20

(University of Choice)

MASINDE MULIRO UNIVERSITY OF SCIENCE AND TECHNOLOGY (MMUST)

MAIN CAMPUS

UNIVERSITY EXAMINATIONS

2021/2022 ACADEMIC YEAR

SPECIAL/SUPPLEMENTARY THIRD YEAR EXAMINATIONS

FOR THE DEGREE

OF

BACHELOR OF SCIENCE COMPUTER SCIENCE & INFORMATION TECHNOLOGY

COURSE CODE: **BCS 375E/BIT 328**

COURSE TITLE: **APPLIED CRYPTOGRAPHY/CRYPTOGRAPHY AND NETWORK SECURITY**

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

INSTRUCTIONS TO CANDIDATES

Question ONE (1) is compulsory
Answer THREE (3) questions

TIME: 2 Hours

MMUST observes ZERO tolerance to examination cheating

QUESTION ONE (30 MARKS COMPULSORY)

a. Briefly explain the following terms as applied to security of data. Give two examples as to how you would implement each. 6 Marks

   i. Non-Repudiation:
   ii. Authentication:
   iii. Confidentiality:
   iv. Integrity:

b. State and explain the four different types of attacks applied in cryptology 6 Marks
c. Identify the two different types of symmetric cryptography and briefly explain each 4 Marks
d. Explain the concept of asymmetric cryptography 3 Marks
e. Explain the principle of hashing function as applied in cryptography 3 Marks
f. Explain the Playfair cipher. 4 Marks
g. Encrypt the message "HELLO MY DEAR," using the key shown in fig.1. 4 Marks

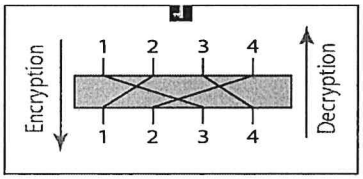


Fig.1.

QUESTION TWO 20 MARKS

a. Compare and contrast Rijndael and AES 4 Marks
b. The following shows a plaintext and its corresponding ciphertext. Is the cipher mono-alphabetic? Justify your answer. 2 Marks

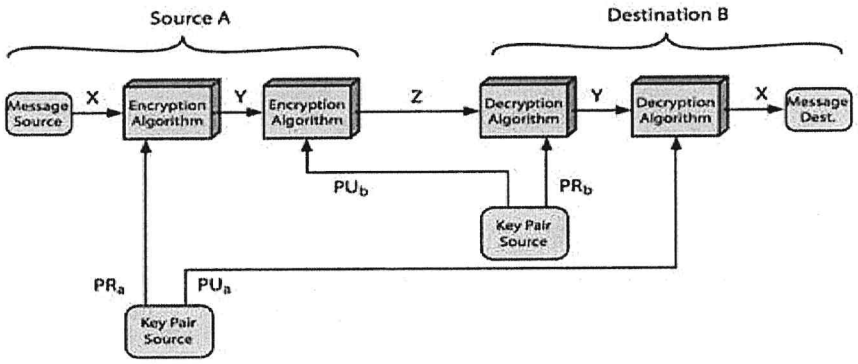
Plaintext: HELLO
Ciphertext: ABNZF

c. Briefly explain the Hill Cipher; apply this principle to ciphertext the word "COE" using ANOTHERBZ as the key. 7 Marks
d. Differentiate between a mono-alphabetic cipher and a polyalphabetic cipher. 3 Marks
e. Explain the various components of Asymmetric and Symmetric encryptions 4 Marks

QUESTION THREE 20 MARKS

a. State Kerckhoff's principle. 2 Marks
b. Briefly describe the Shift Rows and Byte Substitution layers of Rijndael. 4 Marks
c. Identify and briefly explain each of the two key issues which led to the development of Public Key Cryptography 4 Marks

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



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

QUESTION FOUR 20 MARKS

a. By use of a well labeled diagram, explain a symmetric cipher model 6 Marks
b. Briefly explain why a cryptosystem designed by someone who follows Kerckhoff's principle is likely to be stronger than one designed by someone who does not. 3 Marks
c. You have intercepted a message encrypted with an affine cipher. The ciphertext starts with BBDJ and you know the plaintext starts with oops. Find the key. 5 Marks
d. Consider a substitution cipher where 52 symbols were used instead of 26. In particular, each symbol in the cipher text is for either a lowercase English letter, or an uppercase English letter. (For example, let E be the encryption function then we could have E('S') = 'p' and E('s')='m'.) Such a modification augments the key space to 52! Does this provide added security compared to a standard substitution cipher? Explain. 3 Marks
e. How can non-repudiation be achieved in designing e-cash based system? 3 Marks

QUESTION FIVE 20 MARKS

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]