

International Islamic University Chittagong
 Department of Computer Science and Engineering
 B. Sc. in CSE Midterm Examination, Autumn 2022
 Course Code: CSE-4743 Course Title: **Computer Security**
 Time: 1 hour and 30 minutes Full Marks: 30
 The figures in the right-hand margin indicate full marks

Bloom's Levels of the Questions						
Letter Symbols	R	U	App	An	E	C
Meaning	Remember	Understand	Apply	Analyze	Evaluate	Create

1. a) Explain how passwords are stored nowadays. Give examples of tradeoffs between usability and security considering "Authentication". CO1 An 5
- b) "Software and system security is all about managing risk"-Do you agree with this statement? Why? CO2 E 5

Calculate Annualized Loss Expectancy (ALE) for each loss type. Consider the probability of small ATM fraud is five times higher than that of large ATM fraud.

Loss type	Amount	Incidence	ALE
SWIFT* fraud	Tk. 20,000,000	0.005	?
ATM fraud (large)	Tk. 250,000	0.10	?
ATM fraud (small)	Tk. 20,000		?
Teller theft	Tk. 3,240	300	?

2. a) Explain the CIA triad with necessary examples. What is its significance? CO1 U 5
- b) Write down an algorithm (i.e. pseudocode) to cryptanalyze a transposition cipher. You can consider a suitable ciphertext example if required. CO2 An 5

OR

Analyze and explain the strength of a one-time pad with any suitable key, plaintext, and ciphertext example. CO2 An 5

3. a) Describe how communication is secured using end-to-end encryption. CO1 U 5

OR

Explain congruence with an example. Show the additive and multiplicative inverses for modulo 7 arithmetic.

- b) Briefly describe the logical and physical access control methods. CO1 U 5