



University of Colombo, Sri Lanka



University of Colombo School of Computing

BIT

DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY (EXTERNAL)

Academic Year 2024 — 3rd 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 15 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**.
- *All Rights Reserved.* This question paper can NOT be used without proper permission from the University of Colombo School of Computing.

**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 digital signature ensures data **confidentiality**.

(03 marks)

ANSWER IN THIS BOX**False**

A digital signature ensures both data integrity and authenticity.

- (b) **Perfect forward secrecy** ensures that **future** communications remain secure even if the private key is compromised.

(03 marks)

ANSWER IN THIS BOX**False**

Perfect forward secrecy ensures that **past** communications remain secure even if the private key is compromised.

- (c) The Advanced Encryption Standard (AES) algorithm encrypts **thirty three (33)** bytes of a plain text message to **thirty three (33)** bytes of a cipher text message when it uses **Counter mode (CTR)** of operation.

(03 marks)

ANSWER IN THIS BOX**True**

In CTR mode, block cipher encrypts counters and

then the plaintext XOR with encrypted counters.

Thus ciphertext and plaintext lengths 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 $x=5$ and B generates the private key $y=2$, 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 $X = g^x \text{ mod } n$.

public key of A (X) = $3^5 \text{ mod } 17$; $X = 243 \text{ mod } 17$, $X = 5$

public key of B (Y) = $3^2 \text{ mod } 17$; $Y = 9 \text{ mod } 11$, $Y = 9$

Session key $k = X^y \text{ mod } n$: $k = 5^2 \text{ mod } 17$, $k = 8$ OR

Session key $k = 9^5 \text{ mod } n$: $k = 8$

- (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 **23** together with **n=187**.

(03 marks)

ANSWER IN THIS BOX**True**

$$e \cdot d \text{ mod } (p-1)(q-1) = 1$$

$$7 \cdot 23 \text{ mod } 10 \cdot 16 = 161 \text{ mod } 160 = 1$$

Thus private is is correct.

- (f) Kamal has an RSA public key $(e, n) = (7, 33)$ and a private key $= (d, n) = (3, 33)$. Suppose Nimal encrypts a plain text message $M=5$ to Kamal. Then Kamal receives cipher text message **C = 14**.

(03 marks)

ANSWER IN THIS BOX**True**

$$C = P^e \text{ mod } n$$

$$C = 5^7 \text{ mod } 33 = 78125 \text{ mod } 33 = 14$$

- (g) Kamal has an RSA public key $(e, n) = (7, 33)$ and a private key $= (d, n) = (3, 33)$. Suppose Kamal signs a plain text message $M=7$ to Nimal. Then Nimal receives signature **S = 13**.

(03 marks)

ANSWER IN THIS BOX**True**

$$S = P^d \bmod n$$

$$C = 7^3 \bmod 33 = 343 \bmod 33 = 13$$

- (h) The **SHA1** hash algorithm generates a **128** bit hash from an input message of **sixty four (64)** bits.

(03 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) Elliptic Curve Cryptography (**ECC**) provides the same level of security with **smaller** key sizes compared to **RSA**.

(03 marks)

ANSWER IN THIS BOX**True**

Elliptic Curve Cryptography (ECC) achieves the same level of security as RSA with significantly smaller key sizes due to the mathematical complexity of the elliptic curve discrete logarithm problem (ECDLP). In simple terms, solving ECDLP is computationally much more difficult than solving the integer factorization problem.

- (j) The Greatest Common Divisor (GCD) of **5460** and **3220** is equal to 140.

(03 marks)

ANSWER IN THIS BOX**True**

$$5460 = 1 * 3220 + 2240 \Rightarrow GCD(3220, 2240) \Rightarrow 3220 = 1 * 2240 + 980 \Rightarrow GCD(2240, 980)$$

$$2240 = 2 * 980 + 280 \Rightarrow GCD(980, 280) \Rightarrow 980 = 3 * 280 + 140 \Rightarrow GCD(280, 140)$$

$$280 = 2 * 140 + 0 \Rightarrow GCD(140, 0)$$

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

- a) Which hashing algorithm is considered **insecure** and is no longer recommended for general use?
- MD5
 - SHA256
 - bCrypt
 - SHA512

(03 marks)

ANSWER IN THIS BOX**(i) CORRECT:**

MD5 generates 128 bit hash value and it can be brute forced. In addition to that, cryptographers demonstrated a practical collision attack against MD5, showing two different files could have identical MD5 hashes.

