

Department of Computer Engineering  
Malaviya National Institute of Technology  
**MTech Full Time (Computer Engineering)**  
(2012-13 onwards)

**I Semester (Autumn Semester)**

S.No	Course Code	Course Title	Subject AREA	Credit	L	T	P	Exam Duration	Relative Weightage*				
									CWS	PRS	MTE	ETE	PRE
1	CP-501	Topics in Algorithms	PC	3	3	0	0	2	20	-	30	50	-
2	CP-513	Topics in Databases	PC	3	3	0	0	2	20	-	30	50	-
3	CP-523	Topics in Computing	PC	3	3	0	0	2	20	-	30	50	-
4	CP-505	System Design Lab	PC	3	1	0	3		-	60	-	-	40
5	CP-509	Programming Lab – I	PC	3	1	0	3		-	60	-	-	40
6	CP-506	Security in Computing	PC	3	3	0	0	2	20	-	30	50	-
<b>Total</b>				<b>18</b>									

\* Typical distribution. Can be changed by Course Instructor/Coordinator by announcing at beginning of semester.

**II Semester (Spring Semester)**

S.No	Course Code	Course Title**	Subject AREA	Credit	L	T	P	Exam Duration	Relative Weightage*				
									CWS	PRS	MTE	ETE	PRE
1		Elective-I	PE	3	3	0	0	2	20	-	30	50	-
2		Elective-II	PE	3	3	0	0	2	20	-	30	50	-
3		Elective-III	PE	3	3	0	0	2	20	-	30	50	-
4		Elective-IV	PE	3	3	0	0	2	20	-	30	50	-
5		Elective-V	PE	3	3	0	0	2	20	-	30	50	-
6		Lab Elective-I	PE	3	1	0	3		-	60	-	-	40
<b>Total</b>				<b>18</b>									

\* Typical distribution. Can be changed by Course Instructor/Coordinator by announcing at beginning of semester.

\*\* Two Electives need to be taken from Department Elective List.

**TOTAL CREDITS (Sem I-II)**

**36**

Department of Computer Engineering  
 Malaviya National Institute of Technology  
**MTech Full Time (Computer Engineering)**  
 (2012-13 onwards)

**III Semester (Autumn Semester)**

S.No	Course Code	Course Title	Subject AREA	Credit	L	T	P	Exam Duration	Relative Weightage*				
									CWS	PRS	MTE	ETE	PRE
1	CP-600	Seminar	PC	4	-	-	-	-	-	-	-	100	-
2	CP-601	Dissertation	PC	16	-	-	-	-	-	-	-	-	-
<b>Total</b>				<b>20</b>									

**IV Semester (Spring Semester)**

S.No	Course Code	Course Title	Subject AREA	Credit	L	T	P	Exam Duration	Relative Weightage*				
									CWS	PRS	MTE	ETE	PRE
1	CP-602	Dissertation	PC	16	-	-	-	-	-	-	-	-	-
<b>Total</b>				<b>16</b>									

<b>TOTAL CREDITS (Sem III-IV)</b>	<b>36</b>
-----------------------------------	-----------

<b>TOTAL CREDITS (Sem I-IV)</b>	<b>72</b>
---------------------------------	-----------

RAM model – Notations, Recurrence analysis - Master's theorem and its proof - Amortized analysis - Advanced Data Structures: B-Trees, Binomial Heaps, Fibonacci Heaps, AVL trees, Red-black trees, B-trees, Splay trees.

Disjoint set – union and path compression, Amortized analysis

Recurrence equations. Time and space complexity, NP, NPC and NP-Hard problems, undecidability.

Convex hull and Voronoi diagrams, line segments, Optimal polygon triangulation.

Primality testing, Integer factorization, Randomized algorithms, Probabilistic algorithms.

Dynamic programming: Longest common subsequence. Chain of matrix multiplication,

Approximate Algorithms: Vertex-cover, set-covering problems, Travelling Salesman problem.

Combinatorial algorithms,

Randomized algorithms: Use of probabilistic inequalities in analysis, applications using examples. Graph algorithms: Matching and Flows.

Parallel algorithms: Basic techniques for sorting, searching, merging..

Complexity classes - NP-Hard and NP-complete Problems - Cook's theorem NP completeness reductions.

**Texts/References:**

- 1) Cormen, Leiserson, Rivest: Introduction to Algorithms, Prentice Hall of India.
- 2) Horowitz and Sahani: *Fundamental of Computer algorithms*.
- 3) Aho A.V , J.D Ulman: *Design and analysis of Algorithms*, Addison Wesley
- 4) Brassard : *Fundamental of Algorithmics*, PHI.
- 5) Sara Baase: *Computer Algorithms: Introduction to Design and Analysis*, Pearson Education.
- 6) Papadimitriou, Steiglitz: *Combinatorial Optimization: Algorithms and Complexity*, PHI.
- 7) Motwani and Raghavan: *Randomized Algorithms*, Cambridge University Press
- 8) Joseph Ja'Ja': *Introduction to Parallel Algorithms*, Addison-Wesley
- 9) Vaizirani: *Approximation Algorithms*, Springer Verlag
- 10) N. Deo: *Graph Theory with Application to Engineering and Computer Science*, Prentice-Hall.
- 11) N. Deo: *Combinatorial Algorithms: Theory and Practice*, Prentice-Hall.

