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: 11 August 2020, Time 08:00 am
    - Submit a printed copy of your solutions.
4. This assignment will carry a weight of 20 marks.

Question 1

Alice and Bob are using the Diffie-Hellman key exchange protocol with (g, p) = (19, 13) to agree on a key for a shift cipher. Bob's secret key is 5, and he receives the message 11, PTCNFUXGHFT.

a) What message did Alice send to him? **(5 marks)**
b) What information did Bob exchange with Alice to notify her of the key they would be using? **(5 marks)**

Question 2

As a consultant with the *Nyungu Consulting* Co., you have been asked to determine how encrypted documents containing sensitive information can be made available to several hundred office workers in the *Kufukiza* Company. The encrypted files can be downloaded from an internal web site at *Kufukiza*. What considerations and methods can be used to ensure easy downloading and reading of the encrypted documents while minimizing the risk of compromise? **(10 marks)**