M. Tech. - Information Technology

Course Structure and Syllabus

Indian Institute of Information Technology
Allahabad - 211012

M.Tech. IT-(Wireless Communication Engineering) Courses

	M.Tech. IT-(Wireless Communication Engineering)			
	FIRST	**SECOND**	**THIRD**	**FOURTH**
C O U R S E	IINP140C IAAP140C IWCS140C IPSP140C	IWNS240C IGRT240C ELT-1 ELT-2	ELT-3 ELT-4 ITHS312P	ITHS420P

IINP140C	Internet Protocols
IAAP140C	Algorithmic Analysis and Programming Practices
IWCS140C	Wireless Communications
IPSP140C	Probability & Stochastic Processes
IWNS240C	Wireless Networks
IGRT240C	Graph Theory
ITHS312P	M. Tech. Thesis
ITHS420P	M. Tech. Thesis

Electives (ELT) II Semester

IMWS240E	Mobile & Wireless Security
IOCN240E	Optical Communication
IDSS240E	Distributed Systems
IITC240E	Information Theory and Coding
ISCO240E	Soft Computing
IARD240E	Antenna and RF Design
IDSP240E	Digital Signal Processing

Electives (ELT) III Semester

IWSN340E	Wireless Sensor Networks
IMSE340E	Mobile Software Engineering
IMDM340E	Mobile Data Management
ICIS340E	Cryptography and Information Security
ICLN340E	Cellular Networks
ISAS340E	Smart Antennas

M.Tech. IT-(Software Engineering) Courses

	M.Tech. IT-(Software Engineering)			
	FIRST	**SECOND**	**THIRD**	**FOURTH**
C O U R S E	IAAP140C IOOS140C ISOM140C ISRE140C	ISTQ240C IASS240C ELT-1 ELT-2	ELT-3 ELT-4 ITHS312P	ITHS420P

IAAP140C	Algorithmic Analysis and Programming Practices
IOOS140C	Object Oriented Software Engineering
ISOM140C	Software Metrics
ISRE140C	Software Requirements and Estimation
ISTQ240C	Software Testing & Quality Management
IASS240C	Architecture of Software Systems
ITHS312P	M. Tech. Thesis
ITHS420P	M. Tech. Thesis

Electives II Semester

IERP240E	Enterprise Resource Planning
ISKD240E	Software for Data & Knowledge Engineering
IADM240E	Advanced Database Management System

Electives III Semester

IMSE340E	Mobile Software Engineering
IEMS340E	Embedded Systems
IABS340E	Agent Based Systems
IGCT340E	Green ICT
ICIS340E	Cryptography & Information Security

M.Tech.IT-(Robotics) Courses

	M.Tech.IT-(Robotics)			
	FIRST	**SECOND**	**THIRD**	**FOURTH**
C O U R S E	IMFR140C IAAP140C ICII140C ICSE140C	IALS240C ISCO240C ELT-1 ELT-2	ELT-3 ELT-4 ITHS312P	ITHS420P

IMFR140C	Mathematical Foundation of Robotics
IAAP140C	Algorithmic Analysis and Programming Practices
ICII140C	Computational Intelligence
ICSE140C	Control System Engineering
IALS240C	Artificial Life simulation
ISCO240C	Soft Computing
ITHS312P	M. Tech. Thesis
ITHS420P	M. Tech. Thesis

Electives II Semester

IIVP240E	Image and vision processing
IWSN240E	Wireless Sensor Networks

Electives III Semester

IHUR340E	Humanoid robotics
INDS340E	Nonlinear Dynamics

M.Tech.IT-(Human Computer Interaction) Courses

	M.Tech.IT-(Human Computer Interaction)			
	FIRST	**SECOND**	**THIRD**	**FOURTH**
C O U R S E	ICCP140C ICII140C IAAP140C IPID140C	IIVP240C IAGA240C ELT-1 ELT-2	ELT-3 ELT-4 ITHS312P	ITHS420P

ICCP140C	Cognition and Cognitive Process Modelling
ICII140C	Computational Intelligence
IAAP140C	Algorithmic Analysis and Programming Practices
IPID140C	Principles of Interaction Design
IIVP240C	Image and Vision Processing
IAGA240C	Advanced Graphics and Animation
ITHS312P	M. Tech. Thesis
ITHS420P	M. Tech. Thesis

Electives II Semester

IADM240E	Advanced Database Management System
ISKD240E	Software for Data & Knowledge Engineering
ISOC240E	Soft Computing
IDSS240E	Distributed Systems

Electives III Semester

IPRXI40E	Intellectual Property Rights
INRXI40E	Information Retrieval

.

M.Tech.IT-(Intelligent System) Courses

	M.Tech.IT-(Intelligent System)			
	FIRST	**SECOND**	**THIRD**	**FOURTH**
C				
O	IAIS140C	ISOC240C	ELT-3	
U	ICCP140C	IIVP240C	ELT-4	ITHS420P
R	ICII140C	ELT-1	ITHS312P	
S	IAAP140C	ELT-2		
E				

AIS940IT	Architecture of Intelligent System
ICCP140C	Cognition and Cognitive Process Modelling
ICII140C	Computational Intelligence
IAAP140C	Algorithmic Analysis and Programming Practices
ISOC240C	Soft Computing
IIVP240C	Image and Vision Processing
ITHS312P	M. Tech. Thesis
ITHS420P	M. Tech. Thesis

Electives II Semester

IDSD240E	Digital System Design
ISKD240E	Software Systems for Data Mining & Knowledge Engineering
IADM240E	Advance DataBase Management System
IWSN240E	Wireless Sensor Networks

Electives III Semester

IIPRXI40E	Intellectual Property Rights
IVIRXI40E	Virtual Reality
IINRXI40E	Information Retrieval
IABSXI40E	Agent Based System
IGCTXI40E	Green ICT
IHURXI40E	Humanoid Robotics

M.Tech.IT-(Cyber laws and Information Security) Courses

	M.Tech.IT-(Cyber laws and Information Security)			
	FIRST	**SECOND**	**THIRD**	**FOURTH**
C				
O	IINP140C	IADC240C	ELT-3	
U	ICRP140C	INSE240C	ELT-4	ITHS420P
R	IAAP140C	ELT-1	ITHS312P	
S	ICLS140C	ELT-2		
E				

IINP140C	Internet Protocols
ICRP140C	Introduction to Cryptography
IAAP140C	Algorithmic Analysis and Programming Practices
ICLS140C	Cyber Laws and Security Standards
IADC240C	Advanced Cryptography
INSE240C	Network Security
ITHS312P	M. Tech. Thesis
ITHS420P	M. Tech. Thesis

Electives II Semester

IMWS240E	Mobile & Wireless Security
ICFN240E	Computer Forensics
ISAC240E	Security Architecture
ITRA240E	Technical Risk Assessment
ISSE240E	Software Security
IISA240E	Information Security Audit
IIAM240E	Identity and Access Management
IWSN240E	Wireless Sensor Networks

Electives III Semester

IDBS340E	Database Security
IOSS340E	Operating System Security
IBCP340E	Business Continuity Planning and Disaster Recovery Planning
ISCA340E	Security Audit
ICVS340E	Cloud and Virtualization Security
IISP340E	Information and Information System Privacy

IINP 140C **Internet Protocol**

Introduction: The layered networking model Hypermedia Uniform Resource Identifiers WWW Client Server Model HTTP HTTP Headers

Network Layer Protocols: IPv4 IPv6 RIP OSPF BGP ICMP IGMP

Transport Layer Protocols: UDP TCP

Internet Protocols and Email Protocols: Internet Protocol SMTP POP3 IMAP

Telnet and FTP

Text Books:

1. Network Security - Private Communication in a Public World by Charlie Kaufman, Radia Perlman and Mike Speciner
2. Computer Security by Dieter Gollmann
3. Computer security : art and science by Matt Bishop.
4. Cryptography and Network Security : Priciples and Practice by William Stallings.
5. Information security : principles and practices by Mark Merkow and Jim Breithaupt.
6. Charles P.Pfleeger, Security in Computing, Fourth Edition, Pfleeger Consulting Group, RAND corporation, Prentice Hall.
7. Shon Harris, CISSP Exam Guide Fourth Edition, McGraw Hill.

