DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Scheme of Instruction and Syllabus of

M.Tech (CYBER SECURITY)

Full-Time & CEEP

2025-2026

UNIVERSITY COLLEGE OF ENGINEERING
(Autonomous)
Osmania University
Hyderabad – 500 007, TS, INDIA

INSTITUTE

Vision

The Vision of the institute is to generate and disseminate knowledge through harmonious blending of science, engineering and technology.

To serve the society by developing a modern technology in students‟ heightened intellectual, cultural, ethical and humane sensitivities, fostering a scientific temper and promoting professional and technological expertise.

Mission

- To achieve excellence in Teaching and Research
- To generate , disseminate and preserve knowledge
- To enable empowerment through knowledge and information
- Advancement of knowledge in Engineering, Science and Technology
- Promote learning in free thinking and innovative environment
- Cultivate skills, attitudes to promote knowledge creation
- Rendering socially relevant technical services for the community
- To impart new skills of technology development
- To inculcate entrepreneurial talents and technology appreciation programmes
- Technology transfer and incubation

DEPARTMENT

Vision

To be a leading academic department in the area of Computer Science and Information Technology with Learning and research processes of global standards that contribute to innovations in various scientific disciplines and societal needs and also motivate young engineers to face future technological challenges.

Mission

- To achieve excellence in teaching in the field of Computer Science and Engineering
- To promote learning in critical thinking and innovative environment with the state-of-art-technologies
- To cultivate skills to promote information and communication technology
- Advancement of knowledge in various specializations of Computer Science and Engineering

- To impart skills to develop technical solutions for societal needs and inculcate Entrepreneurial talents

Programme Educational Objectives (PEO)

PEO 1	To understand the principles and methods of securing computing infrastructure.
PEO 2	To acquire skill to analyze threats, attacks and knowledge of Risk Assessments and auditing of Cyber Systems.
PEO 3	To acquire research and technical communication skills.
PEO 4	To impart professional ethics and lifelong learning skills for professional advancement.

Programme Outcomes (PO)

PO 1	An ability to apply principles, methods in design and development of secure software and hardware systems.
PO 2	An ability to analyze cryptographic protocols using the principles of computational hardness.
PO 3	To demonstrate the usage of Digital Forensic and Vulnerability Assessment tools.
PO 4	Able to apply systems thinking in Risk Assessments and auditing of IT/Cyber Infrastructure.
PO 5	Able to do research and develop solutions to practical problems while adhering to professional ethics.
PO 6	Able to do systematic literature survey, identify emerging trends and prepare technical reports.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, U.C.E., O.U
M. Tech. (CYBER SECURITY)

Type of course	Course Code	Course Name	Contact hours per week		Scheme of Evaluation		Credits
			L	P	CIE	SEE	
SEMESTER-I							
Core-I	CS 101	Mathematical Foundations of Computer Science	3	-	40	60	3
Core-II	CS 102	Advanced Data Structures	3	-	40	60	3
Core-III	CS 501	Cryptography – I	3	-	40	60	3
Program Elective-I	CS 511	Cryptanalysis	3	-	40	60	3
	CS 512	Operating System Security					
	CS 513	Firewall and VPN Security					
	CS 514	Malware Analysis and Detection					
	CS 515	Ethical Hacking					
Program Elective-II	CS 521	Threat Intelligence	3	-	40	60	3
	CS 522	Web Application security					
	CS 523	Hardware Security					
	CS 524	Auditing IT Infrastructures for Compliance					
	CS 525	Block Chain Technologies					
Program Elective-III	CS 531	Bayesian Methods for Hackers	3	-	40	60	3
	CS 532	Internet Of Things Security					
	CS 533	Penetration Testing and Vulnerability Assessments					
	CS 111	Sentiment Analysis					
	CS 301	Machine Learning					
Lab-I	CS 161	Security Lab - I	-	2	50	-	1
Workshop	CS 561	Security Lab - II	-	2	50	-	1
TOTAL			**18**	**4**	**340**	**360**	**20**
SEMESTER-II							
Core- IV	CS 502	Digital Forensics	3	-	40	60	3
Core - V	CS 503	Cryptography - II	3	-	40	60	3
Core - VI	CS 504	Secure System Development	3	-	40	60	3
Program Elective-IV	CS 541	Post Quantum Cryptography	3	-	40	60	3
	CS 542	Cyber Forensics, Audit & Investigation					
	CS 543	Secure Multi Party Computation					
	CS 544	Social Media Analytics					
	CS 141	Cyber Systems Security					
Program Elective-V	CS 551	Database Security	3	-	40	60	3
	CS 552	Cloud Security					
	CS 553	Programming Quantum					

