Syllabus

for

2-Years M. Tech. in Computer Science & Engineering (Specialisation: Information Security)

Effective from 2015-2016 Academic Session

Department of Computer Science and Engineering
National Institute of Technology Sikkim
South Sikkim - 737 139

CSE 2111	Number Theory & Cryptography	3-0-0	3

Module 1

Algebra: Group, cyclic group, cyclic subgroup, field, probability.

Number Theory: Fermat's theorem,Cauchy's theorem, Chinese remainder theorem, primality testing algorithm, Euclid's algorithm forintegers, quadratic residues, Legendre symbol, Jacobi symbol etc.

Module 2

Cryptography and cryptanalysis, Classical Cryptography, substitution cipher, different type of attack:CMA,CPA, CCA etc. Shannon perfect secrecy, OTP,

Pseudo random bit generators, stream ciphers andRC4.

Module 3

Block ciphers: Modes of operation, DES and its variants, AES, linear and differential cryptanalysis; One-way function , Trapdoor one-way function, Public key cryptography, RSA cryptosystem, Diffie-Hellman key exchange algorithm, Elgamal Cryptosystem; Cryptographic hash functions, Secure hash algorithm, Message authentication, digital signature, RSAdigital signature, Elgamal digital signature.

Module 5

IKE and IPSec; SSL/TLS; E-mail Security and PGP

Text Book

Behrouz A. Forouzan and Debdeep Mukhopadhyay, Cryptography and Network Security, Second edition, Tata McGraw Hill, 2011

Reference Books

1. W. Stallings, Cryptography and Network Security Principles and practice, 5/e, Pearson EducationAsia, 2012.
2. Stinson. D. Cryptography: Theory and Practice, third edition, Chapman & Hall/CRC, 2010.
3. Thomas Koshy, Elementary Number Theory with applications, Elsevier India, 2005

MAT2111	Computational Mathematics	4-0-0	4

Module 1

Definitions, examples of problems in graph theory, Adjacency and incidence matrices, isomorphisms, Paths, walks, cycles, components, cut-edges, cut-vertices, Bipartite graphs, Eulerian graphs, Vertex degrees, reconstruction conjecture, Directed graphs, Orientations and tournaments. Trees and forests, characterizations of trees, Cayley's formula, Counting spanning trees, Minimum spanning trees, shortest paths, Matchings, Chinese postman and traveling salesman problems, maximal and maximum matchings

Module 2

Min-max theorems, maximum matchings and vertex covers, independent sets and edge covers. Ramsey theorem, Turan theorem, Schur theorem, Connectivity, vertex cuts, Edge-connectivity, blocks, k-connected graphs, line graphs, Vertex colorings, bounds on chromatic numbers, Chromatic numbers of graphs constructed from smaller graphs, chromatic polynomials, Properties of the chromatic polynomial, Planar graphs, Euler's formula, Kuratowski's theorem, five and four color theorems

Module 3

Linear and Nonlinear Algebraic Equation. Solutions of linear algebraic equations; forwarding Gaussian elimination, pivoting, scaling, back substitution, LU-decomposition, norms and errors, condition numbers, iterations, Newton's method for systems, computer implementation, Solution of nonlinear equations; bisection method, secant method, Regula falsi method ,Newton's method, fixed point iteration, Muller's

method.

Module 4

Interpolation; Lagrange interpolation, Newton interpolation, inverse interpolation. Numerical Integration; finite differences, Newton cotes rules, trapezoidal rule, Simpson's rule, extrapolation, Gaussian quadrature.Numerical solution of ordinary differential equations; Euler's method, Runge-Kutta method, multi-step methods, predictor-corrector methods, rates of convergence, global errors, algebraic and shooting methods, for boundary value problems, computer implementation.

Text Books

1. Douglas B. West, Introduction to Graph Theory, Prentice Hall India.
2. S. R. K. Iyengar and R. K. Jain, Mahinder Kumar Jain, Numerical Methods for Scientific and Engineering Computation by, New age International.

