

International Islamic University Chittagong

Department of Computer Science and Engineering

B. Sc. in CSE

Mid term Exam, Spring 2025

Course Code: CSE 4743

Time: 1 hour and 30 minutes

Course Title: Computer Security

Full Marks: 30

Part A

[Answer the questions from the followings]

- | | | | | | |
|----|----|---|-----|----|---|
| 1. | a) | Explain Authenticity and Accountability by showing their use in an Information system. | CO1 | U | 5 |
| | | Or, | | | |
| 1. | a) | Explain different types of active attacks. | CO1 | U | 5 |
| 1. | b) | Describe some security mechanisms that are included in ITU X.800 recommendation | CO1 | U | 5 |
| 2. | a) | Explain with example why decrypting one time pad is extremely difficult for an attacker. | CO1 | U | 5 |
| 2. | b) | Analyze the differences between cryptanalysis of Transposition cipher and Caesar cipher. | CO2 | An | 5 |
| | | Or, | | | |
| 2. | b) | What is prime field and extension field? Write down the polynomials elements in $GF(2^3)$. | CO2 | An | 5 |

Part B

[Answer the questions from the followings]

- | | | | | | |
|----|----|---|-----|---|---|
| 3. | a) | Why do we need both End to end and Link encryption? Explain with example. | CO1 | E | 5 |
| 3. | b) | Explain each step of the following key distribution scenario. | CO2 | E | 5 |