		Computers					
	CS 554	Game Theory based Network Security					
	CS 153	Storage Management					
Open Elective	OE 941 BM	Medical Assistive Devices	3	-	40	60	3
	OE942 BM	Medical Imaging Techniques					
	OE941 CE	Green Building Technology					
	OE942 CE	Cost Management of Engineering Projects					
	OE 941 CS	Business Analytics					
	OE 941 EC	Elements of Embedded Systems					
	OE 941 EE	Waste To Energy					
	OE 942 EE	Power Plant Control and Instrumentation					
	OE 941 ME	Operations Research					
	OE 942 ME	Composite Materials					
	OE 943 ME	Industrial Safety					
	OE 941 LA	Intellectual Property Rights					
Lab-II	CS 562	Digital Forensics Lab	-	2	50	-	1
Lab-III	CS 563	Security Lab - III	-	2	50	-	1
Mini Project	CS 171	Mini Project	-	4	50	-	2
TOTAL			**18**	**8**	**390**	**360**	**22**
SEMESTER-III							
Audit - I	AC 040	Research Methodology	2	-	40	60	0
Audit-II	AC 031	English for Research Paper Writing	2	-	40	60	0
	AC 032	Disaster Mitigation and Management					
	AC 033	Sanskrit for Technical Knowledge					
	AC 034	Value Education					
	AC 035	Stress Management by Yoga					
	AC 036	Personality Development through Life Enlightenment					
	AC 037	Constitution of India					
	AC 038	Pedagogy Studies					
	AC 039	E-Waste Management					
Dissertation-I	CS 581	Dissertation Phase -I	-	20	100	-	10
TOTAL			**4**	**20**	**180**	**120**	**10**
SEMESTER-IV							
Dissertation-II	CS 582	Dissertation Phase -II		**32**	**100**	**100**	**16**
GRAND TOTAL			**40**	**64**	**1010**	**940**	**68**

CS 101	**MATHEMATICAL FOUNDATIONS OF COMPUTER SCIENCE**					
(CORE - I)						
Pre-requisites	Discrete Mathematics Probability and Statistics		**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	**60 Marks**	**CIE**		**40 Marks**	

Course Objectives :	
1	To understand the mathematical fundamentals in probabilistic and statistical concepts
2	To develop the understanding of the mathematical and logical basis of various modern techniques in information technology like machine learning, programming language design, and concurrency.
3	To study various Graph Theory problems.

Course Outcomes:	
On completion of this course, the student will be able to:	
CO-1	Understand the basic notions of discrete and continuous probability.
CO-2	Apply the methods of statistical inference, and learn application of sampling distributions in Data mining and Machine Learning.
CO-3	Apply statistical analysis to algorithmic problems of simple to moderate complexity in different domains.
CO-4	Model different applications of Computer science as graph theory problems

Unit – I
Density, and cumulative distribution functions, Expected value, conditional expectation, Applications of the univariate and multivariate Central Limit Theorem, Probabilistic inequalities, Markov chains.

Unit – II
Random samples, sampling distributions of estimators**,** and Maximum Likelihood**.**

Unit – III
Statistical inference**,** Introduction to multivariate statistical models: classification problems, principal component analysis**,** The problem of over fitting model assessment.

