Shobhit
Institute of Engineering & Technology
Deemed to-be-University
EDUCATION EMPOWERS

School of Engineering & Technology

Scheme of Teaching and Syllabi
For
M.Tech. (Computer Science & Engineering)

Department of Computer Science & Engineering

Approved and adopted in year 2019 (Board of Studies, August 6, 2019)
By 24th Academic council (Agenda No 3.2 d)

Index

M. Tech. (Computer Engineering)
(Effective from session 2019-20)

Subject Code	Subject Name	L T P	Cr
1st Semester			
CSMT-501	Computer System Software	3 - 1 - 0	4
CSMT-503	Data Structure and Algorithm	3 - 1 - 0	4
CSMT-505	Advanced Database Management Systems	3 - 1 - 0	4
CSMT-507	Computer Communication and Networks	3 - 1 - 0	4
CSMT-551	Object Oriented Programming Lab	0 - 0 - 4	2
CSMT-581	Seminar	0 - 3 - 0	2
CSMT-509	Fundamentals of Computers & Programming (Audit)	2 - 1 - 0	0
CSMT-511	Fundamentals of Mathematics (Audit)	2 - 1 - 0	0
2nd Semester			
CSMT-502	Resource Management in Computer Systems	3 - 1 - 0	4
CSMT-504	Soft Computing	3 - 1 - 0	4
CSMT-506	High Performance Computer Architecture	3 - 1 - 0	4
CSMT-522	Analysis and Design of Algorithms/ Mobile & Wireless communication/ Security of Information systems/ Network Security	3 - 1 - 0	4
CSMT-552	Operating System Lab	0 - 0 - 4	2
CSMT-582	Seminar	0 - 3 - 0	2
3rd Semester			
CSMT-601	Knowledge based System Design	3 - 1 - 0	4
CSMT-603	Internet and Web technology	3 - 1 - 0	4
CSMT-605	System and Network Administration	3 - 1 - 0	4
CSMT-621	Embedded systems/ Software Verification, validation and testing/ Advanced Microprocessors/ Software Project Management	3 - 1 - 0	4
CSMT-671	Minor Project	0 - 0 - 4	2
CSMT-681	Seminar	0 - 3 - 0	2
4th Semester			
CSMT-692	Dissertation	0 - 0 - 28	14
	Grand Total		74

Programme Objectives: (University Level, M.Tech.)

PO1. To apply knowledge of mathematical, scientific, and computer science to evaluate, analyze, synthesize, model and integrate technologies to develop new computer system for applied engineering systems.

PO2. To generate optimized solutions by formulating and implementing analytical tools for upcoming issues in the field of computer science and engineering.

PO3. To design and develop a system to meet desired needs within social areas such as economics, environmental, and ethics.

PO4. To work upon unfamiliar problems through investigative studies and research and contribute to the development of technological knowledge and intellectual property

PO5. To transfer technology effectively on broadly defined engineering needs with engineering community and with society at large, by being able to comprehend and write effective technical reports, presentations and software tools.

PO6. To possess knowledge for functioning effectively, as a member or team leader, in software projects considering multidisciplinary environments.

PO7. To learn reflectively from mistakes, engage in lifelong learning, adapt new developments and participate in continuing education opportunities to foster personal and organizational growth.

PO8. To demonstrate independent learning and scholarship by adopting research pursuits.

PO9. To use the techniques, skills, and modern engineering tools, including simulation and modeling for engineering needs.

PO10.To understand contemporary issues in providing technology solutions for sustainable development considering impact on economic, social, political, and global issues and thereby contribute to the welfare of the society.

PO11.To demonstrate integrity, ethical behavior and commitment to code of conduct of professional practices and standards.

Programme Educational Objectives: (Department Level, M.Tech.-CS)

PEO-1: To produce post graduate (PG) engineers who are ready to contribute research & development (R&D) effectively to the advancement of Computer Science applications.

PEO-2: To Engage in professional practices to promote the development of innovative systems and optimized solutions.

PEO-3: To work collaboratively on multidisciplinary projects and exhibit high levels of professional and ethical values within organization and society globally.

PEO-4: To Enhance skills and adapt new computing technologies for attaining professional excellence and carrying research.

PEO-5: To impart knowledge and skills to analyze, design, test and implement various software's and be engaged in life - long learning.

Programme Specific Objectives (PSOs)

PSO-1: To apply Software Engineering Principles and Practices to provide software solutions.

PSO-2: To design and Develop Network, Mobile and Web-based Computational systems under realistic constraints.

PSO-3: To design efficient algorithms and develop effective code.

1st Semester

CSMT-501	Computer System Software	3 - 1 - 0	4

Course Objective

To describe concepts and principles of object oriented programming.

