(University of Choice)

MASINDE MULIRO UNIVERSITY OF SCIENCE AND TECHNOLOGY (MMUST)

MAIN CAMPUS

UNIVERSITY EXAMINATIONS

2021/2022 ACADEMIC YEAR

SPECIAL/SUPPLIMEMTARY

FOURTH YEAR EXAMINATIONS

FOR THE DEGREE

IN

COMPUTER SCIENCE & INFORMATION TECHNOLOGY

COURSE CODE: BIT 426E

COURSE TITLE: ADVANCED CRYPTOGRAPHY

DATE: TUESDAY 02-08-2022 **TIME:** 8:00a.m-10:00a.m

INSTRUCTIONS TO CANDIDATES

- Answer **Questions ONE** and **ANY OTHER TWO.**

TIME: 2 Hours

Question 1 COMPULSORY (30 MARKS)

a) Briefly explain what you understand by hashing and explain its working principle.

(6 marks)

b) Threats in computer security can be divided into four main categories. Name and briefly explain each of these categories giving an example of each. **(12 marks)**

c) Briefly explain the following cryptographic concepts:

- Plain text.
- Cipher text.
- Encryption
- Decryption

(12 marks)

Question 2 (20 MARKS)

a) Briefly state and explain any four common attacks on cryptographic algorithms.

(8 marks)

b) Explain why is public-key encryption currently confined to key management and signature applications only? **(4 marks)**

c) Explain the difference between cryptography and steganography **(4 marks)**

d) Explain what PKI entity is responsible for generating, digitally signing and selling digital certificates. **(4 marks)**

Question 3 (20 MARKS)

a) State the key lengths for the following algorithms:

DES

3DES

AES.

(3 marks)

b) Which symmetrical encryption algorithms is considered the strongest? Justify your answer by showing the working principle of the algorithm. **(8 marks)**

c) Explain the working principle of Diffie-Hellman.

(7 marks)

d) Name two examples of symmetrical encryption algorithms **(2 marks)**

Question 4 (20 MARKS)

a) The objective of this simple cryptosystem is that at the end of the process, only the sender and the receiver will know the plaintext. Explain with the use of a diagram the components of a Cryptosystem **(10 marks)**

b) **Consider the following numbers:**

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20.

Calculate the number of co-primes if n and Ø(n) = (33,20). **(10 marks)**

Question 5 (20 MARKS)

a) By using the **Playfair cypher**, and plaintext message "Hello World" calculate the cipher text using the key "**crypto**".

(10 marks)

b) You are doing some cryptanalysis on a known message in an attempt to determine the key that has been used. You know that the sender is using the Rail Fence cipher and you are trying to find the key (depth) they used to produce the ciphertext.

If the known message is: MEET ME AT THE PARTY

and the ciphertext is: MTER YE AT PME EHATT

c) Calculate the key (depth) has been used? **(10 marks)**