(KNOWLEDGE FOR DEVELOPMENT)

KIBABII UNIVERSITY

(KIBU)

UNIVERSITY EXAMINATIONS

2020/2021 ACADEMIC YEAR

END OF SEMESTER EXAMINATIONS

YEAR THREE SEMESTER TWO

FOR THE DEGREE OF

(COMPUTER SCIENCE)

COURSE CODE: CSC 374E

COURSE TITLE: APPLIED CRYPTOGRAPHY

DATE: 07/10/2021 TIME: 02.00 P.M – 04.00 P.M

INSTRUCTIONS

ANSWER QUESTIONS ONE AND ANY OTHER TWO.

QUESTION ONE (COMPULSORY) [30 MARKS]

a. Distinguish the following terms as used in applied cryptography **[6 marks]**

   i. Passive vs. active security threats

   ii. Encryption algorithm vs. Decryption algorithm

   iii. block cipher vs. a stream cipher

b. There are three major characteristics that separate modern cryptography from the classical approach. **[6 marks]**

c. Mr. Wandahuhu, a small scale business man in Chapalungu intends to automate most of his business operations but has been warned a security expert on the need to ensure that his systems meets the tenets of information security. Using a well labelled diagram, demystify to him what this means. **[6 marks]**

d. Hackers gained access to Wambirianga's email account, altered the bank account details on a supplier's invoice Xu Ltd and resent the email to Wambirianga masquerading to be from Xu Ltd something that saw Wambirianga lose money to the hackers. Discuss any three security attacks Wambirianga suffered and prefer appropriate remedy for each. **[6 marks]**

e. Discuss any three elements of a cryptosystem. **[6 marks]**

QUESTION TWO [20 MARKS]

a. A security treat can be defined as an object, person, or other entity that represents a constant danger to an asset. Discuss any three categories of threats and highlight the major causes. **[6 marks]**

b. Show how you would encrypt the word FORCE using the Vignere cipher GOD as the key word. **[6 marks]**

c. Discuss the four basic information security services that are achieved through cryptography. **[8 marks]**

QUESTION THREE [20 MARKS]

a. Employees are the weakest link in information security. Argue for and against. **[6 marks]**

b. We can define 3 levels of impact from a security breach. Discuss and give appropriate example for each level. **[6 marks]**

c. Given 3 as the encryption key, demonstrate by use of a diagram how you would decrypt "**FRRNLH**" using a shift cipher. **[8 marks]**

QUESTION FOUR [20 MARKS]

a. Explain the following terms in relation to computer security

i. Asymmetric Encryption **[1 mark]**

ii. Frequency analysis **[1 mark]**

iii. Computational Security **[1 mark]**

iv. Cryptanalysis **[1 mark]**

b. There are two restrictive challenges of employing symmetric key cryptography. Discuss. **[4 marks]**

c. Demonstrate why information is regarded as an asset to an organization. **[6 marks]**

d. Explain three ways the complexity of an attack can measured. **[6 marks]**

QUESTION FIVE [20 MARKS]

a. Explain what you understand by differential cryptanalysis. **[2 marks]**

b. Discuss any three ways attacks on cryptosystems are categorized. **[6 marks]**

c. Explain six different modes of operation in DES? **[6 marks]**

d. Discuss the four requirements for the use of a public-key certificate scheme. **[6 marks]**