THE OPEN UNIVERSITY OF SRILANKA
DEPARTMENT OF COMPUTER SCIENCE
B.SC.DEGREE PROGRAMME 2024/2025
FINAL EXAMINATION
CSU 5309-INFORMATION SECURITY AND CRYPTOGRAPHY
DURATION: TWO HOURS ONLY (02 HOURS)

DATE: 28.04.2025 **TIME: 1.30 pm – 3.30 pm**

Answer **FOUR (04) Questions ONLY.** All questions carry equal marks.

Q1.

i. What are the three (3) essential components of security?

ii. What is the difference between a threat and an attack in Computer Security?

iii. Briefly describe the following terms related to fundamental Security Design Principles.

a) Complete Mediation

b) Least Privilege

c) Least Common Mechanism

d) Open Design

iv. Describe the components of Security Systems Development Life Cycle.

Q2.

i. What is IPsec? Explain the main security services that IPsec provides to protect data.

ii. What is default operating system (OS) security? Explain how it helps protect a computer.

iii. How can cultural differences influence people's views on ethical computer use?

iv. What is the differences between a denial-of-service attack and a distributed denial of service attack? Which is more dangerous? Why?

Q3.

i. What is a Policy?

ii. Describe the secure coding mechanisms that can be used in following cases:

a. Buffer Overflows

b. Code Injection

iii. Briefly describe the following goals of security.

a. Authenticity

b. Availability

c. Integrity

iv. What is known as Pseudo random Number Generator? Briefly describe.

Q4.

i. State four (4) block cipher schemes.

ii. Briefly describe the function of Triple DES. (Use a diagram)

iii. What are the functions of the mixing algorithm and the salt in generating KEK?

iv. What is steganography and what can it be used for?

Q5.

i. State five (5) critical characteristics of information.

ii. Discuss example scenarios where symmetric cryptography and asymmetric key cryptography can be used.

iii. Briefly explain about transposition cipher using an example.

iv. Briefly describe how HMAC works with help of a diagram.

Q6.

i. State four (4) software engineering process models.

ii. What is Digital Envelope? Describe the process.

iii. What are the components of PKI? Briefly describe them.

iv. Explain the role of a mixing algorithm and salt in Password-Based Encryption (PBE).

-End of Examination Paper-

100