Study Scheme & Syllabus of

Master of Technology
Computer Science & Engineering with specialization in Cyber Security

Batch 2018 onwards

By

Board of Study Computer Science Engineering

Department of Academics

IK Gujral Punjab Technical University

First Semester

Sr. No	Course Code	Course Type	Course Title	Load allocation			Marks Distribution		Total Marks	Credits
				L*	T*	P	Internal	External		
1.	MTCS 101-18	Program Core I	Mathematical foundations of Computer Science	3	0	0	40	60	100	3
2.	MTCS 102-18	Program Core II	Advanced Data Structures	3	0	0	40	60	100	3
3.	MTCY 101-18	Program Elective I	Digital Forensics	3	0	0	40	60	100	3
	MTCY 102-18		Ethical Hacking							
	MTCY 103-18		Intrusion Detection							
4.	MTCY 104-18	Program Elective II	Malware Analysis &Reverse Engineering	3	0	0	40	60	100	3
	MTCS 207-18		Secure Software Design and Enterprise Computing							
	MTCS 105-18		Machine Learning							
5.	MTRM 101-18		Research Methodology & IPR	2	0	0	40	60	100	2
6.	MTA-***		Audit Course	2	0	0	0	0	0	0
7.	MTCS 103-18	Laboratory 1	(Advanced Data Structures)	0	0	4	60	40	100	2
8.	MTCY 106-18	Laboratory 2	(Based on Electives)	0	0	4	60	40	100	2
9.		**TOTAL**		**16**	**0**	**8**	**320**	**380**	**700**	**18**

Second Semester

Sr. No	Course Code	Course Type	Course Title	Load allocation			Marks Distribution		Total Marks	Credits
				L*	T*	P	Internal	External		
1.	MTCS 201-18	Program Core III	Advance Algorithms	3	0	0	40	60	100	3
2.	MTCS 202-18	Program Core IV	Soft Computing	3	0	0	40	60	100	3
3.	MTCY 201-18	Program Elective III	Cryptography	3	0	0	40	60	100	3
	MTCY 202-18		Steganography & Digital Watermarking							
	MTCY 203-18		Information Theory &Coding							
4.	MTCY 204-18	Program Elective IV	Security Assessment and Risk Analysis	3	0	0	40	60	100	3
	MTCY 205-18		Secure Coding							
	MTCY 206-18		Biometrics							
5.	MTA-***	Program Core	Audit Course	2	0	0	40	60	100	0
6.	MTCS 203-18	Program Core	Laboratory 3 (Based on cores)	2	0	0	0	0	0	2
7.	MTCY 207-18	Program Core	Laboratory 4 (Based on Electives)	0	0	4	60	40	100	2
8.	MTCY 208-18	Program Core	Mini Project with Seminar	2	0	4	60	40	100	2
9.			**TOTAL**	**16**	**0**	**0**	**320**	**380**	**700**	**18**

Third Semester

Sr. No	Course Code	Course Type	Course Title	Load allocation			Marks Distribution		Total Marks	Credits
				L*	T*	P	Internal	External		
1.	MTCY 301-18	Program Elective V	Ethics and Law of Cyber Security	3	0	0	40	60	100	3
	MTCY302-18		Proactive Security Tools and Technique	3	0	0	40	60	100	3
	MTCY303-18		Data base Security and Access control	3	0	0	40	60	100	3
2.	MTOE 301-18	Open Elective	Business Analytics	3	0	0	40	60	100	3
	MTOE 302-18		Industrial Safety							
	MTOE 303-18		Operations Research							
	MTOE 304-18		Cost Management of Engineering Projects							
	MTOE 305-18		Composite Materials							
	MTOE 306-18		Waste to Energy							
3.	MTCY 302-18		Dissertation-I	0	0	4	60	40	100	2
4.	MTCY 303-18		Industrial / Institution Project	0	0	0	60	40	100	2
5.		**TOTAL**		**16**	**0**	**4**	**320**	**380**	**700**	**18**

Note: This is to be taken up after second semester, for 6-8 weeks in summer, in industry/institution of repute

Course Code	Course Type	Course Title	Load allocation			Marks Distribution		Total Marks	Credits
			L *	T *	P	Internal	External		
MTCS 401-18	Thesis	Dissertation - II	0	0	32	-	-	S/US	16
	TOTAL		**0**	**0**	**32**				**16**

Audit course 1 & 2

1. English for Research Paper Writing
2. Disaster Management
3. Sanskrit for Technical Knowledge
4. Value Education
5. Constitution of India
6. Pedagogy Studies
7. Stress Management by Yoga
8. Personality Development through Life Enlightenment Skills.

