30

(*University of Choice*)

MASINDE MULIRO UNIVERSITY OF SCIENCE AND TECHNOLOGY

(MMUST)

UNIVERSITY EXAMINATIONS

2022/2023 ACADEMIC YEAR

THIRD YEAR SECOND SEMESTER EXAMINATIONS

FOR THE DEGREE OF BACHELOR OF SCIENCE

(COMPUTER SCIENCE & INFORMATION TECHNOLOGY)

COURSE CODE: **BCS 375 & BIT 328**

COURSE TITLE: **APPLIED CRYPTOGRAPHY & NETWORK SECURITY**

DATE: 19/04/2023 **TIME:** 3.00- 5.00PM

INSTRUCTIONS TO CANDIDATES

- Answer **QUESTION ONE** and attempt **ANY OTHER TWO** questions

Question One (30 Marks)

a. Identify and briefly explain each of the principal elements of a public-key cryptosystem. **9 Marks**

b. Identify and briefly explain three classes of intruders **6 Marks**

c. Discuss using real life examples, where each of the following security objectives are needed :

i. Confidentiality. **5 Marks**

ii. Integrity. **5 Marks**

iii. Non-repudiation. **5Marks**

Suggest suitable security mechanisms to achieve each

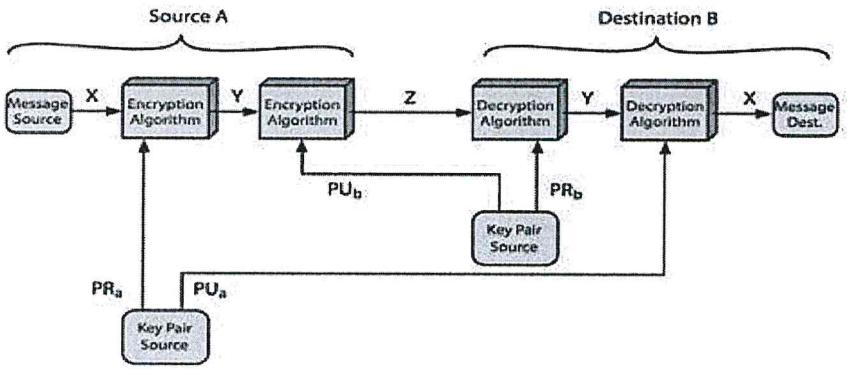
Question Two (20 Marks)

a. What are the two general approaches to attacking a cipher **2 Marks**

b. Using Playfair Cipher, encrypt the message "come, let us reason together". Use the word **"EXPLAIN"** as your keyword. **7 Marks**

c. Using the following Algorithm, C = E(p) = (p+3) mod 26, encrypt the message; "Let us meet in class later in the afternoon". **5 Marks**

d. Briefly explain the process depicted in the diagram below as it relates to public key, authentication and confidentiality **6 Marks**



Question THREE (20 Marks)

a. Briefly explain the concept of Blockchain technology and Cryptography. **7 Marks**

b. Solve for X in the following problems; justify your answer: **9 Marks**

i. $23 \equiv X \pmod 5$

ii. $-11 \equiv X \pmod 8$

iii. *iii.* $81 \equiv X \pmod{27}$

c. Explain the various components of Asymmetric and Symmetric encryptions **4 Marks**

Question FOUR (20 Marks)

a. Explain the drawbacks of substitution ciphers **2 Marks**

b. Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system and, in each case, indicate the degree of importance of the requirement. **5 Marks**

c. State and explain the four different types of attacks applied in cryptology **6 Marks**

d. Perform encryption and decryption using RSA Algorithm for the p= 7; q= 11; e= 17; and M= 8 **7 Marks**

Question FIVE (20 Marks)

a. State the two standard ways for finding GCD **2 Marks**

b. Use either of the methods to compute gcd(482, 1180) **6 Marks**

c. Identify the two different types of symmetric cryptography and briefly explain each **4 Marks**

d. Compare and contrast steganography and digital watermarking. **4 Marks**

e. Identify **TWO (2)** threats to a wireless network that could compromise security. You should state the security attribute that is compromised by each threat. **4 Marks**