ANNEXURE-IV

SCHEME FOR M. TECH (FULL-TIME) IN COMPUTER SCIENCE & ENGINEERING

SEMESTER – I

S. No.	Course no.	Subjects	L	T	P	Credit
1.	CS - 5xx	Core Subject - I	3	0	0	3
2.	CS - 5xx	Core Subject - II	3	0	0	3
3.	CS - 5xx	Core Subject - III	3	0	0	3
4.	CS - 5xx	Core Subject - IV	3	0	0	3
5.	CS -5xx	Elective-I	3	0	0	3
6.	CS – 5xx	Lab - I	0	0	3	2
7.	CS – 5xx	Lab - II	0	0	3	2
		Total	**15**	**0**	**6**	**19**

SEMESTER – II

S. No.	Course no.	Subjects	L	T	P	Credit
1.	CS - 5xx	Core Subject - V	3	0	0	3
2.	CS - 5xx	Core Subject - VI	3	0	0	3
3.	CS - 5xx	Core Subject - VII	3	0	0	3
4.	CS - 5xx	Core Subject - VIII	3	0	0	3
5.	CS -5xx	Elective-II	3	0	0	3
6.	CS – 5xx	Lab - III	0	0	3	2
7.	CS – 5xx	Lab - IV	0	0	3	2
		Total	**15**	**0**	**6**	**19**

Dr B R Ambedkar National Institute of Technology, Jalandhar
Scheme of M. Tech Programme in Computer Science and Engineering
M. Tech Computer Science and Engineering With Specialization in Information Security to be applicable from 2019 Batch onwards

SEMESTER – III

S. No.	Course no.	Subjects	L	T	P	Credit
1.	CS - 600	M Tech Dissertation Phase-I	0	0	12	6
2.	CS - 601	Project Seminar/ Independent study	0	0	6	3
3.	CS - 5xx	Elective-III	3	0	0	3
4.	CS - 5xx	Elective-IV	3	0	0	3
		Total	**6**	**0**	**18**	**15**

SEMESTER – IV

S. No.	Course no.	Subjects	L	T	P	Credit
1.	CS-600	M Tech Dissertation Phase – II	0	0	24	12
		Total	**0**	**0**	**24**	**12**

GRAND TOTALS OF CREDITS = 65

Dr B R Ambedkar National Institute of Technology, Jalandhar
Scheme of M. Tech Programme in Computer Science and Engineering
M. Tech Computer Science and Engineering With Specialization in Information Security to be applicable from 2019 Batch onwards

LIST OF DEPARTMENTAL CORES FOR M.TECH PROGRAMME IN COMPUTER SCIENCE AND ENGINEERING

Course Code	Course Title	Hrs/week			Credits
		L	T	P	
CS-501	Cryptography	3	0	0	3
CS-502	Advanced Computer Networks	3	0	0	3
CS-503	Advanced Databases and Data Mining	3	0	0	3
CS-504	Advanced Data Structures and Algorithms	3	0	0	3
CS-505	Digital Image Processing	3	0	0	3
CS-506	Machine Learning	3	0	0	3
CS-507	Software Project Management	3	0	0	3
CS-554	Network Security	3	0	0	3
CS-511	Cryptography Laboratory	0	0	3	2
CS-512	Advanced Computer Networks Laboratory	0	0	3	2
CS-513	Advanced Databases and Data Mining Laboratory	0	0	3	2
CS-514	Advanced Data Structures and Algorithms Laboratory	0	0	3	2
	Total	**24**	**0**	**12**	**32**

CS- 501 Cryptography **[3 0 0]**

Course Outcomes: At the completion of the course, students will be able to

CO1: Understand Mathematical foundations of Cryptography theory.

CO2: Analyze the robustness of Cryptosystems.

CO3: Design robust cryptosystem for real time applications.

CO4: Develop prototype Cryptosystems and demonstrate their performance.

