50

(University of Choice)

MASINDE MULIRO UNIVERSITY OF SCIENCE AND TECHNOLOGY (MMUST)

MAIN CAMPUS

UNIVERSITY EXAMINATIONS

2021/2022 ACADEMIC YEAR

FOURTH YEAR SECOND SEMESTER EXAMINATIONS

FOR THE DEGREE

IN

COMPUTER SCIENCE & INFORMATION TECHNOLOGY

COURSE CODE: BIT 426E

COURSE TITLE: ADVANCED CRYPTOGRAPHY

DATE: 25/04/2022 **TIME:** 8:00a.m-10:00a.m

INSTRUCTIONS TO CANDIDATES

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

TIME: 2 Hours

MMUST observes ZERO tolerance to examination cheating

This Paper Consists of 3 Printed Pages. Please Turn Over.

Question 1 COMPULSORY (30 MARKS)

a) Briefly name and explain the 3 security primitives of Information Security. **(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:

- Symmetric encryption.
- Asymmetric encryption.
- Steganography
- Hashing **(12 marks)**

Question 2 (20 MARKS)

a) Briefly state and explain any four common attacks on cryptographic algorithms. **(8 marks)**

b) Kerckhoff principle is applied in virtually all the contemporary encryption algorithms such as DES, AES, etc. and makes public algorithms to be thoroughly secure. Explain the Kerckhoff principle **(4 marks)**

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

d) Explain if the RSA algorithm can be hacked or not. Explain reasons for your answer. **(4 marks)**

Question 3 (20 MARKS)

a) Calculate the number of encryption keys that are required to implement a symmetric algorithm with 12 participants. **(5 marks)**

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

c) Symmetric keys should be kept secret from other parties than the participants in the scheme. Explain how this can be achieved. **(5 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 **(15 marks)**

b) Explain why triple DES is more secure compared to DES **(5 marks)**

Question 5 (20 MARKS)

a) By using the **Playfair cypher**, prove that the plaintext message "hide money" translates to cipher text QC EF NU MF ZV using the key "**tutorial**".

(10 marks)

b) By using the **Ceaser cypher**, and an algorithm C= E(5,p) = (p+5) mod (26), calculate the cipher text of the paint text message "I have the money" **(10 marks)**