MCIT - 201 Information Security System

Unit 1
Introduction: Basic objectives of cryptography, secret-key and public-key cryptography, one-way and trapdoor one-way functions, cryptanalysis, attack models, classical cryptography. Block ciphers: Modes of operation, DES and its variants, RCS, IDEA, SAFER, FEAL, BlowFish, AES, linear and differential cryptanalysis. Stream ciphers: Stream ciphers based on linear feedback shift registers, SEAL, unconditional security.

Unit 2
Message digest: Properties of hash functions, MD2, MD5 and SHA-1, keyed hash functions, attacks on hash functions. Public-key parameters: Modular arithmetic, gcd, primality testing, Chinese remainder theorem, modular square roots, finite fields.

Unit 3
Intractable problems: Integer factorization problem, RSA problem, modular square root problem, discrete logarithm problem, Diffie-Hellman problem, known algorithms for solving the intractable problems.

Unit 4
Public-key encryption: RSA, Rabin and EIGamal schemes, side channel attacks. Key exchange: Diffie-Hellman and MQV algorithms. Digital signatures: RSA, DAS and NR signature schemes, blind and undeniable signatures. Entity authentication: Passwords, challenge-response algorithms, zero-knowledge protocols. Standards: IEEE, RSA and ISO standards

Unit 5
Network issues: Certification, public-key infrastructure (PKI), secured socket layer (SSL), Kerberos. Advanced topics: Elliptic and hyper-elliptic curve cryptography, number field sieve, lattices and their applications in cryptography, hidden monomial cryptosystems, cryptographically secure random number generators.
Reference Books:

1. William Stallings, Cryptography and Network Security, PHI
2. Atul Kahate, “ Cryptography and Network Security”, TMH
3. Calabrese, Info security intelligence-cryptography principles appl., Cengage Learn
4. Krawetz, Intro to network security, Cengage Learning.

MCIT - 202 Distributed Computing

Unit 1 INTRODUCTION
Characterization of Distributed Systems - Examples - Resource Sharing and the Web - Challenges - System Models - Architectural and Fundamental Models - Networking and Internetworking - Types of Networks - Network Principles - Internet Protocols - Case Studies.

Unit 2 PROCESSES AND DISTRIBUTED OBJECTS
Interprocess Communication - The API for the Internet Protocols - External Data Representation and Marshalling - Client-Server Communication - Group Communication - Case Study - Distributed Objects and Remote Invocation - Communication Between Distributed Objects - Remote Procedure Call - Events and Notifications - Java RMI - Case Study.

Unit 3. OPERATING SYSTEM ISSUES – I
The OS Layer - Protection - Processes and Threads - Communication and Invocation – OS Architecture - Security - Overview - Cryptographic Algorithms - Digital Signatures - Cryptography Pragmatics - Case Studies - Distributed File Systems - File Service Architecture - Sun Network File System - The Andrew File System

Unit 4. OPERATING SYSTEM ISSUES – II
Name Services -Domain Name System - Directory and Discovery Services - Global Name Service - X.500 Directory Service - Clocks, Events and Process States - Synchronizing Physical Clocks - Logical Time And Logical Clocks - Global States - Distributed Debugging - Distributed Mutual Exclusion – Elections – Multicast Communication Related Problems.

Unit 5. DISTRIBUTED TRANSACTION PROCESSING
Transactions - Nested Transactions - Locks - Optimistic Concurrency Control - Timestamp Ordering - Comparison - Flat and Nested Distributed Transactions - Atomic Commit Protocols - Concurrency Control in Distributed Transactions - Distributed Deadlocks - Transaction Recovery - Overview of Replication And Distributed Multimedia Systems

Reference Books:

1. G Coulouris, J Dollimore, T Kindberg, Distributed Sys Concept- Design, Pearson
2. Sape Mullender, Distributed Systems, Addison Wesley,
3. A Fleishman, Distributed Systems- Software Design and Implementation, S Verlag
4. M.L.Liu, Distributed Computing Principles and Applications, Pearson Education
5. AS Tanenbaum, Maartenvan, ,Distibuted System Principles Paradigms, Pearson
6. M Singhal, Niranjan, Shivaratri, Advanced Concept in Operating System, TMH
7. Flynn, Underatanding Operating System, Cengage (Thomson)

MCIT - 203 Advance Computer Architecture

UNIT 1
Flynn's and Handler's Classification of parallel computing structures. Pipelined and Vector Processors.

UNIT 2
Data and control hazards and method to resolve them. SIMD multiprocessor structures.