Course Contents

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, Modes of Operation (ECB, CBC, OFB,CFB), Strength (or Not) of DES.

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.

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

Hashes and Message Digests: Message Authentication, MD5, SHA, RIPEMD, HMAC, Digital Signatures, Certificates, User Authentication: Digital Signature Standard (DSS and DSA), Security Handshake Pitfalls, Elliptic Curve Cryptosystems.

Authentication of Systems: Kerberos V4 and V5, X.509 Authentication Service.

Electronic Mail Security: Pretty Good Privacy (PGP), S/MIME, X.400, IP and Web Security, IPSec and Virtual Private Networks, Secure Sockets and Transport Layer (SSL and TLS).

Electronic Commerce Security: Electronic Payment Systems, Secure Electronic Transaction (SET), CyberCash, iKey Protocols, Ecash (DigiCash), Digital Watermarking and Steganography.

Text/References:

1. C.Y. Hsiung, "Elementary Theory of Numbers", World Scientific Pub Co Inc, 1992.
2. W. Stallings, "Cryptography and Network Security Principles and Practice", Prentice Hall, 5/e, 2010.
3. Charlie Kaufman, Radia Perlman, "Network Security: Private Communication in a Public World", Prentice

CS- 502 Advanced Computer Networks

Course Outcomes: At the completion of the course, students will be able to

CO1: Understand packet switching networks and routing in packet switching networks with different routing algorithms.

CO2: Describe traffic management at packet level, flow level and flow aggregate levels of packet switching networks.

CO3: Explain the architecture of TCP/IP and protocols associated with TCP/IP and to analyze the network applications, network management and security issues

CO4: Apply the knowledge about QoS, VPNs, and tunneling and overlay networks and to understand mobile networking and wireless sensor networking

Course Contents

Reliable Protocol:

Transmission Control Protocol (TCP): Error Control, Flow Control, Congestion Control, Timers, And TCP Options: NOP, MSS, Window Scale Factor, Timestamp, SACK-Permitted And SACK Options

Stream Control Transmission Protocol (SCTP): Introduction, Services, Features, Packet Format, Association, State Transition Diagram, Flow Control, Error Control, Congestion Control

Congestion Control and Resource Allocation: Issues In Resource Allocation: Network Model, Taxonomy, Evaluation Criteria; Queuing Disciplines: FIFO, Fair Queuing; TCP Congestion Control: Additive Increase/Multiplicative Decrease, Slow Start, Fast Retransmit and Fast Recovery; Congestion-Avoidance Mechanisms: DECbit, Random Early Detection (RED), Source-Based Congestion Avoidance; Quality of Service: Application Requirements, Integrated Services (RSVP), Differentiated Services (EF 516, AF), Equation-Based Congestion Control

Next Generation Network: Unicast Routing Protocols: RIP, OSPF; Multicasting And Multicast Routing Protocols: Introduction, Multicast Addresses, IGMP, Multicast Routing, Routing Protocols, MBone

Internet Protocol Version 6: IPV6 Addressing: Introduction, Address Space Allocation, Global Unicast Addresses, Auto configuration, Renumbering; IPV6 Protocol: Packet Format, Transition from Ipv4 TO Ipv6; Generic Routing Encapsulation (GRE) For Tunnelling.

ICMPv6: Error Messages, Informational Messages, Neighbours-Discovery Messages, Group Membership Messages

Wireless LAN: Infrared vs. Radio Transmission, Infrastructure and Ad Hoc Networks. IEEE 802.11, System Architecture, Protocol Architecture, Physical Layer, Medium Access Control Layer, MAC Management, Future Development, HIPERLAN, Protocol Architecture, Physical Layer, Channel Access Control Sublayer, Medium Access Control Sublayer, Information Bases and Networking, Bluetooth, User Scenarios, Physical Layer, MAC Layer, Networking, Security, Link Management

Text/References:

1. Behrouz A. Forouzan , "TCP/IP Protocol Suite", McGraw- Hill, 4/e, 2009.
2. Larry L. Peterson & Bruce S. Davie, "Computer Network: A System Approach", Morgan Kaufmann, 5/e, 2012.