Course Code	MTCS101-18
Course Name	Mathematical Foundation of Computer Science
Credits	3
Pre-Requisites	Discrete Mathematics

Total Number of Lectures:48

COURSE OBJECTIVE
• To understand the mathematical fundamentals that is prerequisites for a variety of courses like Data mining, Network protocols, analysis of Web traffic, Computer security, Software engineering, Computer architecture, operating systems, distributed systems, Bioinformatics, Machine learning.
• To develop the understanding of the mathematical and logical basis to many modern techniques in in for technology like machine learning, programming language design, and concurrency.
• To study various sampling and classification problems.

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Unit 1 Probability mass, density, and cumulative distribution functions, Parametric families of distributions, Expected value, variance, conditional expectation, Applications of the univariate and multivariate Central Limit Theorem, Probabilistic inequalities, Markov chains	7
Unit 2 Random samples, sampling distributions of estimators**,** Methods of Moments and Maximum Likelihood**,**	7
Unit 3 Statistical inference**,** Introduction to multivariate statistical models: regression and classification problems, principal components analysis**,** The problem of overfitting model assessment.	8
Unit 4 Graph Theory: Isomorphism, Planar graphs, graph colouring, hamilton circuits and euler cycles. Permutations and Combinations with and without repetition. Specialized techniques to solve combinatorial enumeration problems	11
Unit 5 **Computer science and engineering applications** Data mining, Network protocols, analysis of Web traffic, Computer security, Software engineering, Computer architecture, operating systems, distributed systems, Bioinformatics, Machine learning.	10
Unit 6 Recent Trands in various distribution functions in mathmatical field of computer science for varying fields like bioinformatic, soft computing, and computer vision.	5

COURSE OUTCOMES
After completion of course, students would be able to:
• To understand the basic notions of discrete and continuous probability.
• To understand the methods of statistical inference, and the role that sampling distributions play in those methods.
• To be able to perform correct and meaningful statistical analyses of simple to moderate complexity.

References

1. John Vince, Foundation Mathematics for Computer Science, Springer.
2. K. Trivedi.Probability and Statistics with Reliability, Queuing, and Computer Science Applications. Wiley.
3. M. Mitzenmacher and E. Upfal.Probability and Computing: Randomized Algorithms and Probabilistic Analysis.
4. Alan Tucker, Applied Combinatorics, Wiley

Course Code	MTCS102-18
Course Name	Advanced Data Structures
Credits	3
Pre-Requisites	UG level course in Data Structures

Total Number of Lectures:48

COURSE OBJECTIVE
• The student should be able to choose appropriate data structures, understand the ADT/libraries, and use it to design algorithms for a specific problem.
• Students should be able to understand the necessary mathematical abstraction to solve problems.
• To familiarize students with advanced paradigms and data structure used to solve algorithmic problems.
• Student should be able to come up with analysis of efficiency and proofs of correctness.

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Unit 1 **Dictionaries:** Definition, Dictionary Abstract Data Type, Implementation of Dictionaries. **Hashing:** Review of Hashing, Hash Function, Collision Resolution Techniques in Hashing, Separate Chaining, Open Addressing, Linear Probing, Quadratic Probing, Double Hashing, Rehashing, Extendible Hashing.	7
Unit 2 **Skip Lists:** Need for Randomizing Data Structures and Algorithms, Search and Update Operations on Skip Lists, Probabilistic Analysis of Skip Lists, Deterministic Skip Lists	5
Unit 3 **Trees:** Binary Search Trees, AVL Trees, Red Black Trees, 2-3 Trees, B-Trees, Splay Trees	9
Unit 4	12
Text Processing: Sting Operations, Brute-Force Pattern Matching, The Boyer-Moore Algorithm, The Knuth-Morris-Pratt Algorithm, Standard Tries, Compressed Tries, Suffix Tries, The Huffman Coding Algorithm, The Longest Common Subsequence Problem (LCS), Applying Dynamic Programming to the LCS Problem.	
Unit 5 **Computational Geometry:** One Dimensional Range Searching, Two Dimensional Range Searching, Constructing a Priority Search Tree, Searching a Priority Search Tree, Priority Range Trees, Quadtrees, k-D Trees.	10
Unit 6 Recent Trands in Hashing, Trees, and various computational geometry methods for effeciently solving the new evolving problem	5

COURSE OUTCOMES
After completion of course, students would be able to:
• Understand the implementation of symbol table using hashing techniques.
• Develop and analyze algorithms for red-black trees, B-trees and Splay trees.
• Develop algorithms for text processing applications.
• Identify suitable data structures and develop algorithms for computational geometry problems.