- b) Which cryptographic function is **not** used for user **authentication**?
- bCrypt
 - RSA
 - AES
 - ECC

(03 marks)

ANSWER IN THIS BOX**(iii) CORRECT:**

bCrypt is a hash function and it is used to save passwords.

AES is an encryption algorithm and not used for user authentication.

RSA and ECC are public key cryptographic algorithms and digital signatures are used for user authentication.

- c) Which cryptographic algorithm is commonly used for **encryption, digital signature and key exchange**?
- RSA
 - AES
 - Diffie-Hellman
 - ECC

(03 marks)

ANSWER IN THIS BOX**(i) CORRECT:**

- AES is used for data encryption and decryption.
 ECC is used for digital signatures.
 Diffie-Hellman is used for key exchange.
 RSA is used for encryption, digital signature and key exchange.

Academic Year 2023 - 3rd Year Examinations Semester 3 Academic Year 2024 - 3rd Year Examinations

d) What is the primary **disadvantage** of **asymmetric-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**(i) CORRECT:**

An asymmetric key algorithm uses complex mathematical calculations for encryption and decryption.

Thus asymmetric key encryption is slower than the symmetric key encryption.

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

- i. TLS
- ii. **PGP**
- iii. IPSec
- iv. SSH

(03 marks)

ANSWER IN THIS BOX**(ii) CORRECT:**

- PGP is an e-mail security protocol.
 SSH is used for remote access the servers.
 TLS is used to protect the web communication.
 IPSec is used to protect IP packets.

- f) What does a '**Salting**' process prevent in password storage?
- Brute-force attacks
 - SQL Injection
 - Rainbow Table Attacks**
 - Man-in-the-Middle attacks

(03 marks)

ANSWER IN THIS BOX**(iii) CORRECT:**

With salts, attackers would need to precompute a unique rainbow table for each possible salt with every word, which is computationally infeasible.

- g) What is the primary goal of **Social Engineering** attacks?
- To manipulate individuals into disclosing confidential information.**
 - To exploit system vulnerabilities and gain unauthorized access.
 - To disrupt network communication and cause denial of service.
 - To encrypt a victim's files and demand a ransom for decryption.

(03 marks)

ANSWER IN THIS BOX**(i) CORRECT:**

Social Engineering refers to the manipulation of individuals into divulging confidential or personal information that can be used for malicious purposes.

- h) What is the purpose of Online Certificate Status Protocol (**OCSP**) in public key infrastructure (PKI)?
- Encrypting data at rest
 - Managing user access controls
 - Authentication of public keys
 - Check the revocation status of a digital certificate**

(03 marks)

ANSWER IN THIS BOX**(iv) CORRECT:**

OCSP plays a critical role in PKI by providing a real-time, efficient, and reliable way to verify the revocation status of digital certificates, ensuring the integrity and trustworthiness of secure communications.

- i) Which of the following describes the principle of least privilege?
- Only essential users have access to the highest level of security.
 - Users are given access to the minimum amount of information necessary to perform their duties.**
 - All users have equal access to sensitive information.
 - The system automatically grants access based on user role.

(03 marks)

ANSWER IN THIS BOX**(ii) CORRECT:**

The Principle of Least Privilege is a security concept that dictates that users, systems, and applications should be granted the minimum level of access or privileges necessary to perform their tasks or functions.

- j) Which of the following is an example of an **Administrative** security control?
- Firewall
 - Risk assessments**
 - Biometric access control
 - Intrusion Detection System (IDS)

(03 marks)

ANSWER IN THIS BOX**(ii) CORRECT:**

Firewall and IDS considered as technical security controls.

Risk assessments is an administrative control.

Biometric controls physically accessing a computer resource and thus it is physical control.

