

M.Tech Computer Science: Specialization in Data Security

Semester – I									
Sl. No.	Course code	Course Title	Core/ Elective	Credits	Le c.	Lab	Marks		
							Int.	ES	Total
1	CSD3101	Mathematical Foundations of Computer Science	C	4	4		50	50	100
2	CSD3102	Computer Networking	C	4	3	2	50	50	100
3	CSD3103	Design and Analysis of Algorithms	C	4	3	2	50	50	100
4	-	Elective I	E	3	3	0	50	50	100
5	-	Elective II	E	3	3	0	50	50	100
6	-	Computer Networking Lab	C	1		5	100		100
Total for Semester I				19	16	9	600		
Electives									
CSD 3104: Theory of Computation									
CSD 3105: Software Engineering & Management									
CSC 3106: Parallel Computer Architecture									
Semester – II									
1	CSD 3201	Information Systems Control & Audit	C	4	4	0	50	50	100
2	CSD 3202	Cryptography & Network Security	C	4	3	3	50	50	100
3	CSD 3203	Seminar	C	1	0	0	50		50
4	-	Elective III	E	3	3	0	50	50	100
5	-	Elective IV	E	3	3	0	50	50	100
6	-	Elective V	E	3	3	0	50	50	100
		Network Security Lab	C	1			100		100
Total for Semester II				19	16	9	650		
Electives									
CSD 3204: Data Compression									
CSD 3205: Data Warehousing & Data Mining									
CSD 3206: Digital Image Processing & Pattern Recognition									
CSD 3207 :Number Theory & Cryptography									
Semester – III									
1	CSD 3301	Project & Viva Voce	C	18	0	15	100	200	300
Semester – IV									
1	CSD 3302	Project & Viva Voce	C	18	0	15	100	250	350
Total credits							Marks : 1900		

CSD3101: MATHEMATICAL FOUNDATIONS OF COMPUTER SCIENCE

Module 1

Modeling computation and languages: Finite state machines, deterministic and non deterministic finite state machines, Turing machines, Recursive and Recursively Enumerable languages, Decidability, Resource bounded computation, Complexity classes, Complexity measures. Relationships among complexity measures, Polynomial time and space, Theory of NP-completeness.
Formal languages — classes of grammars-type 0 —context sensitive —context free — regular grammars.

Module 2

Crisp sets and Fuzzy Sets: Basic concepts- Fuzzy Logic-Fuzzy predicates-Fuzzy quantifiers.
Operations on Fuzzy Sets: Fuzzy Complement-Fuzzy unions-Fuzzy Intersection-combinations of operations-Theorems. Crisp Relations and Fuzzy Relations-Binary Relation-one-to-one and onto relation-Inverse fuzzy relation.

Module 3

Linear algebra: Vector spaces, Orthogonality, Eigen-value analysis, Vector and matrix norms, Multivariable analysis, Vector and matrix calculus, Unconstrained and constrained optimization problem solving methods.

Module 4

Simulation and stochastic process. Random variables, Functions of random variables, Sequences of random variables, Stochastic processes, Markov chains, Markov processes and queuing theory. Simulation : Discrete Event Simulation — Monte — Carlo Simulation — Stochastic Simulation — Applications to Queuing systems.

Module 5

Queuing models. Queuing theory: General Concepts - Arrival pattern - service pattern - Queue disciplines - Markovian Queues - Single and Multi-server Models The Markovian model M/M/1 - steady state solutions — Little's formula.

References

1. An introduction to formal languages and automata By Peter Linz
2. Robertazzi. J.G. "Computer Networks and Systems — Queuing Theory and Performance Evaluation", Third Edition, Springer, 2002 Reprint.
3. Ross. S.M., "Probability Models for Computer Science", Academic Press, 2002.
4. R. P. Grimaldi, Discrete and Combinatorial Mathematics: An Applied Introduction, 3/e, Addison-Wesley, New Delhi, 1994.
5. B. Kolman and R.C. Busby, Discrete Mathematical Structures for Computer Science, P1-il, New Delhi, 1994.
6. J. Clark and D. A. Holton, A First Look at Graph Theory, Allied Publishers (World Scientific), New Delhi, 1991.
7. Ross. S.M., "Probability Models for Computer Science", Academic Press, 2002.
8. George J. Klir and Tina A. Folger- Fuzzy sets, Uncertainty and Informations — Eastern Economy Edition

