I SEMESTER

MAT-511 COMPUTATIONAL METHODS AND STOCHASTIC PROCESSES

[3 1 0 4]

Probability and distribution, Stochastic processes and Queuing theory, Optimization Techniques. Numerical solutions to BVP's by finite difference and finite element methods. Solution of parabolic, elliptic, hyperbolic PDEs: Linear Algebra, Eigen values, Eigen vectors, Matrix computation and SVD.

References:

1. A Papoulis and S.U.Pillai, "Probability, Random Variables and Stochastic Processes", McGraw Hill.
2. P.Z.Peebles Jr., "Probability, Random Variables and Random Signal Principles", McGraw Hill.
3. S.C Chapra and RP Canale, "Numerical Methods for Engineers", Tata McGraw Hill.

CSE-521 DISTRIBUTED COMPUTING SYSTEMS

[3 1 0 4]

Introduction to Distributed Computing Systems, Evolution and models of Distributed Computing System, Introduction and issues in Designing a Distributed Operating System, Distributed Computing Environment (DCE), High-level protocols. Distributed shared memory Introduction, Design and implementation issues, Consistency models. CORBA Case Study : CORBA services. Threads, Virtualization, Clients, Servers, Code migration. Distributed Object-Based Systems Architecture, Processes, Communication, Naming, Synchronization, Consistency and replication. Adaptive fault-tolerance, Fault detection and location in real-time systems. Security Engineering, Protocols, Hardware protection, Cryptography: The Random Oracle model, Symmetric and Asymmetric Crypto-primitives, Modes of operations, Hash functions, Dependability concepts, Byzantine failures, Fault injection, Fault-tolerant techniques, performability metrics. Issues of Survivability, Emission Security: Introduction, Technical Surveillance and countermeasures, Passive Attacks, Active Attacks. Information warfare.

References:

1. Pradeep. K. Sinha, "Distributed Operating Systems: Concepts and Design**"**, PHI, 2007.
2. Andrew S. Tennenbaum, and Maarten Van Steen, "Distributed Systems", PHI, 2008.
3. George Coulouries, Jean Dollimore, Tim Kindberg "Distributed Systems Concepts and design" III Edition, Pearson Education Asia, 2004.
4. Ross J Anderson and Ross Anderson, "Security Engineering: A guide to building dependable distributed systems", Wiley, 2001.
5. Relevant research paper from the journals.

CSE-523 NUMBER THEORY & CRYPTOGRAPHY

[3 1 0 4]

Introduction Historical Perspective, Modern Cryptography. Background Theory Elements of Number Theory, Algebraic Structures in Computing, Complexity of Computing. Private Key Cryptosystems Classical ciphers, DES family, Modern private key cryptographic algorithms. Public Key Cryptosystems Concept of public key cryptography, RSA cryptosystems, Elliptic cryptosystems, Probabilistic encryption. Pseudorandomness Number generators, Polynomial indistinguishability, RSA Pseudorandom bit generators, next bit test, Pseudorandom function generators, Pseudorandom function generators, Super pseudo random permutation generators. Hashing Properties of hashing, Birthday paradox, Serial and parallel hashing, Theoretic constructions, Hashing based on Cryptosystems, MD5, Keyed hashing. Digital Signatures Properties of digital signatures, Generic signature schemes, RSA signatures, Blind signatures, Undeniable signatures, Fail-stop signatures, Timestamping. Authentication Active opponents, Model of authentication systems, Information theoretic bounds Zero-Knowledge Proof Systems. Interactive proof systems, perfect Zero-Knowledge proofs, Computational zero knowledge proofs.

References:

1. J. Pieprzyk, T. Hardjono and J. Seberry, "Fundamentals of Computer Security", Springer International Edition, 2003.
2. S. Vaudenay, "A Classical Introduction to Cryptography: Applications for Communications Security", Springer International Edition, 2006.
3. W. Mao, "Modern Cryptography Theory and Practice", Pearson Education Ltd., 2005.
4. N. Koblitz, "Course on Number Theory and Cryptography", Springer Verlag 1986.
5. A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.
6. I. Niven, H. S. Zukerman and H. L. Montgomery, "An Introduction to the Theory of Numbers", Fifth edition, Wiley, 1991.
7. Relevant research paper from the journals.

CSE-503 ADVANCED COMPUTER NETWORKS

[3 1 0 4]

Brief Overview of TCP/IP suite of protocols- IP, ARP, ICMP, UDP, TCP, SMTP, FTP, HTTP. IPv6 and ICMPv6- basic protocol, extensions and options, support for QoS, security, etc., neighbor discovery, auto-configuration, routing, Changes to other protocols. Application Programming Interface for IPv6, Message Format, Error Messages, Informational Messages Neighbor Discovery, Address Resolution, Router Discovery, Redirection, Group Membership, ICMPv6 Autoconfiguration, MAC protocols for high-speed LANS, MANs, and wireless LANs- DQDB, HIPPI, Gigabit Ethernet, Wireless Ethernet Fast access technologies: ADSL, Cable Modem, etc. Optical Networks: WDM, Wavelength routing, LightPaths/Lighttrails, Wavelength conversion and rerouting, Network Survivability and Provisioning, IP over DWDM, Next generation Optical Networks: Optical Circuit Switching, Optical Burst Switching, Optical Packet Switching, Multi-Protocol Label Switching (MPLS): MPLS Architecture and related protocols,

Traffic Engineering (TE) and TE with MPLS, Transport protocols and congestion control, Quality of Service (QoS) with MPLS technology, Network recovery and restoration with MPLS technology, Voice over IP(VOIP):VOIP protocols: overview of H323 and SIP(session initiation protocol).Overview of VOIP call flows, IVR calls ,Advanced Routing and switching: Review of networking devices, routing and switching, VLAN, VTP, STP, Distance Vector Routing: RIP, algorithm, routing table format, routing update format, Link State Routing: OSPF, algorithm, routing table format, routing update format

