Programme Project Report (PPR)

MASTER OF SCIENCE (CYBER SECURITY)

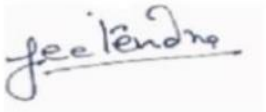
a. **Programme's mission & objectives:** To equip students with the vital knowledge of sophisticated applications of Cyber Security and train them on the necessary skills required for the application of electronics for telecommunication and its usefulness in software development. The course is designed for those who wish to extend their capability for an accelerated early career in cyber/information security. It will prepare learners for a successful career in the various roles directly and indirectly connected to the world of computer, network and information security. The Master of Science (cyber security) programme is a computer-based degree that includes studying communication networks and technologies while including a discussion of legal and ethical issues in computer security. The learners have the opportunity to learn about forensic issues that help find the source of a data hack.

b. **Relevance of the program with HEIs Mission and Goals:** One of the important aims of higher education is the training for leadership in the profession and public life. Master of Science (cyber security) is a two-year (four semesters) professional Master's Degree in computer science which is designed for those wishing to develop a career as a cyber security professional, or to take a leading technical or managerial role in an organisation critically dependent upon data and information communication technology.

c. **Nature of prospective target group of learners:** Master of Science (cyber security) programme is suitable for those from a computer science or information technology education background. The programme is also able to cater for those with no formal studies in computer science but where significant interest in cyber security can instead be demonstrated. The students who wish to join this program is required to have a Bachelors degree in any stream from a recognized institution/university with mathematics as a subject at graduation or 10+2 level. In case the candidate do not have mathematics subject, a bridge course on mathematics is mandatory. The candidate who poses 1 year PG Diploma in Cyber Security from a reputed university or its equivalent course are eligible for lateral entry to third semester of this programme.

d. **Appropriateness of programme to be conducted in Open and Distance Learning mode to acquire specific skills and competence**: The Open and Distance Learning (ODL) University system is more learner-oriented where of the instruction is imparted through distance mode with only a small component of face-to-face communication. The University follows the Credit System for its programmes. Each credit is worth 30 and the student has to be an active participant in the teaching-learning process. Most
hours of student study time, comprising all the learning activities. Thus, a four-credit course involves 120 study hours. This helps the student to understand the academic effort one has to put into successfully complete a course. Completion of the programme requires






successful completion of both assignments and the Term-End Examination of each course along with practical examination of practical oriented courses of the programme. The specially designed printed Self Learning Material for different subject along with other support material is provided to the learners through post/ study center. The study material can also be downloaded through the Universities' e-repository. The University follows a multi-channel approach for the delivery of instruction. It comprises a suitable mix of:

- self-instructional printed material
- audio / video cassettes and CDs
- audio-video programmes transmitted through Hello Haldwani FM Radio and EduSat, and at study centre.
- face-to-face counselling at study centres by academic counselors
- reference library at study centre
- web based academic support
- assignments
- practical

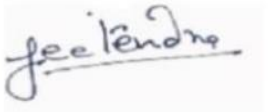
The practical sessions are held in the computer centres / labs of the Study Centres. In these computer labs, the participants have the facility to use the computer and software packages relevant to the syllabus.

e. Instructional Design: Open and Distance learning (ODL) is an innovative approach of providing opportunity of learning through Self Learning Material (SLM) and certain other strategies in a flexible manner at the pace of learners. In this mode, the learner is also provided academic support in the form of counseling and audio/video material in addition to SLM. The University follows the Credit System for its programmes. Master of Science (cyber security) programme is of 80 credits and each credit is worth 30 hours of student study time, comprising all the learning activities. Thus, a four-credit course involves 120 study hours. This helps the student to understand the academic effort one has to put into successfully complete a course.

f. Procedure for admissions, curriculum transaction and evaluation: Direct admission to Master of Science (cyber security) program is offered to the interested students. This programme has been designed with a semester approach in mind. The first year courses are aimed at skills development in computers using various technologies, the second year is more focused on core courses providing conceptual framework, specialization and the project work. The total numbers of courses in this programme are 17 along with 2 practical and 1 major project and the total number of credits is 80. Evaluation for each course covers two aspects:

- Continuous evaluation through Assignment with a weightage of 30%.
- Term-end examination with a weightage of 70%.






To fulfill the requirements for acquiring the Master of Science (cyber security), a student may clear all the courses in a minimum of 2 years and a maximum of 4 years. In case the student is unable to pass all the courses of the Master of Science (cyber security) programme in 4 years, s/he can continue for another two years by seeking Re-admission to the courses which s/he is unable to successfully complete. Completion of the programme requires successful completion of both assignment component and the Term-end Examination component for each course in the programme. The term-end examination of the practical courses consists of several sections. Each section is evaluated separately. The viva-voce for each section will also be separate. The 60% marks of the practical exam are for practical questions and remaining 40% for viva-voce. A student needs to obtain a minimum of 40% in each section of the term-end practical examination for successful completion of that particular section. In case a student does not secure the minimum passing marks in a section, s/he needs to appear for the term-end practical examination again for that section only.