References:

1. Mark Allen Weiss, Data Structures and Algorithm Analysis in C++, 2nd Edition, Pearson, 2004.
2. M T Goodrich, Roberto Tamassia, Algorithm Design, John Wiley, 2002.

Course Code	MTCY101-18
Course Name	Digital Forensics
Credits	3
Pre-Requisites	Cybercrime and Information Warfare, Computer Networks

Total Number of Lectures: 48

COURSE OBJECTIVE
• Provides an in-depth study of the rapidly changing and fascinating field of computer forensics.
• Combines both the technical expertise and the knowledge required to investigate, detect and prevent digital crimes.
• Knowledge on digital forensics legislations, digital crime, forensics processes and procedures, data acquisition and validation, e-discovery tools
• E-evidence collection and preservation, investigating operating systems and file systems, network forensics, art of steganography and mobile device forensics

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Unit 1: **Digital Forensics Science:** Forensics science, computer forensics, and digital forensics. **Computer Crime:** Criminalistics as it relates to the investigative process, analysis of cyber-criminalistics area, holistic approach to cyber-forensics	9
Unit 2: **Cyber Crime Scene Analysis:** Discuss the various court orders etc., methods to search and seizure electronic evidence, retrieved and un-retrieved communications, Discuss the importance of understanding what court documents would be required for a criminal investigation.	8
Unit 3: **Evidence Management & Presentation:** Create and manage shared folders using operating system, importance of the forensic mindset, define the workload of law enforcement, Explain what the normal case would look like, Define who should be notified of a crime, parts of gathering evidence, Define and apply probable cause.	9
Unit 4: **Computer Forensics:** Prepare a case, Begin an investigation, Understand computer forensics workstations and software, Conduct an investigation, Complete a case, Critique a case, **Network Forensics:** open-source security tools for network forensic analysis, requirements for preservation of network data.	10
Unit 5: **Mobile Forensics:** mobile forensics techniques, mobile forensics tools. **Legal Aspects of Digital Forensics:** IT Act 2000, amendment of IT Act 2008.	8
Unit 6: Recent trends in mobile forensic technique and methods to search and seizure electronic evidence	4

COURSE OUTCOMES
After completion of course, students would be able to:
• Understand relevant legislation and codes of ethics
• Computer forensics and digital detective and various processes, policies and procedures
• E-discovery, guidelines and standards, E-evidence, tools and environment.
• Email and web forensics and network forensics

References:

1. John Sammons, The Basics of Digital Forensics, Elsevier
2. John Vacca, Computer Forensics: Computer Crime Scene Investigation, Laxmi Publications

Course Code	MTCY102-18
Course Name	Ethical Hacking
Credits	3
Pre-Requisites	Computer Programming, Web Programming, Computer Networks

Total Number of Lectures: 48

COURSE OBJECTIVE
• Introduces the concepts of Ethical Hacking and gives the students the opportunity to learn about different tools and techniques in Ethical hacking and security and practically apply some of the tools.

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Unit 1: Introduction to Ethical Disclosure: Ethics of Ethical Hacking, Ethical Hacking and the legal system, Proper and Ethical Disclosure	9
Unit 2: Penetration Testing and Tools: Using Metasploit, Using BackTrackLiveCD Linux Distribution	8
Unit 3: Vulnerability Analysis: Passive Analysis, Advanced Static Analysis with IDA Pro, Advanced Reverse Engineering	9
Unit 4: Client-side browser exploits, Exploiting Windows Access Control Model for Local Elevation Privilege, Intelligent Fuzzing with Sulley, From Vulnerability to Exploit	10
Unit 5: Malware Analysis: Collecting Malware and Initial Analysis, Hacking Malware	8
Unit 6: Case study of vulnerability of cloud platforms and mobile platforms & devices.	4

COURSE OUTCOMES
After completion of course, students would be able to:
• Understand the core concepts related to malware, hardware and software vulnerabilities and their causes
• Understand ethics behind hacking and vulnerability disclosure
• Appreciate the Cyber Laws and impact of hacking
• Exploit the vulnerabilities related to computer system and networks using state of the art tools and technologies