References:

1. W. R. Stevens. TCP/IP Illustrated, Volume 1: The protocols, Addison Wesley, 1994.
2. TCP/IP Protocol Suite, Behrouz A.Forouzan, Tata McGraw Hill 4th Edition, 2010.
3. G. R. Wright and W. R. Stevens."TCP/IP Illustrated", Volume 2: The Implementation, Addison Wesley, 1995.
4. W. R. Stevens. TCP/IP Illustrated, Volume 3: TCP for Transactions, HTTP, NNTP, and the Unix Domain Protocols, Addison Wesley, 1996.
5. Peter Loshin. IPv6 Clearly Explained, Morgan Kauffman, 1999.
6. M. Gonsalves and K. Niles. IPv6 Networks, McGraw Hill, 1998.
7. Bruce S. Davie, Adrian Farrel,MPLS: Next Steps,Morgan Kaufmann, 2008
8. RFCs and Internet Drafts, available from Internet Engineering Task Force.
9. Articles in various journals and conference proceedings.
10. Krishna M.Sivalingham, Suresh Subramaniam,Emerging Optical Network Technologies,Springer,2004
11. Relevant research papers from the journals

CSE-525 SECURITY ARCHITECTURE-DESIGN & ANALYSIS

[3 1 0 4]

Introduction Security System Development and Operation Overview, Security Programming. Architecting secure software systems. Building secured systems, Security requirement analysis, Threat modeling, Security design, Security coding, Safe programming, Security review, generating the executable, Security testing, Secured deployment, Security remediation, Security documentation, Security response planning. Designing secure networks. Device hardening, General design considerations, Identity design considerations ,Wireless LANs, IP telephony. E-mail, DNS, HTTP, FTP, IP sec VPN Design consideration, Other security options, Topology considerations, site-to-site deployment example, IP sec outsourcing. Security threat analysis, Threat profile and risk analysis, web service security model, Threat identification, Threat analysis. Campus security design – A Case study,

References:

1. Sean Convey "Network Security Architectures", Pearson Education, 2004.
2. Asoke K Talukdar and Manish Chaithanya "Architecting secure Software Systems", CRC Press, 2009.
3. Joseph Migga Kiizza "A Guide to Computer Network Security Model", Springer International Edition, 2009.
4. Relevant research papers from the journals

.

HSS-501 RESEARCH METHODOLOGIES AND TECHNICAL COMMUNICATION.

[1 0 3 2]

Mechanics of Research Methodology - Types of Research, Significance of research, Research framework, Case study method, Experimental method, Sources of data, Data collection using questionnaire, Interviewing and experimentation. Research formulation-Components, selection and formulation of a research problem, Objectives of formulation, and Criteria of a good research problem. Research hypothesis – Criterion for hypotheses construction, Nature of hypotheses, need for having a working hypothesis, Characteristics and Types of hypothesis, Procedure of hypotheses testing. Sampling Methods Introduction to various sampling methods and their applications. Data Analysis–Sources of data, Collection of data, Measurement and scaling technique, and Different techniques of Data analysis. Thesis Writing and Journal Publication-Writing thesis, Writing journal and conference papers, IEEE and Harvard styles of referencing, Effective presentation, Copyrights, and avoiding plagiarism.

References:

1. Dr.Ranjit Kumar, "Research Methodology: A Step-by-Step Guide for Beginners", SAGE,2005
2. Geoffrey R. Marczyk, David DeMatteo & David Festinger, "Essentials of Research Design and Methodology", John Wiley & Sons, 2004.
3. John W.Creswel, "Research Design : Qualitative, Quantitative, and Mixed Methods Approaches", SAGE 2004
4. Suresh C.Sinha and Anil K.Dhiman, "Research Methodology (2 Vols-Set)",Vedam Books, 2006.
5. C.R.Kothari, "Research Methodology: Methods and Techniques", New Age International Publisher, 2008.

CSE- 531 INFORMATION SYSTEMS LAB I

[0 0 6 2]

Experiments/mini project based on the syllabus specified in Advanced Computer Networks, Cryptography and Security Architecture.

II SEMESTER

CSE-501 ADVANCED CONCEPTS IN DATA BASE MANAGEMENT SYSTEMS

[3 1 0 4]

Overview of Relational Model, Query Processing - Measures of Query Cost, Selection Operation, Sorting, Join Operation, Other Operations, Evaluation of Expressions. Query Optimization - Transformation of Relational Expressions, Estimating Statistics of Expression Results, Choice of Evaluation of Plans, Materialized Views, Physical DB Design and Tuning. Object and Object Relational Databases - Complex Data Types, Implementing Object and Object-Relational Features, SQL3, Parallel Databases - Database System Architectures, I/O Parallelism, Data Partitioning, Interquery, Intraquery, Intraoperation and Interoperation Parallelisms. Distributed Databases - Distributed data storage, Transactions, Commit Protocols, Concurrency Control, Availability, Query Processing. Data Warehouse and OLAP Technology, Semi Structured Data and XML - Structure of XML data, XML document schema, Querying and Transformation, Storage of XML data. Other Emerging Database Technologies and Applications

References:

1. Silberschatz, Korth and Sudarshan, "Database System Concepts", McGraw Hill, Sixth Edition, 2011.
2. Ramez Elmasri and S B Navathe, "Fundamentals of Database Systems", Pearson Education, Fifth Edition , 2007.
3. Thomas Connolly, Carolyn Begg, "Database Systems – A Practical Approach to Design, Implementation and Management", Pearson Education, 3rd Edition, 2003.
4. Ramakrishnan and Gehrke, "Database Management Systems", McGraw Hill, Third Edition, 2003.
5. Relevant research papers from the journals