References

A. Bondy and U.S.R. Murty, Graph Theory, Springer

CSE2112	Advance Computer Networks	3-0-0	3

Module 1

Review of Networking Concepts. MAC layer issues: MAC protocols for high-speed LANS, MANs, wireless LANs and mobile networks, VLAN. Fast access technologies, Ethernet 802.3, ARP, IP addressing and Subnetting, NAT and PAT, Variable Length Subnet Masking, CIDR

Module 2

End to End protocols (10) TCP connection establishment and termination, Sliding window concepts, other issues: wraparound, silly window syndrome, Nagle's algorithm, adaptive retransmission, TCP extensions. Congestion and flow control, Queuing theory, TCP flavors: Tahoe, Reno, New-Reno, TCP-SACK, TCP-RED and TCP-Vegas. Transport protocol for real time (RTP), Quality of service: Integrated Services, Differentiated services, TCP extensions for high-speed networks, transaction-oriented applications.

Module 3

Routing and Multicast. Structure of internet: Autonomous systems, Intra-domain routing: OSPF and RIP, Inter-domain routing: BGP. Multicasting: Group Management (IGMP), Internet scale multicasting: Reverse path broadcast, MOSPF, DVMPRP, PIM. IPv6: Why IPv6, basic protocol, extensions and options, support for QoS, security, neighbour discovery, auto-configuration, routing. Changes to other protocols. Application Programming Interface for IPv6, 6bone. IP Multicasting, wide area multicasting, reliable multicast. Routing layer issues, ISPs and peering, BGP, IGP, Traffic Engineering, Routing mechanisms: Queue management, packet scheduling. MPLS, VPNs

Module 4

Peer to peer and overlay networks. Concept of overlays, Unstructured Overlays: overlay networks, Internet traffic modelling, P2P Network, Gnutella, Concepts of Distributed Hash Table, Structured Overlays: Chord, CAN, Pastry.

Text Books

1. Computer Networks: A Systems Approach, by Peterson and Davie, 5th Ed. Morgan Kauffman, 2011
2. Computer Networking: Top Down Approach, by Kurose and Ross, 6th Ed. Pearson, 2011

Reading List

1. V. Paxson. "End-to-end Internet packet dynamics," in IEEE/ACM Transactions on Networking, Vol. 7, No 3, June, 1999.

2. W. Stevens, "TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms," RFC2001.3. K. Fall and S. Floyd, "Simulation-based comparison of Tahoe, Reno, and SACK TCP," Computer Communication Review, vol. 26, pp. 5--21, July 1996.
3. L. Brakmo and L. Peterson, "TCP Vegas: End-to-End Congestion Avoidance on a Global Internet," IEEE Journal on Selected Areas in Communications, 13(8), October 1995, 1465--1480.
4. Stoica, I., Morris, R., Karger, D., Kaashoek, F., Balakrishnan, H.: Chord: A scalable peer-to-peer lookup service for Internet applications.
5. Rowstron, A., Druschel, P.: Pastry: Scalable, decentralized object location and routing for large-scale peer to peer system
6. W. R. Stevens, TCP/IP Illustrated, Volume 1: The protocols, Addison Wesley, 1994.
7. G. R. Wright, TCP/IP Illustrated, Volume 2: The Implementation, Addison Wesley, 1995.
8. W. R. Stevens, TCP/IP Illustrated, Volume 3: TCP for Transactions, HTTP, NNTP, and the Unix Domain Protocols, Addison Wesley, 1996.
9. Articles in various journals and conference proceedings.
10. RFCs and Internet Drafts, available from Internet Engineering Task Force.

CSE 2121	Number Theory & Cryptography Laboratory	0-0-2	1

1. Simple shit cipher and transposition cipher in a client server mode using socket programming.
2. Implementation of protocol cipher having specific number of rounds in fiestal and non-fiestal mode
3. Creation of key pair in PGP sending mail using PGP and S-MIME
4. Invenstigation of cryptanalysis in veginere cipher
5. Cryptanalysis of affine cipher for a known plan text attack
6. Investigation of ssecurity whole in linux and windows-OS
7. Test of linear and differential cryptanalysis on DES
8. Implementation of two fish/blow fish cipher
9. Solving simple security problems using the tools such as Wireshark, NMAP etc.

Text Book

Saiful Azad and Al-Sakib Khan Pathan, “Practical Cryptography: Algorithms and Implementations Using C++”.