**CPT602    Parallel and Distributed Computing****3-0-0**

Introduction to parallel computing. Parallel processing terminology, Pipelining Vs Data parallelism, Control parallelism, Scalability, Control parallel approach, Data parallel approach, Data parallel approach with I/O

Parallel reduction, Prefix sums, List ranking, Preorder tree traversal, Merging two sorted lists, Graph coloring, Reducing the number of processors, Problems defying fast solutions on PRAMS

Thread and process level parallel architectures: MIMD, multi-threaded architectures. Distributed and shared memory MIMD architectures.

Dynamic interconnection networks.

Mapping and scheduling: Mapping data to processors on processor arrays and multicomputers, Dynamic Load Balancing on multicomputers, Static scheduling on UMA multiprocessors, Deadlock.

Parallel programming and parallel algorithms: Programming models, parallel programming on multiprocessors and multicomputers. Parallel algorithm structure, analyzing parallel algorithm.

Elementary parallel algorithms, Matrix algorithms, sorting, Graph algorithms.

**Text & References:**

- 1) Quinn, *Parallel computing – theory and practice*, Tata McGraw Hill.
- 2) Sima and Fountain, *Advanced Computer Architectures*, Pearson Education.
- 3) Mehdi R. Zargham, *Computer Architectures single and parallel systems*, PHI.
- 4) Ghosh, Moona and Gupta, *Foundations of parallel processing*, Narosa publishing.
- 5) Ed. Afonso Ferreira and Jose' D. P. Rolin, *Parallel Algorithms for irregular problems - State of the art*, Kluwer Academic Publishers.

- 6) Selim G. Akl, *The Design and Analysis of Parallel Algorithms*, PH International.

**CPT603 Selected Topics in Operating System**

**3-0-0**

Introduction: Goals, Functions, Design issues of Distributed OS, Distributed v/s network operating system.

Communication: Client Server, RPC

Distributed OS: Issues, process management, inter-process communication, scheduling, deadlocks

Design and implementation of distributed file systems, distributed shared memory

Security: Concepts and Distributed Systems

Distributed Concurrency, Transactions.

Case study: Unix, Amoeba.

**Text/References:**

- 1) Tanenbaum: *Distributed Operating Systems*, Pearson Education.
- 2) Bach, *Design of Unix O/S*.
- 3) Coulouris et al, *Distributed Systems: Concepts and Design*, Addison Wesley.
- 4) Mullender: *Distributed Systems*, Addison Wesley.
- 5) Tanenbaum and Steen: *Distributed Systems: Principles and Paradigms*, Pearson Education

## CPT627 Information System Security

3-0-0

**Number theory:** Prime numbers, modular arithmetic, Fermat's theorem, Euler's theorem, Chinese remainder theorem, Discrete logarithms, Random number generation, factoring, prime number generation, one-way hash functions – MD5, SHA (Secure Hash Algorithm).

**Cryptography:** Need, conventional techniques, stream ciphers, block cipher, steganography. Public v/s private key cryptography.

**Stream Ciphers:** Caesar Cipher, mono-alphabetic and poly-alphabetic ciphers, Playfair Cipher, Hill Cipher, Rotor machines, One time pad,.

**Steganography:** Visual, Textual, Cipher hiding, False errors.

**Private-key cryptography:** Feistel structure, DES (Data encryption standard), design of S-boxes, AES, Triple DES,

**Public key cryptography:** Key management, Key exchange – Diffie-Hellman, Authentication, Signatures, Deniability, RSA.

**Digital Signature:** DSA and its variants, discrete logarithm based digital signatures.

**Cryptanalysis:** Differential and linear cryptanalysis - cracking DES.

Rabin, ElGamal, Goldwasser-Micali, Blum-Goldwasser cryptosystems.

**Digests:** Message authentication, digital signature algorithms. Security handshake pitfalls, Strong password protocols.

### Text & References:

1. Stallings, *Cryptography and Network Security*, Pearson Education.
2. B Schneier, *Applied Cryptography*, Wiley. ISBN 0-471-11709-9
3. D Kahn. *The Codebreakers*, Sphere books. ISBN 0-7221-51497
4. A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, *Applied Cryptography*, CRC Press.
5. D.R. Stinson, *Cryptography - Theory and practice*, CRC Press.

## CPT611 Advanced Topics in Computer Graphics

3-0-0

**Visibility:** Polygon Meshes, Depth Sorting. Triangle decomposition, Geometric Sort, Warnock's Methods

**Hidden Lines and Surfaces:** Special cases, Surfaces defined by a function  $y=f(x,y)$ , Grid surfaces, visible surface determination .

**Colour in Computer Graphics:** Color Vision, Measuring Color, Color Models, Color output, color usage.

**Object Lighting and Shading:** Illumination and shading models, Local reflection models, shading surfaces, Texture and transparency, Forward & backward Ray-tracing  
Global Illumination and classical radiosity.

**Modeling natural phenomena:** Fractals and chaos.

**Animation Techniques:** Position, speed or orientation. Animation by hierarchic control, scenario-based systems, movement control.

