THE INSTITUTE OF FINANCE MANAGEMENT

FACULTY OF COMPUTING, INFORMATION SYSTEMS AND MATHEMATICS

Assignment

Module: CSU 08209 Network Security

Instructions

1. This is a group assignment.
2. Each group should consist of not more than three (3) students.
3. Submission procedures :
    - Submission Date and time: 10 June 2022, Time 23:59
    - Submit a hand-written copy of your solutions.
4. This assignment will carry a weight of 20 marks.

Question 1

As a consultant with the *Cyber Works Ltd*., you have been asked to determine how encrypted documents containing sensitive information can be made available to several hundred office workers in the *Salama Company*. The encrypted files can be downloaded from an internal web site at *Salama Company*.

Required:

Describe considerations and methods can be used to ensure secure and reliable downloading and reading of the encrypted documents while minimizing the risk of compromise?
(14 marks)

Question 2
Write short notes on the following terms as related to hash functions: **(6 marks).**

a) Preimage Resistance
b) Second-Preimage Resistance
c) Collision Resistance