References:

1. Shon Harris, Allen Harper, Chris Eagle and Jonathan Ness, Gray Hat Hacking: The Ethical Hackers' Handbook, TMH Edition
2. Jon Erickson, Hacking: The Art of Exploitation, SPD

Course Code	MTCY103-18
Course Name	Intrusion Detection
Credits	3
Pre-Requisites	Computer Networks, Computer Programming

Total Number of Lectures: 48

COURSE OBJECTIVE
• Compare alternative tools and approaches for Intrusion Detection through quantitative analysis to determine the best tool or approach to reduce risk from intrusion
• Identify and describe the parts of all intrusion detection systems and characterize new and emerging IDS technologies according to the basic capabilities all intrusion detection systems share.

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Unit 1: The state of threats against computers, and networked systems-Overview of computer security solutions and why they fail-Vulnerability assessment, firewalls, VPN's -Overview of Intrusion Detection and Intrusion Prevention-Network and Host-based IDS	10
Unit 2: Classes of attacks - Network layer: scans, denial of service, penetration-Application layer: software exploits, code injection-Human layer: identity theft, root access-Classes of attackers-Kids/hackers/sop Hesitated groups-Automated: Drones, Worms, Viruses	8
Unit 3: A General IDS model and taxonomy, Signature-based Solutions, Snort, Snort rules, Evaluation of IDS, Cost sensitive IDS	8
Unit 4: Anomaly Detection Systems and Algorithms-Network Behavior Based Anomaly Detectors (rate based)-Host-based Anomaly Detectors-Software Vulnerabilities-State transition, Immunology, Payload Anomaly Detection	10
Unit 5: Attack trees and Correlation of alerts-Autopsy of Worms and Botnets-Malware detection-Obfuscation, polymorphism-Document vectors	8
Unit 6: Email/IM security issues-Viruses/Spam-From signatures to thumbprints to zero-day detection-Insider Threat issues-Taxonomy-Masquerade and Impersonation-Traitors, Decoys and Deception-Future: Collaborative Security	4

COURSE OUTCOMES
After completion of course, students would be able to:
• Apply knowledge of the fundamentals and history of Intrusion Detection in order to avoid common pitfalls in the creation and evaluation of new Intrusion Detection Systems. Evaluate the security an enterprise and appropriately apply Intrusion Detection tools and techniques in order to improve their security posture

References:

1. The Art of Computer Virus Research and Defense, Peter Szor, Symantec Press ISBN 0-321-30545-3
2. Crimeware, Understanding New Attacks and Defenses, Markus Jakobsson and Zulfikar Ramzan, Symantec Press, ISBN: 978-0-321-50195-0 2008

Course Code	MTCY 104-18
Course Name	Malware Analysis and Reverse Engineering
Credits	3
Pre-Requisites	Computer Programming, Compiler Design

Total Number of Lectures: 48

COURSE OBJECTIVE
• The objective of this course is to provide an insight to fundamentals of malware analysis which includes analysis of JIT compilers for malware detection in legitimate code. DNS filtering and reverse engineering is included.

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Unit 1: Fundamentals of Malware Analysis (MA), Reverse Engineering Malware (REM) Methodology, Brief Overview of Malware analysis lab setup and configuration, Introduction to key MA tools and techniques, Behavioral Analysis vs. Code Analysis, Resources for Reverse-Engineering Malware (REM) Understanding Malware Threats, Malware indicators, Malware Classification, Examining ClamAVSignatures, Creating Custom ClamAV Databases, Using YARA to Detect Malware Capabilities, Creating a Controlled and Isolated Laboratory, Introduction to MA Sandboxes, Ubuntu, Zeltser'sREMnux, SANS SIFT, Sandbox Setup and Configuration New Course Form, Routing TCP/IP Connections, Capturing and Analyzing Network Traffic, Internet simulation using INetSim, Using Deep Freeze to Preserve Physical Systems, Using FOG for Cloning and Imaging Disks, Using MySQL Database to Automate FOG Tasks, Introduction to Python ,Introduction to x86 Intel assembly language, Scanners: Virus Total, Jotti, and NoVirus Thanks, Analyzers: Threat Expert, CWSandbox, Anubis, Joebox, Dynamic Analysis Tools: Process Monitor, Regshot, HandleDiff, Analysis Automation Tools: Virtual Box, VM Ware, Python , Other Analysis Tools	12
Unit 2:Malware Forensics Using TSK for Network and Host Discoveries, Using Microsoft Offline API to Registry Discoveries , Identifying Packers using PEiD, Registry Forensics with Reg Ripper Plu-gins:, Bypassing Poison Ivy's Locked Files, Bypassing Conficker's File System ACL Restrictions, Detecting Rogue PKI Certificates.	7
Unit 3:Malware and Kernel Debugging Opening and Attaching to Processes, Configuration of JIT Debugger for Shellcode Analysis, Controlling Program Execution, Setting and Catching Breakpoints, Debugging with Python Scripts and Py Commands**,** DLL Export Enumeration, Execution, and Debugging**,** Debugging a VMware Workstation Guest (on Windows)**,** Debugging a Parallels Guest (on Mac OS X). Introduction to WinDbg Commands and Controls, Detecting Rootkits with WinDbgScripts**,** Kernel Debugging with IDA Pro.	9
Unit 4:Memory Forensics and Volatility Memory Dumping with MoonSols Windows Memory Toolkit**,** Accessing VM Memory Files Overview of Volatility, Investigating Processes in Memory Dumps**,** Code Injection and Extraction**,** Detecting and Capturing Suspicious Loaded DLLs**,** Finding Artifacts in Process Memory**,** Identifying Injected Code with Malfind and YARA.	8

