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: info@must.ac.ke Email: info@must.ac.ke

University Examinations 2023/2024

THIRD YEAR SECOND SEMESTER EXAMINATION FOR THE DEGREE OF BACHELOR OF BUSINESS INFORMATION TECHNOLOGY, BACHELOR OF INFORMATION TECHNOLOGY, BACHELOR OF INFORMATION SCIENCE AND BACHELOR OF SCIENCE IN EDUCATION

CCS 3402: COMPUTER SECURITY AND CRYPTOGRAPHY

DATE: APRIL 2024 **TIME: 2 HOURS**

INSTRUCTIONS: *Answer question **one** and any other **two** questions*

QUESTION ONE (30 MARKS)

a) Given the word Balloon as the keyword, use play fair cipher to encrypt the word football (5 marks)

b) Given 162453 as the key, Show how you can encrypt the message, "I must go for vacation" using rail fence cipher (3 marks)

c) Show how Host intrusion Detection and Network intrusion Detection systems differ (4 Marks)

d) Discuss any components of a good security policy (3 marks)

e) Given the Equation E(x) = (5x + 8)MOD26. Use affine Cipher to encrypt the message **Dolphin** (5 Marks)

f) Identify any four biometric modalities (4 marks)

g) Identify the key difference between abnormally based IDS and Signature based IDS (4 marks)

h) Highlight any two purposes of a firewall (2 Marks)

QUESTION TWO

a) Given 635124 as the Key, use Rail Fence Cipher to encrypt the message " We are under attack save yourself (4 Marks)

b) If the keyword is WIND and the plaintext is GO AHEAD MAKE MY DAY, use Vigelì ere Cipher to find the ciphertext (5 Marks)

c) Define identification and authentication in the context of cybersecurity. Explain the difference between the two concepts and their importance in access control systems. (4 marks)

d) Firewalls play a critical role in protecting networks from unauthorized access, cyber attacks, and other security threats. Identify any three types of fireswalls and describe how they operate (6 Marks)

e) Define the term Computer Security (1 mark)

QUESTION THREE

a) What is difference between a block cipher and a stream cipher (2 Marks)

b) Discuss any five requirements for a hash function (5 marks)

c) Given Key=MLX use affine cipher to encrypt the message "Holiday" (4 Marks)

d) Discuss the concept of diffusion and Confusion as proposed by Claud Shannon in the context of improving encryption. (4 marks)

e) Identify any three reasons why computers are becoming less secure (3 marks)

f) Discuss how Quantum cryptography works (2 Marks)

QUESTION FOUR

a) Alice and Bob have agreed to use the Diffie Hellman key exchange mechanism. Given the p = 37 and g = 13, show how the key is generated. [6 Marks]

b) Identify any thee application areas of public key cryptography (6 Marks)

c) Identify any four malicious software and how they can controlled (8 marks)

QUESTION FIVE

a) Using Hill Cipher Encrypt the message **INDENT** given the matrix show as the Key (7 Marks)

$$\begin{pmatrix} 13 & 12 & 23 \\ 20 & 0 & 16 \\ 10 & 6 & 15 \end{pmatrix}$$

b) Explain the concept of zero-trust authentication and its implications for network security (3 marks)

c) Discuss any two security models (4 marks)

d) Briefly describe the following access control methods (6 marks)

i. Mandatory access control

ii. Role based access control

iii. Discretion access control

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y