Unit – IV
Graph Theory: Isomorphism, Planar graphs, graph coloring, Hamilton circuits and Euler cycles. Permutations and Combinations with and without repetition. Specialized techniques to solve combinatorial enumeration problems.

Unit –V
Number Theory: Elementary number theory, unique factorization, Euler's function, modular arithmetic, Fermat's little theorem, Chinese remainder theorem, modular exponentiation, RSA public key encryption.

Suggested Readings:

1	John Vince, Foundation Mathematics for Computer Science, Springer, 2015.
2	K. Trivedi, Probability and Statistics with Reliability, Queuing, and Computer Science Applications, Wiley, 2001.
3	M. Mitzenmacher and E. Upfal, Probability and Computing: Randomized Algorithms and Probabilistic Analysis, 2005.
4	Alan Tucker, Applied Combinatorics, Wiley, 2012.

CS 102	**ADVANCED DATA STRUCTURES**					
CORE – II						
Pre-requisites	Data Structures and Design and Analysis of Algorithms		**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	**60 Marks**	**CIE**		**40 Marks**	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Understand the ADT/libraries and choose appropriate data structures to design algorithms for a specific problem.
2	Understand the necessary mathematical abstraction to solve problems.
3	To familiarize students with advanced problem-solving paradigms and data Structure used to solve algorithmic problems.
4	Analysis of efficiency and proof of correctness

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Understand the implementation of symbol table using hashing techniques.
CO-2	Develop and analyse algorithms for red-black trees, B-trees and Splay trees.
CO-3	Develop algorithms for text processing applications.
CO-4	Identify suitable data structures and develop algorithms for computational geometry problems.

UNIT – I
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.

UNIT – II
Skip Lists: Need for Randomizing Data Structures and Algorithms, Search and Update Operations on Skip Lists, Probabilistic Analysis of Skip Lists, Deterministic Skip Lists.

UNIT– III
Trees: Binary Search Trees, AVL Trees, Red Black Trees, 2-3 Trees, B-Trees, Splay Trees

UNIT – IV
Text Processing: String 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 –V
Computational Geometry: One Dimensional Range Searching, Two-Dimensional Range Searching, constructing a Priority Search Tree, Searching a Priority Search Tree, Priority Range Trees, Quad trees, k-D Trees.

Suggested Reading:

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.

CS 501	**CRYPTOGRAPHY - I**					
CORE- III						
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives:	
The course is taught with the objectives of enabling the student to:	
1	Understand basics of Cryptography and Network Security.
2	Secure a message over insecure channel by various encryption and decryption algorithms
3	Learn about how to maintain the Confidentiality, Integrity and Availability of a data.
4	Understand various protocols for network security to protect against the threats in the networks.

Course Outcomes:	
On completion of this course, the student will be able to:	
CO-1	Provide security of the data over the network.
CO-2	Apply the Encryption and decryption algorithms
CO-3	Analyze the public key cryptography techniques
CO-4	Apply the various advanced protocols to protect against attacks

UNIT – I

Cryptographic Techniques and Algorithms

Course Introduction: History of Cryptography, Security Overview.

Classical Encryption Techniques: Symmetric Cipher Model, Some Basic Terminology, Cryptography Classification, Cryptanalysis, Substitution, One-Time Pad, Transposition, (Permutation) Ciphers, Product Ciphers, Rotor Machines, Rotor Machine Principle, Steganography.

Block Ciphers and DES: Block vs. Stream Ciphers, Shannon‟s S-P Networks, Feistel Cipher Structure, Feistel Cipher Design Elements, Data Encryption Standard (DES), Avalanche Effect, Avalanche in DES, Strength of DES, Differential Cryptanalysis, Linear Cryptanalysis, Block Cipher Design Principles.