Unit 5:Researching and Mapping Source Domains/IPs Using WHOIS to Research Domains**,** DNS Hostname Resolution**,** Querying Passive DNS**,** Checking DNS Records**,** Reverse IP Search New Course Form**,** Creating Static Maps**,** Creating Interactive Maps.	7
Unit 6: Case study of Finding Artifacts in Process Memory, Identifying Injected Code with Malfind and YARA	5

COURSE OUTCOMES
On completion of the course the student should be able to
• To understand the concept of malware and reverse engineering.
• Implement tools and techniques of malware analysis.

References:

1. Michael Sikorski, Andrew Honig "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software" publisher Williampollock

Course Code	MTCS207-18
Course Name	Secure Software Design and Enterprise Computing
Credits	3
Pre-Requisites	Computer Programming, Software Engineering

Total Number of Lectures:48

COURSE OBJECTIVE
• To fix software flaws and bugs in various software.
• To make students aware of various issues like weak random number generation, information leakage, poor usability, and weak or no encryption on data traffic
• Techniques for successfully implementing and supporting network services on an enterprise scale and heterogeneous systems environment.
• Methodologies and tools to design and develop secure software containing minimum vulnerabilities and flaws.

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Unit 1: **Secure Software Design** Identify software vulnerabilities and perform software security analysis, Master security programming practices, Master fundamental software security design concepts, Perform security testing and quality assurance.	8
Unit 2: **Enterprise Application Development** Describe the nature and scope of enterprise software applications, Design distributed N-tier software application, Research technologies available for the presentation, business and data tiers of an enterprise software application, Design and build a database using an enterprise database system, Develop components at the different tiers in an enterprise system, Design and develop a multi-tier solution to a problem using technologies used in enterprise system, Present software solution.	11
Unit 3: **Enterprise Systems Administration** Design, implement and maintain a directory-based server infrastructure in a heterogeneous systems environment, Monitor server resource utilization for system reliability and availability, Install and administer network services (DNS/DHCP/Terminal Services/Clustering/Web/Email).	
Unit 4: Obtain the ability to manage and troubleshoot a network running multiple services, Understand the requirements of an enterprise network and how to go about managing them.	8

Unit 5: Handle insecure exceptions and command/SQL injection, Defend web and mobile applications against attackers, software containing minimum vulnerabilities and flaws.	9
Unit 6: Case study of DNS server, DHCP configuration and SQL injection attack.	4

COURSE OUTCOMES
After completion of course, students would be able to:
• Differentiate between various software vulnerabilities.
• Software process vulnerabilities for an organization.
• Monitor resources consumption in a software.
• Interrelate security and software development process.

References:

1. Theodor Richardson, Charles N Thies, Secure Software Design, Jones & Bartlett
2. Kenneth R. van Wyk, Mark G. Graff, Dan S. Peters, Diana L. Burley, Enterprise Software Security, Addison Wesley.

Course Code	MTCS105-18
Course Name	Machine learning
Credits	3
Pre-Requisites	

Total Number of Lectures:48

COURSE OBJECTIVE
• To learn the concept of how to learn patterns and concepts from data without being explicitly programmed in various IOT nodes.
• To design and analyse various machine learning algorithms and techniques with a modern outlook focusing on recent advances.
• Explore supervised and unsupervised learning paradigms of machine learning.
• To explore Deep learning technique and various feature extraction strategies.