CSD3102: COMPUTER NETWORKING

Syllabus

1. Fundamentals of Data transmission - Components of a network - LAN Technology - Ethernet - CSMA/CD - Switched Ethernet
2. Internetworking with TCP/IP- IP addressing - Subnetting - Routing - Intra and Inter-domain routing protocols
3. End-to-End Reliability - TCP and UDP - Congestion Control - Quality of Service - Internet traffic and Traffic Engineering - Real time traffic and scheduling
4. High-level Network Services - DNS, HTTP, SMTP - Network Security - IPTables - Network Management - SNMP
5. Emerging Trends - MPLS - Active Networks - Gigabit Networking - Photonic Networks

REFERNCES:

1. Computer Networks- A Systems Approach(4th ed.) Larry L. Peterson and Bruce S. Davie, 4th Edn 2007
2. Data & Computer Communications(,(8th ed.) W. Stallings ,PH(2006)
3. Internetworking with TCP/IP Principles,Protocols & Architecture(1th ed.): Douglas E. Comer
4. Essential SNMP(2ND ed.): Douglas Mauro and Kevin Schmidt, O'Reilly Media(2005)
5. Web Resources: ieee.org, cisco.com, linuxnetworks.org

CSD3103: DESIGN AND ANALYSIS OF ALGORITHMS

Course Description:

Discrete mathematics is the study of mathematical structures that are fundamentally discrete in nature. It is concerned with techniques to solve certain types of problems such as how to count or enumerate quantities. The course is intended to cover the main aspects which are useful in studying, describing and modeling of objects and problems in the context of computer algorithms and programming languages.

Course Objectives

- To study the basic set theory
- To familiarize different mathematical structures
- To study the different properties of graphs
- To study the basic search algorithms to find the shortest path
- To familiarise the mathematical modeling of networks.

Course Content

Basics of Algorithms Analysis - Computational Tractability - Asymptotic Order of Growth Notation - A Survey of Common Running Times. Graphs - Basic Definitions and Applications- Graph Connectivity and Graph Traversal – Implementation - Connectivity in Directed Graphs - Directed Acyclic Graphs and Topological Ordering - Shortest Paths in a Graph - The Minimum Spanning Tree Problem – Clustering - Huffman Codes and the Problem of Data Compression

1. **Divide and Conquer** - Recurrence Relations - Counting Inversions - Integer Multiplication - Convolutions and the Fast Fourier Transform Dynamic Programming - Weighted Interval Scheduling - Subset Sums and Knapsacks- Sequence Alignment
2. **Network Flow** - Maximum Flow Problem - Maximum Flows and Minimum Cuts in a Network - The Bipartite Matching Problem - Extensions to the Maximum Flow Problem NP and Computational Intractability - Polynomial-time Reductions - NP-Complete Problems - Sequencing Problems - Partitioning Problems - Graph Coloring - co-NP and the Asymmetry of NP
3. **Approximation Algorithms** - The Center Selection Problem - The Pricing Method - Arbitrarily Good Approximations Local Search - The Landscape of an Optimization Problem - Maximum Cut Approximation via Local Search - Best-Response Dynamics and Nash Equilibria
4. **Randomized Algorithms** - Contention Resolution - Random Variables and their Expectations - A Randomized Implementation of Dictionaries - Randomized Caching - Chernoff Bounds

REFERNCES

1. Algorithm Design: Jon Kleinberg and Eva Tardos, AW (2005)
2. Anany V. Levitin. Introduction to the Design & Analysis of Algorithms (2nd Ed): A W (2006)
3. The Algorithm Design Manual(2nd Ed): Steven S. Skiena, Springer(2008)
4. Computer Algorithms: Introduction to Design and Analysis (3rd Ed): Sara Baase and Allen Van Gelder. AW (1999)
5. Fundamentals of Computer Algorithms: Ellis Horowitz, Sartaj Sahni and Rajasekaran Sanguthevar Galgotia (2008)

CSD3104: THEORY OF COMPUTATION..