Shadows, Morphing, Texture mapping

### Text/ References:

- 1) J. Foley et al : *Computer Graphics-Principles and Practice*, Addison Wesley.
- 2) Alan Watt- *3D Computer Graphics*.
- 3) A. Watt, M. Watt: *Advanced Animation & Rendering Techniques*, Addison-Wesley.
- 4) D. Rogers and Adams: *Mathematical Elements of Computer Graphics*, Mc Graw Hill.
- 5) Thomas Moller: *Real-time Rendering*, Eric Haines, A.K Peters Ltd

**CPT613 Topics in Databases****3-0-0**

Issues in Implementation of Database Systems, Query Processing, Query Optimization, Transaction Processing, Concurrency, Recovery Management. Database System Architectures, Distributed Databases, Distributed Transactions, Distributed Query Processing, Parallel Databases, Times in Databases, Multimedia Databases.

**Text/References**

- 1) Silberschatz A, Korth HF, Sudarshan S, Database System Concepts, McGraw Hill.
- 2) Elmasri R and Navathe SB, *Fundamentals of Database Systems*, 3rd Edition, Addison Wesley, 2000. This book covers most of the material on the course.
- 3) Ceri S, Pelagatti G, Distributed Databases – Principles and Systems, McGraw Hill.
- 4) Date CJ, *An Introduction to Database Systems*, 7th Edition, Addison Wesley.
- 5) Khashafian S and Baker AB, *Multimedia and Imaging Databases*, Morgan Kaufmann.

**CPT615 Network Performance Modeling****3-0-0**

Networking as resource sharing: current practices, Traffic Multiplexing, Traffic analysis, Stochastic Traffic Models, Multiple Access: Wireless Networks. Routing: Virtual path routing and Elastic Aggregates, Routing of Stream Type sessions, Routing in Ad-hoc and Sensor Networks. Introduction to High Performance Switching and Routing. QoS and Modeling issues of the Networks.

**Text & References:**

- 1) Communication Networking: An Analytical Approach, Anurag Kumar, D.Manjunath, Joy Kuri, Elsevier
- 2) High Performance Communication Networks, Jean Walrand, P.Vaiya, Elsevier
- 3) Selected papers and online references.

**CPT617 Software Testing and Validation****3-0-0**

Basic software testing principles – Software Quality, Software testing and test management. Acceptance Testing: User acceptance testing, alpha and beta testing. Functional and Non-functional system testing. Static and dynamic testing, Black-box or functional testing, structural, white box or glass box testing. Integration testing, component testing. Software testing tools. Software Validation: Issues and Challenges.

**Books/References:**

- 1) Selected papers and online references.

**CPT619 Topics in SOC Design****3-0-0**

Methodologies and design flows of front end and back end designs. Introduction to intellectual property core types and their design issues. Integration issues of IPs on SOC designs. Low power design issues and methodologies. Testing standards and architecture of SOCs.

**Text/Reference:**

- 1) Farzad Nekoogar , F.Nekooqar, From ASICs to SOCs: A Practical Approach, Pearson.
- 2) Steve B. Furber, ARM System-on-Chip Architecture (2nd Edition), AWL
- 3) Recent papers from conferences and journals.

**CPT621 Advances in Compiler Design****3-0-0**

A Tour of Compiler Design, LR Parsers, Lex and Yacc Tools, Control-flow Analysis, Control-flow Graphs, Basic Blocks, Data-flow Analysis, Dependence Analysis, Global Optimizations, Loop Optimizations, Peephole Optimization and Optimal Code Generation, Data Dependence Analysis in Loops, Loop Scheduling, Static Single Assignment, Just-In-Time (JIT) and Adaptive Compilation, Runtime System Architectures and Automatic Memory Management Techniques.

**Text/Reference:**

- 1) Aho, Alfred V., Sethi, Ravi, Ullman, Jeffrey D., *Compilers: Principles, Techniques and Tools*, Addison-Wesley.
- 2) Steven Muchnick, *Advanced Compiler Design & Implementation*, Morgan Kaufmann.
- 3) Keith Cooper and Linda Torczon, *Engineering a Compiler*, Morgan Kaufmann.

**CPT623 Topics in Computing****3-0-0**

Advanced Architectures relevant to Modern OS. Multi core architectures (Power performance issues, virtualisation etc.). GPU Architecture. Architecture for cloud computing. Advanced concepts for multi media OS and scheduling. Disk management. MLFQ scheduling, Linux kernel features, hardware abstraction layer, Completely fair scheduling. Virtualisation and Cloud computing. Mobile OS. DVM and ART. Comparative study of mobile and desktop OS. Advanced topics on Networking: flow control in Networks. Software Defined Networks. QoS issues at transport and application layer of networks.

Special and emerging topics in different areas of CSE.

**Text and References:**

1. Recent papers from Journals
2. Computer Networks: Peterson and Davie
3. Linux kernel Internals

**CPT625 Wireless Sensor Networks****3-0-0**

Wireless Sensor Networks: Introduction, Overview and Applications.  
Sensor node – Design issues, power consumption, operating environment, sensor examples.  
Architecture - Single node, Network, Single hop v/s multi-hop, Performance metrics, QoS  
Wireless communication – Fundamentals, spread spectrum techniques, CDMA  
Protocols – Physical layer, MAC, link layer, Routing, middleware.  
Network management, Topology, operating system.  
Security in sensor networks.  
Open issues and Challenges.

**Texts/References:**

- 1) Holger Karl, Andreas Willig. *Protocols and Architectures for Wireless Sensor Networks*, Wiley Interscience.
- 2) Kazem Sohraby, Daniel Minoli, and Taieb Znati: *Wireless Sensor Networks: Technology, Protocols, and Applications*, Wiley Interscience.
- 3) Selected papers and online reference material.