CSE-524 NETWORK SECURITY

[3 1 0 4]

Network Attacks, Types of Attacks, Model for Internetwork Security. Firewalls, Packet filters, Application gateways, Circuit level Gateways, Stateful packet inspection, Security advantages of SPI, Implementation methods. Advanced Firewall Functionality., System Security. Intruders. Malicious Softwares: IPsec IPv4 and Ipv6., SKIP, IKE phases, Phase 1 IKE: Session Keys, Message IDs, Phase 2/Quick Mode, Traffic selectors, IKE Phase 1 protocols, Phase-2 IKE: Setting up IPsecs SAs, ISAKMP/IKE Encoding: Fixed Header, Payload of ISAKMP Messages, SSL/, SSL/TLS Basic protocol, Session resumption, Computing the keys, Client authentication, PKI as deployed by SSL, Version Numbers, Negotiating cipher suites, Negotiating compression method, Attacks fixed in v3, Exportability, Encoding. PGP (Pretty Good Privacy) Signature Types, Key rings, Anomalies and Object formats. Kerberos V4, Realms, Interrealm authentication, Key version numbers, Encryption for privacy and Integrity, Encryption for Integrity Only, Network Layer addresses in tickets, Message formats. Kerberos V5 ASN.1, Evading password Guessing attacks, Key Inside Authenticator, Double TGT Authentication, PKINIT-Public Key for Users, KDC Database, Kerberos V5 Messages

References:

1. William Stallings, "Network Security Essentials: Applications and Standards" Pearson Education, 4th edition, 2010
2. Keith E. Strassberg, Richard J. Gondek, GaryRollie, "Firewalls - The Complete Reference", Tata McGraw-Hill Edition, 2003
3. Charlie Kaufman , Radia Perlman, Mike Speciner, "Network Security Private Communication in Public World", PHI Ltd, 2nd Edition, 2002
4. Atul Kahate, "Cryptography and Network Security" Tata McGraw Hill, 2007
5 Relevant research papers from the journals

CSE-532 INFORMATION SYSTEMS LAB-II

[0 0 6 2]

Experiments/mini project based on the syllabus specified in Elective I and Elective III.

CSE-514 SEMINAR [0 0 3 1]

Each student has to present a seminar individually, on any technical topic related to the subject, but not covered in the syllabus. The time duration for presentation is 45 minutes and 15 minutes is devoted for question and answer session. Slides have to be prepared for the presentation. A seminar report has to be submitted one week before the day of the presentation.
Ref. Materials : IEEE transactions, Technical journals, Proceedings of National and International Conferences, Web sites.

PROGRAM ELECTIVES

CSE 505 OBJECT ORIENTED SYSTEM DEVELOPMENT

[3 1 0 4]

Introduction to information systems, Object Basics: encapsulation, Association and Aggregation, Inheritance, Dynamic and static type systems, Polymorphism, Dynamic Binding. Software development Methodologies, Requirements: Business perspective, Developer perspective. Introduction to OOAD with UML 2.0: structure diagrams, behavior diagrams, extension mechanisms Analyzing the problem: static and dynamic analysis, Designing the system architecture: priorities, system design, concurrency, security, Choosing technologies, typical front end configurations, back-end configurations. Designing subsystems: mapping the analysis class model into the design class model, handling persistence with a relational database, designing user interfaces, using patterns, frameworks and libraries, handling multiple activities. Reusable design

patterns: patterns template, common design patterns. Specifying the interfaces of classes. Testing: automating tests, testing strategies, test driven development using JUnit.

References:

1. Mike O'Docherty, "Object-Oriented Analysis & Design- understanding System Development with UML 2.0", Wiley India Pvt. Ltd., 2010.
2. A. Dennis, B.H. Wixom and D. Tegarden, "Systems analysis and Design with UML version 2.0- an object oriented approach", Second edition, Wiley India Edition, 2006
3. Ali Bahrami, "Object Oriented Systems Development using the unified modeling language", McGraw Hill International Edition, 1999.
4. UML 2.0 Superstructure - Final Adopted Specification. Object Management Group, 2003 http://www.omg.org/docs/ad/03-08-02.pdf.
5. Relevant research papers from the journals

CSE-540 ADVANCED DATA STRUCTURES AND ALGORITHMS

[3 1 0 4]

Amortized Analysis - Aggregate analysis, The accounting method, The potential method, Dynamic Tables B-Trees - Definition of B-Trees, Basic operations on B-Trees, Deleting a key from a B-Tree. Binomial Heaps - Binomial trees and Binomial heaps, Operations on Binomial heaps. Fibonacci Heaps - Structure of Fibonacci heaps, Mergeable heap operations, Decreasing a key and deleting a node. Data structures for Disjoint sets – Disjoint-set operations, Linked-list representation of disjoint sets, Disjoint set forests. Minimum Spanning trees - Growing a minimum spanning tree, the algorithms of Kruskal and Prim Single-source Shortest Paths - The Bellman-Ford algorithm, Single-source shortest paths in directed acyclic graphs, Dijkstra's algorithm. All-Pairs Shortest Paths - Shortest Paths and matrix multiplication, The Floyd-Warshall algorithm, Maximum Flow - Flow Networks, The Ford-Fulkerson method, Maximum bipartite matching

References:

1. Cormen T.H., Leiserson C.E, Rivest R.L. and Stein C. "Introduction to Algorithms" Prentice-Hall India, Second Edition, 2001.
2. Baase Sara and Gelder A.V - Computer Algorithms – "Introduction to Design and Analysis", Pearson Education, Third Edition, 2000.
3. Relevant research papers from the journals.