- 3) (a) Discuss the concepts of **Confidentiality**, **Integrity**, and **Availability** in information security. Provide examples of how each principle is applied in real-world scenarios and analyse the challenges associated with implementing them effectively.

(06 marks)

ANSWER IN THIS BOX

Confidentiality ensures that information is accessible only to those who are authorized to have access.

Examples in Real-World Scenarios:

Encryption: Data is encrypted during storage and transmission using protocols like SSL/TLS for secure web communication.

Access Controls: User authentication mechanisms, such as passwords, multi-factor authentication (MFA), and biometric systems, restrict access to sensitive data.

Integrity ensures that data remains accurate, consistent, and unmodified unless authorized. It protects data from unauthorized changes, either accidental or malicious.

Examples in Real-World Scenarios:

Hash Functions: Data integrity is verified using hash algorithms like SHA-256.

Version Control: Systems like Git track changes to files and help ensure data integrity.

Availability ensures that authorized users have timely and reliable access to information and systems when needed.

Examples in Real-World Scenarios:

Disaster Recovery Plans: Backup systems and disaster recovery sites ensure system availability after failures.

Load Balancing: Distributing workloads across multiple servers prevents overloading and downtime.

- (b) Explain the role of **encryption** in information security.

(04 marks)

ANSWER IN THIS BOX

Encryption plays a critical role in ensuring the confidentiality, integrity, and sometimes availability of information in information security.

- (c) Compare **stream ciphers** and **block ciphers**, highlighting the **advantages** and **disadvantages** of the **block cipher**.

(06 marks)

ANSWER IN THIS BOX

Advantages of Block Ciphers:

Stronger Security: Better resistance to statistical analysis attacks.

Multiple Modes of Operation: Can adapt to different security requirements.

Scalability: Suitable for large datasets.

Disadvantages of Block Ciphers:

Slower Processing: Block ciphers require more computational resources.

Error Propagation: An error in one block can affect subsequent blocks, depending on the mode of operation.

- (d) Why is **symmetric** key encryption is still widely used despite the availability of public key cryptography?

(04 marks)

ANSWER IN THIS BOX

Symmetric key encryption remains widely used alongside public key cryptography for several reasons:

Performance: Symmetric key algorithms are generally faster than public key algorithms.

Simplicity: The design and implementation of symmetric key algorithms are often simpler than those of public key algorithms.

- 4) a) How can one ensure the authenticity of a public key?

(05 marks)

ANSWER IN THIS BOX

Public Key Infrastructure (PKI) provides a framework for managing and authentication public keys. Within this infrastructure, keys are distributed as digital certificates and verified through established protocols, ensuring that users can trust the public keys they receive.

- b) What is Online Certificate Status Protocol (**OCSP**), and how does it differ from traditional Certificate Revocation List (**CRL**) methods?

(05 marks)

ANSWER IN THIS BOX

The Online Certificate Status Protocol (OCSP) and Certificate Revocation Lists (CRLs) are both methods used to check the revocation status of digital certificates in a Public Key Infrastructure (PKI).

OCSP is generally more efficient than CRLs, as it allows clients to check the status of a single certificate without downloading a potentially large list.

- c) Explain the concept of **SQL Injection** attacks and describe preventive measures to protect databases against such attacks.

(05 marks)

ANSWER IN THIS BOX

SQL injection occurs when an attacker manipulates a database query by injecting malicious SQL code through user input fields. This can lead to unauthorized access, data theft, data corruption, or even complete control of the database. Following actions can be taken to minimize the risk.

Validate user inputs against expected formats (e.g., email addresses, phone numbers).

Reject inputs containing special characters like ', --, ;.

Use placeholders instead of directly inserting user input into SQL queries.

- (d) Discuss the balance between **digital privacy** and **national security** in the context of information security regulations.

(a) CORRECT

(b) CORRECT

(c)

(05 marks)**ANSWER IN THIS BOX**

The intersection of digital privacy and national security remains one of the most debated topics in modern society. Governments and security agencies require access to information to prevent criminal activities, terrorism, and cyber threats, while individuals and organizations demand the protection of their digital privacy rights.

Students should give their own answer based on the above facts.