UNIT – II

Basic Concepts in Number Theory and Finite Fields : Euclid's Algorithm, Modular Arithmetic, Algebraic Structures, Galois Fields, Polynomial Arithmetic.

Advanced Encryption Standard (AES) : Basic Structure of AES, Substitute Bytes, Shift Rows, Mix Columns, AES Arithmetic, Add Round Key, AES Key Expansion, AES Example Key Expansion, AES Example Encryption, AES Example, Avalanche AES Decryption.

Block Cipher Operations: Double-DES, Triple-DES, DES-X, Electronic Code Book (ECB), Cipher Block Chaining (CBC), Message Padding, Cipher Text Stealing (CTS), Cipher Feedback (CFB), Output Feedback (OFB), Counter (CTR).

UNIT– III

Pseudo Random Number Generation and Stream Ciphers: Pseudo Random Numbers, A Sample Generator, Terminology, Linear-Congruential Generators, Blum Blum Shub Generator, Random & Pseudorandom Number Generators, Using Block Ciphers aes PRNGs, RC4 Stream Ciphers.

Public Key Cryptography: Mathematical Background (Fermat's Little Theorem, Euler Totient Function , Euler's Theorem Chinese Remainder Theorem etc.) Public Key Encryption, Symmetric vs. Public-Key, RSA Public Key Encryption, RSA Key Construction, Exponentiation, RSA Issues, Factoring.

Cryptographic Hash Functions: Hash Function, Cryptographic Hash Functions, Applications of Crypto Hash Functions, Birthday Problem, Block Ciphers as Hash Functions, Secure Hash Algorithm (SHA)

UNIT – IV

Message Authentication Codes: Message Security Requirements, MAC, HMAC, Using Symmetric Ciphers for MACs. Cipher-based Message Authentication Code (CMAC), Authenticated Encryption, CCM.

Digital Signatures: Digital Signature Model, Attacks, Forgeries, Digital Signature, Requirements, Digital Signature Standard (DSS), DSS vs. RSA Signatures, Digital Signature Algorithm (DSA), DSA Key Generation, DSA Signature Creation, DSA Signature Verification.

Key Management and Distribution: Key Distribution Using KDC, Key Distribution Using Public Keys, Secret Key Distribution with Confidentiality and Authentication, Distribution of Public Keys, Public-Key Certificates PKI, PKIX, and X.509, CA Hierarchy.

User Authentication Protocols: User Authentication, Replay Attacks, Needham Schroeder Protocol Denning‟s Modification, One-Way Authentication for Email, Kerberos, Remote User Authentication Using Public Keys

UNIT –V

Advanced Protocols: Zero knowledge Proofs, Identity based public key, Secure elections, Secure multi-party computation, Digital cash.

Secure Socket Layer: Web Traffic Security Approaches SSL Architecture, SSL Handshake Protocol, SSL Handshake Protocol Actions, Handshake Messages, Security Capability Negotiation, Cryptographic Computations, SSL Change Cipher Spec Protocol, SSL Alert Protocol, SSL Record Protocol Services, SSL Record Protocol Operation.

Transport Level Security (TLS): HTTPS, HTTPS Use, Secure Shell (SSH), SSH Protocol Stack, SSH Transport Layer Protocol, SSH User Authentication Protocol, SSH Connection Protocol, Port Forwarding.

Wireless Network Security: Wireless Network Threats, Countermeasures Mobile Device Security Wi-Fi Operation IEEE 802.11 Architecture IEEE 802.11 Services Wired Equivalent Privacy (WEP), 802.11i Wireless LAN Security.

Electronic Mail Security, IP Security, Intrusion Detection, Malicious Software.

Suggested Reading:

1	William Stallings, "Cryptography and Network Security: Principles and Practice," 6th Edition, Pearson, 2014
2	Behrouz A. Forouzan and Debdeep Mukhopadhyay, Cryptography and Network Security, Tata McGraw Hill.
3	D. R. Stinson: Cryptography: Theory and Practice (Discrete Mathematics and Its Applications), 3rd Edition, CRC Press, 2005.
4	B. Schneier: Applied cryptography: protocols, algorithms, and source code in C, 2nd Edition, John Wiley & Sons.
5	Bernard Menezes: Network Security & Cryptography, First Edition, Cengage Learning, Delhi, 2011.