IAAP 140C Advanced Algorithms and Programming Practices

Coding Convention Motivation Kernel coding style

Automatic Documentation Generators Necessity for documentation Doxygen

Shell scripting in Linux Environment Introduction Simple shell scripts

whiptail Automatic testing using shell scripts Revision Control Systems Introduction Necessity Bazaar and loggerhead

Algorithms & Data Structures n-d arrays n-d arrays on hard disk Linked list Linked list on hard disk Dynamic tables Heaps using trees AVL trees Splay tree B-tree Depth first search Breadth first search Shell scripting Disjoint sets using trees Kruskal using disjoint sets Eulerian path Traveling salesman problem Hamiltonian cycle Hashing by chaining Cuckoo hashing Perfect hashing Interval tree

Text Books:

1. The Art of Multiprocessor Programming by Maurice Herlihy and Nir Shavit, Morgan Kaufmann Publishers
2. The Art of Concurrency by Clay Breshears, O Reilly
3. Introduction to Parallel Computing (2 Ed) by Ananth Grama, Anshul Gupta, George Karypis, Vipin Kumar, Addison Wesley
4. Professional C++ by M Gregoire, NA Solter, SJ Kleper (2Ed)

IWCS 140C Wireless Communication Engineering

Characteristics of interference and noise limited systems, Physical modeling for wireless channels, Input /output model of the wireless channel, Time and frequency coherence, Statistical channel models

Fundamentals of CDMA, OFDMA and MIMO technologies, Point-to-point communication: detection, diversity and channel uncertainty

Introduction of the capacity of wireless channels and Multiuser capacity and opportunistic communication.

Latest research findings and developments at physical layer.

IPSP 140C Probability & Stochostic Process

INTRODUCTION to PROBABILITY : Definitions, sample, space & events, joint & conditional probability, dependent events. Elementary theory of probability, Bayes theorem.

RANDOM VARIABLES : Introduction, distribution & density functions, discrete & continuous random variables, special distributions : binominal, Poisson, uniform, exponential, normal, rayleigh. Central limit theorem.

Expectation, Conditional Distribution and Conditional Expectation : Vector random variable, Expectation of random variable, joint distribution functions, joint probability density function, conditional distribution & density functions, Conditional Expectation. Mean & variance, chebyshevs inequality, characteristic functions & moment generating function.

STOCHASTIC PROCESSES: Introduction, Random process , Bernoulli Process, Poisson Process, Renewal theory, Markov Chains and random Walk.

References:

1. 1. Introduction to probability models, Sheldon M. Ross.
2. A First Course in Probability, Sheldon M. Ross .
3. Stochastic Process, Sheldon M. Ross .
4. Introduction to Probability, D.P. Bertsekas and J. N. Tsitsiklis, MIT.
5. Probability and Statistics with Reliability, Queuing, and Computer Science Applications, K. S. Trivedi.

IWNS 240C **Wireless Networks**

Review of the networking fundamentals, the requirements of wireless networking at various layers.

WiFi Network, WiMax Network

Manet, Vehicular adhoc Network

Latest research findings and developments in the above networking technologies

IGRT 240C Graph Theory

Introduction: Definition of a graphs, Paths, Cycles, and Trails, Vertex Degrees and Counting, Directed Graphs

Trees and Distance: Basic Properties, Spanning Trees and Enumeration, Optimization and Trees

Matchings and Factors: Matchings and Covers, Algorithms and Applications, Matchings in General Graphs

Connectivity and Paths: Cuts and Connectivity, k-connected Graphs, Network Flow Problems

Coloring of Graphs: Vertex Colorings and Upper Bounds, Structure of k-chromatic Graphs, Enumerative Aspects

Planar Graphs: Embeddings and Euler's Formula, Characterization of Planar Graphs, Parameters of Planarity

Edges and Cycles: Line Graphs and Edge-Coloring, Hamiltonian Cycles, Planarity, Coloring, and Cycles

Text Book:

1. Introduction to Graph Theory by Douglas B. West

IDSS 240E Distributed Systems

Introduction to Distributed Systems: Basic assumptions of Distributed Systems; Interaction Model; Failure Model.

Architectures for Distributed Systems: Client - server architecture; Master - slave architecture; Master - slave architecture with multiple masters; Service oriented architecture. Each architecture is analyzed w.r.t. their respective interaction and failure model.

Technologies for Distributed Systems: Sockets; RPC; RMI; Web Service.

Physical Clock synchronization: Internal and external synchronization of physical clocks; Christian's algorithm; Berkeley algorithm.

Logical clocks: Events; the 'happened before' relation; Lamport clock; Vector clock (with proof of correctness).

Global State: Need for obtaining global state; expressing global state as a history of events; cuts; consistent and in-consistent cuts; Chandy-Lamport snapshot algorithm.

Traversal algorithms: Need for traversal algorithms; initiators and non-initiators; traversal algorithms for the following topologies (along with analysis of complexity): ring, tree, mesh, hypercube.

Election algorithms: Need for election algorithms; election algorithms for the following topologies (along with complexity analysis and proof of correctness): ring, tree, mesh, hypercube.

Multicasting: Basic muticasting; ensuring the 'all or none' property; receipt and delivery of multicast messages; hold-back queue; FIFO ordered multicasting; causal ordered multicasting; total ordered multicasting.

Introduction to distributed transaction processing: pessimistic and optimistic approaches to transaction processing.

ISCO 240C Soft Computing
ISCO 240E

Artificial intelligence systems: Neural networks, fuzzy logic, genetic algorithms. Artificial neural networks: Biological neural networks, model of an artificial neuron, Activation functions, architectures, characteristics learning methods, brief history of ANN research-Early ANN architectures (basics only)-McCulloch & Pitts model, Perceptron, ADALINE, MADALINE

Backpropagation networks: architecture, multilayer perceptron, backpropagation learning-input layer, hidden layer, output layer computations, calculation of error, training of ANN, BP algorithm, momentum and learning rate, Selection of various parameters in BP networks. Variations in standard BP algorithms- Adaptive learning rate BP, resilient BP, Levenberg-Marquardt, and conjugate gradient BP algorithms (basic principle only)-Applications of ANN

Fuzzy LogicCrisp & fuzzy sets fuzzy relations fuzzy conditional statements fuzzy rules fuzzy algorithm. Fuzzy logic controller fuzzification interface knowledge base decision making logic defuzzification interface design of fuzzy logic controller case studies.

Genetic algorithms: basic concepts, encoding, fitness function, reproduction-Roulette wheel, Boltzmann, tournament, rank, and steady state selections, Elitism. Inheritance operators, Crossover-different types, Mutation, Bit-wise operators, Generational cycle, Convergence of GA, Applications of GA case studies. Introduction to genetic programming- basic concepts.