CS-503 Advanced Databases and Data Mining **[3 0 0]**

Course Outcomes: At the completion of the course, students will be able to

CO1: Understand the advanced concepts of Databases, security and privacy issues and the techniques to handle that.

CO2: To design and develop data warehouses and data marts models and their applications.

CO3: Learn and apply the data mining techniques to find out the hidden patterns and to turn into useful knowledge.

Course Contents

Database Management system: ER Model, Database models, Representation and Evaluation of Relationship Review of Relational Database Design, Normalization, Storage, Access Structures, Query Processing.

Data Warehousing: Overview of data warehousing, Data warehouse design, OLAP technologies, Data cubing. Dimension reduction techniques, Data summarization methods, Clustering, Dimensional Modeling, Metadata, Performance issues and indexing, VLDB issues, Development life cycle, Merits, Tools, Applications and Case Studies.

Data Mining: Overview of knowledge discovery and data mining, Data mining techniques, steps in data mining process, Classification, Decision tees, Patterns, Association rules algorithms, Review of Al-methods, Relation to statistics, databases, machine learning, Visualization, deterministic models, Clustering Regression analysis, Time series analysis, Bayesian learning.

Security and Privacy Protection: An authorization mechanism for a relational database system, Warfare Attacks on Databases, Watermarking Relational Databases, Recent Advances in Access Control Models, Trust Management, Secure Group Key Management, Hippocratic Databases.

Text/References:

1. U. M. Fayyad, G. P. Shapiro, P. Smyth and R. Uthurusamy, "Advances in Knowledge Discovery and Data Mining", The M.IT. Press, 1996.
2. Jiawei Han and Micheline Kamber, "Data Mining Concepts and Techniques", Morgan Kauffmann Publishers, 3/e, 2011.
3. Sean Kelly, "Data Warehousing in Action", John Wiley & Sons Inc., 1997.
4. Michael J. A. Berry, Gordon S. Linoff, "Mastering Data Mining", Wiley, 1999.

CS-504 Advanced Data Structures and Algorithms **[3 0 0]**

Course Outcomes: At the completion of the course, students will be able to

CO1: Enhance their expertise in algorithmic analysis and algorithm design techniques.
CO2: Analyze, design, apply and use data structures and algorithms to solve engineering problems and evaluate their solutions
CO3: Understand and apply amortized analysis on data structures, including binary search trees, merge able heaps and graphs.
CO4: Have an idea of applications of algorithms in a variety of areas including string matching, and databases etc

Course Contents

Elementary Data Structures and Complexity Analysis: Overview of Basic Data Structures: Arrays, Linked List, Stack, Queues. Implementation of Sparse Matrices, Algorithm Complexity: Average, Best and worst case analysis, asymptotic notations, Simple Recurrence Relations and use in algorithm analysis

Search Structures: Binary search trees, AVL trees, 2-3 trees, 2-3-4 trees, Red-black trees, Btrees.

Graph Algorithms: Representation of Graphs, Traversals, Single-source shortest path Algorithms, All-pairs shortest path algorithms, Sub graphs, Disjoint Graphs, Connected Components, Articulation Points, Spanning tree, Minimum Spanning Trees Algorithms, Topological sort

String Matching Algorithms: Introduction, The Brute-Force- Algorithm, Rabin-Karp Algorithm, String Matching

with Finite automata, Knuth-Marries-Pratt Algorithm

Heap Structures: Min-max heaps, Deaps, Leftist heaps, Binomial heaps, Fibonacci heaps, Skew heaps

Multimedia Structures: Segment trees, k-d trees, Point Quad trees, MX-Quad trees, R-trees.

