

Graphs, Elementary Graph operations, Traversal methods: Breadth First Search and Depth First Search.
(16 Hours)
Textbooks : 1. Ellis Horowitz and Sartaj Sahni, 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 Objectives : 1. To make the student aware of the tool kit of mathematics required for cryptography 2. To make the student aware of the relationship between mathematical objects and the algorithms
Course Outcomes : 1. Student gets required awareness stated in the Objectives, to build cryptographic algorithms 2. Student gets required awareness stated in the Objectives, to build cryptographic protocols which are build against attacks by hackers
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)
Textbooks : 1. "Hardware Security Design, Threats, and Safeguards", Debdeep Mukhopadhyay Rajat Subhra Chakraborty, CRC Press, 2015 2. "Hardware IP Security and Trust", Prabhat Mishra, Swarup Bhunia, Mark Tehranipoor, Springer, 2017 3. "Fault Tolerant Architectures for Cryptography and Hardware Security", Sikhar Patranabis Debdeep Mukhopadhyay, Springer, 2018 4. "Security of Block Ciphers - From Algorithm Design to Hardware Implementation", Kazuo Sakiyama, Yu Sasaki, Yang Li, Wiley, 2015
CSCS 405 : PROBLEM SOLVING USING PYTHON
Course Objectives : 1. To empower the student with the most versatile computer language available for wide variety of tasks in cybersecurity 2. To make the student aware of the different language components which serve different purposes in programming
Course Outcomes : 1. Student gets the knowledge about the right choice of data structures for a task 2. Student gets the feel for applying a programming language for different scenarios in cybersecurity.
UNIT I A Gentle Introduction to Python: A proper introduction, Enter the Python, About Python, What are the drawbacks, Who is using Python today?, Setting up the environment, Installing Python, How you can run a Python program, How is Python code organised? Python's execution model, Guidelines on how to write good code, Built-in Data Types: Mutable or immutable? That is the question Numbers, Immutable sequences, Mutable sequences, Set types, Mapping types – dictionaries, The collections module, Enums, Final considerations.
(12 Hours)
UNIT II Iterating and Making Decisions Conditional programming: Looping, Putting all this together, A quick peek at the itertools module, Functions, the Building Blocks of Code: Why use functions?, Scopes and name resolution, Input parameters, Return values, A few useful tips, Recursive functions, Anonymous functions, Function attributes, Built-in functions, One final