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 2024/2025

FOURTH YEAR FIRST SEMESTER FOR THE DEGREE OF BACHELOR OF CMPUTER SCIENCE, BACHELOR OF EDUCATION ARTS, BACHELOR OF DATA SCIENCE, BACHELOR OF EDUCATION ARTS, BACHELLOR OF COMPUTER TECHNOLOGY, BACHELOR OF EDUCATION ARTS(MATHS/COMPUTER), BACHELOR OF EDUCATION SCIENCE (PHYSICS/COMPUTER)

CCS 3402: COMPUTER SECURITY AND CRYPTOGRAPHY

DATE: JANUARY 2025 **TIME: 2 HOURS**

INSTRUCTIONS: *Answer question **ONE** (Compulsory) and any other **TWO** questions*

QUESTION ONE (30 MARKS)

a) Explain the key concepts of confidentiality, integrity, and availability in the context of information security. (6 Marks)

b) Explain the difference between a substitution cipher and a transposition cipher (4 Marks)

c) Using a suitable diagram describe the conventional encryption model (5 marks)

d) Give the following matrix as the key $\begin{pmatrix} 20 & 17 & 12 \\ 0 & 19 & 0 \\ 26 & 21 & 8 \end{pmatrix}$, Show how you can encrypt the message "thank you" (6 Marks)

e) Use play fair cipher algorithm to Encrypt the message "I must win" given the word **TROPHY** as the keyword (5 Marks)

f) Given the equation $E(x) = (5x + 8) \bmod 26$. Use it to encrypt the message "cryptography" (4 Marks)

QUESTION TWO (20 MARKS)

a) Discuss how the following access control mechanisms work. (6marks)

i. Mandatory Access control

ii. Discretion Access Control

iii. Role based access control

b) An encryption scheme is unconditionally secure or computionally secure. Discuss (4Marks)

c) $\Sigma = \{A, \ldots, Z\}$, $l = 2$, $k = XY$: Use this to encrypt the message The game has been postponed" (6 Marks)

d) Discuss the two requirements for secure use of conventional encryption (4 Marks)

QUESTION THREE (20 MARKS)

Differentiate between Polyalphabetical and mono alphabetical ciphers (4 Marks)

a) Giving suitable example Explain the difference between symmetric and asymmetric encryption (4 Marks)

b) Cryptographic systems are characterized along three independent dimensions; discuss these dimensions (6 Marks)

c) Describe how **steganography a**nd show how it differ from encryption? (3 Marks)

d) Identify any three malware that computers face today (3 marks)

QUESTION FOUR (20 MARKS)

a) Discuss any Five biometric modalities (5 Marks)

b) Show the importance of a Security policy in an organization (2 marks)

c) Identify any five Requirements for Hash Function (5 Marks)

d) Given **7652314** as the key, use Rail fence to encrypt the message "Attack postponed until two am (5 Marks)

e) Identify three possible approaches of attacking RSA algorithm (3 Marks)

QUESTION FIVE (20 MARKS)

a) Alice and Bob have agreed to use the Diffie Hellma key exchange mechanism. Explain how this system works. Given the $p = 37$ and $g = 13$, show how this mechanism can be used to send keys secretly. (6 Marks)

b) Discuss any two types of firewalls (4 Marks)

c) Show the main differences between Host Intrusion Detection systems and network intrusion Detection (4 Marks)

d) Differentiate between Zero Trust Security and Perimeter based Security showing how each can be achieved. (6 marks)

Vigenère Table

	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