To describe various system software

Course Outcomes

CO1: Demonstrate a basic understanding of **computer** hardware and **software**

CO2: Demonstrate problem-solving skills

CO2: Apply logical skills to programming in a variety of languages

Course Content

Unit 1

Object oriented programming and object oriented design,

Unit 2

System software design issues, Language translators, Macro Pre-processors,

Unit 3

Assemblers, Pass-I and pass-II assemblers,

Unit 4

Linkers and Loaders

Unit 5

Run-time environment management

TextBook:

1. D. M. Dhamdhere, “Systems Programming and Operating Systems”, Second RevisedEdition, Tata McGraw-Hill, 1999.

Reference books:

1. Leland L. Beck, “System Software–An Introduction to Systems Programming”, 3rdEdition, Pearson Education Asia, 2000.

2.Santanu Chattopadhyay, “System Software”, Prentice-Hall India,2007

3.AlfredV. Aho, Monica S. Lam, Ravi Sethi, Jeffrey D. Ullman, “Compilers: Principles,Techniques, and Tools”,2nd Edition, Pearson Education Asia

CSMT-503	Data Structure and Algorithm	3 - 1 - 0	4

Course Objective

To understand basic and dynamic data structures and their implementations in real life applications

Course Outcomes

CO1: Explain the time and space complexity of the algorithm.
CO2: Describe elementary data structure like binary search tree, Red Black tree, binomial, B tree and Fibonacci heap.
CO3: Compare between design techniques of algorithm like Divide and Conquer, Dynamic algorithm, Greedy algorithm, backtracking and Amortized algorithm.
CO4: Demonstrate different graph traversal algorithm like BFS, DFS, Prim's, Kruskal's, single source shortest path and all pair shortest path .
CO5: Examine different string matching algorithm like naïve string matching, robin-karp algorithm, kurth-morrispratt algorithm.

Course Content

Unit 1
Introduction to Algorithms Analysis of algorithm, Design of algorithm, complexity of algorithm, asymptotic notations, Recurrences. Sorting in polynomial time: Insertion sort, Merge sort, Quick sort, heap sort. Sorting in linear time: counting sort, bucket sort, radix sort. Medians and order statics.

Unit 2
Elementary data structure binary search tree. Advanced data structure Red Black tree, Augmenting data structure, binomial heaps, B-tree, Fibonacci heap and data structure for disjoint sets.

Unit 3
Advanced design and analysis techniques Dynamic programming, Greedy algorithm, Backtracking, Amortized analysis.

Unit 4
Graph algorithm Breadth first search, Depth first search, Minimum spanning tree, Kruskal's algorithms, Prim's algorithms, Single source shortest path, All pair shortest path, Maximum flow and Traveling salesman problem.

Unit 5
String matching: The naïve String Matching algorithm, The Rabin-Karp Algorithm, String Matching with finite automata, The Knuth-Morris Pratt algorithm.Randomized algorithms, string matching, NP-hard and NP-completeness, Approximation algorithms.

Reference Books:

1. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein, *Introduction to Algorithm,* Tata Mc-Graw Hill, 2nd Edition, 2003.
2. Horowitz Sahani, *Fundamentals of Computers Algorithm*, Golgotia Publications, 1998.
3. Parag H. Dave, Himanshu B. Dave, *Design and Analysis of Algorithms*, Pearson Education, 2008.

CSMT-505	Advanced Database Management Systems	3 - 1 - 0	4

Course Objective

The course should enable the student to Present an introduction to database management systems, with an emphasis on how to organize, maintain and retrieve - efficiently, and effectively information from a DBMS.

Course Outcomes:

Upon successful completion of this course, students should be able to:

CO1: Describe the fundamental elements of relational database management systems

CO2: Explain the basic concepts of relational data model, entity-relationship model, relational database design, relational algebra and SQL.

CO3: Design ER-models to represent simple database application scenarios

CO4: Convert the ER-model to relational tables, populate relational database and formulate SQL queries on data.

CO5: Improve the database design by normalization.

Course Content

Unit-I

Introduction: Concept & Overview of Database management system(DBMS), Comparison of DBMS with file processing system, Data Models- Entity-Relationship, Network, Relational and Object Oriented Data Models, Database Languages, Database Users, Three Schema architecture of DBMS, overall structure of DBMS. Entity-Relationship (ER) Model: Basic concepts, Design Issues, Mapping Constraints, Keys, Entity-Relationship Diagram, Weak Entity Sets, Extended E-R features.

Unit-II

Relational Database Design: Basic terminologies, integrity constraints, Functional Dependency, Different anomalies in designing a Database, Decomposition and its properties, Normalization using functional dependencies (1NF, 2NF, 3NF,BCNF), Normalization using multi-valued dependencies(4NF, 5NF).

Unit-III

Query Languages: Relational Algebra, characteristics and various operations, **Structured Query Language(SQL):** Characteristics of SQL, SQL data types and literals. Concept of Data definition language, Data manipulation language, Data Control Language. Basic Structure, Set operations, Aggregate Functions, Null Values, views, Sub-queries. Introduction to Tuple Calculus.

Unit-IV

Transaction Processing: Transaction system, Testing of serializability, recoverable schedule, Concurrency control, Locking techniques for concurrency control, Time stamping protocols for concurrency control, Validation based protocol, Recovery from transaction failures, log based recovery, checkpoints, shadow paging, deadlock handling.

Unit-V

File Organization & Data warehousing: File & Record Concept, Fixed and Variable sized Records, Types of Single-Level Index. Data warehousing: Introduction, basic concepts, data warehouse architecture, various models, basic operations.

Reference Books:

1. Henry F. Korth and Silberschatz Abraham, "*Database System Concepts*", Mc.Graw Hill.5th edition, 2006.
2. Elmasri Ramez and Novathe Shamkant, "*Fundamentals of Database Systems*", Addision Wesley Publishing Company, 6th edition, 2010.
3. Ramakrishnan: "*Database Management System"*, McGraw-Hill, 3rd edition, 2007.
4. Date C J, "*An Introduction to Database System*", Addision Wesley, 8th edition, 2004.
5. Ivan Bayross, "*SQL, PL/SQL: The programming language with oracle*" BPB

CSMT-507	Computer Communication and Networks	3 - 1 - 0	4

Course Objectives

The course should enable the student to-

1. To understand the basic concepts of data communication, layered model, protocols and interworking between computer networks and switching components in telecommunication systems.
2. Discuss the nature, uses and implications of internet technology
3. To understand the functioning of Frame Relay, ATM.
4. An overview of security issues related to data communication in networks.