UNIT 3
nterconnection networks. Parallel Algorithms for array processors, Search algorithms, MIMD multiprocessor systems,

UNIT 4
Scheduling and load balancing in multiprocessor systems, Multiprocessing control a algorithms.

Reference Books:

1. Advance Computer Architecture, parthsarthy, Cengage (Thomson)
2. Computer Architecture and Organisation- John Hays, Mc.Graw-Hill.
3. Computer Architecture and Parallel Processing- Hwang And Briggs, TMH.

MCIT - 204 Soft Computing

INTRODUCTION: production systems, Study and comparison of breadth first search and depth first search. Techniques, other Search Techniques like hill Climbing, Best first search. A* algorithm, AO* algorithms. Knowledge Representation, Problems in representing knowledge, knowledge representation using prepositional and predicate logic, Resolution, Refutation, theorem proving, monotonic and nonmonotonic reasoning.

ARTIFICIAL NEURAL NETWORKS : Basic concepts - Importance of tolerance of imprecision and uncertainty. Biological and artificial neuron, Single layer perception - Multilayer Perception - Supervised and Unsupervised learning – Back propagation networks - Kohnen's self organizing networks - Hopfield network.

FUZZY SYSTEMS : Introduction, History of the Development of Fuzzy Logic, Fuzzy sets and Fuzzy reasoning - Fuzzy matrices - Fuzzy functions - Decomposition - Fuzzy automata and languages - Fuzzy control methods - Fuzzy decision making.

NEURO - FUZZY MODELING : Adaptive networks based Fuzzy interface systems - Classification and Regression Trees - Data clustering algorithms - Rule based structure identification - Neuro-Fuzzy controls - Simulated annealing – Evolutionary computation.

GENETIC ALGORITHMS: Survival of the Fittest - Fitness Computations - Cross over - Mutation - Reproduction - Rank method - Rank space method.

Reference Books :

1. Rajsekaran &amp; Pai – Neural Networks, fuzzylogic &amp; Genetic algorithms, PHI
2. Rich E and Knight K, Artificial Intelligence, TMH, New Delhi.
3. Hagan, Dernuth &amp; Beale, Neural network design, Thomson learning, VP.
4. Philip D. Wasserman, Neural Computing, Van Nostrand Reinhold Pub.
5. Kecman: Learning &amp; soft Computing, Pearson Edu.

MCIT - 205 Mobile Computing

UNIT 1

Introduction to cellular mobile systems: Basic cellular system, performance, criteria, Uniqueness of mobile Radio environment, operation of cellular systems, marketing Image of Hexagonal shaped cells, Planning of cellular system, Analog cellular systems, digital cellular systems, cell splitting.

UNIT 2

Cell coverage for signal &amp; Traffic: Introduction, obtaining the mobile point to point model, Propagation over water or flat open areas, Foliage loss, Propagation in near in distance, long distance Propagation obtain path less from a point to point Prediction model, call-site antenna Heights &amp; Signal coverage calls, mobile to mobile Propagation.

UNIT 3

Co channel Interference reduction: Co channel interference , exploring co channel interference area, in a system, Real time co channel interference measurement at mobile radio Transceivers, Decision of an omni directional antenna system, Design of a directional antenna system,. Lowering the antenna height, reduction of co channel interference by mean of a notech in the tilted antenna Pattern, Power control.

UNIT 4

Frequency management &channel Assignment: Frequency management, Frequency-spectrum utilization, set up channels definition of channel assignment, fixed channel assignment, non fixed channel assignment algorithms How to operate north additional spectrum, Traffic &amp; channel assignment, Perception of call blocking from the subscribers.

UNIT 5

Handoffs &amp; Dropped calls: Value of Implementing Handoffs, initiation of a hand off, Delaying ahandoff, Forced Handoffs, Queuing of Handoffs, power difference handoff , Mobile assisted handoff &amp; soft Handoff, call site Handoff only, intersystem Handoff, introduction to dropped call rate, Formula of Dropped call rate, Finding the values of g &amp; u.

UNIT 6

Special topics: Wireless and Mobile Computation – SS7, GSM, CDMA, Mobile IP, Wireless Mobile ATM, Multicast Routing Protocols, Location Management, Mobile Agents, Mobility Management.

Reference Books:

1. J. Schiller, Mobile Communication, Pearson Press.
2. Wireless Network, Kaveh Pahalwan
3. Adhoc Networking by Charles E. Perkins, Addison Wisely
4. Mobile cellular Telecommunications by William C.Y. Lee TMH