g. **Requirement of the laboratory support and Library Resources:** The practical sessions are held in the computer centres / labs of the Study Centres. In these computer labs, the participants will have the facility to use the computer and software packages relevant to the syllabus. The SLM, supplementary text audio and video material of the various courses of the program is available through the e-repository of the University. The University also has a subscription of National Digital Library to provide the learners' with the ability to enhance access to information and knowledge of various courses of the programme.

h. **Cost estimate of the programme and the provisions:** The Master of Science (cyber security) Programme is a two year program with consists of 17 courses, 2 laboratory courses and 1 project. 9 courses of the above programme is adopted from the MCA/MSc(IT) program. Therefore only 8 new courses are needed to be developed. One course is of 4 credits which consists of approx. 16 units. Hence the total expenditure on the development of 8 four credit courses is:

S. No.	Item	Per unit Cost (Writing & Editing)	Total Cost(Rs.)
1	Total no. of units in 8 courses of 4 credits each= 128	9000	11,52,000
2	Expert Committee, BOS Meetings, etc.		1,00,000
		Total	12,52,000

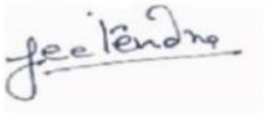
Hence, Rs. 12,52,000/- are required for the development, implementation and maintenance of the programme.

i. **Quality assurance mechanism and expected programme outcomes:** The program structure is developed under the guidance of the expert committee and Board of studies of the School based on the model curriculum of the programme recommended by AICTE. The

program structure and syllabus is approved by the Academic Council of the University. The course structure and syllabus is reviewed according to the needs of the IT Industry every five years. Master of Science (cyber security) programme has been designed to prepare graduates for attaining the following program outcomes:

- Cyber security strategy, and how to organize and set a strategic direction for an organization to best prepare itself for operations in a contested environment.
- Cyber security business services, including but not limited to acquisition, procurement, policy, human resource, and budgeting.
- Cyber security management, that focuses on decision making, trade-offs, requirement building, team building, leading, and other human factors not often taught in traditional program.






Appendix-I

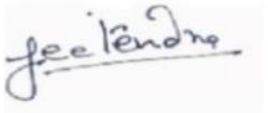
Title of Programme: Master of Science (cyber security)
Programme Code: MSC-CS-21
Programme Mode: Semester
Admission Cycle: Twice every Year in Jan and July
Eligibility: Graduation (Science/IT).
Lateral Entry(3rd Semester): Post Graduate Diploma/Certificate in Cyber Security
Duration: **Min:** 2 Years **Max:** 4 Years
SLM Availability Medium : English
Total Credit :80

Programme Fee:

Semester	Programme Fee	Exam Fee	Project Fee	Practical Fee	Viva-voce	Miscellaneous	Degree Fee	Total
First	10000	1250	NA	-	NA	150		11400
Second	10000	1000	1000	-	NA	-		12000
Third	10000	1000	NA	500	NA	-		11500
Fourth	10000	1000	1000	-	NA	-	300	12300

Objective of the Programme: To equip students with the vital knowledge of sophisticated applications of Cyber Security and to equip learner with the skills required for the application of electronics for telecommunication and its usefulness in software development.






Programme Structure:

First Semester

S.No.	Paper	Paper Code	Marks			Credits	Minimum Counseling Hours
			Theory	Assignment	Total		
1	Fundamentals of Information Security	MIT(CS)-101	70	30	100	4	12
2	Cyber Security Techniques	MIT (CS)-102	70	30	100	4	12
3	Cyber attacks and counter measures: user perspective	MIT (CS)-103	70	30	100	4	12
4	Information System	MIT (CS)-104	70	30	100	4	12
5	Introduction to Cyber Security	FCS	70	30	100	4	12

Second Semester

S.No.	Paper	Paper Code	Marks			Credits	Minimum Counseling Hours
			Theory	Assignment	Total		
1	Information Security Assurance : Framework, standards and Industry best practices	MIT (CS)-201	70	30	100	4	12
2	Digital Forensic	MIT (CS)-202	70	30	100	4	12
3	Advanced cyber security techniques	MIT (CS)-203	70	30	100	4	12
4	Cryptography & Network Security	MIT (CS)-204	70	30	100	4	12
5	Project + Viva	MIT (CS)-P2	-	-	150	4	12

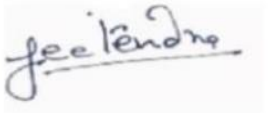
Third Semester

S.No.	Paper	Paper Code	Marks			Credits	Minimum Counseling Hours
			Theory	Assignment	Total		
1	Introduction to Computing	MIT (CS)-301	70	30	100	4	12
2	Introduction Digital Systems	MIT (CS)-302	70	30	100	4	12
3	Object Oriented Programming Using C++	MIT (CS)-303	70	30	100	4	12
4	Introduction to Operating System	MIT (CS)-304	70	30	100	4	12
5	Practical (C++)	MIT (CS)-P3	-	-	100	4	12