**CPT641 Digital Image Analysis****3-0-0**

Digital Image Fundamentals, Point operations.  
Smoothing, Sharpening, Crispening, Image Enhancement in Spatial Domain, Image Enhancement in Frequency Domain  
Image Transforms: Hotelling, Hit and Miss transform.  
Color Image Processing, Multiview Image Processing, Epipolar geometry  
Image Warping and Restoration.  
Image Segmentation, Representation and Description  
Morphological Operators, Erosion, Dilation, Medial Axis, Thining, Skeleton.  
Image Matching and Classification

**Texts/References:**

- 1) Rafael C Gonzalez, Richard E Woods, *Digital Image Processing*, Addison-Wesley.
- 2) Milan Sonka, Vaclav Hlavac, Roger Boyale, *Image Processing, Analysis and Machine Vision*: PWS Publishing (ITP-International Thomson Publishing).
- 3) Anil K Jain: *Fundamentals of Digital Image Processing*, Printice Hall of India (PHI).

**CPT643 Data Mining and Data Warehousing****3-0-0**

Introduction to Decision Support Systems, Data Warehouse and Online Analytical Processing. Data Warehouse Architecture: System Processes, Process Architecture: Load Warehouse, Query, Detailed and Summarized Information.  
Design: Data Base Schema Facts, Dimensions and Attributes. Data Base and Metadata.  
Data Mining : Introduction and need, Descriptive and Predicative Data Mining.  
Data Processing : Data Cleaning, Data Integration and Transformation, Data Reduction.  
Data Mining Primitives:, Language DMQL and its Preliminary Clauses.  
Data Mining Methods: Association – Single and Multilevel, Characterization and Comparison, Regression Analysis, Classification and Predication.  
Data Mining Algorithms: Clustering, Association, Regression, Decision Trees.  
Application and Trends in Data Mining. Data Warehouse Implementation.



Text & References:

- 1) Data Warehousing in the Real World – Anahory and Murray, Pearson Education.
- 2) Data Mining – Concepts and Techniques – Jiawei Han and Micheline Kamber.
- 3) Building the Data Warehouse – WH Inmon, Wiley.

**CPT645 Topics in High Speed Networking****3-0-0**

Overview of Internet Technologies, Issues in next generation Internet - Routing, Multicasting, Packet Scheduling, Quality of Service etc. Admission control in Internet: Effective bandwidth, Differentiated services, Policy-based networking, Real time communications over Internet, Internet telephony, Voice over IP, Integrated services. Web QoS, Intelligent caching, Traffic measurement and characterization.

**Text/References:**

- 1) Kurose: *Computer Networking A Top Down Approach*, Pearson.
- 2) Peterson and Davie: *Computer Networks: A systems approach*, Morgan Kaufman and Elsevier.
- 3) J.Walrand, *High Performance Computer Networks*, Elsevier
- 4) A.Kumar, D.Manjunath, *Communication Network* MKP.
- 5) Recent papers from conferences and journals.

**CPT647 e-Commerce****3-0-0**

Introduction and concepts: networks and commercial transactions, the Internet environment, online commerce solutions. A generic business model for e-commerce.

Security technologies: Introduction to cryptography, key distribution and clarification.

Architecture for e-commerce: online commerce environment, servers and commercial environments, strategies, techniques and tools.

Electronic payment methods: Secure online transaction models, digital payment system, cyber cash, digital currencies, Smart cash, digital purse, anonymity and authentication.

Protocol for the public transport of private information: security protocols, secure socket layer.

Open issues: legal and technical issues.

**Text & References:**

- 1) Pete Loshin, Paul A Murphy: *Electronic e-commerce*, Jaico book.
- 2) Paul May: *The Business of e-commerce*, Cambridge University Press.
- 3) Recent papers from conferences and journals

**CPT649 High Level Synthesis of Digital Systems****3-0-0**

Overview. Design methodologies. Abstractions and views.

Review of basic concepts in algorithms and graph theory

Design representation and modeling, Modeling languages, Abstract models

Synthesis at higher levels of abstraction

Scheduling, Resource sharing

Structural synthesis: Module selection. Pipeline. Control

Synthesis at lower levels of abstraction, Logic synthesis

**Text/Reference:**

- 1) G. D. Micheli. *Synthesis and optimization of digital systems*.
- 2) N.D. Dutt, D. D. Gajski. *High level synthesis*, Kluwer, 2000.
- 3) T. H. Cormen, C. E. Leiserson and R. L. Rivest, "Introduction to Algorithms," McGraw-Hill, 1990.
- 4) Recent papers from journals and conferences.

## CPT651 Parallelizing Compiler

3-0-0

Motivation and overview, structure of a parallelizing compiler. Review of code optimization techniques in compilers for sequential machines. Parallelism detection - data dependence analysis, direction vectors, loop carried and loop independent dependences; tests for data dependence and their applicability, construction of data dependence graph. Control dependence and control dependence graph. Restructuring transformations and automatic extraction of parallelism; representation of iteration spaces of multiply nested loops; loop based transformations such as loop distribution, loop coalescing, loop inter-change and cycle shrinking transformation.