Syllabus

1. Numbers and their Representation - Problems, Instances, and Solutions - Asymptotic Notation – Graphs - Alphabets, Strings, and Languages - Functions and Infinite Sets - Pairing Functions - Cantor's Proof: the Technique of Diagonalization - Implications for Computability
2. Finite automata and Regular Languages: States and Automata - Finite Automata as Language Acceptors - Determinism and Non-determinism - Checking vs. Computing - Properties of Finite Automata - Equivalence of Finite Automata Epsilon Transitions - Regular Expressions and Finite Automata - Reviewing the Construction of Regular Expressions from Finite Automata.
3. Universal Models of Computation - Encoding Instances - Choosing a Model of Computation - Issues of Computability - The Turing Machine - Multitape Turing Machines - The Register Machine - Translation Between Models - Computability Theory - Primitive Recursive Functions -Defining Primitive Recursive Functions - Partial Recursive Functions - Rice's Theorem and the Recursion Theorem - Degrees of Unsolvability
4. Complexity Theory: Classes of Complexity - Hierarchy Theorems - Model-Independent Complexity Classes - Deterministic Complexity Classes - Certificates and nondeterminism - Complete Problems. NP-Completeness: Cook's Theorem - Space Completeness - Polynomial Space - Polylogarithmic Space - Provably Intractable Problems
5. Complexity Theory in Practice: Circumscribing Hard Problems - Restrictions of Hard Problems - Promise Problems - Strong NP-Completeness - The Complexity of Approximation – Definitions - Constant-Distance Approximations - Approximation Schemes - Fixed-Ratio Approximations and the Class OptNP - The Power of Randomization.

REFERNCES:

1. The Theory of Computation – Bernard Moret, AW, 1998
2. Introduction to Automata Theory, Languages and Computation – John E Hopcroft, AW, 2001
3. Theory of Computation – Formal Languages, Automata and Complexity, AW, J. Glenn Brookshear Models of Computation – Exploring the power of Computing – John Savage
4. Models of Computation –Exploring the power of computing-john savage(1998)

CSD3105: SOFTWARE ENGINEERING & MANAGEMENT

1. Software Life Cycle Models: Waterfall — Spiral — Prototyping — Fourth generation techniques — Software Process — Software Requirement Specification (SRS) Characteristics of good SRS — Unambiguous, complete, verifiable, consistent, modifiable, traceable and usable SRS during the operation and maintenance phase — Prototype outline for SRS
2. System Analysis and Design: Communication skills for the system analyst — Review/Inspection procedure- Document composition of the inspection team — Check list — recording of defects and action recommended — System analysis tools & techniques — DFD — ER diagrams — Project Dictionary
3. Software Design: System design — Tools and techniques- Prototyping — User interface design — Elements of good design — Design issues — Features of a Modern GUI — menus, scrolling, windows, icons, panels, error messages etc.
4. Software Configuration Management: Baseline — SCM process — Version control — Change Management — CASE tools for project management support — Analysis and design- Programming — Prototyping — Maintenance
5. Software Testing: Purpose of testing — Test case and the expected output — Test coverage — Unit testing — Domain and path testing — Equivalence class based portion testing — component testing — Aggregation of components — System testing — Requirements based testing — Acceptance testing — Test reporting — Bug fixing — regression and stress testing — Testing for performance — Security — installation-recovery — configuration sensitivity — Capture /relay — Report database — Test automation

REFERNCES:

1. Software Engineering, A Practitioners Approach — Roger S. Pressman, 3rd Ed. McGraw Hill
2. System Anal'sis and Design Methods — Whitten, Bentley & Baslow, 2nd Ed. Galgotia
3. An Integrated approach to Software Engineering — Pankaj Jalote, Springer Verlag 1997
4. Software Testing Techniques — Boris, Beizer 2nd Ed. Van Nostrand Reinhold 1990

CSD3106: PARALLEL COMPUTER ARCHITECTURE..