Text / References:

1. E. Horowitz, S.Sahni and Dinesh Mehta, Fundamentals of Data structures in C++, Galgotia, 1999.
2. Adam Drozdex, Data Structures and algorithms in C++, Second Edition, Thomson learning – vikas publishing house, 2001.

CS-505 Digital Image Processing **[3 0 0]**

Course Outcomes: At the completion of the course, students will be able to

CO1: Understand the fundamental concepts of a digital image processing system.
CO2: Evaluate the techniques for image enhancement and image restoration in spatial and frequency domain.
CO3: Categorize various compression techniques.
CO4: Interpret image segmentation and representation techniques.
CO5: Acquire an appreciation for the image processing issues and techniques and apply these techniques to real world problems

Course Contents

Digital Image Fundamentals: Why is Computer Vision Difficult?, Different stages of image processing and analysis, Components of image processing system, Sampling and Quantization, Some basic relationships like neighbor's connectivity, distance measure between pixels.

Image Enhancement and Restoration: Basic Intensity Transformation Functions, Histogram processing, Spatial Domain methods: Fundamentals of spatial filtering, Smoothing Spatial Filters, Sharpening Spatial Filters, Frequency domain methods: low pass filtering, High pass filtering, Image Degradation/Restoration model

Image Compression: Fundamentals of image compression, error criterion, Coding Inter-pixel and Psycho visual redundancy, Image Compression models, Error free compression: Huffman, Arithmetic, Run length Coding, Lossy Compression: Block Transform Coding based on DCT and DWT, Image Compression standard: JPEG.

Morphological image processing: Basic Morphology concepts, Binary dilation and erosion, Opening and Closing operations, Basic Morphological Algorithms: Boundary extraction, Hole Filling, Extraction of Connected Components.

Image Segmentation and Edge Detection: Fundamentals, Point, Line and Edge Detection: Detection of isolated points, lines, Basic Edge Detection, Advanced Edge detection using Canny edge detector, Laplacian edge detector and Laplacian of Gaussian edge detector. Edge Linking and Boundary Detection, Thresholding: Basic Global Thresholding and Optimum Global Thresholding using Otsu's Method, Region Based Segmentation: Region Growing, Region Splitting and Merging

Representation and Description: Representation schemes like chain coding, Polygonal approximation using minimum perimeter polygon, Signatures, Boundary Descriptors: Shape Numbers, Fourier, and Statistical moments. Regional Descriptors: Topological Descriptors, Texture, Moment Invariants

Recognition and Interpretation: Pattern and pattern classes, Decision Theoretic methods: minimum distance classifier, matching by correlation, Structural Methods: Matching Shape Numbers

Text/References:

1. Rafael C. Gonzales and Richard E. Woods, "Digital Image Processing", Pearson Education, 3/e, 2007.
2. Milan Sonka, Vaclav Hlavac and Roger Boyle, "Digital Image Processing and Computer Vision", Cengage Learning, 2007.

CS-507 Software Project Management **[3 0 0]**

Course Outcomes: At the completion of the course, students will be able to

CO1: Learn Conventional Software Management and Evolution of Software Economics

CO2: Understand Project Organizations and Responsibilities

CO3: Understand the evolution and applications of operations in various fields, mathematically formulate linear programming problems and solve them using different techniques

CO4: Construct a project network and apply program evaluation review technique and critical path method to find date of completion of project and other project related metrics

Course Contents

Introduction: Project Management (PM) Fundamentals, People, Process, and Product, Technology Classic mistakes, PMI Processes, Software project phases, Organizational structures, Project charter Statement of Work (SOW)

Planning Phase: Development lifecycle models, Matching lifecycles to projects, Project plans Work Breakdown Structures (WBS)

Estimation and Budgeting: Estimation, Budgeting, Project selection, NPV, ROI, Payback models

Scheduling: Project network diagram fundamentals, PERT techniques, Gantt charts, Critical chain scheduling