Text Books:

1. R. Rajasekaran and G. A. Vijayalakshmi Pai, Neural Networks, Fuzzy Logic, and Genetic Algorithms: Synthesis and Applications, Prentice Hall of India, New Delhi, 2003

2. L. Fausett, Fundamentals of Neural Networks, Prentice Hall, Upper Saddle River, N.J, 1994.

Reference Books

1. 1. D. E. Goldberg, Genetic Algorithms in Search, Optimisation, and Machine Learning, Addison-Wesley, Reading, MA, 1989 2. M. T. Hagan, H. B. Demuth, and M. H. Beale, Neural Network Design, PWS Publishing, Boston, MA, 1996. 3. T. Ross, Fuzzy Logic with Engineering Applications, Tata McGraw Hill, New Delhi, 1995 4. J. R. Koza, Genetic Programming: On the Programming of Computers by Natural Selection, MIT Press, Cambridge, 1992. 5. B. Yegnanarayana, Artificial Neural Networks. Prentice Hall of India, New Delhi, 199

IARD 240E Antenna and RF Design

Review of basic radiation theory, the antenna parameters and their importance.

Antenna and feed network design for low power applications.

Antenna and feed network design for high power applications.

Latest research findings and developments.

IDSP 240E Digital Signal Processing

Review of Discrete Fourier Transform, Fast Fourier transform algorithms, Introduction to Digital Signal Processors.

Various structures for realization of discrete time systems, multirate digital signal processing.

Introduction of IIR filter design, FIR filter design, Predictive systems and Weiner filter, Power estimation techniques.

Latest research findings and developments

IWSN 340E **Wireless Sensor Networks**

Basics of wireless sensor network: Sensor network architecture Individual components of sensor network nodes. Wireless sensor network as embedded system Tired architecture in sensor bnetwork Routing and addressing in tired architecture Draw backs of tired architecture. Communication Protocols in sensor networks Energy efficient design of Wireless sensor nodes.

Taxonomy of routing techniques inn sensor networks: Routing Protocols in WSN Reilable Transport in Sensor Networks Routing on a curve Medium access control in wireless sensor network A survey of MAC protocol for sensor network Dissemination Protocols for large sensor networks

Models of programmability in sensor network: Differences between sensor network and traditional network Need for sensor network programming Major models of programming Framework of system level prog. Localization in WSN

Application layer protocols Localisation protocols Positioning and location tracking in WSN
Configuring Wireless sensor network Simulators in WSN Tools and languages in WSN

Coverage and Connectivity

Computation and networking problems Coverage algo Connectivity Algo Area coverage Point Coverage Barrier Coverage

Applications Simulations Information Retrival in SN Sensor Fusuion
Text Books:

1. Protocols and Architectures for Wireless Sensor Networks. H. Karl and A. Willig. John Wiley & Sons, June 2005.
2. Wireless Sensor Networks: Technology, Protocols, and Applications. K. Sohraby, D. Minoli, and T. Znati. John Wiley & Sons, March 2007.
3. Wireless Sensor Networks. C. S. Raghavendra, K. M. Sivalingam, and T. Znati, Editors. Springer Verlag, Sep. 2006.
4. Wireless Sensor Networks: Architectures and Protocols. E. H. Callaway, Jr. AUERBACH, Aug. 2003.
5. Networking Wireless Sensors. B. Krishnamachari. Cambridge University Press, Dec. 2005.
6. Wireless Sensor Networks: An Information Processing Approach. F. Zhao and L. Guibas. Morgan Kaufmann, Jul. 2004.
7. Sensor Networks and Configuration: Fundamentals, Standards, Platforms, and Applications. N. P. Mahalik. Springer Verlag, Nov. 2006.
8. P. Levis, N. Lee, M. Welsh, and D. Culler. TOSSIM: Accurate and Scalable Simulation of Entire TinyOS Applications, The First ACM Conference on Embedded Networked Sensor Systems (Sensys03), November 2003.

IMSE 340E Mobile Software Engineering

Embedded Software Vs Mobile Software, Characteristics of Mobile Software, Existing Smartphone Platforms and Languages, Description of iOS and Android OS features for development of Apps, Category of Mobile Apps: Native Apps & Web Apps. When to use Native and when to use Web Apps: Hybrid Apps-Solution worth consideration. Principles of software engineering for Mobile devices and best practices, including Software process model for Mobile Apps: Recent Mobile Software Process Model, Usability & User Experience design, Mobile Interaction Design, Interaction Designs: Hub and Spoke, Bento, tabbed View and other mobile Interaction designs. Android Case Study: Application development with Android: Basic Building Blocks, Activity, Service, Intent & IPC (Inter Process Communication in Android), Security Breach & Attack points. Malware and type of security attacks and privacy breach in Android Apps. Code reviews, source control, and unit tests. Evaluation and usability of mobile devices and services. Testing of Mobile Web Apps and Native apps. Projects and Case Studies:

IMDM 340E Mobile Data Management

Mobile Software Architectures

Mobile Computing Models: Software architectures ranging from client-servers and proxies to software mobile agents are introduced

Environmental Awareness: Concepts such as application-awareness of location and disconnection, and adaptation to varying connectivity conditions

Web Browsing: realization of mobile architectures and concepts through their deployment in the design of an example web-browsing application. Disconnected Operation and Weak Connectivity Techniques for sustaining frequent network disconnections and weak connectivity within the context of file, database management, workflow management, object-based, and web systems.

Mobility: relocating data and computation Failure Recovery and distributed checkpointing Case studies on CMU's Coda file system Coda, IBM's WebExpress web browsing system and Xerox's Bayou weak replication storage system

Location and handoff management
Concurrency control mechanism schemes
Transaction management
Mobile database recovery
Text Books:

1. 1. Data Management for Mobile Computing by Evaggelia Pitoura, George Samaras, Kluwer Academic Publishers, ISBN: 0-7923-8053-3 2. Mobile Database Systems by Vijay Kumar, Wiley Publication, ISBN: 978-0-470-04828-3 3. Research papers

ICIS 340E Cryptography & Information Security

Introduction: Classical Encryption Schemes, Principles of Modern Cryptography. Perfect Secrecy and Its Limitations. Private-Key Encryption: Computational Security, Pseudo-random Generators and Stream Ciphers, Pseudorandom Functions and Block Ciphers, Modes of Encryption, Security against Chosen-Ciphertext Attacks and Padding-Oracle Attacks. Message Authentication: Secrecy vs. Integrity, Message Authentication Codes, CBC-MAC, Authenticated Encryption. Hash Functions: Security Requirements, HMAC, Additional Applications of Hash Functions.Number Theory. Public-Key Revolution: Key Distribution and Key Management, Diffie-Hellman Key Exchange. Public-Key Encryption: Definitions of Security, Hybrid Encryption and the KEM/DEM Paradigm, El Gamal Encryption and DHIES, RSA Encryption and the RSA PKCS #1 Standard. Digital Signatures: Signatures vs. MACs, RSA-Based Signatures and the RSA PKCS #1 Standard, DSA/ECDSA, Public-Key Infrastructures.

Text Books:

1. Introduction to Modern Cryptography by J. Katz and Y. Lindell.
2. Handbook of Applied Cryptography by A. Menezes, P. Van Oorschot, S. Vanstone.

ICLN 340E **Cellular Networks**

Fundamentals of cellular Networks, FDMA and TDMA systems and other relevant technologies and issues.

GSM, GPRS, EDGE, IS-95, UMTS systems architecture and protocols

LTE and advanced LTE networks architecture and protocols, HSPA, MBMS etc. technologies of 3G and 4G networks.

Latest research findings and developments at physical layer.

ISAS 340E **Smart Antennas**

Applications of smart antenna in Wireless Networks and Radar systems, Various smart antenna processors for narrowband and wideband applications

The antenna response to short sinusoidal pulse, Direction estimation algorithms.

Multiple Input Multiple Output (MIMO) and associated technologies.

Latest research findings and developments.