CSE-542 DATA MINING AND BUSINESS ANALYTICS

[3 1 0 4]

Introduction to Business Intelligence, Basics of Data Integration ,Introduction to Multi-Dimensional Data Modeling, Basics of Enterprise Reporting**,** Data Mining functionalities Major issues in Data Mining, Applications and Trends in Data Mining, Association Rules Mining, Algorithms for discovering frequent itemsets, Mining various kinds of association rules, classification and Prediction , Clustering Analysis, Interactive Visual Data Analysis Sensing and Analyzing Univariate Data, Sensing and Analyzing Time Series Data

References:

1. Jiawei Han and Micheline Kamber, Data Mining: Concepts and Techniques, Second Edition, Elsevier
2. Michael Berry and Gordon Linoff, *Data Mining Techniques*, Wiley Publishing, 2004.
3. Kimball and Ross, The Data Warehouse Toolkit, Second Edition, John Wiley & Sons, 2002.
4. T. Davenport, "Competing on Analytics," Harvard Business Review (Decision Making), January 2006.
5. Fundamentals of Business Analytics by R.N Prasad , Seema Acharya
6. Business Intelligence by David Loshin
7. Business intelligence for the enterprise by Mike Biere
8. Business intelligence roadmap by Larissa Terpeluk Moss, Shaku Atre
9. An introduction to Building the Data Warehouse – IBM
10. Business Intelligence For Dummies – Swain Scheps
11. Successful Business Intelligence: Secrets to making Killer BI Applications by Cindi Howson
12. Information dashboard design by Stephen Few

CSE-546 SECURE E-COMMERCE

[3 1 0 4]

Introduction to eCommerce: Illustration, eCommerce framework, Media Convergence, Anatomy of eCommerce application, Types of e Commerce: Interorganizational, intra organizational, C2B eCommerce, Communication Security goals; Consumer Oriented e Commerce: Major components of eCommerce, E commerce privacy policy, Network security policy, Firewall security policy, Requirements of transaction security, E commerce encryption, Mercantile Process Models: Illustration with case study; Digital Money Security Payment Transaction, Electronic Security basics, Limitation of eCommerce Security measures; Electronic Payment System: Limitations of traditional payment systems, Types of electronic payment systems, Digital token based system, Smartcard, Credit card based payment systems, eCash/e Cheques, Risk and e Payment system. Automatic Teller Machine[ATM], ATM encryption, ATM fraud and Consequences for bankers; Security services: Payment transaction Security, Anonymity, Transaction untracebility, Confidentiality of payment transaction, Secure e Transaction [SET], Consumer, Legal, Business issues, Illustration with case discussion; Essentials of Crypto: Encryption Building blocks, Random Key generation, Properties of good crypto algorithm and their selection, Digital Signature, Public Key certificates; Illustration of e Commerce: Electronic Data Interchange [EDI], Supply Chain Management [SCM] fundamentals-Models-Elements, Online sales force automation, Software agents-Characteristics, technology, Telescript Agent Language; E commerce and online publishing: Strategies, Approaches, Illustration, Digital copyright protection methods, Charting the online marketing process, Illustration with an example; Consumer search and resource discovery: Paradigms, Information filtering and retrieval; Mobile commerce: Wireless communication, WAP programming model; Customer effective web design: Illustration and Illustration with case study.

References:

1. Ravi Kalakota and Andrew Whinston –"Frontiers Electronic Commerce", 2nd Edition, Addison-Wesley,1999
2. P.T.Joseph, S.J, "E Commerce", Prentice Hall, 2nd Edition, 2008
3. Anup Gosh, "E-Commerce Security and Privacy", 2001
4. Relevant research papers from the journals

CSE-562 WEB SERVICES

[3 1 0 4]

Introduction to XHTML and Javascript, XML Concepts: What is XML, XML Elements and Attributes, XML Document Structure, Elements and Attributes Structure, XML Namespaces, XML Data Validation, XML 1.1 new features. XML Documents: XML document structure and Syntax, XML Namespaces, Element name tips. XML Data Format and Validation: XML parsers for data validation, Document Type Definitions, W3C XML Schemas. XML Parsing Concepts: Parsing XML with Document Object Model (DOM), Parsing XML with Simple API for XML(SAX) XSLT concepts and XSL transformations ,XForm, XML and Data Binding : DSOs, Storing and Binding data in HTML, Navigation from record to record, Binding XML data, Using DATA islands, Extracting data from DSO, Binding XML data into HTML tables. XML and Jscript: Reading Xml and Extracting data from it, Creating a DOM Document Object , Getting a Document's Document Element, Searching for XML Elements by name, Extracting Data from XML attributes. Xquery and usage of Xquery functions. Building Blocks of Web Services: Design of Information system, Architecture of an Information system, Middleware: Understanding Middleware, RPC and related Middleware, TP Monitors, object Brokers, Message Oriented Middleware, Web Service concept, SOAP, WSDL, UDDI. Microsoft.NET and Web Services: Creating and deploying .NET Web Services, Accessing .NET Web Services, Building a .NET Web Services Client. Advanced Web Services: Accessing Relational Data via Web Services, Authentication and Security for Web Services. Semantic Web – A layered approach, Semantic Web Technologies.