CSE 2122	Advance Computer Networks Laboratory	0-0-2	1

Experiment 1: Implementing fully concurrent application with a TCP server acting as a directory server and client programs allowing concurrent connection and message transfer (Eg. Chat system).
Experiment 2: Fully decentralized application like a Peer to Peer system. This program is to implement without a designated Sever as in the case of experiment 5.
Experiment 3: Experiments with open source firewall/proxy packages like iptables,ufw, squid etc.
Experiment 4: Experiments with Emulator like Netkit, Emulab etc.
Experiment 5: Experiments with Simulator like NS2, NCTU NS etc.

Text Books

W. Rıchard Stevens, Unix Network Programming – Networking APIs: Sockets and XTI Volume 1, 2nd Edition, Pearson Education, 2004.

CSE 2131	Pattern Recognition	4-0-0	4

Module 1

Introduction: Machine Perception, Pattern Recognition Systems, The Design Cycle, Learning and Adaptation. Bay’s Decision Theory: Bayes Decision Theory, Minimum Error rate Classification, Classifiers, Discriminant functions and Decision Surfaces, Normal Density, Discriminant functions for the Normal Density, Bayes Decision Theory for Discrete features

Module 2
Maximum Likelihood and Bayesian Parameter Estimation: Maximum Likelihood Estimation, Bayesian Estimation, Bayesian Parameter Estimation, Gaussian Case and General Theory.Hidden Markov models; Non Parametric Techniques: Density Estimation, Parzen Windows, K- Nearest Neighbor Estimation, Nearest Neighbour rule, Metrics and Nearest Neighbour Classification, Fuzzy Classification, k-Means Clustering, Self-Organizing Maps.

Module 3
Linear Discriminant Functions: Linear Discriminant Functions and Decision Surfaces, Generalized Discriminant Functions, The two-category linearly separable case, Minimizing the perceptron criterion function, relaxation procedures, non- separable behavior, Minimum Squared- Error procedures. Support vector machines, Algorithm-independent machine learning-Bias and Variance, Bootstrapping-Adaboost Algorithm, Boosting, Bagging

Module 4
Multi-Layer Neural Networks: Feed-forward Operation, Classification, Back – propagation Algorithm, Error Surfaces, Back-propagation as Feature mapping, Radial Basis Function Networks, Decision trees: Axis-parallel, Oblique, Impurity measures; Graphical Model,

Text Book

R. O. Duda, P. E. Hart and D. G. Stork, Pattern classification, John Wiley & Sons, 2002.

References

1. C. M. Bishop, Neural Networks for Pattern Recognition, Oxford University Press, 1995.
2. V. N. Vapnik, The Nature of Statistical Learning Theory, Springer, 2000.
3. N. Cristianini and J. Shawe-Taylor, An Introduction to Support Vector Machines, Cambridge University Press, 2000.

CSE 2132	Public Key Infrastructure and Trust Management	4-0-0	4

Module 1
Asymmetric key cryptography: RSA cryptosystem, RABIN Cryptosystem ElGamal Cryptosystem, message Integrity & Authentication; Random Oracle model, message authentication, Cryptographic hash functions; MD hash families, Whirlpool, SHA-512

Module 2
Digital Signature; Process and services, attacks on digital signatures, Digital Signature Schemes; Digital certificates and PKIs; Different PKIs: PGP (Pretty Good Privacy): Web of trust, applications; X.509: X.500, Certification Authority (CA), Registration Authority (RA), Root-CA, X.509 Protocols, Simple PKI (SPKI), Simple Distributed Security Infrastructure (SDSI);

Module 3
Entity Authentication; Passwords and Challenge Response, zero-knowledge and bio-metrics, Key management; security key distribution, Kerberos, Symmetric Key aregreement, Public Key Distribution and Hi-jacking, Issues of revocation, Anonymity and Privacy Smartcard integration with PKIs, Trust management systems, PGP (Pretty Good Privacy)- Web of trust, applications, SSL/TLS, Internet Key Exchange Protocol(IKE)

Module 4
Elliptic curve Cryptography (ECC), ECC-based PKI: IKE, PKIX.509; Research based problem identification and discussion

Text Books

1. C. Adams and S. Lloyd, Understanding PKI: Concepts, Standards, and Deployment Considerations, Addison-Wesley Professional.
2. T. Austin, PKI - Public Key Infrastructure, John Wiley & Sons.
3. A. Karamanian, S. Tenneti and F. Dessart, "PKI Uncovered", Cisco Press

Reference

Joel Weise, "Public Key Infrastructure Overview", Sun Blue Prints, 2001.