Forth Semester

S.No.	Paper	Paper Code	Marks			Credits	Minimum Counseling Hours
			Theory	Assignment	Total		
1	Data Structure	MIT (CS)-401	70	30	100	4	12
2	Introduction to DBMS	MIT (CS)-402	70	30	100	4	12
3	Introduction to Networking	MSIT (CS)-403	70	30	100	4	12
4	Computer Organization and Architecture	MIT (CS)-404	70	30	100	4	12
5	Practical (DS & DBMS)	MIT (CS)-Project	-	-	100	4	12






SYLLABUS

FUNDAMENTALS OF INFORMATION SECURITY
MIT(CS)-101

BLOCK I: INTERNET, E-COMMERCE & E-GOVERNANCE BASICS

Unit I: Introduction and History, Internet address, Domain Naming System, Internent infrastructure, ISP, Role of ISP, International & National ISP's, ccTLD (Country Code Top Level Domain), TLD (Top Level Domain) Types of accounts. Worldwideweb (WWW), Application areas of Internet. E-Governance: Need of E-Governance, Issues in E-Governance applications and the Digital Divide; Evolution of E-Governance, Its scope and content; growth in E-Governance global trends, Other issues.

Unit II: Model of Digital Governance: Broadcasting/ Wilder Dissemination Model, Critical Flow Model, Comparative Analysis Model, Mobilization and Lobbying Model, Interactive-service Model/Government-to-Citizen-to-Government Model (G2C2G); Evolution in E-Governance and Maturity Models: Five Maturity Levels, Characteristics of Maturity Levels, Key areas, Government framework, Digital India Program, Towards Good Governance through E-Governance Models.

Unit III: E-readiness: Digital System Infrastructure, Legal Infrastructural Preparedness, Institutional Infrastructural Preparedness, Human Infrastructural Preparedness, Technological Infrastructural Preparedness; Evolutionary Stages in E-Governance.

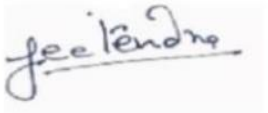
.

Unit IV: E-Commerce: Definition of E-commerce, Business Models of E-commerce and Infrastructure; B2B, B2C, B2G and other models of e-commerce; Types of payment systems - e-cash and currency servers, e-cheques, credit cards, smart cards, electronic purses and debit cards; e-wallet, Google Wallet, Digital locker and other initiatives of Central government and state Governments.

BLOCK II: CYBER CRIME

Unit I: Introduction to computer crime and cyber crimes, Distinction between cyber crime and conventional crimes, Reasons for commission of cyber crime, Some basic terminologies- Virus, Malware, worm, trojan, spyware, scareware, botnets, ransomware and zombies.






Unit II: Kinds of cyber crimes – Hacking, cyber stalking, cyber pornography; online forgery and fraud, Cyber terrorism, Cracking software, Downloading illegal music files, Creating and distributing viruses on other computers, Posting confidential business information on the internet, copyright infrigment, identity theft, phishing/spoofing, credit card fraud, on-line auction fraud, spamming, denial of service attack, debt elimination, internet extortion, cyber defamation, Smart Phone Auditing.

Unit III: Cyber criminals, Organized cyber crimes, Classification of cyber crimes, Cyber crime and Cyber terrorism, Information Warfare and Surveillance, Introduction to IT act.

Unit IV: Case Studies: Cyber Threats and Attacks, Impacts and response actions**.**

BLOCK III: INFORMATION SECURITY

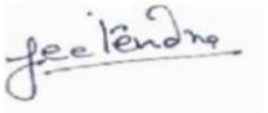
Unit I: Introduction to Cyber Security, Security principles, Security triad: Confidential, Integrity, Availability;
UNIT II: Introduction to ISMS
Unit III: Cyber security techniques for secure e-commerce: authentication, encryption, digital signatures, antivirus,firewall; Computer forensics, steganography
Unit IV: Ethical aspect of Cyber Security ,Tips for computer security: Think before you click, Update everything, Backup your files, Secure your wireless network, Use strong passwords, etc.

CYBER SECURITY TECHNIQUES
MIT(CS)-102

BLOCK I

Unit I: : Information Technology Security Policy , Aspects of Organizational security- IT security, Physical security, financial security, Legal security, online security.
Unit II: Modes of Attack- Insider attack, outsider attack. Why to report a cyber crime?, Reporting a cyber crime- How and when to report an incident?
Unit III: Intrusion Detection System/Prevention Systems and Incident Handling.






Unit IV: securing IT assets, Implementing Hardware Based Security, Software Based Firewalls, Securing IS assets, Prevent your network from anonymous attack, Wireless Security, WEP or WPA, Protect USB port

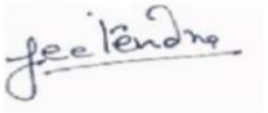
BLOCK II

Unit I: Security Standards & assurance frame work.
Unit II: desktop security and malware
Unit III: e-commerce & application security.
Unit IV: social engineering.