IOOS 140C Object Oriented Software Engineering

The Course introduces the characteristic differences between Procedural and Object Oriented approach for programming, Concepts of Class, Objects and Object Oriented Characteristics. Building upon basic programming skills in OO, specifically using basic Java programming constructs for object oriented problem solving (e.g., Classes: Abstraction, inheritance, interfaces, polymorphism), Methods in OO Programming: Method overloading and overriding. Structured Software Engineering Principles.

To appreciate the role of Object orientation in problem solving and to be able to design and implement a Java program to model a real world system, and subsequently analyze its behavior. Java implementation for GUI, Event handling and Applets for Web enabled applications. Developing Applications with GUI and Database connectivity.

This module focuses on the design and analysis of larger, more complex programs using Object Oriented Modeling with UML. Why build models of software, Why should we build comprehensive designs before coding Static and Dynamic modeling diagrams and role of Use Case Diagrams.

Overview of UML for Java Programmers: Class Diagrams Object Diagrams. Sequence Diagrams, Collaboration Diagrams, Static Diagrams: Working with Diagrams and role of Modeling, Making Effective use of UML, Communicating with Others, Back end documentation What to keep, and What to throw away, Iterative Refinement Behavior, Iterative Refinement Minimalism, When to draw diagrams, and when to stop. OO Design Patterns.

Design Metrics: Cohesion and Coupling- CRC. Class Diagrams & OO Relationships: Inheritance, Aggregation and Composition. OO Design Principles: Open Close Principle, Interface segregation principle, Liskov Substitution Principle. Dynamic modeling diagrams. Oo Testing and maintenance. Reuse & OO Frameworks.

Text Books:

1. Objects First with Java, 5th edition, David Barnes and Michael Kolling.
2. UML distilled by Martin Fowler.
3. Object Oriented Analysis & Design.

ISOM 140C **Software Metrics**

Theoretical foundations for software metrics, Introduction to the measurement theory.

The representational theory of measurement. Empirical and numerical systems. Representation condition.

Measurement scales. Meaningfulness in measurement. Operations on measures. Data collection and analysis, Statistical analysis and tools, The Goal-Question-Metric based framework for software measurement, Classification of software measures, Specification measures, Design measures.

Complexity measures, Code related measures, Software testing measures, Software reliability measures and models, Measuring the software development and maintenance processes.

Experimental design and analysis, Software metrics validation, Predication systems. Calibration and validation of predication systems.

Setting up a measurement program, Application of software metrics.

Text Books:

1. Software Metrics Edited by Alan J Perlis, Frederick Sayward and Mary Shaw.

ISRE 140C Software Requirements and Estimation

Software Requirements: What and Why,Essential Software Requirement, Good practices for requirement engineering, Improving requirements processes, Software Requirements and Risk Management.

Software Requirements Engineering: Requirements elicitation, Requirement analysis documentation, review, elicitation techniques, analysis models, software quality attributes, Risk reduction through prototyping, setting requirements priorities, verifying requirements quality, software requirements modeling, Use case modelling, Analysis model, dataflow diagrams, state transition diagram, class diagram, object analysis, problem frames.

Software Requirements Management: Requirements management principles and practices, Requirement attributes, change management process, Requirement traceability matrix, Links in requirements chain Requirement management tool, benefits of requirement management tools, commercial requirement management tools, Rational Requisite pro, Caliber-RM, Implementing requirement management automation,

Software Estimation: Components of software estimation, software estimation models, Problems associated with estimation, Key project factors that influence estimation, Size estimation- two views of sizing, Function point analysis, Mark II FPA, full function point, LOC estimation, conversions between size measures.

Effort Schedule and Cost estimation: What is productivity, estimation factors, approaches to effort and schedule estimation, COCOMO II, Putnam estimation model, Algorithmic models, cost estimation, software estimation tools, desirable features of software estimation tools, IFPUG, USCs COCOMO II, SLIM (Software Lifecycle Management) tools.

References:

1. Software Engineering: A Practitioner's Approach: McGraw-Hill Series in Computer Science, Roger S. Pressman.
2. Software Requirements And Estimation: Kishore & Naik, Swapna Kishore, Kishore & Naik.
3. Recent research papers of IEEE, ACM , Elsevier. Etc. In area of Software Requirement Estimation and Engineering.

ISTQ 240C Software Testing & Quality Management

Text Books:

1. Books Name

IASS 240C Architecture of Software Systems

Introduction to Software Architecture, the 4+1 View of Software Architecture, Examples of Software Architecture.

Architecture Design: Quality attributes; Attribute Driven Design, Architecture Centric Software Development Methodology, Design Patterns.

Software Design Function Oriented vs. Object Oriented, Documenting Software Architecture Stakeholders, Views, Viewsets, View-based documentation.

IEEE 1471, ISO 42010, Architecture Description Languages, Architecture Evaluation, Product line architectures, Enterprise Architecture, Architecture Knowledge Management.

Text Books:

1. Software Architecture: Foundations, Theory, and Practice, Taylor et al., John Wiley, 2010.

IADM 240E Advanced Database Management Systems

Overview of DBMS, Introduction to DD, Types of DD, Homogeneous and heterogeneous DD, Issues in DD (Network topology, distribution, cost, performance and scalability etc.)

Architectures: Distributed DBMS, Parallel DBMS, MDBS, Peer-to-peer, Client/Server

Data distribution: Fragmentation, replication and mix type, transparencies.

Data Allocation Problem: Optimization problem formulation and solution.

Semantic Data Control: View Management, Data Security, Semantic integrity control

Query Processing: Distributed query processing and Query plan, Query Optimization, joins strategies of Queries (Simple, parallel, semi-join etc.)

Transaction Management: Distribute transaction management, serializability issues,

Concurrency Control: Protocols and their limitations (2PC, 3PC, Timestamp based, Majority, biased, quorum consensus, write-only etc.), Deadlock Handling: Issues and protocols

Text Books:

1. M. Tamer Oezsu, Patrick Valduriez "Principles of Distributed Database Systems, Second Edition" Prentice Hall,

2. A. Silverschatz, H. S. Korth and S. Sudarshan : Database System Concepts, Mc-Graw Hill

IMFR 140C **Mathematical Foundation of Robotics**

Introduction to the Profession , mathematical foundation for spatial rigid body representation , Spatial orientation transformation-Eulerian and quaternion representation , Homogenous Coordinate Transformation Matrix and its inversion principle , Forward and Inverse Kinematics Problem , D-H Principle , modeling principle of a Cyber physical system , manipulator jacobian and singularity , robot modeling using its dynamics- both N-E and Lagrangian method , Trajectory planning , robot control principle- basic master slave control architecture , PD-PID control, computed torque/model based methodology, nonlinear control, sensory devices for robots-both external and internal sensors, sensory information fusion using D-S theory, Robot programming- both offline and real time programming methodologies.

ICII 140C Computational Intelligence

Bayesian classification* - Review of Bayes Theorem; a priori, class conditional and posterior probabilities; using Bayes theorem as a classifier; Bayesian belief networks.

Nearest Neighbor* *- *Nearest neighbor classification; K Nearest neighbor classification; weighted K Nearest neighbor classification.

Machine learning - Supervised, unsupervised and semi-supervised learning. Supervised learning* - Discriminant functions; learning linear discriminant functions; Decision boundaries; learning linear decision boundaries; Perceptron learning; Single perceptron; Multi layer perceptrons. Unsupervised learning* - K means clustering.

Fuzzy sets* - Introduction to fuzzy sets; mathematical operations on fuzzy sets; fuzzy decision theory; fuzzy K means clustering. Evolutionary methods* - Genetic algorithms; proof of convergence based on Holland's theorem; Ant colony optimization; Particle swarm optimization.