CSE 2133	Information Theory	4-0-0	4

Module 1

Overview of Entropy: Entropy of discrete random variables- Joint, conditional and relative entropy- Chain rule for entropy, Mutual information and conditional mutual information, Relative entropy and mutual Information;

Overview of Lossless source coding: Discrete Memory-less sources, Uniquely decodable codes- Instantaneous codes- Kraft's inequality – Average codeword length, Optimal codes- Huffman coding, Arithmetic Coding, Lemplel-Ziv Coding, Shannon's Source Coding Theorem.

Lossy source coding: preliminaries, Markov sources, Rate distortion theory, data compression schemes.

Module 2

Review of Channel Capacity and Coding Theorem: Channel Capacity- Discrete memory-less channels (DMC) and channel transition probabilities, Capacity computation for simple channels- Shannon's Channel Coding Theorem for DMC, Converse of Channel Coding Theorem

Review of Continuous Sources and Channels: Differential Entropy: Mutual information- Waveform channels- Gaussian channels- Shannon-Harley Theorem, Shannon limit, efficiency of digital modulation schemes-power limited and bandwidth limited systems.

Discrete channels with memory, finite memory semi-continuous channel.

Module 3

Network source coding, Joint network source coding, Linear network codes, feedback in network codes, multiple access networks (lossless and near lossless source coding), broadcast channels, feedback.

Module 4

A review of convolutional codes, introduction to quantum information theory.

Book

Thomas M. Cover and Joy A. Thomas, "Elements of Information Theory", John Wiley & Sons, 2006

References

1. Shu Lin and Daniel. J. Costello Jr., "Error Control Coding: Fundamentals and applications", 2nd Ed., Prentice Hall Inc, 2004.
2. Robert Gallager, "Information Theory and Reliable Communication", John Wiley & Sons, 1968.
3. R. E. Blahut, "Theory and Practice of Error Control Codes", Addison-Wesley, 1983.

CSE2134	Security Engineering: Dependable Distributed System	4-0-0	4

Module 1

Problem, Process and Product, Problems of software practitioners, approach through software reliability engineering, experience with SRE, SRE process, defining the product, Testing acquired software, reliability concepts- software and hardware reliability. Implementing Operational Profiles, Developing, identifying, crating, reviewing the operation, concurrence rate, occurrence probabilities, applying

operation profiles.

Module 2
Engineering "Just Right" Reliability, Defining "failure" for the product, Choosing a common measure for all associated systems. - Setting system failure intensity objectives, Determining user needs for reliability and availability, overall reliability and availability objectives, common failure intensity objective., developed software failure intensity objectives. Engineering software reliability strategies. Preparing for Test, Preparing test cases. Planning number of new test cases for current release. Allocating new test cases. Distributing new test cases among new operations. Detailing test cases. Preparing test procedures

Module 3
Executing Test: Planning and allocating test time for the current release, Invoking test identifying failures, Analysing test output for deviations, Determining which deviations are failures. Establishing when failures occurred. Guiding Test, Tracking reliability growth, Estimating failure intensity, Using failure intensity patterns to guide test, Certifying reliability. Deploying SRE, Core material, Persuading your boss, your co-workers, and stakeholders, Executing the deployment, Using a consultant.

Module 4
Using UML for Security: UM L diagrams for security requirement, security business process, physical security, security critical interaction, security state. Analyzing Model. Notation, Formal semantics, security analysis, important security opportunities. Model based security engineering with UML - UML sec profile- Design principles for secure systems, Applying security patterns.

Module 5
Applications - Secure channel - Developing Secure Java program- More case studies. Tool support for UML Sec - Extending UML CASE TOOLS with analysistools - Automated tools for UML SEC. Formal Foundations - UML machines, Rely guarantee specifications- Reasoning about security properties.