Course Outcomes:

CO1: Understand the basics of data communication, networking, internet and their importance.
CO2: Analyze the services and features of various protocol layers in data networks.
CO3: Differentiate wired and wireless computer networks
CO4: Analyze TCP/IP and their protocols.
CO5: Recognize the different internet devices and their functions.
CO6: Identify the basic security threats of a network.

Course Contents:

Unit-1

Introduction to data communication and networks 7 Hours Data communication-data representation, data flow, components. Definition of node, link, branch, network, network criteria. Physical structures-types of connection, working of different network topologies, network configuration and their advantages, concepts and comparison of LAN, MAN, WAN. Switching - concepts of circuit switching, packet switching & message switching and their applications.

Unit-2

Networking protocols and OSI model 7 Hours Protocol layering-Scenarios, principles. Logical connection-connection oriented and connection less. Protocols in computer communications, OSI reference model - functions of all layers. Data link control- concept of framing, flow control and error control.MAC protocol- addressing mechanism. Concept of encapsulation and decapsulation.

Unit-3

Computer Networks 11 Hours Local area network-wired LANs features and classification. Ethernet- properties, frame format (IEEE 802.3), addressing, simple problems on addressing .virtual LAN- working, advantages. Access method–CSMA/CD. Token passing LANS- properties, token bus maintenance and working. Token ring properties, mechanism. FDDI – operation, self healing, Wireless LANS - features, Bluetooth architecture (IEEE 802.15). Basic concepts of WIMAX, cellular telephony, satellite networks.

Unit-4

TCP/IP 11 Hours TCP/IP-Model, protocols layers, INTERNET Address, logical address, Physical address, UDP/IP Datagram Format, classes of IP address, Dotted Decimal notation of IP address, basics of IPv4 and IPv6,simple problems on addressing. Address mapping –static mapping, dynamic mapping. ARP- need, methods, need of RARP and ICMP. Definition of fragmentation and reassembly. Features of TCP, relationship between TCP and IP.

Unit-5

Communication protocols 8 Hours Concepts of Ports and Sockets. Domain Name System (DNS) -name system, name space, working of DNS server. Email- architecture, protocols, advantages of IMAP. Basics of FTP, FTP Connections - Control and Data transfer Connection. Frame relay- Need, Working of frame relay, ATM- Architecture, characteristics.

Text Books

1. Data Communications and Networks- 2nd edition -Achyut S Godbole- and Atul Kahate Tata McGraw-Hill
2. Data Communications & Networking – 5th Edition- B A Forouzan- Tata McGraw-Hill.
3. Computer Networks- 4th Edition- Andrew S Tanenbaum- Pearson-Prentice Hall
4. Computer Networking - James F. Kurose & Keith W. Ross- PEARSON
5. Computer Communications and Networking Technologies - Michael A. Gallo & William M. Hancock- BROOKS&COLE

CSMT-509	**Fundamentals of Computers & Programming (Audit)**	**2 - 1 - 0**	**0**

Course Objective: The student will acquire basic knowledge of computer.

Course Outcome:
The student will able to basic knowledge of Computer and Ms Office etc.

Course Contents

Unit I **Introduction to Computer:** Generations of Computer (I-V), Computer Definition, Block Diagram of a Computer, Advantages of Computer, Limitation of Computer, Characteristics of Computer, Application of Computer.

Unit II **Input and Output Devices:** Functions of the Different Units, Input unit, Output unit, Memory unit, CPU (ALU+CU), Input & Output Devices Input Devices, Data Scanning devices, Output Devices

Unit III **Memories:** RAM/ROM, Binary Number System, Bits, Bytes.

Software: System Software, Utility Programs, Application Software

Unit IV **Internet:** WWW, Domain name, IP Address, MAC address, Create E-Mail ID, Write a mail, attachment, send a mail, and read a mail, CC, BCC

Unit V **MS office**: Microsoft Word, Microsoft Excel, Microsoft PowerPoint Microsoft Flash, and Paint Brush.

.

Reference Books:

1. Sharma, A.K. *Fundamentals of Computers and Programming with C*. Dhanpat Rai Publications, New Delhi, 2005.
2. *Using Information Technology*, 5th Edi, Brian K Williams & Stacey C. Sawyer, 2003, TMH
3. *Information technology*, Dennis P. Curtin, Kim Foley, Kunal Sen, Cathleen Morin, 1998, TMH.

2nd Semester

CSMT-502	**Resource Management in Computer Systems**	**3 - 1 - 0**	**4**

Course Objective

At the end of the course students will understand how to manage Computer system resources including processor, memory and files.

Course Outcomes

CO1: To describe process, threads, scheduling and synchronization.

CO2: To understand the management of computer memory.

CO3: To understand device and file management

Course Content

Unit 1

Historical perspectives interrupt mechanism, concurrent processes; mutual exclusion and synchronization,

Unit 2

System calls and protection; context switching and the notion of a process and threads; synchronization and protection issues; scheduling;

Unit 3

Memory management including virtual memory and paging techniques;

Unit 4

I/o architecture and device management; file systems; distributed file systems; deadlock detection and protection.