BLOCK III

Unit I: Risk management.
Unit II: Computer forensics & Collection of Digitial Evidence
Unit III: Cyber Security initiatives in India: National Information Security Assurance Programme (NISAP), Indian Computer Emergency Response Team (Cert-In), Indo US Cyber Security Forum (IUSCSF), National counter terrorism centre (NCTC) of India, National Critical Information Infrastructure Protection Centre (NCIPC) of India, Institute for Defence Studies and Analyses(IDSA), National Intelligence Grid (Natgrid) project of India, Crime and Criminal Tracking Networks and systems (CCTNS) project of India, national cyber cordination center, botnet cleaning center, malware analysis center.
Unit IV: Cyber Laws, National Cyber security policy, national cyber crisis plan.






CYBER ATTACKS AND COUNTER MEASURES: USER PERSPECTIVE
MIT(CS)-103

BLOCK I

Unit I: cyber attacks, types of attacks motivation.
Unit II: Assests Threats and Vulnerabilities , Risk Management.
Unit III: Information Security Framework: Organisation and Responsibilities, The Organisation's Management of Security, Organisational Policy, Standards and Procedures
Unit IV: Information Security Governance, Information Security Implementation, Security Information Management, Legal Framework , Security Standards and Procedures

BLOCK II

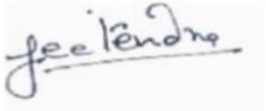
Unit I: Procedural / People Security Controls: People, User Access Controls, Communication, Training and Awareness
Unit II: Technical Security Controls, Protection from Malicious attacks, Networks and Communications, External Services, Cloud Computing, IT Infrastructure
Unit III: Software Development and Lifecycle: Testing, Audit and Review, Systems Development and Support

BLOCK III

Unit I: Authentication and password security
Unit II: Wireless security
Unit III: Investigation and forensic technique, investigate fraud email, fake social media profile investigation, investigate origin of spoof mail and genuine mail
Unit IV: introduction and application of cryptography

INFORMATION SYSTEM
MIT(CS)-104






BLOCK I

Unit I: Networking and Communications

Unit II: Cryptography

Unit III: VA/PT- Basics

Unit IV: Network Security, Email Security, Infrastructure & Web Application Security

BLOCK II

Unit I: History of Cryptography, Basic concepts of Cipher, simple cipher, digital cipher, Key management.

Unit II: Cryptographic Algorithms, symmetric cipher, asymmetric ciphers, data integrity algorithms

Unit III: Key management and distribution, user authentication Protocols

Unit IV: Network and internet security, Transport level security, wireless network security, e-mail Security, IP Security.

BLOCK III

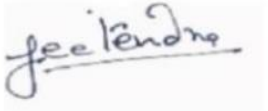
Unit I: footprinting and reconnaissance

Unit II: scanning and enumeration

Unit III: gaining access and exploitation

Unit IV: post exploitation activities






FCS

Introduction to Cyber Security

FCS is a foundation course and Course contents are available at

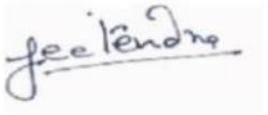
https://uou.ac.in/sites/default/files/slm/Introduction-cyber-security.pdf

INFORMATION SECURITY ASSURANCE : FRAMEWORK, STANDARDS AND INDUSTRY BEST PRACTICES

MIT(CS)-201

BLOCK I






Unit 1: Interrelationship between Regulation, policies, standard procedures and guidelines, Standards for Information Security: ISO standards- ISO/IEC 27002:2005 (Code of Practice for Information Security Management), ISO/IEC 27001:2005 (Information Security Management System - Requirements),

Unit II: Regulations related to Information Security- SOX, GLBA, COSO, HIPPA, FISMA, FIPS, FFIEC, common elements of compliance, Security controls, common pitfalls of a effective Information Security program.

Unit III: ISO/IEC 15408 (Evaluation Criteria for IT Security), ISO/IEC 13335 (IT Security Management); Payment Card Industry data security standards, COBIT, ITIL (OR ISO/IEC 20000 SERIES)

Unit IV: Introduction to industry best practices including NIST, SANS ,OWASP

BLOCK II

Unit I: Overviews of ISO-27K.

Unit II: ISO 27001

Unit III: ISO-27002

Unit IV: Other standards, guidelines, ISO- 27005

BLOCK III

Unit I: Security auditing

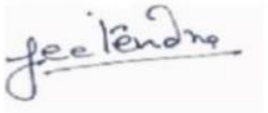
Unit II: Information security

Unit III: Disaster recovery

Unit IV: Business continuity planning and management

DIGITAL FORENSIC
MIT(CS)-202






BLOCK I

Unit I: Introduction to Computer Forensic, evolution and objective, goals of forensic readiness, role of forensic investigators,
Unit II: Computer forensic investigation process
Unit III : Digital Evidence and first responder procedure
Unit IV : Understanding storage media and file system

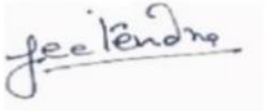
BLOCK II

Unit I: Windows forensic- data acquisition and duplication, recovering deleted files and deleted partitions.
Unit II: Application password crackers, Image forensic, log capturing and events correlation
Unit III: Network Forensic
Unit IV: Investigating wireless attacks

BLOCK III

Unit I: Investigating web attacks
Unit II: Investigating email attacks
Unit III: Mobile forensic
Unit IV: Investigative reports and becoming expert witness, cyber regulations and IT act






ADVANCED CYBER SECURITY TECHNIQUE

MIT (CS)-203

BLOCK I

Unit I: Perimeter Devices Security

Unit II: Data Center Security

Unit III: Secure Network design/Implementation

Unit IV: Physical and environment security

BLOCK II

Unit I: server security- patch management, server hardening.