### Texts/References

- 1) Selected papers and online reference material

## CPT653 Quantum Cryptography

3-0-0

Finite Dimensional Hilbert Spaces – Tensor Products and Operators on Hilbert Space – Hermitian and Trace Operators - Basic Quantum Mechanics necessary for the course.  
Quantum Gates and operators and Measurement – Quantum Computational Model – Quantum Complexity – Schemes for Physical realization (Only peripheral treatment expected).  
Shor's Algorithm – Application to Integer Factorization – Grover's Algorithm –  
Quantum Cryptography: Encryption and decryption schemes.

### Texts/References

- 1) Nielsen M. A. and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2002.
- 2) J. Gruska, *Quantum Computing*, McGraw Hill, 1999.
- 3) P. R. Halmos, *Finite Dimensional Vector Spaces*, Van Nostrand, 1958.
- 4) Selected papers and online material.

## CPT655 Public Key Infrastructure and Trust Management

3-0-0

Public key infrastructure - components and architecture.  
PKI interoperability, deployment and assessment  
PKI data structures – certificates, validation, revocation, authentication, cross-certification.  
Repository, Certification Authority (CA) and Registration Authority (RA), trusted third party, digital certificates.  
PKI services – authentication, non-repudiation, privilege management, privacy, secure communication.  
Key management – certificate revocation list, root CA, attacks on CA, key backup.  
PKI standards – SSL, LDAP, IPSec, X.500, X.509, S/MIME  
Trust models – strict v/s loose hierarchy, four corner, distributed.  
Certificate path processing – path construction and path validation.

### Texts/References

- 1) Ashutosh Saxena, *Public Key Infrastructure*, Tata McGraw Hill
- 2) Carlisle Adams, Steve Lloyd. *Understanding PKI: Concepts, Standards, and Deployment Considerations*, Addison Wesley.
- 3) John R. Vacca. *Public Key Infrastructure: Building Trusted Applications and Web Services*, AUERBACH.
- 4) Messaoud Benantar, *Introduction to the Public Key Infrastructure for the Internet*, Pearson Education.

### **CPT606 Selected Topics in Cryptography**

**3-0-0**

Elliptic Curve Cryptography

Secret Sharing, Threshold cryptography – Robust ElGamal system

Visual Cryptography

Interactive zero knowledge proofs, witness hiding protocols.

Group encryption, decryption. Group signatures, ring signatures.

EVoting: requirements, issues and challenges, existing solutions, write-in ballots.

Pair based cryptography – Weil and Tate pairing.

#### **Text & References:**

- 1) Selected paper and online reference material.

### **CPT612 Robotics and Control**

**3-0-0**

**Robotics:** Introduction to robotics, advantages, applications.

**Robotic kinematics and dynamics:** Direct and inverse kinematics problem. Axis transformations; DH matrix; forward and reverse kinematics, trajectory planning. manipulators and their control.

**Robot sensors:** Active and passive robot sensors, Construction of tactile, touch and vision sensors; interpretation of sensory information; vision processing; kinematic information from sensory data.

**Robot Intelligence:** Robot learning, State space search, robotics in computer vision applications.

**Robotic end effectors:** Stable grip; constraints; types of contact; mathematical representation of stable grip; use of screw twist, and wrench gripper design; tools as end effectors.

Problems of implementation of automatic systems.

#### **Text & References:**

- 1) Fu K, Gonzalez R and Lee C, *Robotics - Control Sensing Vision & Intelligence*, McGraw Hill.
- 2) Craig J J, *Introduction to Robotics, Mechanics and Control*, Addison Wesley, 1993.
- 3) McKerrow P J, *Introduction to Robotics*, Addison Wesley, 1993.
- 4) Selig M, *Introductory Robotics*, Prentice Hall, 1992.

### **CPT614 FPGA based System Design**

**3-0-0**

Introduction to FPGA Architectures. FPGA design flow, partitioning, placement and routing algorithms. Technology mapping for FPGAs, case studies.

#### **Text/References:**

- 1) Brown, Francis, Rose and Vranesic. *Field programmable Gate arrays*. Kluwer.
- 2) Betz, Rose, Marquardt, *Architecture and CAD for Deep-submicron FPGAs*. Kluwer.
- 3) Trimberger, *FPGA Technology*. Kluwer, 1992.
- 4) Oldfield, Dorf. *FPGAs: Reconfigurable logic for rapid prototyping and implementation of digital systems*. John Wiley.
- 5) Recent papers from conferences and journals.

### **CPT616 Network Security**

**3-0-0**

Review of wired/wireless network protocols, intrusion detection systems, malicious software.

Review of cryptographic algorithms, protocols, cryptanalysis, authentication and signature protocols.

Kerberos, PKI, real-time communication security, IPSec: AH, ESP, IKE.

SSL/TLS, e-mail security, PEM and S/MIME, PGP, web security, network management security, wireless security.

Threats in networks, network security controls, firewalls, intrusion detection, administering security

Honeypots, password management, malicious software, viruses and countermeasures

**Text/References:**

- 1) C. Kaufman, R. Perlman, *Network Security*, Prentice Hall.
- 2) Kurose & Ross, *Computer Networking*, Pearson Education.
- 3) Schiller J., *Mobile Communications*, Pearson Education.
- 4) W. Stallings, *Cryptography and Network Security Principles and practice*, Pearson Education.

**CPT618 Security in Computing**

**3-0-0**

Computer security, threats, attacks, computer criminals, defense methods, information and network policies, cryptography, symmetric and public-key encryption, uses of encryption.

Secure file systems and database security.