Risk and Change Management: Risk management, Change control, More MS-Project

Development Management: Team models, Requirements process, Configuration management, Software metrics, Programming languages & tools, Managing conflict and motivating, MS-Project: Assigning Resources

Status reporting: Project metrics, Earned value analysis, Communications Techniques, Process Improvement,

MS Project:

(a) Resource leveling (b) Other views

System Test Process: Test specifications, Black box and white box testing, Test scripts, Unit and integration testing, Acceptance test specifications, Test tools, MS Project: (a) Reporting

Final Phases & Other Issues: Project Recovery, Documentation, Cutover/Migration, Post Project Reviews, Closing, MS Project: (a) Advanced features

Project Success: Management support, Expectations, Success metrics

Text / References:

1. Kathy Schwalbe, "Information Technology Project Management", Cengage Learning, 7/e, 2013.
2. M. Cottrell and B. Hughes, "Software Project Management", McGraw-Hill, 5/e, 2009.

CS-506 Machine Learning **[3 0 0]**

Course Outcomes: At the completion of the course, students will be able

CO1: Understanding about the basic principles, techniques and applications of machine learning.

CO2: Broad understanding of machine learning algorithms and their use in data-driven knowledge discovery and program synthesis.

CO3: Knowledge of the strengths and weaknesses of different machine learning algorithms (relative to the characteristics of the application domain).

CO4: The ability to adapt or combine some of the key elements of existing machine learning algorithms to design new algorithms as needed.

Course Contents

Introduction: Well-Posed Learning Problems, Designing a Leaning System, Perspectives and Issues in Machine Learning.

Concept Learning and the General-to-Specific Ordering: Introduction, A Concept Learning Task, Concept Learning as Search, FIND-S: Finding a Maximally Specific Hypothesis, Version Spaces and the CANDIDATE-ELIMINATION Algorithm.

Decision Tree Learning: Introduction, Decision Tree Representation, Appropriate problem for Decision tree Learning, The Basic Decision Tree Learning Algorithm, Hypothesis Space Search in Decision Tree Leaning, Inductive Bias in Decision Tree Leaning, Issues in Decision Tree Leaning

Artificial Neural Networks: Introduction, Natural Network Representations, Appropriate Problems for Neural Network Learning, Perceptions, Multilayer Network and the BACKPROPAGATION Algorithm

Bayesian Learning: Introduction, Bayes Theorem, Bayes Theorem and Concept Learning, Bayes Optimal Classifier, Native Bayes Classifier, An Example: Learning to Classify Text.

Instance- Based Learning: Introduction, K-NEAREST NEIGHBOUR Learning, Distance-Weighted NEAREST NEIGHBOUR Algorithm.

Genetic Algorithms: Motivation, Genetic Algorithms, Hypothesis Space Search, Genetic Programming, Parallelizing Genetic Algorithms.

Learning Sets of Rules: Introduction, Sequential Covering Algorithms, Learning Rule Sets: Summary, Learning First-Order Rules, Learning Sets of First-Order Rules: FOIL, Induction as Inverted Deduction, Inverted Resolution.

Support Vector Machine: Maximum margin linear separators, Quadratic Programming Solution to finding maximum margin separators, Kernels for learning non-linear functions.

Text / References:

1. Tom Mitchell, "Machine Learning", McGraw-Hill, 1997.

CS- 512 Advanced Computer Network Laboratory **[0 0 3]**

Course Outcomes: Upon completion of the course, the student should be able to

CO1: Implement various networks environment and passing packets through them using different routing

techniques.

CO2: Design various error control, flow control, and congestion control mechanism in TCP.

CO3: Implement networks environment for simulating various access techniques and Queuing algorithm.

Design scenarios for wireless networks using simulation tools.

Students are required to perform the following list of practicals:

Note: Implementation should be done using C/C++, QualNet/NS2 and other similar tools.

