Check
ii. Data Integrity check
iii. Digital Signatures
iv. Data retrieval in its original form

(02 marks)

ANSWER IN THIS BOX
(iv) CORRECT:
The hash functions are irreversible and has pre-image resistance property.
Therefore it is almost impossible to obtain the original data form its hash value.

e) Which of the following algorithms is used to create a digital signature?

i. ECC

ii. AES

iii. DES

iv. 3DES

(02 marks)

ANSWER IN THIS BOX
(i) CORRECT:
ECC is an algorithm used to digitally sign messages.
AES, DES and 3DES are standard symmetric key encryption algorithms.

f) What is the block size of plaintext in AES algorithm?

i. 64 bits

ii. 128 bits

iii. 192 bits

iv. 256 bits

(02 marks)

ANSWER IN THIS BOX
(ii) CORRECT:
The AES algorithm uses blocks of plain text one at a time to encrypt them into ciphertext.
The size of each block in the AES algorithm is 128 bits.
The AES algorithm has three different key sizes 128, 192 and 256 bits.

g) Which of the following is the main **disadvantage** of the ECB (Electronic Code Book)?

i. It requires large block size.

ii. Padding is done to make the plain text divisible into blocks of fixed size.

iii. It is prone to cryptanalysis since there is a direct relationship between plain text and cipher text.

iv. None of the above.

(02 marks)

ANSWER IN THIS BOX
(iii) CORRECT:

In ECB, there lies a direct relation between the plaintext and the ciphertext.
Therefore, it is easy for an outsider to break the encryption logic and steal the data.

h) What aspect of information security is **not** ensured by cryptography?

i. Confidentiality

ii. Authorization

iii. Integrity

iv. Non-repudiation

(02 marks)

ANSWER IN THIS BOX
(ii) CORRECT:
Confidentiality, which uses encryption algorithms to encrypt and hide data.
Integrity uses hashing algorithms. Non-repudiation uses public key algorithms.
Authorization is the component which cannot archive by the cryptographic algorithms.

i) Which of the following refers to the violation of the principle of a computer is no more accessible?

i. Access control

ii. Confidentiality

iii. Availability

iv. Integrity

(02 marks)

ANSWER IN THIS BOX
(iii) CORRECT:
Access control is a security technique that regulates who or what can view or use resources in a computing environment.
Confidentiality means that only authorized individuals/systems can view sensitive or classified information. Integrity measures protect information from unauthorized alteration.
Availability refers to the violation of principle, if the system is no more accessible.

j) Why are the factors like Confidentiality, Integrity, Availability, and Authenticity considered as the security fundamentals?

i. They help in understanding the hacking process

ii. These are the main elements for any security breach

iii. They help to understand the security and its components in a better manner

iv. All of the above

(02 marks)

ANSWER IN THIS BOX
(iii) CORRECT:
Confidentiality, Integrity, Availability and Authenticity all these four elements
helps in understanding security and its components.

3) (a) What is the main objective of **system security planning**?

(04 marks)

ANSWER IN THIS BOX
Maximize security of a system while minimizing costs.

(b) Name **two (2)** strategies that can be adopted during system security planning to prevent targeted cyber intrusions.

(06 marks)

ANSWER IN THIS BOX
Strategy 1: Patch third-party applications and operating system vulnerabilities.
Strategy 2: Restrict administrative privileges.

(c) Once a system is appropriately built, secured, and deployed, the process of maintaining security should be continuous. This is due to the constantly changing environment, the discovery of new vulnerabilities, and hence, exposure to new threats.
Name **four (4)** activities that can be done related to system security maintenance.

(08 marks)

ANSWER IN THIS BOX
Activity 1: Monitoring and analyzing logging information
Activity 2: Performing regular backups
Activity 3: Regularly testing system security
Activity 4: Regularly updating all software.

(d) Briefly explain the difference between making **data backups** and making **data archives** as a part of security maintenance of systems?

(04 marks)

ANSWER IN THIS BOX
Backup is the process of making copies of data at regular intervals, allowing the recovery of lost or corrupted data over relatively short time periods of a few hours to some weeks.
Archive is the process of retaining copies of data over extended periods of time, being months or years, in order to meet legal and operational requirements to access past data.

(e) What is meant by **inference** with reference to database security?

(04 marks)

ANSWER IN THIS BOX
Inference, as it relates to database security, is the process of performing authorized queries and deducing unauthorized information from the legitimate responses received.

(f) The two SQL commands **GRANT** and **REVOKE** can be used in managing database security. Briefly describe the functionality of them.

(04 marks)

ANSWER IN THIS BOX
GRANT: this can be used to grant one or more access rights or can be used to assign a user to a role.
REVOKE: this facilitates removing any already granted access rights from a user.

4) a) Briefly describe what is meant by **malware**?

(02 marks)

ANSWER IN THIS BOX
A malware is a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim.

b) Provide **four (4)** examples for types of malware that can threaten computer software systems.

(04 marks)

ANSWER IN THIS BOX
Infected content - Viruses

Vulnerability exploit - worms
Social engineering - spam emails, trojans
Attack agents - Zombies, bots
Information theft - Keyloggers, phishing, spyware
Stealthing - Backdoors, rootkits.

c) What is meant by a **backdoor** to a software system?

(04 marks)

ANSWER IN THIS BOX
A backdoor is a secret entry point into a program that allows someone who is aware of the backdoor to gain access without going through the usual security access procedures.

d) During its lifetime, a typical virus goes through the four phases: dormant phase, propagation phase, triggering phase, and execution phase. Briefly describe what occurs in each phase.

(08 marks)

ANSWER IN THIS BOX
Dormant phase: The virus is idle and eventually be activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit.
Propagation phase: The virus places a copy of itself into other programs or into certain system areas on the disk.
Triggering phase: The virus is activated to perform the function for which it was intended.
Execution phase: The intended function is performed.

(e) What is the difference between **computer crime** and **cybercrime**?

(04 marks)

ANSWER IN THIS BOX

The term cybercrime has a connotation of the use of networks specifically, whereas computer crime may or may not involve networks.

(f) What is meant by **pseudonymity** in the context of ensuring privacy of computer users?

(04 marks)

ANSWER IN THIS BOX

Pseudonymity ensures that a user may use a resource or service without disclosing its user identity, but can still be accountable for that use.

(g) Name **two (2)** computer crimes as identified by the Sri Lanka Computer Crime Act, No.24 of 2007.

(04 marks)

ANSWER IN THIS BOX

Securing unauthorised access to a computer

Causing a computer to perform a function without lawful authority

****