References:

1. XML—A Beginner's Guide by Steven Holzner, Tata Mcgraw Hill Edition 2009 (ISBN-13: 978-0-07-014699-0, ISBN-10:0-07-014699-3)
2. Web Services Concepts , Architectures and Applications by Gustavo Alonso, Fabio Casati, Harumi Kuno, Vijay Machiraju by Springer (First Indian Reprint 2009, ISBN: 978-81-8489-170-6)
3. XML 1.1 (covering J2EE, Java, Databases, Web Services and .NET) Programming Bible by Brian Benz with John R.Durant, WILEY Publishing Inc., First edition 2003
4. XML: How to Program, by Deitel, Deitel, Nieto, Lin and Sadhu, Prentice Hall. (new edition is still not out)
5. Web Services: A Technical Introduction: Deitel, Deitel, DuWaldt, and Trees, Prentice Hall. (gives a good perspective of web services)
6. Essential XML Quick Reference: A Programmer's Reference to XML, XPath, XSLT, XML Schema,
7. SOAP, and More by Aaron Skonnard, Martin Gudgin (Paperback)
8. The Official XMLSPY Handbook by Larry Kim (Paperback - February 2003)
9. Microsoft .NET for Programmers by Fergal Grimes (Paperback - January 2002)
10. ASP.NET: The Complete Reference by Matthew Macdonald, Robert Standefer.

11. A Semantic Web primer by Grigoris Antoniou and Frank van Harmelen, PHI 2nd Edition (ISBN: 978-81-203-4054-1)
12. Relevant research papers from the journals

CSE-566 PUBLIC KEY INFRASTRUCTURE (PKI) AND TRUST MANAGEMENT

[3 1 0 4]

Introduction, The Concept of Public Key Infrastructure, PKI services, Trust Models -Strict and Loose Hierarchy of Certification Authorities, Policy-Based Hierarchies, Distributed Trust Architecture, Four-Corner Trust Model Web Model, User-Centric Trust, PKI Data structures, Cross-Certification, Entity Naming, Certificate Path Processing, PKI interoperability; PKI-Enabled Services, Secure communication, secure time stamping, Notarization, Non-repudiation, Privilege Management, Mechanisms Required to create PKI-Enabled Services, Operational Considerations; Certificates and Certification, Certificates, Certificate Policies, Certificate Authority, Registration Authority; PKI Information Dissemination-Private Dissemination, Publication and Repositories, Interdomain Repository Issues and Options, In-band Protocol Exchange; PKI Operational Considerations- Client-Side Software, Off-line Operations, Physical Security, Hardware Components, User Key Compromise, Disaster Preparation and Recovery;Electronic Signature Legislation and Considerations; Major Standards and PKI Interoperability- X.509, PKIX, X.500, LDAP, ISO TC68, ANSI X9F, S/MIME, IPsec, TLS, SPKI, OpenPGP EDIFACT, IEEE, WAP, XML-Based Activities, Other Activities; Deployment Considerations-Draft a certificate policy, Establishing policy mappings and constraints, Local certificate and CRL profiles, Select a PKI product or Service provider, Certification Practice Statement, Critical Deployment issues, Apply for a Licenses Certification Authority, PKI Deployment case studies. PKI Operation Risks Verifying identity, Certificate content, Certificate creation, Distribution, and Acceptance, Internal security concerns, Managing Digital Certificates.

References:

1. Carlisle Adams, Steve Lloyd, "Understanding PKI: Concepts, Standards, andDeployment Considerations", Second Edition, Addison Wesley, 2002
2. Ashutosh Saxena, "Public Key Infrastructure- Concepts, Design and Deployment", TMH.
3. Request For Comments- RFC2510, RFC 2559, RFC 3280, RFC 3379, RFC 3647, RFC 4158, RFC 4476 etc.
4. Relevant research papers from the journals

CSE-568 DATABASE AND APPLICATION SECURITY

[3 1 0 4]

Introduction to databases - Concept of database, Components of the database, Distributed databases - Challenges, Operating system support, Distributed file systems, Fault tolerance and Failure Recovery, Distributed Shared Memory. Database Security - Need for database security, SQL injection, Database security evolution, Multilevel Security in databases, Architectural Components and Security, Secure connectivity to the database, Role based access Control, Security based on Object oriented Encapsulation, Reliability and Integrity, Sensitive Data, DB

Inference, Database Auditing, Multilevel Databases, Data Mining - Privacy and Sensitivity, Data correctness and Integrity, Availability of Data. Protocols Password Eavesdropping Risks, Challenge and response, Manipulating the messages, changing the environment, Chosen protocols attacks, Managing the encryption keys, Banking and Bookkeeping -How Bank Computer Systems Work, Wholesale Payment Systems, biometrics controls for protecting information systems assets, Automatic Teller Machines Monitoring Systems Introduction, Alarms, Prepayment meters, Taximeters, Techographs and Truck speed limiters. Nuclear command and Control - The Kennedy Memorandum, unconditionally secure Authentication codes, Shared Control Schemes, Tamper Resistance. Emission Security - Technical and Surveillance and Countermeasures, Passive Attacks, Active attacks, How Serious are Emsec Attacks? Telecom System - Security Attacks on Metering, Signaling, Switching and Configuration, Mobile phone Cloning, GSM security , Corporate Fraud. Case Studies on Security Single Sign On(SSO), Secure Inter branch Payment Transactions, Denial of Service Attacks, Contract signing, Secret splitting, Virtual Elections, Secure Multi Party Calculation, Cookies and Privacy.