1. Write a program to transfer a file from one system to another system using TCP and UDP sockets.
2. Write a program to demonstrate communication between different processes using IPC.
3. Write a Program to implement Routing Information Protocol (RIP) for a set of nodes.
4. Write a program to implement flow control and congestion control in TCP.
5. Write a program to implement queuing algorithm which will discard the staled packets.
6. Write a congestion control algorithm for routers which will inform the host nodes to stop sending when threshold is reached.
7. Create a network of multiple routers and hosts to simulate RED and Drop Tail Queuing algorithm.
8. Write a program to simulate Group Communication and implement Carrier sensing techniques.
9. Design scenarios for wireless networks using simulation tools.

This is only the suggested list of Practicals. Instructor may frame additional Practicals relevant to the course contents.

CS- 513 Advanced Databases and Data mining Laboratory **[0 0 3]**

Course Outcomes: At the end of this course, students will be able to

CO1: Understand and implement advanced concepts of Data mining on real data.

CO2: Read literature related to the subject and suggest enhancements/ optimizations to the existing work.

CO3: Implement the Data warehouses and perform operations like drill, rollup, and slice etc.

Students are required to perform the following list of practicals:

- Building a Database Design using ER Modeling and Normalization Techniques
- Implementation of functions ,Procedures, Triggers and Cursors
- Feature Selection and Variable Filtering (for very large data sets)
- Association Mining in large data sets
- Interactive Drill-Down, Roll up, Slice and Dice operations
- Generalized EM & k-Means Cluster Analysis
- Generalized Additive Models (GAM)
- General Classification and Regression Trees (GTrees)
- General CHAID (Chi-square Automatic Interaction Detection) Models
- Interactive Classification and Regression Trees
- Boosted Trees
- Multivariate Adaptive Regression Splines (Mar Splines)

- Goodness of Fit Computations
- Rapid Deployment of Predictive Models

This is only the suggested list of Practicals. Instructor may frame additional Practicals relevant to the course contents.

CS- 514 Advanced Data Structure and Algorithm Laboratory **[0 0 3]**

Course Outcomes: After the completion of the course, the students will be able to

CO1: Implement various advance problems using data structures such as stacks, queues, trees, graphs, etc. to solve various computing problems.

CO2: Understand how several fundamental algorithms work particularly those concerned with Stack, Queues, Trees and various Sorting algorithms.

CO3: Design new algorithms or modify existing ones for new applications and able to analyse the space & time efficiency of most algorithms.

CO4: Decide a suitable data structure and algorithm to solve a real-world problem.

Students are required to perform the following list of practicals:

1. Implementation of various algorithms & operations based on Arrays such as Insertion, Deletion, Sorting (Insertion, Bubble, Selection, Shell, Radix, Merge, Quick), Searching (Linear, Binary) and Sparse matrices such as addition, multiplication & transpose.
2. Implementation of Stacks & Queues including priority queues along with various operations on them such as Infix to Postfix conversion, postfix expression evaluation, get minimum element in O(1) time using O(1) additional space using stacks & calculate no. of page faults, reversal of the entire or a part of a queue.
3. Implementation of Linked list and doubly linked list along with solving various problems based on them such as removal of duplicate elements from sorted/Unsorted Linked List, Swapping of nodes by changing link, Segregating odd & even nodes together, binary Search, number of elements in a loop, print nth element from the last, finding the middle element.
4. Implementation of binary trees and various operations based on them such as preorder/ inorder/ postorder traversal using stack, level order traversal, level order traversal in spiral form, left/ right/ top/ bottom view of the tree, vertical order traversal, printing sum of inorder predecessor & successor for each node.
5. Implementation of binary search tree and various problem solving based on them such as finding minimum/ maximum element, traversal in ascending/ descending order, kth largest & kth minimum element, converting binary tree to binary search tree, finding a pair with a given sum.
6. Implementation of AVL trees and various operations based on them such as insertion, deletion and traversal.
7. Implementation of Red/Black trees and various operations based on them such as insertion, deletion and traversal.
8. Implementation of B trees and various operations based on them such as insertion, deletion and traversal.
9. Implementation of heaps & deaps along with various operations based on them such as insertion, deletion, extracting minimum/ maximum element, heap sort, priority queues.
10. Implementation of fibonacci & binomial heaps with various operations based on them such as insertion, union, deletion, extracting minimum/ maximum element.
11. Implementation of various graph based algorithms Dijkstra's shortest path, Warshall's all pair shortest path, breadth & depth first search.
12. Implementation of greedy algorithms like kruskal & prims to find the minimum spanning tree from a given set of nodes and edges.
13. Implementation of various string matching algorithms like brute force, Rabin-karp, Knuth_marries-Pratt and using finite automata.