Text Books

1. John Musa D, "Software Reliability Engineering", 2nd Edition, Tata McGraw-Hill, 2005 (Units I, II and III)
2. Jan Jürjens, "Secure Systems Development with UML", Springer; 2004 (Unit IV and V)

CSE2135	Information Retrieval Techniques and Evaluation	4-0-0	4

Module 1
Introduction: Basic IR system structure; Retrieval techniques: Boolean retrieval, term-vocabulary, postings-lists, Dictionaries, Entropy of information calculations;

Module 2
Inverted indices: Preprocessing steps, tokenization, stemming, stopword removal, term weighting; Index Compression: Data Compression Techniques, Huffman Coding, Arithmetic Coding, compressing posting lists;

Module 3
Models: vector space model, probabilistic model, language models; Evaluation: standard test collection, concept of relevance, precision-recall based metrics, reciprocal rank, DCG; Relevance feedback and query expansion: Rocchio algorithm;
Text classification : Naïve Bayes; Text clustering: Flat Clustering, Hierarchical Clustering; XML Retrieval: Basic concepts, Challenges, Evaluation;

Module 4

Web search: Structure of Web, web graph, Hidden Web, User intent, Web crawl. Link Analysis: Web as a graph, PageRank, Hubs and Authorities; Sentiment analysis of social networking, Question Answering, Collaborative Searching.

Text Book

Christopher D. Manning, Prabhakar Raghavan and Hinrich Schütze, Introduction to Information Retrieval, Cambridge University Press. 2008.

CSE2136	Software Engineering and Project Management	4-0-0	4

Module 1

Development Life Cycle Processes: Overview of software development life cycle – introduction to processes – Personal Software Process (PSP) – Team software process (TSP) – Unified processes – agile processes – choosing the right process Tutorial: Software development using TSP

Module 2

Introduction to object-oriented analysis and design, Object Oriented Analysis - Object Modeling using UML and OOD heuristics, OOD heuristics and OOA using Coad's methodology, Coad's methodology, OOA and OOD - an example.

Module 3

Software Requirements and requirement analysis-functional and nonfunctional requirement, Software Project Management Concepts, The Software Team, The Project Management, Software Size Estimation, Co-Como model, Function Point Counting Process, Software Process and Project Metrics, Software Quality Factors, Metrics for specification quality, Interpreting Measurements, CASE tool.

Module 4

Software Project Planning, Risk analysis and management, Types of Risks, Assessing Risk Impact, Software Project Scheduling and Monitoring, Relationship between people and effort, Project Tracking, Error Tracking, debugger, Software Quality Assurance, Software Configuration Management (SCM), Measuring Change Activity, Business Process Reengineering-business invariants, Software Refactoring, Capability Maturity Model (CMM) and Key Process Area (KPA), process assessment and improvement – CMMI – Six Sigma.

Books and References

1. PankajJalote, “Software Project Management in Practice”, Pearson
2. Chris F. Kemerer, “Software Project Management – Readings and Cases”, McGraw Hill.
3. Watts S. Humphrey, “PSP: A self-improvement process for software engineers”, Addison- Wesley, 2005.
4. Watts S. Humphrey, “Introduction to the Team Software Process”, Addison-Wesley.
5. Orit Hazzan and Yael Dubinsky, “Agile software engineering”, Springer.
6. James R. Persse, “Process Improvement Essentials”, O’Reilly.
7. Roger S. Pressman, “Software Engineering – A Practitioner’s Approach”, Seventh Edition, McGraw Hill.

CSE2211	Advance Data Structure and Algorithms	3-0-0	3

Module 1

Link lists: Single, doubly and Circular linked list, Stack and Queue.

Module 2

Binary search tree (BST): Insertion and deletion of nodes in BSTs, Querying a BST (finding max, min or a given node).AVL Tree (all Rotations), Multi-way Search Trees: B Tree, B+ Trees, Red-Black Trees, Binomial Heaps, Graph Representation, Graph Traversals, DFS, BFS, Shortest path algorithms- Shortest path un weighted graph, Shortest path weighted graph, Dijkstra's algorithms, Minimal spanning tree, Prim's algorithm, Kruskal's algorithm Traveling salesman problems, Floyd warshall algorithms.

Module 3

Divide and Conquer Algorithms, Master Theorem, Dynamic Programming, Hashing, String Algorithms – String Matching Algorithms – Brute Force Method-Robin Karp String Matching Algorithms – String Matching with Finite automata- KMP algorithms – Boyce Moore Algorithms, Approximation Algorithms: Travelling Sales Person Problem, Vertex Cover Problem, Set Cover Problem.

Module 4

Line segments and determine whether any pair of segments intersects. Plane Sweep Techniques with its applications, Convex Hull problem (Extreme point algorithm, incremental algorithm, divide & conquer approach). Randomized algorithms: Use of probabilistic inequalities in analysis, applications using examples. Graph algorithms: Matching and Flows. Parallel algorithms: Basic techniques for sorting, seraching, merging.. Complexity classes - NP-Hard and NP-complete Problems - Cook's theorem NP completeness reductions.

