Text Books:

(1). "Linux Command Line and Shell Scripting Bible", Richard Blum, Wiley Publishing, Inc, 2008.

(2). "Linux Administration Handbook", Evi Nemeth, Garth Snyder & Trent R. Hein, Second Edition, Prentice Hall, 2006.

CSCH 403: DATA STRUCTURES

Course Objective:

The objective of the courses to

1) To understand the fundamentals of data structure.
2) Explore the knowledge on stacks, Linked list and queues.

UNIT 1

Introduction: Data Structures, Classifications (Primitive & Non Primitive), Data structure Operations, Review of Arrays, Structures, Self-Referential Structures, and Unions. Pointers and Dynamic Memory Allocation Functions.Representation of Linear Arrays in Memory, Dynamically allocated arrays.

Array Operations: Traversing, inserting, deleting, searching, and sorting. Multidimensional Arrays, Polynomials and Sparse Matrices.

Strings: Basic Terminology, Storing, Operations and Pattern Matching algorithms. Programming Examples.

16 Hours

UNIT 2

Stacks: Definition, Stack Operations, Array Representation of Stacks, Stacks using Dynamic Arrays, Stack Applications: Polish notation, Infix to postfix conversion, evaluation of postfix expression.

Recursion - Factorial, GCD, Fibonacci Sequence, Tower of Hanoi, Ackerman's function. Queues: Definition, Array Representation, Queue Operations, Circular Queues, Circular queues using Dynamic arrays, Dequeues, Priority Queues, A Mazing Problem. Multiple Stacks and Queues. Programming Examples.

Linked Lists: Definition, Representation of linked lists in Memory, Memory allocation; Garbage Collection.Linked list operations: Traversing, Searching, Insertion, and Deletion. Doubly Linked lists, Circular linked lists, and header linked lists. Linked Stacks and Queues.Applications of Linked lists – Polynomials, Sparse matrix representation.Programming Examples.

16 Hours

UNIT 3

Terminology, Binary Trees, Properties of Binary trees, Array and linked Representation of Binary Trees, Binary Tree Traversals - Inorder, postorder, preorder; Additional Binary tree operations. Threaded binary trees, Binary Search Trees – Definition, Insertion, Deletion, Traversal, Searching, Application of Trees-Evaluation of Expression, Programming Examples. Graphs: Definitions, Terminologies, Matrix and Adjacency List Representation Of Graphs, Elementary Graph operations, Traversal methods: Breadth First Search and Depth First Search. **16 Hours**

Course Outcome:

At the end of the course student will be able to

1) Ability to analyze the algorithm and its correctness.

2) Ability to describe stack, queue and linked list operations.

Text Books:

1. Ellis Horowitz and SartajSahni, Fundamentals of Data Structures in C, 2nd Ed, Universities Press, 2014.
2. Seymour Lipschutz, Data Structures Schaum's Outlines, Revised 1st Ed, McGraw Hill, 2014.

CSCS 404 : MATHEMATICAL FOUNDATIONS

Course Objective:

The objective of the courses to

1) Enable to understand and create mathematical argument and solving them with logical skills.
2) Understanding number theory, ciphers which are applied data security.

UNIT I

Algebra and Number Theory : Modular Arithmetic, Groups, Rings, and Fields, Greatest Common Divisors and Multiplicative Inverse, Subgroups, Subrings, and Extensions, Groups, Rings, and Field Isomorphisms, Polynomials and Fields.

(12 hours)

UNIT II

Construction of Galois Field, Extensions of Fields, Cyclic Groups of Group Elements, Efficient Galois Fields, Mapping between Binary and Composite Fields. **Block Ciphers:** Inner Structures of a Block Cipher, The Advanced Encryption Standard(AES), The AES Round Transformations. **(12 hours)**

UNIT III

Rijndael in Composite Field, Elliptic Curves, Scalar Multiplications: LSB First and MSB First Approaches, Montgomery's Algorithm for Scalar Multiplication.

(12 hours)

Course Outcome:

At the end of the course student will be able to

1) Ability to apply logical and mathematical model in practical application.
2) Ability to employ theory concepts in designing efficient algorithms.

TextBooks:

(1). "Hardware Security Design, Threats, and Safeguards", DebdeepMukhopadhyayRajatSubhraChakraborty, CRC Press, 2015

(2). " Hardware IP Security and Trust", Prabhat Mishra, SwarupBhunia, Mark Tehranipoor,Springer, 2017

(3). "Fault Tolerant Architectures for Cryptography and Hardware Security", SikharPatranabisDebdeepMukhopadhyay, Springer, 2018

(4). "Security of Block Ciphers - From Algorithm Design to Hardware Implementation", Kazuo Sakiyama, Yu Sasaki, Yang Li, Wiley, 2015

(5). "Physically Unclonable Functions From Basic Design Principles to Advanced Hardware Security Applications", Basel Halak, Springer, 2018

(6). "Hardware-Based Computer Security Techniques to Defeat Hackers From Biometrics to Quantum Cryptography", Roger Dube, Wiley, 2008