Program security, secure programs, viruses and other malicious code, control against program threats, protection in general-purpose OS, protected resources and methods of protection, user authentication.

Binding programs to machines.

Language based security, Integrating security in compilers.

Designing trusted OS, models of security, database security, security requirements, reliability and integrity, inference.

Administering security, legal, privacy, and ethical issues in computer security.

**Texts/References**

- 1) Pfleeger and Pfleeger, *Security in Computing*, Pearson Education.
- 2) M. Bishop and S. S. Venkatramanayya, *Introduction to Computer Security*, Pearson Education.
- 3) Stallings W., *Cryptography and Network Security Principles and Practice*, Pearson Education.
- 4) Stallings W., *Network Security Essentials: Applications and Standards*, Pearson Education.

## **CPT620 Intelligent Agents**

**3-0-0**

Introduction to agent-based computing , Motivations for agent-based computing  
Key concepts and models, Agent architectures (deliberative, reactive, hybrid), Rational decision making (decision theoretic, belief-desire-intention)  
Mobile agents, Agent Interactions, Coordination (organisation models, social laws, social dependencies), Cooperation (team-oriented problem solving, coalition formation) Negotiation (mechanism design, heuristic models, argumentation)  
Computational markets (auctions, competition)  
Agent-Oriented Software Engineering, Benefits and Potential Drawbacks, Agent Methodologies, Application Case Studies (agent-mediated electronic commerce, business process management, telecommunications network management)

### **Texts/References**

- 1) M.J.Wooldridge, *An introduction to multi-agent systems*. Wiley (2002)

## **CPT624 Critical Systems**

**3-0-0**

Introduction to time critical systems, Issues, Components, Classification and terminology. Misconceptions about Real-time computing. Real-time System requirements. Specification of timing constraints.  
Real-time scheduling: Requirements and Issues, Terminology, modeling, Introduction static and dynamic scheduling schemes, cyclic scheduling, priority driven scheduling of periodic tasks, schedulability tests, Aperiodic task scheduling: server/non-server based scheduling algorithms. Practical factors/overheads.  
Task Synchronization: Need and priority inversion problem, Priority Inheritance protocol, priority ceiling protocol and stack-based priority ceiling protocol.  
Introduction to multiprocessor real-time systems, problems and issues.  
An overview of an operating system

### **Text & References:**

- 1) J.W.S.Liu: Real-Time Systems, Pearson Education Asia
- 2) S.T.Lavi, A.K.Agrawala: Real-time system Design, McGraw Hill
- 3) Laplante: Real-time Systems Design and Analysis, An Engineer's Handbook, IEEE Press
- 4) Laurence, K.Mauch: Real-time Microcomputer system design, An introduction, McGraw Hill

## **CPT626 Pattern Recognition**

**3-0-0**

Introduction to statistical, syntactic and descriptive approaches, features and feature extraction.  
Bayes Decision theory- continuous case, 2-category classification, minimum error rate classification, discriminant functions and decision surfaces, discrete case.  
Parameter estimation, supervised learning- Maximum likelihood, Bayes, general bayesian learning.  
Nonparametric - density estimation, parzen windows, k-nearest Neighbor, estimation posterior probability.  
Linear discriminant functions- decision surfaces, generalized linear discriminant functions, 2-category linearly separable case, non-separable behavior, linear programming procedures, SVMs.  
Supervised learning: Feed forward Neural networks, Backpropagation algorithm, error surfaces.  
Clustering - data description and clustering, Hierarchical clustering, self organizing maps.

### **Texts/References**

- 1) Duda and Hart P.E, and David G Stork, *Pattern classification* , John Wiley & Sons.
- 2) Duda and Hart P.E, *Pattern classification and scene analysis*, John Wiley and sons..

- 3) Earl Gose, Richard Johnsonbaugh, and Steve Jost; *Pattern Recognition and Image Analysis*, PHI.
- 4) Fu K.S., *Syntactic Pattern recognition and applications*, Prentice Hall.s

## CPT628 Security Analysis of Protocols

3-0-0

Mathematical models of computer security – Abstract state machines, belief logics, provable security, spi-calculus, Communicating Sequential Processes (CSP).

Needham Schroeder – public key, shared key, attacks; security analysis of Kerberos and Shoup-Rupin protocol

Time-stamping and its incorporation in modeling

Authentication protocols, Access control – policies and mechanism, Nominal calculi for security and mobility, classification of security properties.

Protocol verification – case studies.

### Texts/References

- 1) Peter Ryan, Steve Schneider, Michael Goldsmith, and Gavin Lowe. *Modelling & Analysis of Security Protocols*, Addison Wesley.
- 2) Giampaolo Bella. *Formal Correctness of Security Protocols*, Springer.
- 3) Riccardo Focardi and Roberto Gorrieri. *Foundations of Security Analysis and Design: Tutorial Lectures*, Springer.
- 4) Riccardo Focardi and Roberto Gorrieri. *Foundations of Security Analysis and Design II*, Springer.

## CPT691 Object Oriented Systems

3-0-0

Abstractions, Objects, Classes and Methods, Inheritance and Reuse, Replacement and Refinement, Contracts, Design by Contract, Reuse: code vs. design reuse, Design patterns – classification, pattern descriptions, Creational patterns: Singleton, Factory, Prototype, Structural patterns: Adapter, Proxy, Composite, Decorator, Facade, Behavioral patterns: Strategy, State, Observer, Template method, Iterator.