Unit 5

Case studies. Laboratory experiments on internals of Linux, Windows NT.

CSMT-504	**Soft Computing**	**3 - 1 - 0**	**4**

Course Objective

The objective of the course is to understand the concepts of fuzzy logic, ANN and genetic algorithms.

Course Outcomes

At the end of the course **Students will able to:**

CO 1To familiarize with soft computing concepts.
CO2. To introduce the fuzzy logic concepts, fuzzy principles and relations
CO3. To Basics of ANN and Learning Algorithms
CO4. Ann as function approximation
CO5. Genetic Algorithm and its applications to soft computing
CO6. Hybrid system usage, application and optimization

Unit 1

Overview of Soft Computing, Difference between Soft and Hard computing, Brief descriptions of different components of soft computing including Artificial intelligence systems Neural networks, fuzzy logic, genetic algorithms. Artificial neural networks Vs Biological neural networks, ANN architecture, Basic building block of an artificial neuron, Activation functions, Introduction to Early ANN architectures

Unit 2

Artificial Neural Networks: Supervised Learning: Introduction and how brain works, Neuron as a simple computing element, The perceptron, Backpropagation networks: architecture, multilayer perceptron, backpropagation learning-input layer, accelerated learning in multilayer perceptron, The Hopfield network, Bidirectional associative memories (BAM), RBF Neural Network.

Unit 3

Artificial Neural Networks: Unsupervised Learning: Hebbian Learning, Generalized Hebbian learning algorithm, Competitive learning, Self- Organizing Computational Maps: Kohonen Network. Fuzzy Logic Crisp & fuzzy sets fuzzy relations fuzzy conditional statements fuzzy rules fuzzy algorithm. Fuzzy logic controller.

Unit 4

Genetic algorithms basic concepts, encoding, fitness function, reproduction-Roulette wheel, Boltzmann, tournament, rank, and steady state selections, Convergence of GA, Applications of GA case studies. Introduction to genetic programming- basic concepts.

Text Books;

1. R. Rajasekaran and G. A and Vijayalakshmi Pa, *Neural Networks, Fuzzy Logic, and Genetic Algorithms: Synthesis and Applications*, Prentice Hall of India
2. D. E. Goldberg, *Genetic Algorithms in Search, Optimisation, and Machine Learning*, Addison-Wesley

REFERENCES

1. L. Fausett, *Fundamentals of Neural Networks*, Prentice Hall

2. T. Ross, *Fuzzy Logic with Engineering Applications*, Tata McGraw Hill

CSMT-506	**High Performance Computer Architecture**	**3 - 1 - 0**	**4**

Course Objective

To understand Parallelism, Scalability and programmability, Program partitioning and scheduling, Interconnection architecture, Principles of scalable performance, and Pipelining

Course Outcomes

CO1: Comprehend various High Performance Computing (HPC) system architectures
CO2: Identify design issues related to the architectural characteristics and performance of HPC systems
CO3: Design and implement compute intensive applications on HPC platform

Course Content

Unit I

Parallel Computer Models: Computing states, Multiprocessors and Multicomputers, Multivector and SIMD Computers, Conditions of parallelism, Program Partitioning and scheduling, Program flow mechanisms, System interconnect architecture

Unit 2

Principles of Scalable Performance and Processor Hierarchy: Performance Metrics and Measures, Parallel processing applications, Speedup Performance Laws, Scalability Analysis and Approaches, Advanced Processor and Memory Hierarchy Technology, Distributed Shared Memory

Unit 3

Requirement and general issues of High Performance Computing: Dependable Clustered Computing,Metacomputing: Harnessing Informal Supercomputers, Specifying Resources and Services in Metacomputing Systems,High Speed Networks, Lightweight Messaging Systems, Xpress Transport Protocol, Software RAID and Parallel File systems, Load Balancing Over Networks, Job and Resource Management Systems

Unit 4

Parallel Models and High Performance Languages: Scheduling Parallel Jobs on Clusters, Parallel Programming Models, Parallel and High Performance programming languages, Dependence Analysis of Data arrays

Unit 5

Advance Computing: Introduction to Petascale computing, Optical Computing, Quantum computing and its issues

Reference Books

1. Kai Hwang,Advance Computer Architecture: Parallelism, Scalability, Programmability, McGraw Hill International Editions
2. Buyya, Rajkumar, High Performance Cluster Computing : Programming and Applications, Pearson Education
3. Georg Hager and Gerhard Wellein, Introduction to High Performance Computing for Scientists and Engineers, CRC Press

CSMT-522	**Mobile & Wireless communication/ Security of Information systems/ Network Security**	**3 - 1 - 0**	**4**

CSMT-521 Mobile & Wireless Communication

Course Objectives

1. To provide an overview of Wireless Communication networks area and its applications in communication engineering.
2. To appreciate the contribution of Wireless Communication networks to overall technological growth.
3. To explain the various terminology, principles, devices, schemes, concepts, algorithms and different methodologies used in Wireless Communication Networks.
4. To enable students to compare and contrast multiple division techniques, mobile communication systems, and existing wireless networks.

CO1: Understand fundamentals of wireless communications.
CO2:Analyze security, energy efficiency, mobility, scalability, and their unique characteristics in wireless networks.
CO3: Demonstrate basic skills for cellular networks design.
CO4: Apply knowledge of TCP/IP extensions for mobile and wireless networking.