References:

1. Ross Anderson "Security Engineering: A guide to Building Dependable Distributed Systems", Wiley Computer Publishing-2001
2. Charles P. Pfleeger, Shari Lawrence Pfleeger – "Security in Computing", fourth Edition, Prentice Hall of India Private Limited-2008
3. George Coulouris-"Distributed Systems concepts and Design", 3rd Edition, Low Price Edition , Pearson education-2006
4. Atul Kahate- " Cryptography and Network Security", Second Edition. Tata McGraw-Hill Publishing Company Limited- 2008
5. Jay Ramachandran-"Designing Security Architecture Solutions", Wiley Computer Publishing, First Edition-2002
6. Relevant research papers from the journals

CSE-570 INTRUSION DETECTION SYSTEMS

[3 1 0 4]

Introduction: The history of Intrusion Detection. Concepts and Definitions: Security Concepts, Intrusion Detection Concepts. Information Sources: Host-Based Information Sources, Network-Based Information Sources, Information from other Security Products. Analysis Schemes: Definitions, Goals, a Model for Intrusion Analysis, Techniques. Responses: Requirement for Responses, Types of Responses, Covering Tracks during Investigation, Mapping responses to policy. Technical Issues: Scalability, Management, Reliability, Analysis issues, Interoperability, Integration, User Interfaces. Understanding the Real -World Challenge: The roots of Security Problems, Through a Hackers, Eye's, Security versus traditional engineering, Rules for Intrusion Detection Systems. For Users: Determining your requirements, making sense of products, mapping policy to configurations, incident handling and investigation. For Designers: Requirements Security design principles, surviving the design process, Painting Bulls Eye, Advice from Trenches. Future Needs: Future Trends in Society, Technology, Security, A vision for Intrusion Detection. Extrusion Detection: Why Extrusion detection?, Defining the Security Process, Security Principles, Network Security Monitoring Theory, Network Security Monitoring Techniques, Network Security Monitoring Tools. Defensible network architecture: Monitoring and Controlling and minimizing Defensible network, keeping the defensible network current. Extrusion detection illustrated: Intrusion detection and extrusion detection defined, extrusion detection through NSM.

References:

1. Rebecca Gurley Bace, "Intrusion Detection", Macmillan Technical Publishing, ISBN: 1-57870-185-6, 2000.
2. Richard Bejtlich "Extrusion detection-Security Monitoring for Internal Intrusions", Pearson Education, November 2005.
3. Relevant research papers from the journals.

CSE-572 MOBILE AND WIRELESS SECURITY

[3 1 0 4]

Introduction: Threats and Security Goals, Network Security Analysis, Information Security Measures, Important Terms relating to Communication Security, Challenges of Broadcast Communication, Security Requirements for Broadcast Applications; Cryptographic Security: Fundamentals, Broadcast Network Requirements, Cryptographic Primitives, Efficiency in Cryptographic Primitives, Commitment Protocols, Lock and Key analogy, Ciphers, Kerckhoff's Principles, Classical cryptanalysis, Digital cryptography, Pseudo-Random number generator; TESLA Broadcast Authentication: Requirements, Basic TESLA Protocol, TIK: TESLA With Instant Key Disclosure, Time Synchronization, Variations, Denial-of-Service Protection. The BiBa Broadcast Authentication: The BiBa Signature Algorithm, Protocol, Practical Considerations, Variations and Extensions, One-Round BiBa is as Secure as Multi-Round BiBa, Merkle Hash Trees for Ball Authentication; EMSS, MESS and HTSS: Signatures for Broadcast, Efficient Multicast Stream Signature (EMSS), MESS, Variations, HTSS; The wireless Local Area Network (WLAN): Wireless Transmission Media, WLAN Products and Standards, 802.11 security, IEEE 802.11b, Securing WLANs, Countermeasures; Wireless Application Protocol (WAP): Comparison of the TCP/IP, OSI and WAP Models, WAP Security Architecture, Marginal Security; Secure Wireless and Mobile Communications: Security aspects of mobile communications: Security in WLANs, Mobile WANs, Mobile Internet Communications; Bluetooth Technology: Basic specifications, Design specifications, Security architecture, Authentication and encryptions; Sensor Network Security: Background, System Assumptions, Requirements for Sensor Network Security, Additional Notation, SNEP and MicroTESLA, Implementation, Evaluation; Voice over Internet Protocol(VoIP): The Buzz around VoIP, VoIP standards, The rise of VoIP Technology, Technical Issues and Voice network security.

References:

1. Adrian Perrig, J.D. Tygar, "Secure Broadcast Communication: in Wired and Wireless Networks" Allied Publications, 2004.
2. Randall K.Nichols and Panos C.Lekkas, "Wireless Security: Models, Threats and Solutions", McGraw Hill Press,2002.
3. Security in fixed and Wireless Networks by Gunter Schafer; John Wiley publications, 2003.
4. Relevant research papers from the journals

CSE-574 LEGAL ISSUES IN INFORMATION SECURITY

[3 1 0 4]

The Information Technology Act, 2000 (No. 21 OF 2000). The Reserve Bank Of India Act, 1934. The first schedule, Amendments to the Indian Penal Code (45 Of 1860). Amendments to the Indian Evidence Act, 1872, Amendments to the Bankers' Books Evidence act ' 891 (18 of 1891) Amendment to the Reserve Bank of India Act, 1934 (2 of 1934) A Methodology for Developing Trusted Information Systems, A national information infrastructure model for information warfare defense. Intellectual Property, Understand how copyrights, patents, trademarks, and other forms of IP differ, Understand why semiconductor chips aren't protectable by patents or copyrights, Licenses, fighting against macro threats, defensive strategies for governments and industry groups, measures for ensuring data protection and citizen privacy against the threat of crime and terrorism; the European response EU Tackles Cybercrime Background, other related issues, U.S. military response to cyber warfare and USA's view on world cyber security issues, law enforcement: being behind the technology curve and how to change that.