### Text/References:

- 1) Timothy Budd, *An Introduction to Object-oriented Programming*, Pearson Education.
- 2) Erich Gamma, Richard Helm, Ralph Johnson and John Vlissides, *Design Patterns*, Pearson Education.

## CPT693 Data Compression

3-0-0

Compression: Need, Lossless v/s lossy compression, review of information theory, prefix codes, uniquely decodable code.

Huffman coding – minimum variance, optimal, non-binary, extended, adaptive. Applications and limitations of Huffman codes.

Run length encoding, Arithmetic coding, Predictive coding – Burrows-Wheeler transform, Delta modulation, Adaptive delta modulation

Lossy Compression Techniques – JPEG and its application, MPEG

Error detection and correction: Parity, 1,2,n dimensions, Hamming codes, p-out-of-q codes

Dictionary based compression - Lempel-Ziv-Welch, LZ77 and LZ-78

Quantization – Scalar and Vector Quantization.

Video compression, Audio Compression, Fractal techniques.

### Texts/References:

- 1) Khalid Sayood, *Introduction to Data Compression*, Morgan Kaufman
- 2) Greg A. Harris, Darrel R. Hankerson, Peter D. Jr. Johnson, *Introduction to Information Theory and Data Compression*, Second Edition, Chapman and Hall.



- 3) Saloman, Data Compression, Springer Verlag.
- 4) Nelson, The Data Compression book, Hungry Minds.
- 5) Stephen Welstead, *Fractal and wavelet Image Compression techniques*, PHI, NewDelhi-1, 1999.

### **CPT695 Biometric Security**

**3-0-0**

Biometrics: Need, Conventional techniques of authentication, challenges - legal and privacy issues.

Biometrics: DNA, fingerprint, Iris, Face, hand geometry, ear.

Behavioral: Human gait, speech, thermal imaging, infra-red spectrum, signature, keystroke dynamics

Combining biometrics, scaling issues.

Privacy, legal and ethical issues.

#### **Texts/References:**

- 1) Julian D. M. Ashbourn, Biometrics: Advanced Identify Verification: The Complete Guide
- 2) Davide Maltoni (Editor), et al, Handbook of Fingerprint Recognition
- 3) L.C. Jain (Editor) et al, Intelligent Biometric Techniques in Fingerprint and Face Recognition
- 4) John Chirillo, Scott Blaul, Implementing Biometric Security
- 5) Nalini Ratha (Editor), Ruud Bolle
- 6) Authentication: From Passwords to Public Keys, Richard E. Smith

### **CPT697 Digital Forensics**

**3-0-0**

**File System Forensics:** Duplicating hard disks for "dead analysis", reading hidden data on a disk's Host Protected Area (HPA), Direct versus BIOS access, dead versus live acquisition, Disk partitions - DOS, Apple, and GPT partitions, BSD disk labels, Sun Volume; multiple disk volumes - RAID and disk spanning; Analyzing FAT, NTFS, Ext2, Ext3, UFS1, and UFS2 file systems, Finding evidence: File metadata, recovery of deleted files, Using The Sleuth Kit (TSK), Autopsy Forensic Browser, and related open source tools

**Web Forensics:** network-based evidence in Windows and Unix environments, Reconstructing Web browsing, e-mail activity, Tracing domain name ownership and the source of e-mails

**System Forensics:** Windows Registry changes, Duplicating and analyzing the contents of PDAs and flash memory devices

Electronic document, computer image verification and authentication

#### **Texts/References:**

- 1) Brian Carrier. *File System Forensic Analysis*, Addison Wesley.
- 2) Chris Prosise, Kevin Mandia. *Incident Response and Computer Forensics*, McGraw Hill.
- 3) Linda Volonino, Reynaldo Anzaldua, and Jana Godwin. *Computer Forensics: Principles and Practices*, Prentice Hall.
- 4) Keith J. Jones, Richard Bejtlich, and Curtis W. Rose. *Real Digital Forensics: Computer Security and Incident Response*, Addison Wesley
- 5) Vacca, John R., *Computer Forensics Computer Crime Scene Investigation*, Charles River Media.
- 6) Nelson, Phillips, Enfinger, Steuart. *Guide to computer Forensics and Investigation*, Course Technology.

**CPT692 Semantic Web****3-0-0**

Introduction to semantic web, architecture, languages and tools for knowledge management. XML, RDF, OIL, DAML, OWL for semantic web.

Semantic Web Technologies:

Ontology-based Systems: Ontology based knowledge management; ontology construction; generating, storing, aligning and maintaining ontologies for semantic web; information retrieval from natural language based documents; ontology evolution; ontological indexing and searching techniques for Searching web

**Texts/References**

- 1) John Davies, Rudi Studer, and Paul Warren. *Semantic Web Technologies: Trends and Research in Ontology-based Systems*, Wiley.
- 2) John Davies, Dieter Fensel, Frank van Harmelen, and Frank van Harmelen. *Towards the Semantic Web: Ontology-Driven Knowledge Management*, Wiley.

**CPT694 Intrusion Detection****3-0-0**

Introduction- Intrusion detection system (IDS), intrusion prevention system (IPS),

Unauthorized access – buffer overflow, packet fragmentation, out-of-spec packets

Review of Network protocol – TCP/IP,

Intrusion detection through tcpdump.

IDS and IPS – Architecture and internals.

