University of Colombo, Sri Lanka

University of Colombo School of Computing

DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY (EXTERNAL)

Academic Year 2023 — 3^{rd} Year Examination — Semester 5

IT5306 — Principles of Information Security

Structured Question Paper
(2 Hours)

To be completed by the candidate							
Index Number							

Important Instructions

- The duration of the paper is **2 hours**.
- The medium of instructions and questions is English. Students should answer in the medium of English language only.
- This paper has **4 questions** on **12 pages**. Answer **all** questions.
- Question **1 & 2** carry **30** marks each and question **3 & 4** carry **20** marks each.
- Write your answers **only on the space provided** on this question paper.
- Do not tear off any part of this question paper. Under no circumstances may this paper (or any part of this paper), 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 or part of a page is not printed, please inform the supervisor/invigilator immediately.
- Any electronic device capable of storing and retrieving text, including electronic dictionaries, smartwatches, and mobile phones, is not allowed.
- Non-programmable calculators are **allowed**.
-

To be completed by the examiners

1	
2	
3	
4	
Total	

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

(a) A **dictionary** attack involves trying every possible key until the correct one is found.

(03 marks)

ANSWER IN THIS BOX

False

A **brute-force** attack involves trying every possible key until the correct one is found.

A **dictionary** attack involves trying every possible words in a dictionary

until the correct one is found.

(b) **Steganography** is the study of breaking codes and ciphers.

(03 marks)

ANSWER IN THIS BOX

False

Steganography is the technique of hiding data within an ordinary message.

(c) The Advanced Encryption Standard (AES) algorithm encrypts **thirty (30)** bytes of a plain text message to **thirty two (32)** bytes of a cipher text message when it uses **Counter mode (CTR)** of operation.

(03 marks)

ANSWER IN THIS BOX

False

In CTR mode, block cipher encrypts counters and

then the plaintext XOR with encrypted counters.

Thus ciphertext and plaintext length are equal.

(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=3** and the integer **n=17**. If A generates the private key **x=7** and B generates the private key **y=11**, then the session key **k** between A and B is **11**.

(03 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) = $3^7 \bmod 17$; X= 2187 mod 17, X=11

public key of B (Y) = $3^{11} \bmod 17$; Y= 177147 mod 11, Y=7

Session key k = $X^y \bmod n$: k=$11^{11} \bmod 17$, k= 12 OR

Session key k = $7^7 \bmod n$: k= 12

(e) Nimal generates two prime numbers **p=11** and **q=17** during the **RSA** key generation process. He selects his public key **e** as **7** together with **n=187**. Then his private key **d** is equal to **19** together with **n=187**.

(03 marks)

ANSWER IN THIS BOX

False

e*d mod (p-1)(q-1)=1

7*19 mod 10*16= 133 mod 160 =133

Thus private is is wrong.

(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=3** to Nimal. Then Nimal receives cipher text message **C = 29**.

(03 marks)

ANSWER IN THIS BOX

False

$C=P^e \bmod n$

$C=3^7 \bmod 33$= 2187 mod 33=9

(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=5** to Kamal. Then Kamal receives signature **S = 26**.

(03 marks)

ANSWER IN THIS BOX

True

$S=P^d \bmod n$

$C=5^3 \bmod 33= 125 \bmod 33=26$

(h) The **MD5** hash algorithm generates a **128** bit hash from an input message of **sixty four (64)** bits.

(03 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 hash algorithm generates a 128 bit hash value.

(i) **Phishing** attacks involve the use of malicious software attachments in emails.

(03 marks)

ANSWER IN THIS BOX

False

Phishing is a social engineering technique where attackers attempt to deceive

individuals into divulging sensitive information.

(j) The Greatest Common Divisor (GCD) of **12460** and **8468** is equal to 4.

(03 marks)

ANSWER IN THIS BOX

True

12460= 1*8468+ 3992 => GCD(8468,3992)

8468= 2*3992 +484 => GCD(3992,484)

3992= 8*484+120 => GCD(184,120)

484=4*120+4=> GCD(120,4)

120=30*4+0=>GCD(4,0)

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

a) Which encryption algorithm is considered **insecure** and is no longer recommended for general use?

i. Rivest-Shamir-Adleman (RSA) cipher

ii. Data Encryption Standard (DES) Cipher

iii. Diffie-Hellman cipher

iv. Advanced Encryption Standard (AES) cipher

(03 marks)

ANSWER IN THIS BOX

(ii) CORRECT:

DES uses 56 bit keys and thus it can be bruteforse.

b) Which cryptographic function is commonly used for data **integrity** verification?

i. SHA1

ii. RSA

iii. AES

iv. RC4

(03 marks)

ANSWER IN THIS BOX

(i) CORRECT:

SHA1 is a hash function and it uses for check the integrity.

AES and RC4 are encryption algorithms.

RSA is a public key cryptographic algoritm.

c) Which cryptographic algorithm is commonly used for **digital signatures** and **key exchange**?

i. RSA
ii. AES
iii. SHA1
iv. DES

(03 marks)

ANSWER IN THIS BOX

(i) CORRECT:

AES and DES use for data encryption and decryption.

SHA1 uses for digital signature but not use for key exchange.

RSA uses for digital signature and key exchange.

d) What is the primary **disadvantage** of **symmetric-key** cryptography?

i. Slow encryption process
ii. Requires a secure channel for key exchange
iii. Key distribution problem
iv. Vulnerability to brute-force attacks

(03 marks)

ANSWER IN THIS BOX

(iii) CORRECT:

A symmetric key algorithm uses same key for encryption and decryption.

