**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**

SECOND YEAR SECOND SEMESTER EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE IN COMPUTER SECURITY AND FORENSICS

**CCF 3252: FUNDAMENTALS OF CRYPTOGRAPHY**

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

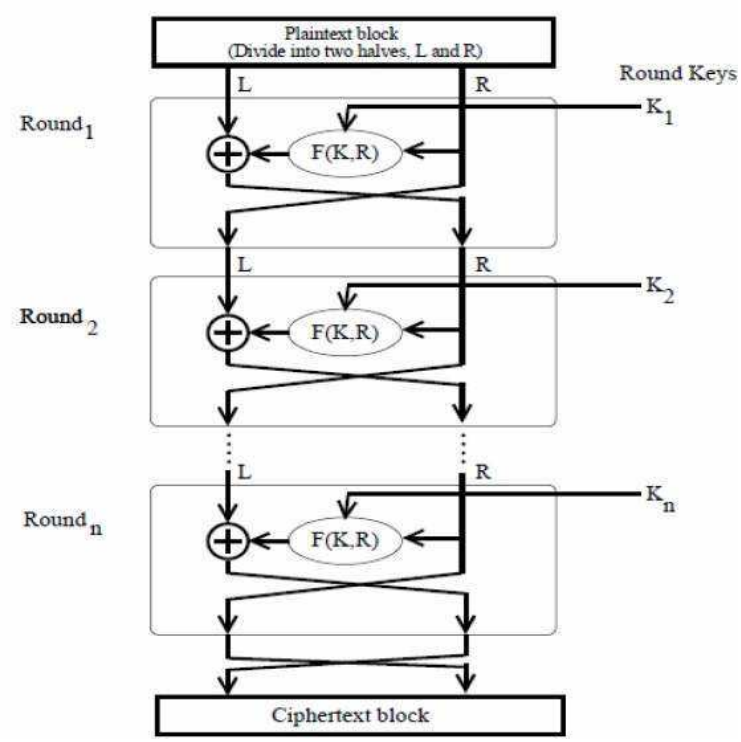
**INSTRUCTIONS:** *Answer question **one** and any other **two** questions*

**QUESTION ONE (30 MARKS)**

a) Given the word WONDERLAND as the keyword, use play fair cipher to encrypt the word **RANGELAND** (5 marks)

b) Using a suitable diagram show the ingredients of symmetric cipher model (6 Marks)

c) Given the diagram below show how Feistel Cipher works (4 marks)




d) Identify any three key characteristics that affect its performance (3 Marks)

e) Using Hill Cipher Encrypt the message **Boiling** given the matrix show as the Key

(7 Marks)

$$\begin{pmatrix} 23 & 12 & 23 \\ 20 & 8 & 16 \\ 20 & 6 & 15 \end{pmatrix}$$

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

**QUESTION TWO (20 MARKS)**

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

b) Identify any three common types of attacks in cryptographic protocols and show how they can be prevented (6 Marks)

c) Giving suitable examples Differentiate between Polyalphabetical cipher and Monoalphebetical Ciphers (4 Marks)

d) Discuss how message Authentication codes works (4 Marks)

e) Identify any two benefits of Digital Signatures (2 Marks)

**QUESTION THREE (20 MARKS)**

a) What is difference between transposition cipher and substitution cipher (2 Marks)

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

c) Describe what are CAPTCHAs and identify any three types of CAPTCHAs (5 Marks)

d) Discuss five applications of cryptography (5 Marks)

e) Discuss any three advantages of Quantum cryptography (3 Marks)

**QUESTION FOUR (20 MARKS)**

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

b) Discuss the concept of Birthday Paradox in Hashing (2 marks)

c) Given p = 3 and q = 11 and e=7 Use RSA algorithm to compute private and public keys (7 Marks)

d) Using a suitable example how Varman Cipher works (5 Marks)

**QUESTION FIVE (20 MARKS)**

a) Using Caesar Cipher encrypt the message **Welcome** Given Key=23. Show your working (4 Marks)

b) Identify any weaknesses with CAESAR cipher (2 Marks)

c) Bob received following encrypted message from Alice "TTNAAPTMTSUOAODWCOIXKNLYPETZ" together with the key 4 3 1 2 5 6 7. Show the decrypted text using Rail fence technique (4 Marks)

d) Using suitable examples discuss any four techniques used in steganography to hide information (4 Marks)

e) Show the differences between Block Ciphers and Transposition Ciphers (2 marks)

f) Discuss any Four ways in which Encryption can take place in cloud computing (4 Marks)