Syllabus

1. Introduction to digital computers – processor design principles - Advanced Processor Technology – Memory and I/O organization- Cache organization – Introduction to parallel processing
2. Parallel processing terminology – Flynn’s Handler’s Classification - Pipelining and Superscalar Techniques: Linear & Nonlinear Pipeline Processors – Instruction and Arithmetic Pipeline design – Superscalar and super pipeline design
3. Parallel and scalable architectures: Multiprocessor System Interconnect – Cache coherence – Uniform and non uniform memory access multiprocessors - Synchronization - Message passing systems
4. Distributed systems – Message passing model – Programming model – Parallel Virtual Machine – Architecture of PVM – Programming model of PVM - Comparison
5. Connectivity: System inter connect architectures – Networks – Routing – Clusters, Linux Clusters .Case Studies on Parallel Architectures developed in India like PARAM, Flosolver etc.

REFERNCES:

1. Computer Architecture and Organization(3rd ed) – John Hayes, McGrawHill (2002)
2. Advanced Computer Architecture – Kai Hwang, McGRAW-HILL - 1993
3. Computer Architecture and Parallel Processing – K. Hwang, F.A. Briggs, McGRAW-HILL
4. Current Literature
5. Computer Architecture, John Hennessy & David A. Pattern, Elsevier,2007 Edn

CSD3201 INFORMATION SYSTEMS CONTROL AND AUDIT

Course Description

Information systems auditing is a function that has been developed to assess whether computer systems safeguard assets, maintain data integrity, and allow the goals of an organization to be achieved effectively and efficiently. Evaluating the reliability of controls in computer systems is more complex than manual information systems where more critical controls are to be considered.

Course Objectives

- To study need and process involved in Information system audit
- To study the management control framework for information system
- To study how control frameworks can be implemented
- To study various auditing practices
- To study information system audit management

Course Content

1. Overview of Information system Auditing –Need for Control Audit of Computers - Conducting an information system audit – Top Management Control – System Development Management Control – Programming Management Control –Data Resource Management Control – Security Management Control – Operational Management Control – Quality Assurance Management Control.
2. Application Control of Frameworks - Boundry Controls – communication Controls – Processing Controls – Database Controls – Output Controls
3. Audit Softwares – Code Review, Test Data, and Code Comparison – Concurrent Auditing Techniques – Interview, Questionnaires, and Control Flow Charts
4. Evaluating Asset Safeguarding and Data Integrity – Evaluating System Effectiveness & Efficiency - Managing the Information Systems and Audit.
5. Security policies, confidentiality policies, Integrity policies, Assurance and trust, building secure and trusted systems – Assurance in SDLC – Ethical issues in Computer Security.

REFERENCES

1. Information system Audit and Control : Ron Weber, Pearson Education
2. Control Objectives for Information and Related Technology Framework: Rolling Meadows , ISACA Foundation
3. Auditing EDP Systems: Wante, Donald A, Peter P B, Prentice Hall
4. Building a Secure Computer System : Gasser, Morrie – Van Nostrand, USA
5. Skill Enhancement for the EDP Auditor : Bruno, Paul R – Auerbach Publications
6. M. Bishop, Computer Security: Art and Science, Pearson Education, 2003.
7. C.P.Fleeger & S.L. Fleeger, Security in Computing, 3/e, Pearson Education, 2003.

CSD 3202 CRYPTOGRAPHY AND NETWORK SECURITY

Course Description

Cryptography deals with the use of mathematical algorithms to transform data in to a form that is not readily intelligible. This is sometimes superior to access control methods when implemented in information systems. Cryptography can be used in data storage and in data communication channels. The various algorithms are dealt in detail in this course.

Course Objectives

- To provide details about classical and modern symmetric key systems
- To study in details various Public Key Encryption Systems
- To study the use of cryptographic algorithms in computer networks
- To study the implementation of cryptography in Information Systems.
- To study about Viruses and Virus Countermeasures

Course Content

1. Overview of Network Security Systems – Classical Encryption Techniques – Block Ciphers and DES – Finite – Fields – Advanced Encryption Standards – Confidentiality in Using Symmetric Encryption
2. Introduction to Number Theory – Public Key Cryptography and RSA – Key Management – Message Authentication and Hash Function- Hash and MAC Algorithm – Digital Signature and Authentication Protocols
3. Kerbos – Pretty Good Privacy - Electronic Mail Security – IP Security Architecture – Encapsulating Security Payload– Web Security Considerations – Secure Socket Layer and Transport Layer Security – Secure Electronic Transaction
4. System Security – Intrusion Detection – Password Management - Malicious Soft wares – Viruses and Related Threats – Virus Countermeasures – Distributed Denial of Service Attacks
5. Firewalls – Firewall Design Principles – Trusted Systems – Common Criteria for Information Technology Security Evaluation