Unit II: services hardening

Unit III: advanced web application security.

Unit IV: E-mail Security

BLOCK III

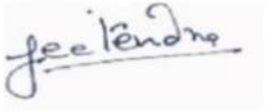
Unit I: desktop hardening

Unit II: mobile devices

Unit III: wireless

Unit IV: advanced persistent threats






CRYPTOGRAPHY AND NETWORK SECURITY

MIT(CS)-204

Block I

Unit I: Introduction to Network Security, Classical Cryptography, Substitution ciphers and Cryptanalysis, Transposition ciphers and Cryptanalysis
Unit II: Number Theory, Modular Arithmetic, Modular Exponentiation, Algebraic Structures and Finite Fields I, Algebraic Structures and Finite Fields II
Unit III: Prime's Euler and Fermat's Theorem
Unit IV: Chinese Remainder Theorem, Exponentiation and Logarithm

Block II

Unit V: Modern Cryptography, Stream cipher and Block Cipher
Unit VI: RC4, Simplified DES
Unit VII: Data Encryption Standard
Unit VIII: Modes of Operation, Advanced encryption standards

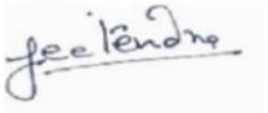
Block III

Unit IX: Public Key Cryptography, RSA Cryptosystem
Unit X: ELGAMMAL Cryptosystem, Elliptic Curve Cryptosystem
Unit XI: Key Management, Diffie-Hellman Key Exchange
Unit XII: Security Models, Hash Algorithms, Hash and MAC algorithms

Block IV

Unit XIII: Digital Signature, Kerberos, Public Key Infrastructure
Unit XIV: Electronic Mail security-PGP, Security Attack, IP Security
Unit XV: Web Security :SSL and TLS, Firewalls, Need of Security in Networks
Unit XVI: Introduction to Wireless LAN Security, WLAN Security






INTRODUCTION TO COMPUTING

MIT (CS)-301

BLOCK I

Unit 1: Computing

Computing: Processes, Procedures, and Computers; Measuring Computing Power: Information, Representing Data, Growth of Computing Power; Science, Engineering, and the Liberal Arts, Summary and Roadmap.

Unit II: Defining Procedures

Language, Surface Forms and Meanings, Language Construction , Recursive Transition Networks, Replacement Grammars.

Unit III Programming

Problems with Natural Languages, Programming Languages, Scheme, Expressions: Primitives, Application Expressions; Definitions, Procedures: Making Procedures, Substitution Model of Evaluation; Decisions, Evaluation Rules.

BLOCK II

Unit IV: Problems and Procedures

Solving Problems, Composing Procedures: Procedures as Inputs and Outputs; Recursive Problem Solving, Evaluating Recursive Applications, Developing Complex Programs: Printing, Tracing .

Unit V: Data

Data Types, Pairs: Making Pairs, Triples to Octuples; Lists, List Procedures: Procedures that Examine Lists, Generic Accumulators, Procedures that Construct Lists; Lists of Lists, Data Abstraction.

Unit VI: Analyzing Procedures

Machines, History of Computing Machines, Mechanizing Logic: Implementing Logic, Composing Operations, Arithmetic; Modeling Computing: Turing Machines .

BLOCK III

Unit VII: Cost

Empirical Measurements, Orders of Growth: Big O, Omega Theta; Analyzing Procedures: Input Size, Running Time, Worst Case Input; Growth Rates: No Growth: Constant Time, Linear Growth, Quadratic Growth, Exponential Growth, Faster than Exponential Growth , Non-terminating Procedures

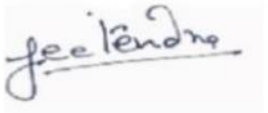
Unit VIII: Sorting and Searching

Sorting: Best-First Sort, Insertion Sort , Quicker Sorting, Binary Trees, Quicksort; Searching: Unstructured Search, Binary Search, Indexed Search;

Unit IX: Improving Expressiveness

Mutation, Assignment, Impact of Mutation: Names, Places, Frames, and Environments, Evaluation Rules with State; Mutable Pairs and Lists, Imperative Programming: List Mutators, Imperative Control Structures






BLOCK IV

Unit X: Objects

Packaging Procedures and State: Encapsulation, Messages, Object Terminology; Inheritance: Implementing Subclasses, Overriding Methods; Object-Oriented Programming.

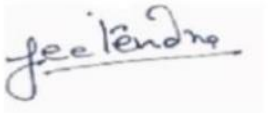
Unit XI: Interpreters

Python: Python Programs, Data Types, Applications and Invocations, Control Statements; Parser, Evaluator: Primitives, If Expressions, Definitions and Names, Procedures , Application , Finishing the Interpreterl Lazy Evaluation: Lazy Interpreter, Lazy Programming.

