JU

(The University of Choice)

MASINDE MULIRO UNIVERSITY OF SCIENCE AND TECHNOLOGY (MMUST)

MAIN CAMPUS

2021/2022 ACADEMIC YEAR

SECOND SEMESTER EXAMINATIONS

FOR THE DEGREE

OF

BACHELOR OF COMPUTER SCIENCES AND INFORMATION TECHNOLOGY

COURSE CODE: BCS 375/ BIT 328

COURSE TITLE: CRYPTOGRAPHY & NETWORK SECURITY

DATE: Thursday, 21st April, 2022 **TIME:** 3:00-5:00PM

INSTRUCTIONS TO CANDIDATES

Question ONE (1) is compulsory
Attempt any TWO (2) questions
TIME: 2 Hours

MMUST observes ZERO tolerance to examination cheating

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

QUESTION ONE (30 MARK-COMPULSORY)

a. Differentiate between passive and active attacks. By use of an illustrative diagram, give an example of each. 6 Marks
b. Distinguish between diffusion and confusion as applied in cryptography 4 Marks
c. Briefly explain the Caesar cipher. 3 Marks
d. Applying the principle of Caesar cipher, where k takes on a value in the range 1 to 25. The decryption algorithm is $p = D(k, C) = (C - k) \bmod 26$. Decrypt the following ciphertext. PHHW PH DIWHU WKH WRJD SDUWB. 5 Marks
e. Explain the drawbacks of substitution ciphers 2 Marks
f. State and explain the four different types of attacks applied in cryptology 6 Marks
g. Identify the two different types of symmetric cryptography and briefly explain each 4 Marks

QUESTION TWO: 20 MARKS

a. Briefly explain the Hill Cipher; apply this principle to ciphertext the word "COE" using ANOTHERBZ as the key. 7 Marks
b. Differentiate between a mono-alphabetic cipher and a polyalphabetic cipher. 3 Marks
c. Explain the various components of Asymmetric and Symmetric encryptions 4 Marks
d. State and explain the four different types of attacks applied in cryptology 6 Marks

QUESTION THREE: 20 MARKS

a. Identify the two different types of symmetric cryptography and briefly explain each 4 Marks
b. Explain the concept of asymmetric cryptography 3 Marks
c. Differentiate between stream and block ciphers. 4 Marks
d. Explain the principle of hashing function as applied in cryptography 3 Marks
e. Briefly explain the following terms: 6 Marks
   Hash functions
   Digital signatures
   Certificate of authority .

QUESTION FOUR: 20 MARKS

a. Encrypt the message "meet me at the usual place at ten rather than eight o'clock" using a hill cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. Show your calculations. 7 Marks
b. What are the two basic functions used in an encryption algorithm 2 Marks
c. Compare and contrast steganography and digital watermarking. 4 Marks
d. How can non-repudiation be achieved in designing e-cash based system? 3 Marks

e. Compare and contrast steganography and digital watermarking. 4 Marks

QUESTION FIVE: 20 MARKS

a. Differentiate between passive and active attacks. By use of an illustrative diagram, give an example of each. 5 Marks

b. Briefly explain the following concepts as they apply to cryptography 6 Marks

   i. Public-key encryption
   ii. Digital Signatures
   iii. Brute force attack

c. Explain how a man-in-the-middle attack on a Wi-Fi network can be defeated. 3 Marks

d. Identify THREE (3) threats to a wireless network that could compromise security. You should state the security attribute that is compromised by each threat. 6 Marks