References:

1. Michael E Whiteman and Herbert "Principles of Information Security", -Second Edition, Thomson Publication
2. The Information Technology 2000 (No. 21 OF 2000)-Bare Act
3. Rasool Azari "Current Security Management & Ethical Issues of Information Technology" ISBN:1931777438 Idea Group Publishing 2003
4. Alexander I., Poltorak Paul, J. Lerner "ESSENTIALS of Licensing Intellectual Property", John Wiley & Sons, Inc.
5. Lech J. Andrew M. Colarik, "Cyber Warfare and Cyber Terrorism".
6. Relevant research papers from the journals

CSE-576 INFORMATION SECURITY MANAGEMENT

[3 1 0 4]

Introduction to Information Security: History of Information Security, Characteristics of Information, NSTISSC Security model, Components of Information System, Security Systems Development life cycle, Security professional. Need for Security: Business needs, Threats, Attacks. Information Security Risk Management: An Overview of Risk Management, Risk Identification Identifying assets, Threats and vulnerabilities Risk Analysis and Assessment Understanding risk analysis, Planning for risk analysis, Performing risk analysis and assessment, Risk Control Strategies and selection. Planning for Security: Information security policy, Standards and practices, The information security blueprint, security education, Training and awareness program. Implementing Information Security: Project Management for Information Security, Technical topics, Nontechnical aspects. Disaster Recovery and Risk Monitoring: Disaster recovery planning, Disaster recovery plan, Risk monitoring Application-Level Risks The Fundamental hacking concept, Network service vulnerabilities and attacks – memory manipulation attacks, Mitigation process manipulation risks. Network Security Assessment and Tools Required: The business benefits, Classifying internet-based attackers, Assessment service

definitions, Network security methodology, The cyclic assessment approach, Free and commercial network scanning tools, Protocol-Dependent assessment tools. Computer Network Vulnerabilities :Sources of vulnerabilities, Vulnerability assessment, Vulnerability identification and assessment. Security Evaluation of Computer Products Product security evaluation process, Computer products evaluation standards, Major evaluation criteria.

References:

1. Michael E. Whitman and Herbert J. Mattord , "Principles of information security" 2nd edition - 2007
2. Chris McNab "Network Security Assessment ", O'Reilly, 2004
3. Joseph Migga Kizza , "Computer Network Security" ,Springer, 2005.
4. Relevant research papers from the journals

CSE-578 CYBER SECURITY STANDARDS AND BEST PRACTICES

[3 1 0 4]

Security problem in computing: definition of secure, Attacks, the meaning of computer security, computer criminals, methods of defense. Administering security: Security planning, Risk analysis, Organizational security policies, Physical security The economics of cyber security: Making a business case, Quantifying security, Modeling cyber security, current research and future directions Privacy in computing: privacy concepts, privacy principles and policies, authentication and privacy, data mining, privacy on the web, e-mail security, impacts on emerging technologies. Legal and ethical issues in computer security: protecting programs and data, information and the law, rights of employees and employers, Redress for software failures, computer crime, Ethical issues in computer security, Case studies of ethics Cyber Security Focus Group, General Drivers of BPs, Cyber security Best Practices Structure, FGIB cyber security proposals, Survey of current Practices, Creation of new practices, NRIC recovery best practices, NRIC Physical security best practices.

References:

1. CharlesP.Pfleegar and Shari Lawrence Pfleeger "Security in Computing" , 4th edition, PHI of India, 2008
2. John W. Rittinghouse and William N. Hancock "Cyber Security Operations handbook", Elsevier
3. www.Bell-labs.com/user/krauscher/nric.\
4. Relevant research papers

CSE-580 BIOMETRIC SECURITY

[3 1 0 4]

Biometrics Fundaments: Introduction, Benefits of biometrics over traditional authentication systems, Benefits of biometrics in identification systems, Selecting a biometric for a system,

Applications, Key biometric terms and processes, Verification versus Identification, Logical versus physical access, How biometric matching works, Accuracy in biometric systems.
Physiological Biometric Technologies: Fingerprints, Facial scan, Iris and Retina Scan, Hand scan and DNA Biometric Technologies, Technical description, Characteristics, Competing technologies, Strengths and weaknesses, Deployment.
Behavioral Biometric Technologies: Handprint Biometrics, DNA Biometrics, Signature and handwriting technology, Technical description , classification, Keyboard /keystroke dynamics, Voice Scan- data acquisition, feature extraction, characteristics, strengths and weaknesses, Deployment.
Multi biometrics: Multi biometrics and multi factor biometrics, Two-factor authentication with passwords, tickets and tokens.
Categorizing Biometric Applications, Executive decision, Case studies on Physiological, Behavioral and multifactor biometrics in identification systems.

References:

1. Samir Nanavathi,Michel Thieme,Raj Nanavathi,"Biometrics -Identity verification in a Networked World", John Wiley & Son, Inc.(Paperback), 2002.
2. John Chirillo and Scott Blaul," Implementing Biometric Security", Wiley Publishing Inc. (Paperback), 2005.
3. Paul Reid, "Biometrics for Network Security", Pearson Education, 2004.
4. John D. Woodward , "Biometrics- The Ultimate Reference", Wiley Dreamtech, 2003.
5. Bhanu, B., Tan, X., "Computational Algorithms for Fingerprint Recognition", Kluwer Academic Publishers, USA, 2004.
6. Ashbourn, J., "Practical Biometrics - From Aspiration to Implementation", Springer Verlag, 2004.
7. Relevant research papers from the journals

CSE-582 AGENT SYSTEMS AND SECURITY

[3 1 0 4]