Unit XII: The Limits of Computing

Computability, Mechanizing Reasoning: Godel's Incompleteness Theorem; The Halting Problem, Universality, Proving Non-Computability.






INTRODUCTION TO DIGITAL SYSTEM
MIT (CS)-302
Block I

Unit I: Number Systems: Introduction to number systems: Binary, Octal & Hexadecimal systems; Conversion of numbers in one radix to numbers in different radix; Different Binary Codes
Unit II: Boolean Algebra, Theorems & Postulates; Logic functions: representation and graphic representation
Unit III: Minimization of logic functions: Algebraic and K-map methods
Unit IV: Minimization using Quine-Mc Clausky

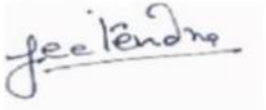
Block II

Unit I: Introduction to combinational circuits, Realization of basic combinational functions.
Unit II: Delays and hazards in design
Unit III: Structure of sequential circuits
Unit IV: Flip-flops

Block III

Unit I: Introduction to Logic families, Electrical Characteristics of logic devices, Characteristics of TTL logic devices, Characteristics of CMOS logic devices
Unit II: Introduction to different types of memories
Unit III: Programmable Logic Devices, Analysis of sequential circuits using timing diagrams, state tables, state diagrams, Design of digital circuits, Design of digital circuits using PLDs.
Unit IV: Introduction to Hardware Descriptive Languages, Defining entities, architecture with different modeling architecture, Designing digital circuits in VHDL.






OBJECT ORIENTED PROGRAMMING USING C++

MIT (CS)-303

Block I

Unit I: Introduction to Object Oriented Programming, Complexity, Programming languages, Features of C++, Type safety, Namespaces, From C to C++, Input and Output examples

Unit II: Object Terminology: abstraction, classes, UML, Encapsulation, Inheritance and Polymorphism.

Unit III: Modularity: Modules, stages of compilation; Basic syntax: keywords, types, declaration and definition, Function rules, Pass by reference.

Unit IV: Member functions: privacy, Empty state; Input/output: streams, Output objects, Input objects, state, robust validation.

Block II

Unit I: Dynamic memory: system memory, Dynamic allocation, memory issues, Single instances; Construction: Basic class features, Constructor, Destructor, Overloading constructors,.

Unit II: Current objects: Member function access, THIS; Class and Resources: Resource instance pointers, Deep copies and assignments, Copy constructor, Assignment operator, Localization, Copies prohibited.

Unit III: Member operators: Operations, Binary operations, Unary operations, Type conversions, Single-argument constructors, Temporary objects; Helpers: Free helpers, Helper operators, Friendship, Custom I/O Operators: Design considerations, Two helper operators, String class.

Unit IV: Custom file operators: File stream classes, File objects, Functional types, Custom types, Nice to know.

Block III

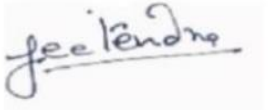
Unit I: Derived classes: Hierarchies, Definition of a derived class, Access; Derived functions: Shadowing, Constructors, Destructors, Helper operators; Derived Class and Resources: Constructors and Destructors, Copy constructor, Copy assignment operator.

Unit II: Polymorphism: Languages, Types, Categories; Virtual Function: Function bindings, Polymorphic objects, Efficiently and Flexibility;.

Unit III: Abstract base classes: Pure virtual functions, Abstract base classes, Unit tests on an interface; Function templates: Template syntax, Explicit specialization, Class template, Type casting.

Unit IV: The ISO/IEC Standard: Milestones, Loose ends;






INTRODUCTION TO OPERATING SYSTEM
MIT (CS)-304
Block I

Unit I: Introduction to Operating System
Operating systems: Application scenarios, kind of resource support needed by applications, what is an "Operating System" and what support is provided to run an application, hardware and software layers, organization of a computer system, operational view of a computing system with resources like processor, memory, input and output, issues in resource management, a bare-bone operating system, introduction to the issues in communication with devices, kernel and shell of an operating system, processes and file

Unit II: File system Management
File systems: What is a file, user view of files, file types and file operations, file types in Unix and Microsoft, file operation commands, file access rights, file storage management, Inode or FAT structure, file control blocks, root file system, directory and file paths, blocks, impact of block size selection, contiguous allocation, chained and indexed allocations, Impact of allocation policy on fragmentation, mapping file blocks on the disk platter, cylinder, disk access control and scheduling

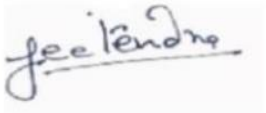
Unit III: Process Management
Processor resource management: Explanation of processor as a resource, definition of a process, processor utilization, multi-processing and time sharing, response time, process state, process state transitions, process scheduling, short-term and long term schedules, non-pre-emptive and pre-emptive scheduling policies, time slice, policies like FCFS, SJF etc. Gantt charts and parameters to compare policy performance, context switching of process state information. Kernel architecture: User and kernel mode of operation, System calls, process states, kernel operations, design of a scheduler.

