University of Colombo, Sri Lanka

University of Colombo School of Computing

UCSC

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

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

(03 marks)

ANSWER IN THIS BOX

(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

(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

(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

(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

(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

(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

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

(03 marks)

ANSWER IN THIS BOX

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

(03 marks)

ANSWER IN THIS BOX

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?

i. MD5

ii. SHA256

iii. bCrypt

iv. SHA512

(03 marks)

ANSWER IN THIS BOX

(b) Which cryptographic function is **not** used for user **authntication**?

i. bCrypt

ii. RSA

iii. AES

iv. ECC

(03 marks)

ANSWER IN THIS BOX

(c) Which cryptographic algorithm is commonly used for **encryption**, **digital signature** and **key exchange**?

i. RSA

ii. AES

iii. Diffie-Hellman

iv. ECC

(03 marks)

ANSWER IN THIS BOX

(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

(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

(f) What does a '**Salting**' process prevent in password storage?

i. Brute-force attacks

ii. SQL Injection

iii. Rainbow Table Attacks

iv. Man-in-the-Middle attacks

(03 marks)

ANSWER IN THIS BOX

(g) What is the primary goal of **Social Engineering** attacks?

i. To manipulate individuals into disclosing confidential information.

ii. To exploit system vulnerabilities and gain unauthorized access.

iii. To disrupt network communication and cause denial of service.

iv. To encrypt a victim's files and demand a ransom for decryption.

(03 marks)

ANSWER IN THIS BOX

(h) What is the purpose of Online Certificate Status Protocol (**OCSP**) in public key infrastructure (PKI)?

i. Encrypting data at rest

ii. Managing user access controls

iii. Authentication of public keys

iv. Check the revocation status of a digital certificate

(03 marks)

ANSWER IN THIS BOX

(i) Which of the following describes the principle of least privilege?

i. Only essential users have access to the highest level of security.

ii. Users are given access to the minimum amount of information necessary to perform their duties.

iii. All users have equal access to sensitive information.

iv. The system automatically grants access based on user role.

(03 marks)

ANSWER IN THIS BOX

(j) Which of the following is an example of an **Administrative** security control?

i. Firewall

ii. Risk assessments

iii. Biometric access control

iv. Intrusion Detection System (IDS)

(03 marks)

ANSWER IN THIS BOX

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.

(06 marks)

ANSWER IN THIS BOX

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

(04 marks)

ANSWER IN THIS BOX

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

(06 marks)

ANSWER IN THIS BOX

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

(04 marks)

ANSWER IN THIS BOX

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

(05 marks)

ANSWER IN THIS BOX

(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

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

(05 marks)

ANSWER IN THIS BOX

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

(05 marks)

ANSWER IN THIS BOX

****