This is only the suggested list of Practicals. Instructor may frame additional Practicals relevant to the course contents.

CS- 540 Statistical Methods for Research **[3 0 0]**

Course Contents

Introduction to Statistics: Role of Statistics in Engineering.

Introduction to Probability: Basic concepts; random variables; probability functions, laws of probability, Mean and standard deviation of discrete and continuous random variables; Percentile of a random variable; Binomial Distribution, Normal distributions; normal probability plot; Poisson Distribution.

Probability and fitting of standard frequency distributions: Sampling techniques, Sampling distributions

Correlation and Regression: Simple correlation and regression analysis, Partial, Multiple and Intraclass correlation, Multiple Regression analysis.

Large sample tests and confidence intervals: t- Test, Chi Square Test Analysis of Variance for one-way and two-way classification, Transformation of Data.

Text/References:

1. Sukhwinder Singh, M. L. Bansal, T. P. Singh and R K Jindal, "Statistical Methods for Research Workers", 1995.
2. S P Gupta, "Statistical Methods", Sultan Chand & Sons, 2011.
3. Jai P. Gupta and S. S. Saini, "Introduction to Statistical methods", Kalyani Publishers, 1980.
4. Ayub Bilal, and Richard H. McCuen, "Probability, Statistics, & Reliability for Engineers", Boca Raton, Florida: CRC Press, 1997.
5. Jay L. Devore, "Probability and Statistics for Engineering and the Sciences", Pacific Grove, California: Brooks/Cole, 5/e, 2000.

DR. B. R. AMBEDKAR NATIONAL INSTITUTE OF TECHNOLOGY JALANDHAR
CS- 511 Cryptography Laboratory
M.Tech (CSE) 2nd Semester

Course Name:	Cryptography Laboratory	Course Code:			CS- 511
Department:	Computer Science and Engineering	Type:			Core
L-T-P Structure	0-0-3	Credits	2	Pre-requisite:	NA

Sr. No.	List of Programmes
1.	Write a program to implement Ceaser Cipher and Rail fence encryption and decryption.
2.	Write a program to implement Play Fair and Affine Cipher encryption and decryption.
3.	Write a program to implement Hill cipher encryption and decryption.
4.	Write a program to implement DES encryption and decryption.
5.	Write a program to implement AES encryption and decryption.
6.	Write a program to implement Chinese Remainder Theorem (CRT).
7.	Write a program to implement Rabin Miller test for primality.
8.	Write a program to implement RSA encryption and decryption.
9.	Write a program to implement Elgamal encryption and decryption.
10.	Write a program to perform the Diffie-Hellman key exchange between two parties, sending the public key values over the network and verify that you get the same secret key after that use the secret key to encrypt any data and check that the other party can decrypt it.
11.	Write a program to implement Cipher Block Chaining Mode encryption and decryption.
12.	Write a program to implement MD5 hash function to validate data integrity.
13.	Write a program to implement SHA 512 hash function to validate data integrity.
14.	Write a program to implement Digital Signature Standard (DSS).
15.	Write a program to implement Elgamal Digital Signature.
16.	Write a program to implement Email security using SSL and TSL.