Course Content

Unit-I

Introduction, issues and challenges in mobile computing, overview of wireless telephony: cellular concept, UMTS, GSM: air-interface, channel structure, location management: HLR-VLR, hierarchical, handoffs, policy based handoff process, channel allocation in cellular systems, CDMA, GPRS.

Unit-II

ISM band, Spread Spectrum, physical layer accessing techniques – FHSS, DSSS, OFDM, (IEEE 802.11a) HR-DSSS, OFDM (IEEE 802.11g)Wireless Networking, Wireless LAN Overview: MAC issues, IEEE 802.11, Blue Tooth, Wireless multiple access protocols, Wireless applications, data broadcasting, Mobile IP-entities and terminology, IP Packet delivery, Agent discovery, Registration, Tunneling and encapsulation, optimization and reverse tunneling WAP: Architecture, protocol stack, application environment, applications.

Unit-III

Data management issues, data replication for mobile computers, adaptive clustering for mobile wireless networks, File system-consistency, CODA, Ficus, MIO-NFS, Rover, Disconnected operations.

Unit-IV

Mobile Agents computing, security and fault tolerance, transaction processing in mobile computing environment, TCP over wireless-Traditional TCP, Indirect TCP, Snooping TCP, Mobile TCP, Fast Retransmit/Fast recovery, Transmission-time out Freezing, selective retransmission, Transaction oriented TCP, TCP over 2 G and 3 G wireless network. 4 G wireless network

Unit-V

Ad Hoc networks, localization, Routing protocols, global state routing (GSR), Destination sequenced distance vector routing (DSDV), Dynamic source routing (DSR), Ad Hoc on demand distance vector routing (AODV), Temporary ordered routing algorithm (TORA), QoS Parameters in Ad Hoc Networks-routing, bandwidth, delay, Jitter, Location management, handoff and energy management, fault tolerance in MANET, MANET applications.

Reference Books:

1. Jochen Schiller, "Mobile *Communications"*, Pearson Education, Second Edition, Second Impression, 2007.
2. Asha Mehrotra, "*GSM System Engineering*", Artech House, Second Edition Illustrated, 1997.
3. M. V. D. Heijden, M. Taylor, "*Understanding WAP Wireless Applications, Devices and Services*" , Artech House, July 2000.
4. Raj Kamal, "*Mobile Computing*", OxfordUniversity Press, First Published 2007.
5. Asoke K. Talukder, Roopa R. Yavagal, "*Mobile Computing: Technology, Applications and Service Creation*", Tata McGraw-Hill Publishing Company Limited, New Delhi, Fifth Reprint, 2007.

CSMT-522 NETWORK SECURITY

CO1.The concepts of classical encryption techniques and concepts of finite fields and number
theory.
CO2. Explore the working principles and utilities of various cryptographic algorithms including secret key cryptography, hashes and message digests, and public key algorithms
CO3. Explore the design issues and working principles of various authentication protocols, PKI standards.
CO4. Explore various secure communication standards including Kerberos, IPsec, and SSL/TLS and email
CO5. The ability to use existing cryptographic utilities to build programs for secure

Course Content
Unit I

Foundations of Cryptography and Security – Ciphers and Secret Messages, Security Attacks and Services, Mathematical Tools for Cryptography, Substitutions and Permutations, Modular Arithmetic, Euclid's Algorithm, Finite Fields, Polynomial Arithmetic, Discrete Logarithms, Conventional Symmetric Encryption Algorithms, Theory of Block Cipher Design, Feistel Cipher Network Structures, DES and Triple DES, Strength of DES.

Unit II

Modern Symmetric Encryption Algorithms, IDEA, CAST, Blowfish, Twofish, RC2, RC5, Rijndael (AES), Key Distribution, Stream Ciphers and Pseudo Random Numbers, Pseudo Random Sequences, Linear Congruential Generators, Cryptographic Generators, Design of Stream Cipher, One Time Pad.

Unit III

Public Key Cryptography – Prime Numbers and Testing for Primality, Factoring Large Numbers, RSA, Diffie-Hellman, ElGamal, Key Excahnge Algorithms, Public-Key Cryptography Standards

Unit IV

Hashes and Message Digests – Message Authentication, MD5, SHA, RIPEMD, HMAC, Digital Signatures, Certificates, User Authentication, Digital Signature Standard, Security Handshake Pitfalls, Elliptic Curve Cryptosystems.

Unit V

Authentication of Systems, Kerberos, Electronic Mail Security, Pretty Good Privacy, IP and Web Security, Secure Sockets and Transport Layer, Electronic Commerce Security, Electronic Payment Systems, Secure Electronic Transaction, Digital Watermarking.

TEXT BOOKS

Behrouz A Forouzan, "Cryptography and Network Security",2nd Ed Tata Mc Graw Hill, 2010

REFERENCES

William Stalings, Cryptography and Network Security, Principles and Practices. 6th Ed., Pearson Education, 2013

CSMT-522 SECURITY OF INFORMATION SYSTEMS

Course Objectives

To understand Encryption and De-encryption, De-encryption cryptosystems, Cipher, Encryption Algorithms and their implementation to solve security issues.