ICSE 140C Control System Engineering

Control System Modeling:Basic Elements of Control System Open loop and Closed loop systems, Transfer Functions: Poles and Zeros, Block diagram reduction Techniques, Signal flow graph, Modelling of various control systems.

Response Analysis:Transient and Steady State Response, Time response analysis: First Order Systems, Second order systems, Steady state errors, Control Actions: P, PI, PD and PID Control.

Analysis: Concept of Stability, Routh-Hurwitz Criterion, Root Locus Technique, Construction of Root Locus, Stability, Dominant Poles, Application of Root Locus Diagram Nyquist Stability Criterion - Relative Stability.

Frequency Response Analysis: Frequency Response Bode Plot, Polar Plot, Nyquist Plot Frequency Domain specifications from the plots Constant M and N Circles Nichols Chart Use of Nichols Chart in Control System Analysis. Compensators of control system: Phase Lead, Phase Lag, and Phase Lead-Lag Compensators.

State Variable Analysis And Design : Concept of State, State Variables, and State Model, State space representation of Continuous Time systems State equations Transfer function from State Variable Representation Solutions of the state equations - Concepts of Controllability and Observability State space representation for Discrete time systems.

IALS 240C **Artificial Life Simulation**

This course provides introduction Artificial Life Simulation related to Robotics.

A Survey of Serve of what is Life, Laws of Nature, Concept of Thermodynamics and entropy. Discussions of Selection Rules in Nature. Comparison of Artificial Life Simulation with Standard Artificial Intelligence.

Revision of Statistical Processes and ANOVA. Revision of linear Optimization: Simplex Method. Lagrange Method for Non-linear. Random Processes, Rule based random Processes, Monte Carlo Simulation, Finite State Automata, Cellular Automata (1D, 2D and multi Dimensional). Conway's Game of Life, Self-organization, Life Patterns, Chaotic Processes, Game Theory, Simulations using OpenGL, MatLab

Fractals, Fractal-Geometry Methods, Fractal-Generation Procedures, Classification of Fractals. Fractal Dimension, Geometric Construction of Deterministic Self-Similar Fractals, Geometric Construction of Statistically Self-Similar Fractals. Random Midpoint-Displacement Methods, Controlling Terrain Topography.

Hierarchical Paradigm, Biological Foundation of the Reactive Paradigm. Horizontal decomposition of task into the Sense, Plan and Act organization of the Hierarchical Paradigm. Vertical decomposition of task into the Sense and Act organization, associated with the Reactive Paradigm Subsumption Architecture, Artificial Self-Replication

Review of papers and implementation in the Fallowing Topics: Ant Colony Optimizations, Swarm Intelligence, Parallel Neural Network analysis, Parallel GA, Subsumption Architecture, Game Theory etc.

Lab Assignments:

1. Implementation of different Simulations using OpenGL, MatLab and other software and if possible on hardware.

IIVP 240C **Image and Vision Processing**
IIVP 240E

Perspective and Importance of Image Processing and Computer Vision :

Introduction to Various types of Images, Human Vision and Computer Vision; Formation of Digital Images, View Geometry and Radiometry, Representation of Color and Color Spaces.

Image Representation in Spatial and Transformed Domains.

Image Enhancement, Filtering and Edge, Corner and Curve Detection,

Segmentation and Feature Extraction : Model based and Probabilistic Methods.

Image Classification, Recognition and Understanding.

Camera Calibration, Stereopsis

3D Shape from Shadow, Motion and Optical Flow

Motion Analysis and Activity Recognition

Research Trends in Image Processing and Computer Vision

IHUR 340E **Humanoid robotics**

Biped Locomotion Control: Inverted Pendulum model, Compass gait model, Equation of motion of Linear Inverted pendulum & simple pendulum. Concept of ZMP, COP, COM, orbital energy. General control architecture of a Humanoid Robot. Humanoid push recovery, Biped locomotion modeling using hybrid automata, Fundamentals of Second order system, concept of PD, PID controller in the context of biped motion control.

Open SIM : Three tutorials, concepts of forward kinematics, inverse kinematics, forward dynamics and inverse dynamics. Assignments.

Concept of Synchronization, Design procedure of CPG (Central Pattern Generator) .

Multimodal Human-Robot interactions : Gesture recognition problem using HMM: all the three problems: Forward Backward Algorithm, Viterbi Algorithm, BaumWelch algorithm and their applications in gesture recognition, Gesture creation(using If THEN Rules), interactive Gesture executions. (It will be presumed that the students already have undergone the courses either RIA or Mathematical Foundation of Robotics)

Cognitive robotics: Reactive approach - Subsumption Architecture, Potential field based architecture, Deliberative approach, hybrid deliberative/Reactive approach for creating intelligent behaviors.

KALMAN Filter, SLAM (Simultaneous Localization and Mapping) .

INDS 340E Non Linear Dynamics

Review of Linear systems and Controls. State Space representation in linear systems and modification due to non linearity. Notation, some features of nonlinear dynamical systems. Scalar differential equations, examples of population dynamics, definition of equilibrium point. Vector differential equations, solution for the linear case. Vector fields and phase portraits. Planar case: classification of equilibrium points, relation with eigenvalues and eigen vectors, phase portraits and vector fields.

Oscillators: van der Pol oscillators, necessary conditions for periodic orbits, sufficient conditions for such orbits. Conditions for existence and uniqueness of solutions, proof using fixed point theorem, examples of non-uniqueness and finite-escape time features.

Lyapunov stability definition and theorem/proof, converse theorems, linearization about an equilibrium point. Nyquist criterion, Feedback interconnections, Absolute stability, Lp stability, Small-gain theorem, Passivity results.

Discrete Time Dynamical Systems, The Logistic Map and Period doubling, Introduction to chaos theory, Introduction to Fractals

Lab Assignment:

1. Implementation of different Simulations in MatLab.

ICCP 140C Cognition and Cognitive Process Modelling

Introduction to Cognition and Cognitive Processes; Perceptual , Attention and Cognitive Processes; Computational Theory of Mind; Connectionist Models.

Learning and Memory Models; Short term and Long term Memory Models; Knowledge Acquisition and Deployment; Learning and Forgetting; Implicit and Explicit Learning; Intelligence Modelling; Social Cognition and Social Intelligence; Evolution and Evolving Machines; Thinking Machines; Modelling Emotion in computation.

Computational Cognitive Architectures: SOAR Architecture for Modelling General Intelligence; ACT-R Architectures; CLARION Architecture; Applications in Intelligent and Interactive Systems : ECA and Talking computers.

Lab Assignment:

1. Implementation of different Simulations in MatLab.

IPID 140C Principles of Interaction Design

Brief overview of HCI: Origins and definitions of HCI, brief history, Components of HCI, Various disciplines that participate in HCI, Motivations for human factors in design, Need to understand people/ users, computers and methods.

Human issues: Cognition, Visual and auditory perception, Memory & learning, Cognitive models & frameworks, Vision, Perception and Interface metaphors.

Interaction: Interaction devices, Models of interaction, Interaction/dialog styles, menu selection, form filling and dialog boxes, command, speech and natural languages, direct manipulation and virtual environments, Effective information presentation and Common interface paradigms.

Interface design methods: User-centered design, LUCID model, User task analysis, Formal methods for user-interface (UI) specifications (including Grammar, Menu Selection Tree, Transition Diagram, Statechart and User action notation) , Prototyping, Storyboards, Design principles and rules, Process of interface design & its elements.

Interface evaluation: Interface evaluation methodologies, Usability issues, ISO 9241 framework of usability, Usability testing steps, Expert reviews, Heuristic evaluation, Cognitive walkthrough, Benchmarks and experiments, Surveys and Acceptance test.