REFERENCES

1. Cryptography and Network Security – Principles and Practices : William Stallings, Pearson Education
2. Mastering Java Security : Cryptography Algorithms and Practices : Rich Helton, Johennie Helton - Wiley
3. Cryptography A Primer- Alan G Konhein, John Wiley & sons.
4. Internet Cryptography- Richard E Smith, Pearson Education
5. Introduction to Cryptography with Java Applet- David Bishop, Narosa Publishing House
6. Computer Cryptography- Karl Anderson, Prentice Hall Inc.

CSD3204: Data Compression

Module I:

Huffman Coding, Shannon Fano Algorithm, Huffman Algorithms, Adaptive Coding, Arithmetic Coding Higher Order Modeling. Finite Context Modeling.

Module II:

Dictionary based Compression, Sliding Window Compression, LZ77, LZW compression, Compression ratio, loss less & lossy compression.

Module III:

Speech Compression & Synthesis: Digital Audio concepts, Sampling Variables, Loss less compression of sound, loss compression & silence compression.

Image Compression, Transform based techniques, Wavelet Methods, adaptive techniques. Images standards, JPEG Compression, Zig Zag Coding

Module IV:

Video representation, Colors, Video Compression, MPEG standards, MHEG Standard recent development in Multimedia Video compression, Audio Compression, Fractal techniques.

Module V:

Comparison of compression algorithms, Implementation of compression algorithms.

REFERENCES

1. David Solomon, *Data compression: the complete reference*, 2nd edition, Springer-verlag, New York. 2000.
2. Stephen Welstead, *Fractal and wavelet Image Compression techniques*, PHI, NewDelhi-1, 1999.
3. Khalid Sayood, *Introduction to data compression*, Morgan Kaufmann Publishers, 2003 reprint.
4. Mark Nelson "Data Compression Book" BPB.
5. Sleinreitz "Multimedia System" Addison Wesley.

CSD 3205 Data Warehousing and Data Mining

Module 1

Data Warehousing and Business Analysis: - Data warehousing Components — Building a Data warehouse — Mapping the Data Warehouse to a Multiprocessor Architecture — DBMS Schemas for Decision Support — Data Extraction, Cleanup, and Transformation Tools — Metadata — reporting — Query tools and Applications — Online Analytical Processing (OLAP) — OLAP and Multidimensional Data Analysis.

Module 2

Data Mining: - Data Mining Functionalities — Data Preprocessing — Data Cleaning — Data Integration and Transformation — Data Reduction — Data Discretization and Concept Hierarchy Generation.

Association Rule Mining: - Efficient and Scalable Frequent Item set Mining Methods — Mining Various Kinds of Association Rules — Association Mining to Correlation Analysis — Constraint-Based Association Mining.

Module 3

Classification and Prediction: - Issues Regarding Classification and Prediction — Classification by Decision Tree Introduction — Bayesian Classification — Rule Based Classification — Classification by Back propagation — Support Vector Machines — Associative Classification — Lazy Learners — Other Classification Methods — Prediction — Accuracy and Error Measures — Evaluating the Accuracy of a Classifier or Predictor — Ensemble Methods — Model Selection

Module 4

Cluster Analysis: - Types of Data in Cluster Analysis — A Categorization of Major Clustering Methods — Partitioning Methods — Hierarchical methods — Density-Based Methods — Grid-Based Methods — Model-Based Clustering Methods — Clustering High-Dimensional Data — Constraint-Based Cluster Analysis — Outlier Analysis.

Module 5

Mining Object, Spatial, Multimedia, Text and Web Data: Multidimensional Analysis and Descriptive Mining of Complex Data Objects — Spatial Data Mining — Multimedia Data Mining — Text Mining — Mining the World Wide Web.