Course Outcomes

CO1: To describe encryption, decryption and cryptosystem

CO2: To understand Key Management Protocols

CO3: To understand Operating System, Database and Program Security

Course Content

Unit-I

Basic Encryption and Decryption: Terminology and Background: **E**ncryption, Decryption and Cryptosystems, Plain Text and Cipher Text, Encryption Algorithms, Cryptanalysis.
Introduction to Ciphers: Monoalphabetic Substitutions such as the Caesar Cipher, Cryptanalysis of Monoalphabetic Ciphers, Polyalphabetic Ciphers such as Vigenere Tableaux, Cryptanalysis of Polyalphabetic Ciphers, Perfect Substitution Cipher such as the Vernam Cipher, Stream and Block Ciphers, Characteristics of 'Good' Ciphers: Shannon Characteristics, Confusion and Diffusion, Information Theoretic Tests, Unicity Distance,

Unit-II

Secure Encryption Systems: Hard' Problems: Complexity: NP-Complete Problems, Characteristics of NP-Complete Problems, The Meaning of NP-Completeness, NP-Completeness and Cryptography.
Properties of Arithmetic Operations: Inverses, Primes, Greatest Common Divisor, Euclidean Algorithm, Modular Arithmetic, Properties of Modular Arithmetic, Computing the inverse, Fermat's Theorem, Algorithm for Computing Inverses, Random number generation
Public Key (Asymmetric key) Encryption Systems: Concept and Characteristics of Public key Encryption System, Introduction to Merkle-Hellman Knapsacks, Rivest-Shamir-Adelman (RSA) Encryption in Detail, Introduction to Digital Signature Algorithms, The Digital Signature Standard (DSA).
Hash Algorithms: Hash Concept, Description of Hash Algorithms, Message Digest Algorithms such as MD4 and MD5, Secure Hash Algorithms such as SHA1 and SHA2.
Secure Secret Key (Symmetric) Systems: The Data Encryption Standard (DES), Analyzing and Strengthening of DES, Key Escrow and Clipper, Introduction to Advance Encryption Standard (AES)

Unit-III

Applied Cryptography, Protocols and Practice: Key Management Protocols:Solving Key Distribution Problem, Diffie-Hellman Algorithm, Key Exchange with Public Key Cryptography.
Public Key Infrastructure (PKI): Concept of Digital Certificate, Certificate Authorities and it's roles, X509 Structure of Digital Certificate, Types of Public Key Infrastructures.
Legal Issues: Copyrights, Patents, Trade Secrets, Computer Crime, Cryptography and the Law.

Unit-IV

Operating System, Database and Program Security: Operating Systems Security:Security Policies, Models of Security, Security Features of Ordinary Operating System, Security Features of Trusted Operating System.
Database Security: Security Requirements of Databases, Reliability and Integrity, Protection of Sensitive Data, Inference Problem: Direct and Indirect Attacks
Program Security: Kinds of Malicious Code, How Viruses Attach and Gain Control, Homes for Viruses, Virus Signatures, Preventing Virus Infection, Trapdoors, Convert Channels, Control Against Program Threats, Java mobile codes.

Unit-V

Network Security: Network Security Issues such as Impersonation, Message Confidentiality, Message Integrity, Code Integrity, Denial of Service, Secure Communication Mechanisms such as IPSec, PKI based Authentication and Kerberos Authentication, Biometrics Authentication Mechanisms, Access Control Mechanisms, Firewalls

Web Security: Solving Privacy Problems, Solving Authentication Problems, Secure Socket Layer (SSL) Protocol, Secure Electronic Transaction (SET) Protocol , Safe Guarding Web Servers.

Secure Electronic Mail: Privacy Enhanced Email (PEM), Pretty Good Privacy (PGP), Public Key Cryptography Standards-PKCS#7, Secure/Multipurpose Internet Mail Extensions (S/MIME)

Reference Books:

1. "*Security in Computing* (Second Edition)", Charles P. Pfleeger, 1996, Prentic-Hall International, Inc.,
2. "*Applied Cryptography* Protocols*, Algorithms, and Source Code in C* (Second edition)", Bruce Schneier, 1995, John
3. "*Security Technologies* for *the World Wide Web*", Rolf Oppliger, Artech House, Inc.
4. "*Digital Certificates* Applied *Internet Security*", Jalal Feghhi, Jalli Feghhi and Peter Williams, Addison Wesley Longman,
5. "*The World Wide Web Security FAQ*", Lincoln D. Stein, World Wide Web Consortium, [Online] Available at http://www.w3.org/Security/Faq/www-security-faq.html
6. Cryptographic Message Syntax Standard, Public-Key Cryptography Standards, RSA Laboratories, [Online] Available at http://www.rsasecurity.com/rsalabs/pkcs/pkcs-7/index.html

3rd Semester

CSMT-601	**Knowledge based System Design**	**3 - 1 - 0**	**4**

Course Objectives

Study knowledge based system architectures, tools and techniques and their use in capturing, storing, locating, evaluating, disseminating knowledge

Course Outcomes

CO1: Identify and analyze the applications of knowledge management (KM);

CO2: Apply KM models and technologies to real life applications

CO3: Create a KM system for an organization

Course Content

Unit 1

Knowledge representation, knowledge engineering, logic and resolution, semantic nets, parallel implementation of semantic nets

Unit 2

Frames. Architecture of knowledge based system design, rule based systems. Frame based systems.

Unit 3

Search, techniques. Control strategies. Software/hardware support for knowledge base systems

Unit 4

Expert system shells. Inference machines, AND/OR parallelism. Case studies.

Reference books

1.M. Lisa Miller, 2009, MIS Cases: Decision Making with Application Software, 4th Ed, Prentice Hall.
2.Hawryszkiewycz, I., 2009, Knowledge Management : organizing knowledge based enterprises, 1st Ed, Palgrave Macmillan.