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Unit 1: **Supervised Learning (Regression/Classification)** • Basic methods: Distance-based methods, Nearest-Neighbours, Decision Trees, Nave Bayes Linear models: Linear Regression, Logistic Regression, Generalized Linear Models • Support Vector Machines, Nonlinearity and Kernel Methods • Beyond Binary Classification: Multi-class/Structured Outputs, Ranking	10
Unit 2: **Unsupervised Learning** • Clustering: K-means/Kernel K-means • Dimensionality Reduction: PCA and kernel PCA • Matrix Factorization and Matrix Completion • Generative Models (mixture models and latent factor models)	7
Unit 3 Evaluating Machine Learning algorithms and Model Selection, Introduction to Statistical Learning Theory, Ensemble Methods (Boosting, Bagging, Random Forests)	6
Unit 4 Sparse Modeling and Estimation, Modeling Sequence/Time-Series Data, Deep Learning and Feature Representation Learning	9
Unit 5 Scalable Machine Learning (Online and Distributed Learning) A selection from some other advanced topics, e.g., Semi-supervised Learning, Active Learning, Reinforcement Learning, Inference in Graphical Models, Introduction to Bayesian Learning and Inference	9

Unit 6: Recent trends in various learning techniques of machine learning and classification methods for IOT applications. Various models for IOT applications.	5

COURSE OUTCOMES
After completion of course, students would be able to:
• Extract features that can be used for a particular machine learning approach in various IOT applications.
• To compare and contrast pros and cons of various machine learning techniques and to get an insight of when to apply a particular machine learning approach.
• To mathematically analyse various machine learning approaches and paradigms.

References:

1. Kevin Murphy, Machine Learning: A Probabilistic Perspective, MIT Press, 2012
2. Trevor Hastie, Robert Tibshirani, Jerome Friedman, The Elements of Statistical Learning, Springer 2009 (freely available online)
3. Christopher Bishop, Pattern Recognition and Machine Learning, Springer, 2007.

Course Code	**MTRM-101-18**
Course Name	**Research Methodology and IPR**
Credits	2
Pre-Requisites	

Total Number of Lectures:48

COURSE OBJECTIVE
• Understand research problem formulation.
• Analyze research related information
• Follow research ethics
• Understand that today's world is controlled by Computer, Information Technology, but tomorrow world will be ruled by ideas, concept, and creativity.
• Understanding that when IPR would take such important place in growth of individuals & nation, it is needless to emphasis the need of information about Intellectual Property Right to be promoted among students in general & engineering in particular.
• Understand that IPR protection provides an incentive to inventors for further research work and investment in R & D, which leads to creation of new and better products, and in turn brings about, economic growth and social benefits.

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Unit 1: Meaning of research problem, Sources of research problem, Criteria Characteristics of a good research problem, Errors in selecting a research problem, Scope and objectives of research problem.Approaches of investigation of solutions for research problem, data collection, analysis, interpretation, Necessary instrumentations	10
Unit 2: Unit 2: Effective literature studies approaches, analysis Plagiarism, Research ethics.	7
Unit 3 Effective technical writing, how to write report, Paper Developing a Research Proposal, Format of research proposal, a presentation and assessment by a review committee	6

Unit 4 Nature of Intellectual Property: Patents, Designs, Trade and Copyright. Process of Patenting and Development: technological research, innovation, patenting, development. International Scenario: International cooperation on Intellectual Property. Procedure for grants of patents, Patenting under PCT.	9
Unit 5 Patent Rights: Scope of Patent Rights. Licensing and transfer of technology. Patent information and databases. Geographical Indications.	9
Unit 6: New Developments in IPR: Administration of Patent System. New developments in IPR; IPR of Biological Systems, Computer Software etc. Traditional knowledge Case Studies, IPR and IITs.	5

References:

1. Stuart Melville and Wayne Goddard, "Research methodology: an introduction for science & engineering students'"
2. Wayne Goddard and Stuart Melville, "Research Methodology: An Introduction"
3. Ranjit Kumar, 2nd Edition , "Research Methodology: A Step by Step Guide for beginners"
4. Halbert, "Resisting Intellectual Property", Taylor & Francis Ltd, 2007.
5. Mayall , "Industrial Design", McGraw Hill, 1992.
6. Niebel , "Product Design", McGraw Hill, 1974.
7. Asimov, "Introduction to Design", Prentice Hall, 1962.
8. Robert P. Merges, Peter S. Menell, Mark A. Lemley, " Intellectual Property in New Technological Age", 2016.

