MERU UNIVERSITY OF SCIENCE AND TECHNOLOGY

P.O. Box 972-60200 – Meru-Kenya.
Tel: +254(0) 799 529 958, +254(0) 799 529 959, +254 (0)712 524 293
Website: www.must.ac.ke Email: info@mucst.ac.ke

UNIVERSITY EXAMINATIONS 2020/2021

FOURTH YEAR FIRST SEMESTER EXAMINATIONS FOR THE DEGREE OF BACHELOR OF SCIENCE IN COMPUTER SCIENCE, BACHELOR OF COMPUTER TECHNOLOGY, BACHELOR OF INFORMATION TECHNOLOGY, BACHELOR OF INFORMATION SCIENCE, BACHELOR OF BUSINESS IN INFORMATION SCIENCE

CCS 3402: COMPUTER SECURITY AND CRYPTOGRAPHY

DATE: SEPTEMBER 2021 **TIME: 2 HOURS**

INSTRUCTIONS: Answer Question ONE and any other TWO questions.

QUESTION ONE (30 MARKS)

a) Given the key below, use Hill Cippher to encrypt the message “we are under attack save yourself” (6marks)

$$K=\begin{bmatrix}17 & 17 & 25\\ 21 & 18 & 21\\ 8 & 8 & 19\end{bmatrix}$$

b) Using play fair Cipher Encrypt the name “ I Cryprography” Use “ Ballon” as your key word (8marks)

c) Outline any four Feistel Cipher Elements (4marks)

d) An encryption scheme is unconditionally secure or computionally secure. Discuss this statement. (4marks)

e) Differentiate between symmetric key cryptography and asymmetric key cryptography. (2marks)

f) Explain the following types of of malicious software (6marks)

i. Worms
ii. Trojans
iii. Logical bombs

UESTION TWO (20 MARKS)

a) The security of a password system is dependent upon keeping passwords secret. Unfortunately, there are many ways that the secret may be divulged. Discuss any four ways through which password can be divulges clearly showing how as security expert how you can deal with them (8marks)

b) Differentiate between symmetric key cryptography and asymmetric key cryptography (1mark)

c) Discuss how the following access control mechanisms and their importance in computer security (6marks)

   i. Access control lists

   ii. Capability lists

   iii. Access control matrices

d) A suitable example show how the users can exchange a key using DIFFIE HELL MAN algorithm (5marks)

QUESTION THREE (20 MARKS)

a) Discuss the following concepts as used in computer security and cryptography (5marks)

   i. Digital Certificate
   ii. Hash function
   iii. Private key

b) An *operating system* (sometimes abbreviated as "OS") is the program that, after being initially loaded into the computer by a boot program, manages all the other programs in a computer. The other programs are called application or application programs. By managing other programs and I/O accessibility, it means that the OS can form first line defence in our computer.

   Giving examples, discuss the following security provided by computer operating systems (6marks)

   i. Discretionary Access Control (DAC
   ii. Mandatory Access Control(MAC)
   iii. Role Based Access (RBA)

c) Discuss three problem that have enable use a brute-force cryptanalysis in Caesar cipher (3marks)

d) Use vigenre cipher to encrypt the message "it is my birthday" given the name "winners" as the key word. (5marks)

QUESTION FOUR (20 MARKS)

a) An important aspect of security is *user education:* describe the main points that you would cover if you were asked to give a presentation on *password management* to all the employees in your company (3marks)

b) Using Caesar ciphy encrypt the message " must win this game" use 21 as the key. (5marks)

c) Data is becoming a vital resource in any organization. Users must authenticate themselves to the system to ensure data remains secure. As a system administrator of an IT firm, discuss any four ways you would use for authenticating users to the server (4marks)

d) The exact realization of a Feistel network depends on the choice of five parameters and design features. Discuss any three parameters and how they affect the model (6marks)

e) Differentiate between weak and strong collision in hashing (2maks)

QUESTION FIVE (20 MARKS)

a) Use the expression E(x)=(9x+5)MOD26 to encrypt the message " The game has been postponed" (5marks)

b) ∑={A,…,Z}, 1=2, k=MJ: use this to encrypt the message. The game has been postponed" (5marks)

c) Discuss the following intrusion detection methods (6marks)

d) HIDS

   i. Signature Based

   ii. Anomally Based

e) Differentiate between active and passive wire tapping (4marks)