CSMT-603	**Internet and Web technology**	**3 - 1 - 0**	**4**

Course Objective

This course is intended to teach the basics involved in publishing content on the World Wide Web.

Course Outcome

CO1:Analyze a web page and identify its elements and attributes.
CO2:Create web pages using XHTML and Cascading Style Sheets.
CO3:Build dynamic web pages using JavaScript (Client side programming).
CO4:Create XML documents and Schemas.

Course Content

Unit-I

Internet Basics communicating on the internet, internet domains, establishing connection on the internet, client IP address, TCP/IP and its services, transmission control protocol, WWW, intranet, extranet.

Unit-II

Introduction to HTML commonly used HTML commands, text formatting, text styles, Lists – types of lists, adding graphics to HTML documents, tables, links – external document references, internal document references, frames.

Unit-III

Javascript javascript in web pages, the advantages of javascript, building javascript syntax – data types, type casting, creating variables, javascript array, operators and expressions, conditional checking, fuctions – build in functions, user defined functions, dialog boxes – alert dialog box, prompt dialog box, confirm dialog box, javascript document object model – understanding objects, forms object methods.

Unit-IV

JSP jsp execution model, components of jsp, using java beans in jsp, directives in jsp-page directive, include directive, taglib directive, standard action tags-<jsp:include>,<jsp:forward>,<jsp:init>, implicit objects in jsp-application, session, pagecontext, out, request, response, error handling in jsp, database connectivity using jsp.

Unit-V

Active Server Pages: Basics, Integrating Script, ASP Objects and Components, configuring and troubleshooting,: Request and response objects, Retrieving the contents of a an HTML form, Retrieving a Query String, Cookies, Creating and Reading Cookies. Using application Objects and Events.

References Books:

1. Ivan Bayross, "*HTML, DHTML, Java Script, Perl cgi*", BPB publication,
2. James Godwill, "*Pure JSP*", Sams publications, edition-2000
3. Bryan Basham, "*Head First in Servlets and Jsp*", O'Rielly publications, March 2008.

CSMT-605	System and Network Administration	3 - 1 - 0	4

Course Objective

This course introduces students to the foundational concepts and experience in networking and systems administration. The course provides the basic theory, concepts and practical experience in the design, installation and configuration of personal computers, peer-to-peer networks and client-server networks meeting user requirements.

Course Outcomes

CO1: Design and configure peer-to-peer networks to share resources;

CO2: Analyse requirements and design network architecture for a given scenario;

CO3: Design and configure IP addressing schemes for a given scenario;

CO4: Design and configure a client-server network and required network services for a given scenario;

CO5: Evaluate and critique a design for a systems and network solution.

Course Content

Unit 1

Introduction, TCP/IP model, IP addressing, Subnetting, NAT, VLAN, Proxy server, Webserver, DNS, Firewall, Router, Mail Server and their respective configuration settings.

Unit 2

Interconnecting Devices, Knowledge about various network related commands.

Unit 3

Concept of security, cryptography techniques, ciphers, Symmetric key algorithms, Authentication algorithms, Digital signatures, Attacks Host Administration,

Unit 4

UNIX administration commands.

Reference Books

1. *UNIX and Linux System Administration Handbook, 4th Ed.*, by Nemeth, Snyder, Hein and Whaley (Prentice Hall, 2010)
2. *The Practice of System and Network Administration, 2nd Ed.*, by Limoncelli, Hogan and Chalup (Addison Wesley, 2007).

CSMT-621	**Embedded systems/ Software Verification, validation and testing/ Advanced Microprocessors/ Software Project Management**	**3 - 1 - 0**	**4**

CSMT-621 EMBEDDED SYSTEMS

Course Objective

To introduce students to the design issues of embedded systems and enable students to analyze and develop software programs for embedded systems

Course Outcomes

CO1:Understand hardware and software design requirements of embedded systems.
CO2:Analyze the embedded systems' specification and develop software programs.
CO3:Evaluate the requirements of programming Embedded Systems, related software architectures and tool chain for Embedded Systems

Course Content

Unit-I

Introduction to embedded systems: Classification, Characteristics and requirements, Applications

Unit-II

Timing and clocks in embedded systems, Task Modeling and management, Real time operating systemissues.

Unit-III

Signals, frequency spectrum and sampling, digitization (ADC, DAC), Signal Conditioning and Processing.Modeling and Characterization of Embedded Computation System.

Unit-IV

Embedded Control and Control Hierarchy, Communication strategies for embedded systems: Encodingand Flow control.

Unit-V

Fault-Tolerance, FormalVerification, Trends in Embedded Processor, OS,Development Language

Reference Books:

1. Prasad, "*Embedded /Real Time System,Concept,Design and Programming Black Book*", Wiley India
2. R.Gupta, "*Co-synthesis of Hardware and Software for Embedded Systems*", Kluwer
3. Shibu K.V., "*Introduction to Embedded Systems*", TMH
4. Marwedel, "*Embedded System Design*", Springer

CSMT-621 SOFTWARE VERIFICATION, VALIDATION AND TESTING

Course Objective

To study fundamental concepts in software testing, including software testing objectives, process, criteria, strategies, and methods

Course Outcome

CO1:Have an ability to apply software testing knowledge and engineering methods.

CO2:Have an ability to design and conduct a software test process for a software testing project.

CO3:Have an ability to identify the needs of software test automation, and define and develop a test tool to support test automation.

CO4:Have an ability understand and identify various software testing problems, and solve these problems by designing and selecting software test models, criteria, strategies, and methods.