   T. Ramappa, "Intellectual Property Rights Under WTO", S. Chand, 2008

LIST of EXPERIMENTS for LABORATORIES of M.TECH- Cyber Security, 2018 onwards (First Semester)

COURSE CODE: MTCS103-18
COURSE NAME: LAB. ON ADVANCED DATA STRUCTURES
CREDITS: 02, HOURS: 04

Programs may be implemented using C/C++/java

EXP 1:WAP to store k keys into an array of size n at the location computed using a hash function, loc = key % n, where k<=n and k takes values from [1 to m], m>n. To handle the collisions use the following collision resolution techniques,

a. Linear probing
b. Quadratic probing
c. Double hashing/rehashing
d. Chaining

EXP 2: WAP for Binary Search Tree to implement following operations:

a. Insertion
b. Deletion i. Delete node with only child ii. Delete node with both children
c. Finding an element
d. Finding Min element
e. Finding Max element
f. Left child of the given node
g. Right child of the given node
h. Finding the number of nodes, leaves nodes, full nodes, ancestors, descendants.

EXP 3: WAP for AVL Tree to implement following operations: (For nodes as integers)

a. Insertion: Test program for all cases (LL, RR, RL, LR rotation)
b. Deletion: Test Program for all cases (R0, R1, R-1, L0, L1, L-1)
c. Display: using set notation.

EXP 4: WAP to implement Red-Black trees with insertion and deletion operation for the given input data as Integers/Strings

EXP 5:WAP to implement insertion, deletion, display and search operation in m-way B tree (i.e. a non-leaf node can have at most m children) for the given data as integers.

EXP 6:WAP to perform string matching using Knuth-Morris-Pratt algorithm.

EXP 7: WAP to perform string matching using Boyer-Moore algorithm.

EXP 8:WAP to implement 2-D range search over computational geometry problem

EXP 9:WAP on latest efficient algorithms on trees for solving contemporary problems.

Mini Project: Student has to do a project assigned from course contents in a group of two or three students. The team will have to demonstrate as well as have to give a presentation of the same.

COURSE CODE: MTCY106-18
COURSE NAME: LABORATORY. 2 (BASED ON ELECTIVE I and II)
CREDITS: 02, (Elective I + Elective II)
HOURS: 2 hours for Lab based on ElectiveI & 2 hours for Lab based on Elective II

ELECTIVE – I

Digital Forensics laboratory

Expt1: Study the adversarial nature of the legal system by preparing arguments on both sides of a case. Legal Aspects of Digital Forensics
Expt2: Expert testimony, preparing an expert report, expert depositions, and getting experts' testimony admitted.
Expt3: Introduction to The Sleuth Kit (TSK) and Autopsy.
Expt 4: Implement NTFS analysis.
Expt 5: Apply concept of File carving.
Expt 6: Implement Deleted file recovery.
Expt 7: Apply concept of Windows application analysis.
Expt 8: to Develop a psychological profile of cyber offenders.
Expt 9: Implementation of Packet capture and protocol analysis
Expt 10: To apply the concept of Evidence acquisition

Ethical Hacking Lab

Expt 1.Apply concept of Foot printing.
Expt 2. Implementation of Network scanning.
Expt 3. Implementation of Steganography under various objects.
Expt 4. Apply the concept of Privilege escalation.
Expt 5. Apply the concept in Building a trojan and virus creation in a batch file.
Expt 6. Implemet Packet sniffing through wireshark.
Expt 7. Implement SQL injections.
Expt 8. Implement Arp poisoning.
Expt 9. Implement Wireless/wifi hacking.
Expt 10. Apply concept of Keyloggers

ELECTIVE II

Secure Software Design and Enterprise Computing Lab

Case Study Analysis:

Based on a real-life situation, for example an armed intervention, a stock market crash or a cyber attack, the students are tasked with a strategic analysis of given problem. In particular, the students are to develop specific criteria and conduct an assessment of the problem as follows:

1. Understanding and documenting types of cyber attacks.
2. Analyzing and mitigating collected data after a cyber attack has occurred.
3. Creating a cyber risk assessment and mitigation Plan.

For case analysis, consider the following proposed process:

Read the situation carefully and consider the key issues.