References

1. T. H. Cormen, C. E. Leiserson, R. L. Rivest, Introduction to Algorithms, Prentice hall.
2. Jon Kelinberg and Eva Tardos, Algorithm Design, Pearson
3. Data Structures Using C Second Edition Reema Thareja
4. Franco P. Preparata and Michael Ian Shamos, Computational Geometry An Introduction, Springer-Verlag

CSE2212	Wireless and Mobile Network Security	4-0-0	4

Module 1

Threats and Security Goals, Network Security Analysis, Information Security Measures, Important Terms relating to Communication Security; Challenges of Broadcast Communication, Security Requirements for Broadcast Applications; Broadcast Network Requirements, IPv-4 vs IPv6,

Module 2

Cryptographic Primitives, Efficiency in Cryptographic Primitives, Commitment Protocols, Lock and Key analogy, Ciphers, Kerckhoff's Principles, Classical cryptanalysis, Digital cryptography, Pseudo-Random number generator;

Module 3

The wireless Local Area Network (WLAN): Wireless Transmission Media, WLAN Products and Standards, 802.11 security, IEEE 802.11b/n/g.., Securing WLANs, Countermeasures;
Wireless Application Protocol (WAP): Comparison of the TCP/IP with mobile TCP/IP, OSI and WAP Models, WAP Security Architecture, Marginal Security;
Secure Wireless and Mobile Communications: Security aspects of mobile communications: Security in WLANs, Mobile WANs, Mobile Internet Communications, Wireless Transport Layer Security;

Module 4

Bluetooth Technology: Basic specifications, Design specifications, Security architecture, Authentication and encryptions;

Voice over Internet Protocol (VoIP): The Buzz around VoIP, VoIP standards, The rise of VoIP Technology, Technical Issues and Voice network security.

Module 5

Hardware Perspectives for End-to-End Security (E2E) in Wireless Applications: Communication - Client-Server versus Peer-to-Peer, Circuit-Switched versus Packet-Switched or Frame-Switched, Unicast versus Broadcast/anycast, LAN-Based versus Wireless-Based Communications,
Transmission Medium, Transmission Nature, Advanced Mobile Phone Services, Internet Telephony, Time Division Multiple Access, GSM, Wideband and narrowband CDMA

Books and References

1. S.K. Makki, P. Reiher, K. Makki, N. Pissinou and S. Makki, Mobile and wireless network security and privacy, Springer.
2. R. Nichols and P. Lekkas, Wireless Security: Models, Threats and Solutions, McGrawhill, 2010.

CSE2213	Machine Learning and Robotics	3-0-0	3

Module 1

Overview and preliminaries, generation of data set, manipulation on data set, storage and representation of data, Dynamic system modelling – Rotational, Translational systems; Interchange of system modelling – Differential, State Space, Transfer Function; Time response of dynamic systems – LTI, Nonlinear Systems

Module 2

Introduction to Neural Networks, SLP, MLP, RBFN, Recurrent Network, SOM, Fuzzy Systems

Module 3

Sensors and Actuators, Mobile Robots, Position, and Orientation, Equations of Motion, Transformations, Path Planning, and Trajectories, Introduction to Robotic Arm/ Manipulator, Forward Kinematics, Inverse Kinematics, Redundancy and redundancy resolution

Module 4

Case study of applications of Neural Network on Mobile Robot, Case study of applications of Neural Network on Robot Manipulator, Case study of applications of Fuzzy Logic on Mobile Robot, Case study of applications of Fuzzy Logic on Robot Manipulator.

Books and References

1. Robot Analysis and Control, H. Asada, J. J. Slotine, Wiley
2. Robot Modeling and Control, Spong, Hutchinson, and Vidyasagar, Wiley
3. A Mathematical Introduction to Robotic Manipulation, Murray,Li,andSastry, CRC
4. IntroductiontoRobotics:MechanicsandControl, Craig, Addison-Wesley
5. Robotics Technology and Flexible Automation, S. R. Deb, S. Deb, McGraw Hill
6. Research Papers from IEEE, Elsevier, Springer.