CO5:Have an ability to use various communication methods and skills to communicate with their teammates to conduct their practice-oriented software testing projects.

Course Content

Unit 1

SDLC, S/w quality, Testing and debugging, Test metrics, Static testing, CFG, Test generation from requirements,

Unit 2

Test adequacy assessment and enhancement, Structural and functional testing, test selection, Minimization and Prioritization, Test adequacy assessment using program mutation, Verification and validation,

Unit 3

Verification activities, requirements, HL design, verification of data design, verification of architectural design, verification of UI design,

Unit 4

Black Box testing, White Box testing, Static testing, Validation Testing, functional testing,

Unit 5

Test Automation and debugging.

Reference Books

1.A Practitioner's Guide to Software Test Design, by Lee Copeland , ed. Artech House, ISBN:158053791x, 2004

2.Software Testing, by Ron Patton, ed. Sams Publishing, ISBN: 0-672-32798-8, 2005.

CSMT-621 ADVANCED MICROPROCESSORS

Course Objective

The objective of this course is to become familiar with the architecture and the instruction set of microprocessors.

Course Outcome

CO1: Describe Intel 8086/8088 architecture with explanation of internal organization of some popular microprocessors

CO2: To Understand the use of various concepts of assembly language programming

CO3: To describe various input output interfaces

Course Content

Unit 1

Digital Computers, Microprocessors, 8086/8088, Architecture, Memory Organization, Addressing Modes,

Unit 2

Assembly directives, Data Definition and storage allocation directives, structures, records. Segments, 8086/8088 Instructions, Instruction Formats, Instruction execution, Arithmetic Instruction, Branch Instruction, and conditional and unconditional, loop instructions, logical instructions, Shift and Rotate Instructions,

Unit 3

Assembly Language Programming, Advanced Processors, Intel 80286, Intel 80386, Intel 80486, Intel Pentium and Intel P6 processor, I/O Programming, I/O Considerations, Programmed I/O, Interrupt I/O, Block, Transfer & DMA.

Unit 4

I/O Design Example, Basic 8086/88 Minimum Mode, maximum mode, Interrupt priority Management,

Unit 5

I/O interfaces, Asynchronous, Synchronous, Programmable Communications interface. Microprocessor Applications

Reference Books:

1. ARM Assembly Language Programming & Architecture By. Muhammad Ali Mazidi, Kindleedition

2. Arm Assembly Language, Fundamentals and Techniques, 2nd edition, William Hohl, Christppher Hinds, CRC Press.
3. Arm System Developer's Guide, Designing and Optimizing Software, Andrew N. Sloss, Dominic Symes, Chris Wwight, Elsevier
4. Arm System-on-chip Architecture, 2nd Edition, Steve Furber, Pearson publication
5. Embedded Systems By. Lyla Das, Pearson publication

CSMT-621 SOFTWARE PROJECT MANAGEMENT

Course Objectives

To understand Project Life Cycle Models, Metrices, Software Configuration Management, Software Quality Assurance, Risk Management, and Project maintenance.

Course Outcomes

CO1:To understand software project management tools and techniques

CO2: To understand and do project planning and scheduling

CO3: To project monitoring and control

CO4: To identify risks and controlling the risks

Course Content

Unit-I
Introduction and Software Project Planning: Fundamentals of Software Project Management (SPM), Need Identification, Vision and Scope document, Project Management Cycle, SPM Objectives, Management Spectrum, SPM Framework, Software Project Planning, Planning Objectives.

Unit-II
Project Organization and Scheduling: Project Elements, Work Breakdown Structure (WBS), Types of WBS, Functions, Activities and Tasks, Project Life Cycle and Product Life Cycle, Ways to Organize Personnel, Project schedule, Scheduling Objectives, Building the project schedule, Scheduling terminology and techniques, Network Diagrams: PERT, CPM, Bar Charts: Milestone Charts, Gantt Charts.

Unit-III
Project Monitoring and Control: Dimensions of Project Monitoring & Control, Earned Value Analysis, Earned Value Indicators: Budgeted Cost for Work Scheduled (BCWS), Cost Variance (CV), Schedule Variance (SV), Cost Performance Index (CPI), Schedule Performance Index (SPI), Interpretation of Earned Value Indicators, Error Tracking, Software Reviews, Types of Review.

Unit-IV
Software Quality Assurance and Testing: Testing Objectives, Testing Principles, Test Plans, Test Cases, Types of Testing, Levels of Testing, Test Strategies, Program Correctness,

Program Verification & validation, Testing Automation & Testing Tools, Concept of Software Quality, Software Quality Attributes, Software Quality Metrics and Indicators, The SEI Capability Maturity Model CMM).

Unit-V

Project Management and Project Management Tools: Software Configuration Management: Software Configuration Items and tasks, Baselines, Plan for Change, Change Control, Change Requests Management, Version Control, Risk Management: Risks and risk types, Risk Breakdown Structure (RBS), Risk Management Process, CASE Tools.

Reference Books:

1. M. Cotterell, "*Software Project Management*", Tata McGraw-Hill Publication.
2. Royce, "*Software Project Management*", Pearson Education
3. Kieron Conway, "*Software Project Management*", Dreamtech Press
4. S. A. Kelkar, "*Software Project Management*", PHI Publication.
5. Harold R. Kerzner, Project Mangment "*A Systems Approach to Planning, Scheduling, and Controlling*"Wiley.
6. Mohapatra, "*Software Project Management*", Cengage Learning