Kasarani Campus
Off Thika Road
Tel. 2042692 / 3
P. O. Box 49274, 00100
NAIROBI
Westlands Campus
Pamstech House
Woodvale Grove
Tel. 4442212
Fax: 4444175

KIRIRI WOMEN'S UNIVERSITY OF SCIENCE AND TECHNOLOGY
UNIVERSITY EXAMINATION, 2023/2024 ACADEMIC YEAR
FOURTH YEAR, FIRST SEMESTER EXAMINATION
FOR THE BACHELOR OF BUSINESS INFORMATION TECHNOLOGY
KCS 410 – SECURITY AND CRYPTOGRAPHY

Date: 11TH December 2023
Time: 8:30AM – 10:30AM

INSTRUCTIONS TO CANDIDATES

ANSWER QUESTION ONE (COMPULSORY) AND ANY OTHER TWO QUESTIONS

QUESTION ONE (30 MARKS)

a) Using Ceasar Cipher method, encrypt the following text with a shift of 4 (6 Marks)

Text : ATTACKATONCE

b) Define the term Threat as used in computer security? (2 Marks)

c) Differentiate between the following terms as used in security:

i) Information security and network security (2 Marks)

ii) An active attack and a passive attack. (2 Marks)

d) Cryptographic systems are generally classified along 3 independent dimensions: (6 Marks)

e) An encryption scheme has five ingredients for Conventional Encryption Principles, discuss them. (5 Marks)

f) Using The rail fence cipher (also called a zigzag cipher) method, encrypt the following plain texts showing your working?

i) Input : "defend the east wall" (4 Marks)

Key = 3

ii) Input : "attack at once" (3 Marks)

Key = 2

QUESTION TWO (20 MARKS)

a) Discuss the three principles of Security as indicated in the network security (6 Marks)

b) Traditionally, computer facilities have been physically protected for three reasons, describe the reasons for the physical protection. (6 Marks)

c) For secure use of symmetric encryption, there are several requirements, elaborate four of them (8 Marks)

QUESTION THREE (20 MARKS)

a) Elucidate the Block Cipher modes of Operation as used in cryptography (8 Marks)

b) With the aid of illustrations, demonstrate the difference between public key and private key in encryption (6 Marks)

c) When working with cryptography algorithms (ciphers), they can all be divided into two main groups, explain these two main divisions. (6 Marks)

QUESTION FOUR (20 MARKS)

a) With the aid of an example, demonstrate how Caesar Cipher is done (8 Marks)

b) Discuss the different keys for decryption and encryption for Public Key (4 Marks)

c) Using illustrations, Explain Data Encryption standard (DES) in detail using expansion permutation and transformation . (8 Marks)

QUESTION FIVE (20 MARKS)

a) Elaborate the three aspects of information security according to network security and cryptography. (6 Marks)

b) Explain the various techniques used for distribution of public keys. (8 Marks)

c) State and prove Euler''s theorem. (6 Marks)