Malicious and non-malicious traffic, IP headers, TDP, UDP and ICMP protocols and header formats,

Header information to detect intrusion, logs and their analysis,

IDS through reaction and response

Intrusion analysis – data correlation, tools, SNORT.

**Text & References:**

- 1) Matt Fearnow, Stephen Northcutt, Karen Frederick, and Mark Cooper. *Intrusion Signatures and Analysis*, SAMS.
- 2) Carl Endorf, Gene Schultz, Jim Mellander, *Intrusion Detection and Prevention*, McGraw Hill.
- 3) Stephen Northcutt and Judy Novak. *Network Intrusion Detection*, SAMS.
- 4) Paul E. Proctor. *The Practical Intrusion Detection Handbook*, Prentice Hall.

**CPT696 Intellectual Property Rights****3-0-0**

Introduction to Intellectual property, Patents, Trademark, Copyright

Patents – process, patentable entities, scope of patent system, patents and free enterprise; cost considerations; antitrust law, patent institutions, infringement, limitations of patents

Copyright – protection, eligibility, fair use; works and rights protection; limitations

Trademark – history, concepts, scope, computer software copyrights, copyright in databases and electronic publishing.

Design protection

Computer contracts, liability for defective hardware and software, software contracts, web and hardware contracts, electronic contracts and torts, liabilities.

Introduction to Cyber laws in India, IT Act 2000, data subjects' rights, ethical issues in computer security.

Case studies.

**Texts/References**

- 1) Robert P. Merges and Jane C. Ginsburg. *Foundations of Intellectual Property*, Foundation Press.

- 2) Tom Greaves. Intellectual Property Rights for Indigenous Peoples: A Source Book,
- 3) Susan K. Sell. Private Power, Public Law: The Globalization of Intellectual Property Rights, Cambridge University Press.
- 4) D. Bainbridge, Introduction to Computer Law, Pearson Education.
- 5) P. Duggal, Cyber law: the Indian Perspective, 2005

**CPT698 Internet Security****3-0-0**

Security protocols: naming and addressing, IPv6, Network address translation, SNMP, remote login, file transfer protocol, RPC based protocol, peer-to-peer communication

Web architecture and protocols, buffer overflow and hacking

Internet threats – password stealing, Trojans, phishing, viruses, worms, DOS attack, backdoors, Botnets, port scanning, hacking techniques.

Security mechanisms – passwords, one-time password – time based, Lamport's, authentication – smart card, biometrics, RADIUS, SASL framework, host to host authentication, PKI.

Firewalls, VPNs, tunneling, Intrusion detection.

Server and client security,

**Text & References:**

- 1) John Chirillo. *Hack attacks denied*, Wiley.
- 2) McClure. *Web Hacking*, Pearson Education.
- 3) John R. Vacca. *Practical Internet Security*, Springer.
- 4) William R. Cheswick, Steven M. Bellovin, and Aviel D. Rubin. *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison-Wesley.
- 5) Kenneth Einar Himma. *Internet Security: Hacking, Counterhacking ,and Security*, Jones & Bartlett Publishers

**CPT634 Malware Analysis and Detection****3-0-0**

Malware: Types – Virus, Worms, Trojans, Logic Bombs, etc., infection modes, payload and its delivery mechanisms.

Analysis Tools and their design: Disassemblers, Unpackers, Scanners, Decompilers, Emulators, Virtualization techniques

Anti-analysis techniques: Obfuscation techniques, Packing, Encryption, Polymorphism, metamorphism.

Analysis Techniques: Signature based, Non-signature based, Static, dynamic, behavioral, anomaly detection.

Case Study: Android Malware

**Text/Reference Books**

1. Peter Szor: *The Art of Computer Virus Research and Defense*, Addison Wesley Professional.
2. Eric Filiol: *Computer Viruses: from theory to applications*, Springer.
3. Michael Sikorski and Andrew Honig: *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*, No Starch Press
4. Christopher Elisan: *Advanced Malware Analysis*, McGraw-Hill Osborne Media.
5. Michael Hale Ligh, Andrew Case: *The Art of Memory Forensics: Detecting Malware*, Wiley.
6. Bruce Dang, Alexandre Gazet: *Practical Reverse Engineering*, Wiley.

**CPT699 Modelling and Simulation****3-0-0**

Analytical v/s simulation modeling, performance measurement and benchmarking, Workload modeling, random variables, commonly used distributions, Stochastic Processes, Performance evaluation methods, Evaluation Metrics

Markov chains, Birth and Death Processes, Markov chain models of Computer systems, Steady-state and transient analysis

Queuing models, M/M systems and their steady state analysis, Single server and multi-server queues, open and closed queuing networks

Petri Net based Performance Modeling : Classical Petri Nets, Timed Petri Nets, Discrete Petri Nets,

Modeling multiprocessor systems

Discrete event simulation – Simulation languages, random number generation and testing, model verification and validation, analysis of simulation results, confidence intervals, variance reduction techniques, Case studies of analytical and simulation studies of computer systems

Text/Reference Books

1. Law and Kelton, Simulation Modeling and Analysis, Mcgraw Hill
2. Raj Jain, The Art of Computer System Performance Analysis, John Wiley
3. K.S.Trivedi, Probability and Statistics with Reliability, Queuing and Computer Science Applications, PHI
4. Kant, Introduction to Computer System Performance Evaluation, Mcgraw Hill