Thus sharing the same key between a sender and a recipient

via the same transmission media is not possible.

e) Which cryptographic protocol is commonly used to secure web communications?

i. TLS

ii. PGP

iii. SMIME

iv. SSH

(03 marks)

ANSWER IN THIS BOX

(i) CORRECT:

PGP and SMIME are e-mail security protocols.

SSH uses for remote access the servers.

TLS uses to protect the web communication.

f) Which is the key length of the Advanced Encryption Standard (**AES**) cipher?

i. 64 bits

ii. 192 bits

iii. 56 bits

iv. 512 bits

(03 marks)

ANSWER IN THIS BOX

(ii) CORRECT:

The AES algorithm uses 128, 192 or 256 bits keys.

g) What does the term "**Phishing**" refer to in the context of information system security?

i. Malware attack

ii. Physical security breach

iii. Social engineering attack

iv. Crypto analysis

(03 marks)

ANSWER IN THIS BOX

(iii) CORRECT:

The most of the cases, phishing attacks collect user credentials by using looks like web sites

thus it is a kind of social engineering attack.

h) What is the purpose of a **Certificate Authority (CA)** in public key infrastructure (PKI)?

i. Encrypting data at rest
ii. Managing user access controls
iii. Authentication of public keys
iv. Filtering email communications

(03 marks)

ANSWER IN THIS BOX

(iii) CORRECT:

A CA issues a public key certificate to an entity. It binds the entity and the public key.

i) What is the purpose of the HTTP Strict Transport Security (HSTS) header?

i. Enforcing HTTPS connections for a specified duration
ii. Blocking malicious websites
iii. Encrypting data at rest
iv. Securing email communication

(03 marks)

ANSWER IN THIS BOX

(i) CORRECT:

HTTP Strict Transport Security (HSTS) is a simple and widely supported

standard to protect visitors by ensuring that their browsers always

connect to a website over HTTPS.

j) Which of the following is an example of a **physical** security control?

i. Firewall

ii. Encryption

iii. Biometric access control

iv. Intrusion Detection System (IDS)

(03 marks)

ANSWER IN THIS BOX

(iii) CORRECT:

Firewall and IDS considered as technical security controls.

Encryption is cryptographic control.

Biometric controls physically accessing a computer resource.

3) (a) Describe the difference between **symmetric** and **asymmetric** key cryptography. Provide an example of when each is commonly used.

(05 marks)

ANSWER IN THIS BOX

Symmetric encryption uses a single key for both encryption and decryption,

whereas asymmetric encryption uses a pair of keys (public and private).

Symmetric encryption is often used for bulk data encryptio.

Asymmetric encryption is commonly used for secure key exchange,

as seen in SSL/TLS protocols for secure web communication.

(b) Briefly explain the importance of regular software updates in maintaining information system security. Provide examples of vulnerabilities that can be mitigated through timely updates.

(05 marks)

ANSWER IN THIS BOX

Regular software updates are crucial for information security as

they patch known vulnerabilities.

For instance, the WannaCry ransomware exploited a vulnerability

in unpatched Windows systems.

Timely updates can prevent such attacks by closing security loopholes.

(c) Explain the concept of **"least privilege"** in the context of database security.

(05 marks)

ANSWER IN THIS BOX

Least privilege means granting users the minimum level of access or permissions

necessary to perform their job functions.

This principle helps minimize the risk of unauthorized access and potential security breaches.

(d) How do cryptocurrencies differ from traditional electronic payment methods?

(05 marks)

ANSWER IN THIS BOX

Cryptocurrencies are decentralized digital currencies that operate on blockchain technology,

whereas traditional electronic payment methods typically involve centralized institutions like banks.

Cryptocurrencies offer increased privacy, global accessibility, and potential for investment, but they also come with volatility and regulatory challenges.

4) a) Explain the impact and both the positive and negative aspects of the **General Data Protection Regulation (GDPR)** on global data protection standards. Include both positive and negative aspects.

(05 marks)

ANSWER IN THIS BOX

The GDPR has significantly influenced global data protection standards.

Positively, it has enhanced individual privacy rights, increased transparency in data processing, and encouraged responsible data handling practices.

However, challenges include the complexity of compliance for businesses, especially smaller ones, and potential conflicts with other jurisdictions' regulations.

b) With the rise of social media platforms, privacy concerns have become paramount.
(i) Elaborate on the challenges faced by users in maintaining their privacy on such platforms.
(ii) Suggest measures that can enhance user privacy.

(05 marks)

ANSWER IN THIS BOX

Social media platforms often collect vast amounts of user data for targeted advertising.

Users face challenges in understanding complex privacy settings,

potential data sharing with third parties, and risks of data breaches.

Enhancing user privacy requires transparent policies,

user-friendly controls, and regulatory oversight.

(c) Briefly explain the importance of **User Awareness** in Information System Security.

(05 marks)

ANSWER IN THIS BOX

User awareness is crucial in information system security as

it directly impacts the human element, often considered the weakest link in cybersecurity.

Educating users about the risks of social engineering, phishing attacks,

and the significance of strong password practices helps create a security-aware

culture within an organization.

When users understand their role in maintaining information security,

they become proactive in identifying and reporting potential threats.

(d) (i) Explain the concept of input validation in program security.
(ii) Why is it crucial for preventing various types of attacks?

(05 marks)

ANSWER IN THIS BOX

Input validation is the process of inspecting and filtering data entered into a software application

to ensure that it meets specified criteria before it is processed or stored.

This is crucial for preventing various types of attacks, such as SQL injection,

cross-site scripting (XSS), and buffer overflows.

By validating input, software can detect and reject potentially harmful or malicious data,

thereby protecting against unauthorized access, data corruption, and other security vulnerabilities.

Proper input validation ensures that only safe and expected data is processed,

reducing the risk of exploitation.

****