CSE2221	Advance Data Structure and Algorithms Laboratory	0-0-2	1

1. Programming on Linked-list, doubly-linked lists
2. Programming on BST (all operations)
3. Programming on AVL trees (all rotations)
4. Programming on Red-Black trees (all rotations)
5. Programming on Approximation Algorithms
6. Programming on Computational Geometry

CSE2222	Machine Learning and Robotics Laboratory	0-0-2	1

1. Familiarization of programming environment (C++, MATLAB, Player-stage, ROS)
2. Data manipulation and storage
3. Solution for dynamic system response – LTI, nonlinear systems
4. Implementation of Neural Network architectures
5. Implementation of a Fuzzy System
6. Case study of applications of Neural Network on Mobile Robot
7. Case study of applications of Neural Network on Robot Manipulator
8. Case study of applications of Fuzzy Logic on Mobile Robot
9. Case study of applications of Fuzzy Logic on Robot Manipulator

Texts/References

1. Robot Analysis and Control, H. Asada, J. J. Slotine, Wiley
2. Robot Modeling and Control, Spong, Hutchinson, and Vidyasagar, Wiley
3. A Mathematical Introduction to Robotic Manipulation, Murray, Li,and Sastry, CRC
4. Introduction to Robotics: Mechanics and Control, Craig, Addison-Wesley
5. Robotics Technology and Flexible Automation, S. R. Deb, S. Deb, McGraw Hill
6. Research Papers from IEEE, Elsevier, Springer.

CSE2231	Computer Forensics and Crime Investigation	4-0-0	4

Module 1

Computer forensics fundamentals, Benefits of forensics, Computer crimes, Computer forensics evidence and courts, Legal concerns and private issues.

Module 2

Understanding Computing Investigations – Procedure for corporate High-Tech investigations, Understanding data recovery work station and software, Conducting and investigations.

Module 3

Data acquisition- understanding storage formats and digital evidence, determining the best acquisition method, acquisition tools, validating data acquisitions, performing RAID data acquisitions, remote network acquisition tools, other forensics acquisitions tools.

Module 4

Processing crimes and incident scenes, securing a computer incident or crime, seizing digital evidence at scene, storing digital evidence, obtaining digital hash, reviewing case.

Module 5

Current computer forensics tools- software, hardware tools, validating and testing forensic software, addressing data-hiding techniques, performing remote acquisitions, E-Mail investigations- investigating email crime and violations, understanding E-Mail servers, specialized E-Mail forensics tool.

Books

1. Warren G. Kruse IIandJay G. Heiser, “Computer Forensics: Incident Response Essentials”, Addison Wesley, 2002.
2. Nelson, B, Phillips, A, Enfinger, F, Stuart, C., “Guide to Computer Forensics and Investigations, 2nd ed., Thomson Course Technology, 2006, ISBN: 0-619-21706-5.

Reference Books

Vacca, J, Computer Forensics, Computer Crime Scene Investigation, 2nd Ed, Charles River Media,

2005, ISBN: 1-58450-3

CSE2233	High Performance and Grid Computing	4-0-0	4

Module 1

Introduction to Computer Systems: Processors, Memory, I/O Devices; Cost, timing, and scale (size) models. Program Execution: Process, Virtual Memory, System Calls, Dynamic Memory Allocation.

Module 2

Machine-Level View of a Program, typical RISC instruction set and execution, Pipelining. Performance issues and Techniques, Cost and Frequency Models for I/O, paging, and caching. Temporal and spatial locality. Typical Compiler Optimizations.

Module 3

Parallel Computing: Introduction to parallel Architectures and Interconnection Networks, communication latencies. Program parallelization: task partitioning and mapping, data distribution, Message passing, synchronization and deadlocks. Distributed memory programming using MPI/PVM. Shared memory parallel programming. Multithreading.

Module 4

Introduction - Definition and Scope of grid computing Grid Computing Organizations and their roles – Grid Computing analog –
Grid Computing road map.

Books and References

1. Dowd, K., High performance Computing, O'Reilly Series, 1993.
2. Culler, D., and Singh, J.P., Parallel Computer Architecture: A Hardware/Software Approach. Morgan Kaufmann Pub., 1999.
3. Gropp, W., Lusk, E., and Skjellum, A., Using MPI: Portable Parallel Programming with the Message-passing Interface, MIT Press, 1997.
4. Joshy Joseph & Craig Fellenstein, "Grid Computing", PHI, PTR-2003.
5. Ahmar Abbas, "Grid Computing: A Practical Guide to technology and Applications", Charles River media – 2003.