User Experience (UX) Design: Define UX design roles and responsibilities, Adapt UX design and Usability Principles and Guidelines, Realized that UIs are "visualized requirements", Base the design thinking on business requirements, Adapt a user-centered business analysis and UX design methodology, Apply change management in deployment of the new user-center methodology.

Contexts for and foundations of designing Interactive systems: CSCW: Working in groups, Agents and avatars, Ubiquitous computing, Mobile computing, Emotion & affective computing, Social interaction.

References:

1. David Benyon, Designing Interactive Systems 2nd Ed., Addison Wesley.
2. Alan Dix et. al., Human-Computer Interaction, Pearson Education.
3. Ben Shnerderman, Designing the user interface: Strategies for Effective Human-Computer Interaction, Pearson Education.
4. Jenny Preece, Human-Computer Interaction, Addison Wesley.
5. Emrah Yayici, "UX Design and Usability Mentor Book: With Best Practice Business Analysis and User Interface Design Tips and Techniques", Paperback, 2014.
6. Christine Faulkner, "The Essence of Human-Computer Interaction", Prentice Hall.
7. Don Norman, Design of Everyday Things, Basic Books.

IAGA 240C Advanced Graphics & Animation

Introduction, 2D and 3D transformations, Matrix representation of transformations, Composite transformations, 2D viewing pipeline, Window-to-viewport coordinate transformation, 3D viewing pipeline, Synthetic camera analogy, Transformation from world-to-viewing coordinates, Projective transformations, Canonical view volume.

Object representation: Hierarchical modeling of polygonal surfaces, Quadric surfaces, Constructive solid geometry methods, Octrees, BSP trees, Fractals, Bezier and B-Spline curves.

Acceleration algorithms: Spatial data structures, Culling techniques, Hierarchical view frustum culling, Level of Detail.

Image-based effects: Fixed-view effects, Skyboxes, Sprites, Billboarding, Particle systems, Impostors, Motion blur, Fog, Volume rendering.

Introduction to OpenGL Graphic programming, OpenGL data types, Using the GL, GLU and GLUT libraries, Basic drawing, Programming assignment (lab work).

Different generations of GPUs, GPU architecture overview, CUDA programming model, Memory models, CUDA hardware interface on the GPU, CUDA programming examples (lab work).

Principles of animation, Overview of various animation techniques, Storyboards for animation, Key-frame system, Tweening and Morphing.

Modeling & Animating Human Figure: Virtual human representation, Reaching & grasping, Walking, Clothing & Hair; Facial Animation: Human face, Facial models, Animating the face, Lip-Sync animation; Physically-based Animation.

Detailed Case study on Real-time Rendering & Visualization of very Large 3D Datasets.

Books:

1. Rick Parent, Computer Animation: Algorithms & Techniques, Morgan Kaufmann Pub.
2. Tomas Akenine-Mller and Eric Haines Naty Hoffman, Real-Time Rendering, 2nd Ed., A.K. Peters.
3. D. Hearn & M.P. Baker, Computer Graphics with OpenGL, 4th Ed., Pearson Education.
4. Francis S Hill Jr., Stephen M Kelley, Computer Graphics Using OpenGL, Prentice Hall of India.
5. NVidia CUDA Repository, URL: http://developer.nvidia.com/category/zone/cuda-zone.

IAIS 240C Architecture of Intelligent System

Text Books:

1. Books Name

ISKD 240E Software System for Data Mining and Knowledge Engineering

Overview: Motivation (for Data Mining),Data Mining-Definition & Functionalities, Data Processing, Form of Data Preprocessing, Data Cleaning: Missing Values, Noisy Data, (Binning, Clustering, Regression, Computer and Human inspection),Inconsistent Data, Data Integration and Transformation. Data Reduction: Data Cube Aggregation,Dimensionality reduction, Data Compression, Numerosity Reduction, Clustering,Discretization and Concept hierarchy generation.

Concept Description: Definition, Data Generalization, Analytical Characterization,Analysis of attribute relevance, Mining Class comparisons, Statistical measures in large Databases. Measuring Central Tendency, Measuring Dispersion of Data, Graph Displays of Basic Statistical class Description, Mining Association Rules in Large Databases. Association rule mining: mining Single-Dimensional Boolean Association rules from Transactional DatabasesApriori Algorithm, Mining Multilevel Association rules from Transaction Databases and Mining Multi-Dimensional Association rules from Relational Databases.

Classification and Predictions: What is Classification & Prediction, Issues regarding Classification and prediction,Decision tree, Bayesian Classification, Classification by Back propagation, Multi-layer feed-forward Neural Network, Back propagation Algorithm, classification methods K-nearest neighbour classifiers, Genetic Algorithm. Cluster Analysis: Data types in cluster analysis, Categories of clustering methods, partitioning methods.Hierarchical Clustering- CURE and Chameleon. Density Based methods-DBSCAN, OPTICS.Grid Based Methods- STING, CLIQUE. Model Based Method Statistical Approach, Neural Network approach, Outlier Analysis.

Data Warehousing: Overview, Definition, Delivery Process, Difference between Database System and Data Warehouse, Multi Dimensional Data Model, Data Cubes,Stars, Snow flakes, Fact Constellations, Concept hierarchy, Process Architecture, 3 Tier Architecture, Data Marting. Aggregation, Historical information, Query Facility, OLAP function and Tools. OLAPServers, ROLAP, MOLAP, HOLAP, Data Mining interface, Security, Backup and Recovery, Tuning Data Warehouse, Testing Data Warehouse.

Text Books:

1. M.H.Dunham, Data Mining:Introductory and Advanced Topics Pearson Education.
2. Jiawei Han, Micheline Kamber, Data Mining Concepts & Techniques, Elsevier
3. Sam Anahory, Dennis Murray, Data Warehousing in the Real World: A Practical Guide for Building Decision Support Systems, 1/e Pearson Education.
4. Mallach, Data Warehousing System, McGrawHill.

IVIR 140E Virtual Reality

Introduction 1,2: The three Is of virtual reality, Brief history of early VR, Goals & applications of VR, Commercial VR technology, Components of a VR system, Computing architectures.

Input Devices 1: Three-dimensional position trackers, Navigation & manipulation interfaces and Gesture interfaces.

Output Devices 1: Graphics displays, Sound displays and Haptic feedback.

Object and Scene Modeling 1,2,4: 3D Graphics fundamentals, Computer graphics principles for VR, Object and Scene modeling, Model management, LOD management, Geometry representation using triangle Strip & triangle Fan, Collision detection, Special effects: Billboarding, Texturing etc.,

Beyond Virtual: 3D augmented reality interfaces. Designing VR Systems2: Spectrum of VR-ness, Building a VR system, Requirement Engineering & Storyboarding for VR systems, Case study of Virtual Ship Simulator. Exploring VR Programming tools1: Constricting virtual reality applications using either Open scene graph, Java3D or VRML scripting or other open source toolkits (programming assignment). Selection and Manipulation3 (3D Interaction Techniques): 3D Manipulation tasks, Manipulation techniques and Input devices, Interaction techniques for 3D manipulation, Design guidelines.

Travel3 (3D Interaction Techniques): 3D Travel tasks, Travel techniques, Design guidelines.

Wayfinding3 (3D Interaction Techniques): Cognitive processes, User-centered wayfinding support, Environment-centered wayfinding support, Evaluating wayfinding aids, Design guidelines.

Modeling Behavior5: Knowing the environment, Aggregate behavior, Primitive behaviors, Modeling intelligent behavior, Crowd management.