Unit IV: Memory Management
Motivation for memory management, when and where primary and secondary memory management is needed, compiled code and memory relocation, linking and loading, processes and primary memory management, memory allocation policies, critique of various policies like first fit, best fit, internal and external fragmentation, secondary memory management, fixed and variable partitions, virtual memory concept, paging and page replacement policies, page faults, thrashing, hardware support for paging, segmentation, segmentation with paging.

Block II

Unit I: Input Output Management






Issues in human centric, device centric and computer centric IO management, input output modes, programmed IO, polling, interrupt mode of IO, various types of interrupts, interrupt servicing, priority interrupts, interrupt vectors, direct memory access (DMA) mode of transfer, setting up DMAs, device drivers, interrupt handling using device drivers, buffer management, device scheduling, disk scheduling algorithms and policies.

Unit II: Resource Sharing and Management

Shared resources, resource allocation and scheduling, resource graph models, deadlocks, deadlock detection, deadlock avoidance, deadlock prevention algorithms, mutual exclusion, semaphores, wait and signal procedures.

Unit III : Interprocess communication

Spawning a new process, parent and child processes, assigning a task to child processes, need for communication between processes, modes of communication, pipes, shared files, shared memory, message based IPC, signals as IPC, the distribute computing environment.

Unit IV: Real time Systems and Microkernels

Characteristics of real-time operating systems, classification of real-time systems, architectures of real-time systems, micro-kernels, scheduling in RTOS, rate monotonic scheduling, priority inversion, RTOS for hand-held devices.

Block III

Unit I: OS and Security

Security breaches, types of attacks, attack prevention methods, security policy and access control, OS design considerations for security, access, policy and access control, OS design considerations for security, access control lists and OS support, internet and general network security.

Unit II : OS primer

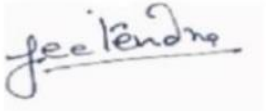
Basic file creation, editing and storage, accessing and organizing files, editor tools and file management operations, Basic string search commands, find commands, commands to sort with their options.

Unit III: AWK tool

AWK tool, AWK syntax, AWK grammar, examples for processing; Shell scripts: Productivity tools, different shells, shell scripts

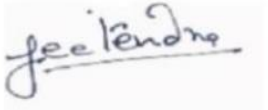
Unit IV: Make tool: When to use Make, how to use Make, macros abstractions and shortcuts; Other useful tool: Tar and other utilities, file compression tools, image and multi-media file formats, profiling tools; Version control tool: Need for version control, sccs, cvs and other version control tools.






Unit V: Window metaphor and GUI: Need for a desktop metaphor, window systems and associated controls, graphical interface (GUI); System administration: Administration tasks, user account management, start and shutdown procedures, setting up operational environment for a new user.






DATA STRUCTURE

MIT (CS)-401

Block I

Unit I: Introduction to Data Structures, Arrays and Strings

Unit II: Introduction to Algorithms: Algorithm Development, Complexity analysis, Recursion

Unit III: Linear Data Structures

Stacks: Operations and Applications; Queues: Operations and Applications; Circular Queues: Operations and Applications.

Unit IV: Links Lists

Operation: Creations, insertion, Deletion; Circular Lists; Doubly Linked List

Block II

Unit I: Sorting: Insertion Sort, Merge Sort, Quick Sort.

Unit II: Searching: Binary Search, Selection.

Unit III: Graphs I: Representation and Traversal: Representation: Matrix, Adjacency list; Traversal: Depth First Search, Breadth First Search.

Unit IV: Graphs II: Basic Algorithms: Minimum Spanning Tree, Shortest Path, All pairs Shortest Path, Transitive Closer.

Block III

Unit I: Binary Trees: Representation; Operations: Insert, Delete; Traversal: Preorder, Inorder, Postorder.

Unit II: Heap Sort Method and Complexity, Priority Queue

Unit III: Search Trees: AVI-trees, B-tree, External Search.

Unit IV: Tables: Hashing Techniques

Block IV

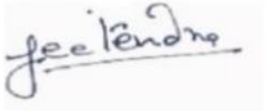
Unit I: Sets: Representation; Operations: Union and Find.

Unit II: String Algorithms: Pattern Matching, Text Editor.

Unit III: Program Development: Program Specification, Pre and post Condition, Program Documentations.

Unit IV: Program Testing and Verification: Testing Methods, Verification Procedures.






INTRODUCTION TO DBMS

MIT (CS)-402

Block I

Unit I: General introduction to database systems; Database-DBMS distinction, Approaches to building a database,

Unit II: Data models, Database management system, Three-schema architecture of a database, Challenges in building a DBMS, Various components of a DBMS.

Unit III: E/R Model: Conceptual data modeling - motivation, Entities, Entity types, Various types of attributes,

Unit IV: Relationships, Relationship types, E/R diagram notation, Examples.

Block II

Unit I: Relational Data Model: Concept of relations, Schema-instance distinction, Keys, referential integrity and foreign keys.