1. Determine which aspects are the most important to consider. For each aspect/area of importance identified, do the following:
   - Identify key/relevant/critical items and compile facts.
   - Identify problems, elements for more in depth analysis and record in comparative matrices.
   - Consider and document the actions that should be taken to correct the particular negative impacts into positive or negligible outcomes.
   - Determine the positive or negative impact that each item will have against one and another by evaluating the effect of these collective impacts. Be sure to discuss the positive and negative influences caused by their collective interactions

MACHINE LEARNING LAB: Programs may be implemented using WEKA/R/PYTHON etc. similar sofftwares

Expt. 1:Study of platform for Implementation of Assignments

Download the open source software of your interest. Document the distinct features and functionality of the software platform. You may choose WEKA, R or any other software.

Expt. 2:Supervised Learning – Regression

Generate a proper 2-D data set of N points.
Split the data set into Training Data set and Test Data set.

i) Perform linear regression analysis with Least Squares Method.
ii) Plot the graphs for Training MSE and Test MSE and comment on Curve Fitting and Generalization Error.
iii) Verify the Effect of Data Set Size and Bias-Variance Trade off.
iv) Apply Cross Validation and plot the graphs for errors.
v) Apply Subset Selection Method and plot the graphs for errors.

Describe your findings in each case.

Expt. 3:Supervised Learning – Classification

Implement Naïve Bayes Classifier and K-Nearest Neighbour Classifier on Data set of your choice. Test and Compare for Accuracy and Precision.

Expt. 4: Unsupervised Learning
Implement K-Means Clustering and Hierarchical clustering on proper data set of your choice. Compare their Convergence.

Expt. 5:Dimensionality Reduction
Principal Component Analysis-Finding Principal Components, Variance and Standard Deviation calculations of principal components.

Expt. 6: Supervised Learning and Kernel Methods
Design, Implement SVM for classification with proper data set of your choice. Comment on Design and Implementation for Linearly non-separable Dataset.

Mini Project: Student has to do a project assigned from course contents in a group of two or three students. The team will have to demonstrate as well as have to give a presentation of the same**.**

Intrusion Detection laboratory
Expt 1. Identify software security countermeasures and network defences in any operating system.
Expt 2. To install an IDS on a real machine on GENI
Expt 3. To use the IDS to detect Distributed Denial of Service Attacks
Expt 4. To create and study IDS rules
Expt 5. To fetch IDS logs and understand them
Expt 6. Explain the functioning, strengths, and weaknesses of cryptography, authentication, access control, and intrusion detection systems. To get you acquainted with different Intrusion Detection Systems (IDSs)
Expt 7. To analyze the computer network traffic from this attack, we will use tool called Wireshark.
Expt 8. To analyze the Iperf tool through command line to generate computer network traffic that resembles regular usage of a computer network.
Expt 9. To analyze Hping3 tool to the any network flood.
Expt 10. To analyse Snort tool to crosscheck given database against signatures.
Expt 11. To analyse Nmap tool to crosscheck vulnerabilities.
Expt 12. To analyse AppSpear tool to crosscheck malwares.

Malware Analysis & Reverse Engineering Laboratory
Expt 1. Build an isolated, controlled laboratory environment for analyzing the code and behavior of malicious programs.
Expt 2. Employ network and system-monitoring tools to examine how malware interacts with the file system, registry, network, and other processes in a Windows environment.
Expt 3. Uncover and analyze malicious JavaScript and VBScript components of web pages, which are often used by exploit kits for drive-by attacks.
Expt 4. Control relevant aspects of the malicious program's behavior through network traffic interception and code patching to perform effective malware analysis.

Expt 5. Use a disassembler and a debugger to examine the inner workings of malicious Windows executables.
Expt 6. Bypass a variety of packers and other defensive mechanisms designed by malware authors to misdirect, confuse, and otherwise slow down the analyst.
Expt 7. Recognize and understand common assembly-level patterns in malicious code, such as DLL injection and anti-analysis measures.
Expt 8. Assess the threat associated with malicious documents, such as PDF and Microsoft Office files, in the context of targeted attacks.
Expt 9. Derive Indicators of Compromise from malicious executables to perform incident response triage.
Expt 10. Utilize practical memory forensics techniques to examine the capabilities of rootkits and other malicious program types.
Expt 11. Analyzing protected malicious browser scripts written in JavaScript and VBScript.
Expt 12. Write a Reverse-engineering malicious Flash program for given drive-by attacks.