Traditional and Emerging VR applications1,4: Medical; Education, arts and entertainment; Military applications; Emerging applications in Manufacturing, Robotics and Information visualization.

Human Factors in Virtual Reality1,4: Methodology and terminology, user performance studies, VR and Society, VR health and safety issues.

Text Books:

1. G.C. Burdea & P. Coiffet, Virtual reality Technology, Second Ed., Wiley-India.
2. GJ Kim, Designing VR Systems: The Structured Approach, Springer.
3. D.A. Bowman et al., 3D User Interfaces: Theory and Practice, Addison Wesley.
4. John Vince, Virtual Reality Systems, Pearson Ed.
5. Rick Parent, Computer Animation: Algorithms & Techniques, Morgan Kaufmann
6. Course Handouts
7. Selected papers from journals & conferences.

ICRP 140C Introduction to Cryptography

Number Theory and Overview of Cryptography: Introduction, Information security and cryptography, Background on functions, Basic terminology and concepts, Symmetric-key encryption, Digital signatures Authentication and identification, Public-key cryptography, Hash functions, Protocols and mechanisms, Key establishment, management, and certification.

Public-Key Parameters: Introduction, Probabilistic primality tests, (True) Primality tests, Prime number generation, Irreducible polynomials over Zp, Generators and elements of high order.

Pseudorandom Bits and Sequences: Introduction, Random bit generation, pseudorandom bit generation, Statistical tests, and cryptographically secure pseudorandom bit generation.

Stream Ciphers: Introduction, Feedback shift registers, Stream ciphers based on LFSRs and Other stream ciphers. Block Ciphers: Introduction and overview, Background and general concepts, Classical ciphers and historical development, DES, IDEA, RC5 and other block ciphers

Hash Functions and Data Integrity: Introduction, Classification and framework, Basic constructions and general results, Unkeyed hash functions (MDCs), Keyed hash functions (MACs), Data integrity and message authentication, Advanced attacks on hash functions

Unit 6: Identification and Entity Authentication: Introduction, Passwords (weak authentication), Challenge-response identification (strong authentication), Customized and zero-knowledge identification protocolsand Attacks on identification protocols.

Unit 7: Key Management Techniques: Introduction, Background and basic concepts, Techniques for distributing confidential keys, Techniques for distributing public keys, Techniques for controlling key usage, Key management involving multiple domains, Key life cycle issues and Advanced trusted third party services. Key Establishment Protocols: Key Transport and Agreement based on Symmetric and Asymmetric techniques.

Text Books:

1. Handbook of Applied Cryptography, by A. Menezes, P. van Oorschot, and S. Vanstone, CRC Press, 1996. Modern Cryptography: Theory and Practice by Wenbo Mao Hewlett-Packard Company, Prentice Hall PTR 2003.

ICLS 140C Cyber Law and Security Standards

IT Act 2000 with all amendments

ISO/IEC 27001:2013 Context Of The Organization Information Security Leadership Planning An ISMS Support Operation Performance Evaluation Improvement Annex A - List of controls and their objectives

PCI-DSS (Requirements, Security Controls and Process of getting comply)

COBIT 5 Corporate Governance, Enterprise Governance and IT Governance Introduction to COBIT 5 and its evolution COBIT 5 Principles COBIT Enablers Process Reference Model RACI Chart

Introduction of SOX, COSO, HIPAA

Text Books:

1. Data Management for Mobile Computing by Evaggelia Pitoura, George Samaras, Kluwer Academic Publishers, ISBN: 0-7923-8053-3
2. Mobile Database Systems by Vijay Kumar, Wiley Publication, ISBN: 978-0-470-04828-3
3. Research papers

IADC 240C Advanced Cryptography

Overview of Cryptography Introduction, Information security and cryptography, Basic terminology and concepts, Symmetric-key encryption , Digital signatures, Public-key cryptography, Hash functions, Protocols and mechanisms, Key establishment, management, and certification, Pseudorandom numbers and sequences, Classes of attacks and security models.

Mathematical Background Probability theory , Information theory, Complexity theory, Number theory, Abstract algebra, Finite fields, The integer factorization problem, The RSA problem, The Diffie-Hellman problem, Composite moduli.

A quick introduction to groups, rings, integral domain and fields (including: Lagrange theorem, Structure of cyclic and abelian groups, isomorphism theorems). 4- Lectures

Fields, Characteristic of a field, prime fields, Arithmetic of polynomials over fields. Field extensions, Galois group of a field extensions, Fixed field and Galois extensions. Minimum polynomial, Construction of fields with the help of an irreducible polynomial. Splitting field of a polynomial, Separable polynomial and Separable extensions. Construction of finite fields and their structure. Enumeration of irreducible polynomials over finite fields. Fundamental theorem of Galois Theory. 8-Lectures

Cyclotomic extensions, Geometric constructions and Galois theory of Equations (Statement only of Abel Ruffini), Solving Cubic and Bi-quadratic polynomials using radicals. 8-Lectures

Unit 6: Key Establishment Protocols
Introduction, Key transport based on symmetric encryption, Key agreement based on symmetric techniques, Key transport based on public-key encryption, Key agreement based on asymmetric techniques, Secret sharing, Key Management Techniques, Techniques for distributing public keys, Techniques for controlling key usage, Key management involving multiple domains.

Text Books:

1. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography CRC Press
2. Cryptography and Network Security: Principles and Practice (ISBN 0131873164), 4/e, by William Stallings
3. B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition, John Wiley & Sons, 1995.
4. Matt Bishop, Computer Security: Art and Science, Addison-Wesley, 2002.
5. Mihir Bellare and Phillip Rogaway, Introduction to Modern Cryptography
6. Field and Galois Theory, By Patrick Morandi GTM
7. Field and Galois Theory, By J.M. Howie (Paperback)
8. Galois Theory, Lecture notes by Emil Artin
9. Galois Theory, TIFR Lecture notes
10. Galois Theory by H.M. Edward (GTM)
11. Algebra , By M. Artin

INSE 240C Network Security

Introduction to Network security, Model for Network security, Model for Network access security.

Real-time Communication Security: Introduction to TCP/IP protocol stack, Implementation layers for security protocols and implications, IPsec: AH and ESP, IPsec: IKE.

Media- Based-Vulnerabilities, Network Device Vulnerabilities, Back Doors, Denial of Service (DoS), Spoofing, Man-in-the-Middle, and replay, Protocol-Based Attacks, DNS Attack, DNS Spoofing, DNS Poisoning, ARP Poisoning, TCP/IP Hijacking .

Virtual LAN (VLAN) , Demilitarization Zone (DMZ) , Network Access Control (NAC), Proxy Server , Honey Pot , Network Intrusion Detection Systems (NIDS) and Host Network Intrusion Prevention Systems Protocol Analyzers, Internet Content Filters, Integrated Network Security Hardware .

Authentication: Kerberos, X.509 Authentication Service, Scanning: Port Scanning, Port Knocking- Advantages, Disadvantages. Peer to Peer security.

Unit 6: Electronic Mail Security: Distribution lists, Establishing keys, Privacy, source authentication, message integrity, non-repudiation, proof of submission, proof of delivery, message flow confidentiality, anonymity, Pretty Good Privacy (PGP)

Unit 7: Firewalls and Web Security: Packet filters, Application level gateways, Encrypted tunnels, Cookies. Assignments on latest network security techniques, Security applications in wireless sensor network and wireless Communication networks

Text Books:

1. Mark Ciampa Security + Guide to Network Security Fundamentals/Edition 3 Cengage Learning publisher, ISBN-10: 1428340661 ISBN-13: 978-1428340664
2. William Stallings, Cryptography and Network Security Principles and Practices, Prentice Hall of India, Third Edition, 2003.