Unit II: Relational algebra operators: Selection, Projection, Cross product, Various types of joins, Division, Example queries,

Unit III: Tuple relation calculus, Domain relational calculus, Converting the database specification in E/R notation to the relational schema.

Unit IV: SQL: Introduction, Data definition in SQL, Table, key and foreign key definitions, Update behaviors. Querying in SQL, Basic select-from- where block and its semantics, Nested queries - correlated and uncorrelated, Notion of aggregation, Aggregation functions group by and having clauses, Embedded SQL.

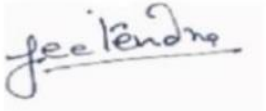
Block III

Unit I: Dependencies and Normal forms: Importance of a good schema design, Problems encountered with bad schema designs, Motivation for normal forms, dependency theory - functional dependencies,

Unit II: Armstrong's axioms for FD's, Closure of a set of FD's, Minimal covers, Definitions of 1NF, 2NF, 3NF and BCNF, Decompositions and desirable properties of them, Algorithms for 3NF and BCNF normalization, Multi-valued dependencies and 4NF, Join dependencies and definition of 5NF.

Unit III: Data Storage and Indexes: File organizations, Primary, Secondary index structures, Various index structures - hash-based, Dynamic

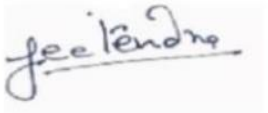





hashing techniques, Multi-level indexes, B+ trees.

Unit IV: Transaction processing and Error recovery: Concepts of transaction processing, ACID properties, Concurrency control, Locking based protocols for CC, Error recovery and logging, Undo, Redo, Undo-redo logging and recovery methods.






INTRODUCTION TO NETWORKING

MIT (CS)-403

Block I

Unit I: Introduction: Sharing of Data; Packetised File Transmission, Layering, Performance Metrics.

Unit II: Basic Building Blocks, Modulation, Physical Media, Transmission, DLL Framing

Unit III: Error Detection, Synthesis, Error control / Reliable Transmission.

Unit IV: Stop and Wait Protocol, Sliding Window Protocol, SW-Analysis, Medium Access Sublayer, ALOHA, The Ethernet Frame Format, Collision free protocols

Block II

Unit I: ATM – Asynchronous Transfer Mode, Token Bus, Token Ring,

Unit II: Fibre Distributed Data Interface, FDDI Analysis

Unit III: Wireless LANs, Bridges and Switches, Connectionless Networks Network Layer

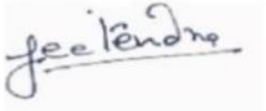
Unit IV: IP Packet/Fragmentation, Router Forwarding, Congestion control

Block III

Unit I: Routing Algorithms, Virtual Networks, Routing Algorithms-LSR, CIDR / BGP

Unit II: The Transport Layer, TCP Connection Management, TCP- Protocol, TCP –Miscellaneous.

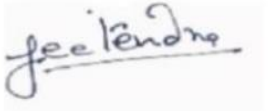





Unit III: Application Layer Protocol, Simple Network Management Protocol, SMTP.

Unit IV: Network Security






COMPUTER ORGANIZATION AND ARCHITECTURE

MIT (CS)-404

Block I

Unit I: Introduction to computer system and its submodules , Number System and Representation of information.

Unit II: Arithmetic and Logical operation and hardware implementation, Software implementation of some complex operation.

Unit III: Arithmetic and Logic Unit, Introduction to memory Unit, control unit and Instruction Set

Unit IV: Working with an ALU, Concepts of Machine level programming, Assembly level programming and High level programming

Block II

Unit I:Various addressing modes and designing of an Instruction set, Concepts of subroutine and subroutine call, Use of stack for handling subroutine call and return.

Unit II: Introduction to CPU design, Instruction interpretation and execution, Micro-operation and their RTL specification.

Unit III: Hardwired control CPU design

Unit IV: Microprogrammed control CPU design

Block III

Unit I: Concepts of semiconductor memory, CPU- memory interaction, organization of memory modules

Unit II: Cache memory and related mapping and replacement policies.

Unit III: Virtual memory

Unit IV: Introduction to input/output processing, working with video display unit and keyboard and routine to control them, Programmed controlled I/O transfer, Interrupt controlled I/O transfer, DMA controller

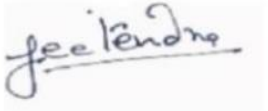
Block IV

Unit I: Secondary storage and type of storage devices, Introduction to buses and connecting I/O devices to CPU and memory

Unit II: Introduction to RISC and CISC paradigm, Design issues of a RISC processor and example of an existing RISC processor, Introduction to pipelining and pipeline hazards, design issues of pipeline architecture

Unit III: Instruction level parallelism and advanced issues, Introduction to interconnection network and practical issues, Examples of interconnection networks






Unit IV: Multiprocessors and its characteristics, Memory organization for multiprocessors systems, synchronization and models of memory consistency, Issues of deadlock and scheduling in multiprocessor systems, Cache in multiprocessor systems and related problems, Cache coherence protocols, Parallel processing concepts, Parallelism algorithm for multiprocessor systems.