An introduction to Software Agents What is a software agent? Why software agents? Intelligent agents, Agents and environments, Good behavior and concept of rationality, The nature of environments, The structure of agents. Goal based agents Problem-solving agents, Example problems, searching for solutions, Uniformed Search Strategies, Avoiding repeated states, searching with partial information. Learning Forms of learning, Inductive learning, learning decision trees, Ensemble learning. Agents in use How will we use agents?, Health, E-mail, Finance, Information, Banks, Retail, Media, Agents in IT, Government. Security in mobile agent system Problems and approaches Mobile agent security , attacks and countermeasures of software system security, security issue in a mobile agent system, New formal model, extended elementary object system (EEOS), Translating the EEOS model to colored petri net model, Simulation and anlysis of the extended elementary object system model of a secure mobile agent system, An introduction to multiagent system, intelligent agents, deductive reasoning agents, practical reasoning agents, reactive and hybrid agents. Introduction, security threats; agent to platform, agent to agent, platform to agent, other to agent platform. Security requirements; Confidentiality, Integrity, Accountability, availability. Anonymity; Countermeasures, protecting the agent platform, protecting agents. Mobile agent applications and security scenarios; E-

commerce, Network management, Personal digital assistants Multiagent systems Multiagent system issues and challenges, Multiagent planning, Multiagent system applications

References:

1. Jeffrey Bradshaw, "Software Agents", nAAAI Press/MIT Press 1997.
2. Richard Murch, Tony Johnson , "Intelligent Software Agents", Prentice Hall 2000.
3. Michael J. Wooldridge "An introduction to Multiagent Systems" copyrights@ 2002 John Wiley and sons.
4. Russel and Norvig, "Artificial Intelligence : a modern approach", Prentice Hall, 1994.
5. Relevant Research papers from the journals.

OPEN ELECTIVE

CSE-536 MULTICORE PROGRAM OPTIMIZATION

[3 0 0 3]

Introduction to parallel computers; Instruction Level Parallelism (ILP); Multiprocessors and thread level parallelism; Shared Memory Multiprocessors; Cache coherence problems; Snoopy protocols: invalidate vs. update; Memory consistency models; Hyper threading technology architecture, multi-core architecture; Multi-threading on single core versus multi-core platforms; Amdahl's law; Power consumption; Synchronization; Introduction to Basic optimization; Hot Spot, Faster Algorithms, Data Dependency, Branching, Memory, Loops, Slow Operations; Introduction to Performance Tools (Intel Software Tools); Introduction to Multi-core Optimization; ILP vs TLP, Data vs Task Parallelism, Threading and Parallel programming constructs, Threading APIs, Multi Threading with OpenMP, Threading Goals and Issues; Multithreaded and Parallel Applications Case studies; Some applications in Integer Programming, Digital Signal Processing(Video Codec)

References:

1. Richard Gerber, Aart J. C Bik, Kevin B. Smith, and Xinmin Tian, The Software Optimization Cookbook High Performance Recipes for IA-32 Platforms, 2nd Edition, Intel Press
2. Shameem Akhter, Jason Roberts. Multi-Core Programming: Increasing Performance through Software Multi-threading
3. J. L. Hennesey and D. A. Patterson. Computer Architecture: A Quantitative Approach, Morgan Kaufmann Publishers, 3rd Edition
4. D. E. Culler, J. P. Singh, with A. Gupta. Parallel Computer Architecture: A Hardware/Software Approach. Morgan Kaufmann Publishers, 2nd Edition
5. Relevant papers from Intel, IEEE and other journals
6. https://computing.llnl.gov/tutorials/pthreads/
7. www.llnl.gov/computing/tutorials/openMP/

CSE-538 INFORMATION STORAGE AND MANAGEMENT

[3 0 0 3]

Introduction to Information Storage and Management, Evolution of Storage Technology and Architecture, Data Center Infrastructure, Information Lifecycle, Storage System Environment, Disk Drive Laws Governing Disk Performance, Logical Components, Application Requirements and Disk Performance, Data Protection, RAID, Implementation, RAID Components, RAID Levels, RAID Comparison, RAID Impact on Disk Performance, Hot Spares, Intelligent Storage System, Components, Intelligent Storage Array, EMC CLARiiON and Symmetrix, Direct Attached Storage and Introduction to SCSI, Types of DAS, Benefits and Limitations, Introduction to Parallel SCSI, SCSI Command Model, Storage Area Networks, The SAN and Its Evolution, Components of SAN, FC Connectivity, Fibre Channel Ports, World Wide Names, Zoning, Fibre Channel Login Types, FC Topologies, EMC Connectrix, Network Attached Storage, Benefits of NAS, Components of NAS, NAS Implementations, NAS File-Sharing Protocols, EMC Celerra, Content-Addressed Storage, Fixed Content and Archives, Types of Archives, Features and Benefits of CAS, CAS Architecture, Object Storage and Retrieval in CAS, CAS Examples, EMC Centera, Storage Virtualization, Forms of Virtualization, Storage Virtualization Configurations, Storage Virtualization Challenges, Types of Storage Virtualization, Backup and Recovery, Backup Purpose, Backup Considerations, Backup Granularity, Recovery Considerations, Backup Methods, Backup Process, Backup and Restore Operations, Backup Topologies, Backup in NAS Environments, Backup Technologies, EMC NetWorker, Local Replication, Remote Replication.

References:

1. G. Somasundaram, Alok Shrivastava, " Information Storage and Management Storing, Managing, and Protecting Digital Information", EMC Education Services, Wiley India Edition, 2009.
2. Marc Farley, "Storage Networking Fundamentals", CISCO Systems, First edition, 2004.
3. Gupta Meena, "Storage Area Network Fundamentals", Pearson Ed.
4. Robert Spalding, "Storage Networks: The Complete Reference", Tata McGraw Hill, 2003.
5. Marc Farley Osborne, "Building Storage Networks", Tata McGraw Hill, Second edition, 2001.
6. Relevant research papers from the journals

III/IV SEMESTER

CSE-699 DISSERTATION/THESIS/PROJECT [- - - 40]

The duration of this major project is one year. Students are required to undertake innovative and research oriented projects, which not only reflect their knowledge gained in the previous two semesters but also reflects additional knowledge gained from their own effort. They must show the phase wise development of their project submitting the appropriate documents at the end of each phase.