Reference Books:

1. Cisco: Fundamentals of Network Security Companion Guide (Cisco Networking Academy Program).
2. Saadat Malik, Saadat Malik. Network Security Principles and Practices (CCIE Professional Development). Pearson Education. 2002. (ISBN: 1587050250)

ITRA 240E **Technical Risk Assessment**

Introduction: Risk, Risk Assessment, Risk Management: Planning, Risk Identification, Assessment Severity, cost, Analysis Prevent, Mitigate, Closure, Tracking, Management, Reporting. Risk types, Why Risk Management? And Risk Management Effectiveness, IT (security) Risk Assessment.

Vulnerability Assessment: Vulnerability, Source of Vulnerability, Vulnerability Assessment, Vulnerability Management, Types of Vulnerability Assessment, Common Vulnerability Scoring System (CVSS), Why CVSS?

CVSS: Base Metrics, Access Vector, Access Complexity, Authentication, Confidentiality Impact, Integrity Impact and Availability Impact. Temporal Metrics: Exploitability, Remediation Level and Report Confidence. Environmental Metrics: Collateral Damage Potential, Target Distribution, Confidentiality Requirement, Integrity Requirement and Availability Requirement.

CVSS Assessment: CVSS Assessment Version 1.0, Base Metrics, Temporal Metrics and Environmental Metrics, Drawback and Need for next version, Case Study vulnerabilities CVSS Evaluation Version 2.0, Base Metrics, Temporal Metrics and Environmental Metrics, Case Study with vulnerabilities

Risk Assessment: Estimating Risk- Risk Assessing via CVSS, FAIR, CRAMM. Comparison of different of Risk Assessment Techniques. Report Preparation and Assessment Templates. Post-Assessment Activities. Case Study with the vulnerabilities.

Reference:

1. 1.Peter Mell, Karen Scarfone and Sasha Romanosky, A Complete Guide to the Common Vulnerability Scoring System Version 2.0, http://www.first.org/cvss/cvss-guide.html.

Lab:

1. Tools: Metasploit, Backtrack and Nessus
2. Test: Penetration and Vulnerability Testing

ICFN 240E Computer Forensics

Understanding Computer Investigation, Computer Forensics Tools and Lab Setup, Processing Crimes and Incident Scenes, Digital Evidence Controls, File Systems of different OS.

Data Acquisition, Computer Forensics Analysis, Recovering Image Files, Network Forensics, Email Investigation, Relevant Law and The Role of Computer Forensics in Courts.

Text Books:

1. Computer Forensics and Investigations, Bill Nelson, Amelia Philips
2. A Step-By-Step Guide To Computer Attacks And Effective Defenses, Skoudis, E., Perlman, R. Counter Hack: Prentice Hall Professional Technical Reference. 2001.
3. Incident Response & Computer Forensics,2nd Edition, Mandia, K, Prosise, C, Pepe, M Osbourne-Mcgraw Hill, 2003.

IIAM 240E Identity and Access Management

Introduction to Identity, Digital Identity, Digitial Identity Life cyle and Integrity, Non-repudiation & confidentiality, Access Management and IAM architecture.

Authentication: Single Sign on, Session Management, Password Service and Strong Authentication.

Authorization: Role based, Rule based, Attribute based and Remote Authorization (RADIUS).

User Management: Delegated Administration, User and Role Management, Provisioning, Password Management and Self-Service.

Central User Repository: Directory, Data Synchronization, Meta-Directory and Virtual Directory.

Interoperability Standards, Federating Identity, Identity Maturity Models and Process Architecture, Identity Data Architectures, Interoperability Frameworks for Identity, Identity Policies, Identity Management Reference Architectures, Building an Identity Management Architecture.

Reference Books:

1. Digital Identity by Phillip J. Windley, Publisher: O'Reilly Media. Reference Web source: IAM web Resource from GAMATECH and other sources

ISAC 240E Security Architecture

Role and importance of security policy Network-related security threats and solutions Learn fundamentals of cryptography Principles of private- and public-key encryption, including number-theoretic foundations Principles of authentication Unit 6: Internet Protocol security architecture (IPSEC) Unit 7: Appreciate network security threats and countermeasures Unit 8: Gain hands-on experience with programming techniques for security protocols Unit 9: Obtain background for original research in Network Security Unit 10: Designing of server networks infrastructure Unit 11: Security Models

Text Books:

1. Network Security - Private Communication in a Public World by Charlie Kaufman, Radia Perlman and Mike Speciner
2. Computer Security by Dieter Gollmann
3. Computer security : art and science by Matt Bishop.
4. Cryptography and Network Security : Priciples and Practice by William Stallings.
5. Information security : principles and practices by Mark Merkow and Jim Breithaupt.
6. Charles P.Pfleeger, Security in Computing, Fourth Edition, Pfleeger Consulting Group, RAND corporation, Prentice Hall.
7. Shon Harris, CISSP Exam Guide Fourth Edition, McGraw Hill.

IISA 240E Information Security Audit

Introduction: What is Computer Auditing, How to Audit Computer Security: System Access Control, Data Access Control, System & Security Administration, System Design; Hardware Security Auditing, Software Security Auditing and controls - internal auditing-practical approach-writing simple auditing programs. Security Policies

Database Security Auditing: Audit Trail: Who logs in, Which Files, What Activities; Comparison of Database and Operating System Access, Field checks, Change logs, Integrity checks, User authentication, Precision checks, Access Control Procedures.

Network & Telecommunication Security Auditing: Confidentiality, Accuracy & Integrity, Authenticity of user, Availability; Tools: encryption, trusted system processing, and firewalls. Detect: security violation, misrouted data, components failure, and signal interception.

Microcomputer Security Auditing: Audit Trail, Auditing Virus Infection, Performing a security Audit; Issue: Future trends, challenges.

Auditing with ISO/IEC 27001: 2013

Knowledge of ISO/IEC 27001:2013, Controls and Objectives, Mapping with Controls, Gap Analysis, Writing Conformities and Non Conformities.

IOSS 340E Operating System Security

Introduction Secure Operating system, Security goals, Trust Model, Threat Model, Protection System, Reference Monitor.

Security in operating system Unix Security and Windows Security.

Security Kernel Secure Communication Processor

Secure Virtual Machine Systems

Securing Commercial Operating System

Case Study : Building a secure operating system for Linux

Case Study : Solaris trusted extension

Security issues in sandboxing designs: design and analysis of Android

Text Books:

1. Trent Jaeger, Operating System Security (Synthesis Lectures on Information Security, Privacy, and Trust), Morgan and Claypool publishers, 2008.

References:

1. Chaudhuri, Avik, Language-based security on Android in Proceedings of the ACM SIGPLAN Fourth Workshop on Programming Languages and Analysis for Security (PLAS 09), 2009, Dublin, Ireland, pp 1-7

2. William Enck, Machigar Ongtang and Patrick McDaniel, Understanding Android Security, IEEE Security and Privacy, Vol 7, 2009,pp.50-57.

IBCP 340E Business Continuity Planning and Disaster Recovery Planning

Business Continuity Planning

Introduction Analysis Impact analysis Threat analysis Definition of impact scenarios Recovery requirement documentation Solution design Implementation Testing and organizational acceptance Maintenance Information update and testing Testing and verification of technical solutions Testing and verification of organization recovery procedures Treatment of test failures

Disaster Recovery Planning

Business data protection Preventions against data loss No off-site data Possibly no recovery Data backup with no hot site Data backup with a hot site Electronic vaulting Point-in-time copies Transaction integrity Zero or near-Zero data loss Highly automated, business integrated solution