REFERENCES

1. Jiawei Han and Micheline Kamber “Data Mining Concepts and Techniques” Second Edition, Elsevier, Reprinted 2008.
2. Alex Berson and Stephen J. Smith “Data Warehousing, Data Mining & OLAP”, Tata McGraw — Hill Edition, Tenth Reprint 2007.
3. K.P. Soman, Shyam Diwakar and V. Ajay “Insight into Data mining Theory and Practice”, Easter Economy Edition, Prentice Hall of India, 2006.
4. G. K. Gupta “Introduction to Data Mining with Case Studies”, Easter Economy Edition, Prentice Hall of India, 2006.
5. Pang-Ning Tan, Michael Steinbach and Vipin Kumar “Introduction to Data Mining”,

CSD 3206 Digital Image Processing & Pattern Recognition

Module 1

Fundamentals of Image Processing: Introduction — Elements of visual perception, Steps in Image Processing Systems, image Acquisition — Sampling and Quantization — Pixel Relationships — Colour Fundamentals and Models, File Formats.

Module 2

Image Enhancement and Restoration: Spatial Domain Gray level Transformations Histogram Processing Spatial Filtering — Smoothing and Sharpening. Frequency Domain: Filtering in Frequency Domain — DFT, FFT, DCT, Smoothing and Sharpening filters — Homomorphic Filtering., Noise models, Constrained and Unconstrained restoration models.

Module 3

Image Segmentation and Feature Analysis: Detection of Discontinuities — Edge Operators Edge Linking and Boundary Detection — Thresholding — Region Based Segmentation — Motion Segmentation, Feature Analysis and Extraction.

Module 4

Overview of pattern recognition - Discriminant functions - Supervised learning - Parametric estimation - Maximum likelihood estimation - Perceptron algorithm - LMSE algorithm - Problems with Bayes approach - Pattern classification by distance functions - Minimum distance pattern classifier.

Module 5

Unsupervised Classification:

Clustering for unsupervised learning and classification - Clustering concept - C-means algorithm — Hierarchical clustering procedures - Graph theoretic approach to pattern clustering - Validity of clustering solutions.

REFERENCES

1. Rafael C. Gonzalez and Richard E. Woods, “Digital Image Processing”, Third Edition, Pearson Education, 2008.
2. Milan Sonka, Vaclav Hlavac and Roger Boyle, “Image Processing, Analysis and Machine Vision”, Third Edition, Third Edition, Brooks Cole, 2008.
3. Anil K. Jain, “Fundamentals of Digital Image Processing”, Prentice-Hall India, 2007.
4. Madhuri A. Joshi, ‘Digital Image Processing: An Algorithmic Approach’, Prentice-Hall India, 2006.
5. Rafael C. Gonzalez, Richard E. Woods and Steven L. Eddins, “Digital Image Processing Using MATLAB”, First Edition, Pearson Education, 2004.
6. Robert J. Schalkoff, Pattern Recognition: Statistical, Structural and Neural Approaches, John Wiley & Sons Inc., New York, 1992.

CSD 3207 Number Theory and Cryptography

Module 1

Divisibility theory, primes and their distribution, theory of congruences, Fermat's theorem, Wilson's theorem, number theoretic functions, Euler's theorem, Congruences in one unknown, Chinese remainder theorem, congruences of higher degree.

Module 2

Primitive roots and indices, numbers in special form, Fermat's last theorem, primality testing, finite fields, polynomial arithmetic, quadratic residues, zero knowledge protocols, elliptic curve arithmetic, recent developments in number theory.

Module 3

Introduction to secure computing, classifying cryptosystems, classical cryptosystems, DES, block cipher modes of operation, triple DES, AES, key distribution.

Module 4

RSA cryptosystem, Diffie-Hellman, elliptic curve cryptosystem, data integrity and authentication, MD5 message digest algorithm, secure hash algorithm, digital signature, DSS.

Module 5

Applications to cryptography and coding theory.

REFERENCES

1. Niven I, Zuckerman H.S and Montgomery h.L, An Introduction to Theory of Numbers, 5/e, John Wiley and sons, 2004
2. Stallings W. Cryptography and Network security: Principles and Practice, 4/e, Pearson Education Asia, 2006.
3. Mano W. Modern Cryptography: Theory & Practice and Pearson Education, 2004.
4. D.A Burton, Elementary Number Theory, 6/e, Tata McGraw Hill, 2007.
5. Delfs H. and Knebel H, Introduction to Cryptography: Principles and Applications., Springer, 2002.