CSE2234	Real Time Wireless and Mobile Operating System	4-0-0	4

Module 1

Introduction: Real-time systems – Applications – Basic Model – Characteristics – Safety and Reliability – Real- Time tasks – Timing Constraints – Modelling Timing Constraints.

Module 2

Types of RT Tasks and their Characteristics – Task Scheduling – Clock-Driven Scheduling – Hybrid Schedulers - Event-Driven Scheduling – EDF Scheduling – RMA – Issues with RMA – Issues in Using RMA in Practical Situations

Module 3: Resource Sharing Among Rt Tasks & Scheduling Rt Tasks

Resource Sharing Among RT Tasks – Priority Inversion – PIP – HLP – PCP – Types of Priority Inversions Under PCP – Features of PCP – Issues in using Resource Sharing Protocol – Handling Task Dependencies – Multiprocessor Task Allocation – Dynamic Allocation of Tasks – Fault- Tolerant Scheduling of Tasks – Clocks in Distributed RT Systems – Centralized and Distributed Clock Synchronization.

Module 4: Commercial Rt Operating Systems

Time Services – Features of RT OS – Unix as a RT OS – Unix Based RT OS – Windows as a RT OS – POSIX – Survey of RTOS: PSOS – VRTX – VxWorks – QNX - µC/OS-II – RT Linux – Lynx – Windows CE – Benching RT Systems. Real time communication

Text Books

1. Rajib Mall, "Real-Time Systems: Theory and Practice," Pearson, 2008.
2. Krishna and Shin, "Real-Time Systems," Tata McGraw Hill. 1999.

CSE2236	Application Oriented Soft Computing	4-0-0	4

Module 1

Soft Computing: soft computing concepts and techniques in designing and implementing soft computing based solutions for real-world and engineering problems. Requirement, different tools and techniques, usefulness and applications.

Module 2

Fuzzy sets and Fuzzy logic: Introduction, Fuzzy sets versus crisp sets, operations on fuzzy sets, Extension principle, Fuzzy relations and relation equations, Fuzzy numbers, Linguistic variables, Fuzzy logic, Linguistic hedges, Applications, fuzzy controllers, fuzzy pattern recognition, fuzzy image processing, fuzzy database.

Module 3

Type-2 Fuzzy Sets: Notion of uncertainty of membership in a fuzzy set, foot print of uncertainty, Measurement of uncertainty, embedded fuzzy sets, operations on type-2 fuzzy sets, type-2 fuzzy relations, type reduction, type-2 fuzzy inference systems.

Fuzzy Clustering: Limitations of hard partitioning and need for fuzzy clustering, FCM, PCM,Neuro Fuzzy Systems: Neuro fuzzy systems of Mamdani, logical, and Takagi-Sugeno type, flexible neuro fuzzy systems.

Module 4

Artificial Neural Network: Introduction, basic models, Hebb's learning, Adaline, Perceptron, Multilayer feed forward network, Back propagation, Different issues regarding convergence of Multilayer Perceptron, Competitive learning, Self-Organizing Feature Maps, Adaptive Resonance Theory, Associative Memories, Applications.

Hybrid Systems: Neural-Network-Based Fuzzy Systems, Fuzzy Logic-Based Neural Networks, Genetic Algorithm for Neural Network Design and Learning, Fuzzy Logic and Genetic Algorithm for Optimization, Applications.

Books and References

1. Rutkowski, Computational Intelligence, Methods and Techniques, Springer
2. Neural Fuzzy Systems, Chin-Teng Lin & C. S. George Lee, Prentice Hall PTR.
3. Fuzzy Sets and Fuzzy Logic, Klir& Yuan, PHI.
4. Neural Networks, Fuzzy logic, and Genetic Algorithms, S. Rajasekaran& G. A. V. Pai, PHI.
5. Neuro-Fuzzy and Soft Computing, Jang, Sun, &Mizutani, PHI.
6. Valente de Oliveira, W. Pedrycz, Advances in Fuzzy Clustering and its Applications, John Wiley & Sons.
7. Hopner, F. Hoppner, F. Klawonn, Fuzzy Cluster Analysis: Methods for Classification, Data Analysis and Image Recognition, John Wiley & Sons.

***