CS 511	**CRYPTANALYSIS**					
PROGRAM ELECTIVE- I						
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives:	
The course is taught with the objectives of enabling the student to:	
1	To learn the classical cryptology methods
2	To understand the Elliptic curves and lattices
3	To understand the digital signatures and its applications
4	To learn the various attacks

Course Outcomes:	
On completion of this course, the student will be able to:	
CO-1	Analyze the classical cryptology methods
CO-2	Apply the Elliptic curves and lattices based on the applications
CO-3	Protect the critical information with digital signatures
CO-4	Analyze the threats and protect with the various techniques

UNIT- I

Introduction to Cryptanalysis, Classical Cryptology methods : Ancient Cryptography, Substitution Alphabet Ciphers, The Caesar Cipher , Modular Arithmetic , Number Theory Notation , The Affine Cipher, The Vigen`ere Cipher , The Permutation Cipher, The Hill Cipher, Enigma and Ultra, Enigma‟s Security, Cracking the Enigma. Combinatoris, Probability and Information theory

UNIT-II

Elliptic curves and Cryptography: Elliptic curves over finite fields, elliptic curve discrete logarithm problem, elliptic curve cryptography, evolution of public key cryptography, Lenstra‟s elliptic curve factorization algorithm.

Lattices and Cryptography: Congruential public key cryptosystem, Subset-sum problems and knapsack cryptosystems, Lattices, short vectors in lattices, Babai‟s algorithm, Cryptosystems based on hard lattice problems, CGH and NTRU public key cryptosystems

UNIT- III

Digital Signatures: RSA digital signatures, Elgamal digital signatures and DSA, CGH lattice – based digital signatures, NTRU digital signatures.

Hash Functions, Random Numbers and pseudorandom number generators, Zero-knowledge

proofs, Secret sharing schemes, Identification schemes, padding schemes and random oracle model, Building protocols from cryptographic primitives, Hyper elliptic curve cryptography, Quantum computing

UNIT- IV

Classical Cryptography Attacks I: Function Preliminaries, Modular Arithmetic and affine cipher, Breaking the Affine cipher, Substitution Alphabet Cipher, Frequency Analysis and the Vigene‟re Cipher, Kasiski Test.

Classical Cryptography Attacks II: Breaking the permutation Cipher, Breaking the Hill Cipher, Running Key Ciphers, One-Time Pads

UNIT- V

Modern Symmetric Encryption: Binary Numbers and Message Streams, Linear Feedback Shift Registers, Known-Plaintext Attack on LFSR Stream Ciphers, LFSRsum, Baby CSS, Breaking Baby CSS, Baby Block, Security Baby Block, Meet-in-the-Middle Attacks

Modern Cryptography: Steganography, Quantum Cryptography. Primality Testing and Factorization, Brute Force Factoring, Fermat‟s Factoring method, Monte Carlo Algorithms and Miller-Rabin Test, Agrawal Kayal Saxena Primality Test.

Suggested Readings:

1.	**Margaret Cozzens and Steven J. Miller, "** *The Mathematics of Encryption: An Elementary Introduction***",** American Mathematical Society, 2013
2.	**Jeffrey Hoffstien, Jill Pipher and Joseph H. Silverman** "*An Introduction to Mathematical Cryptography",* Springer International Publishers, 2014.
3.	*"Basic Cryptanalysis",* Field Manual, Department of the ARMY Washington, 1990.

CS 512	**OPERATING SYSTEM SECURITY**					
PROGRAM ELECTIVE-I						
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Learn how to protect computer operating systems by demonstrating server support skills
2	Design and implement OS security systems and to identify security threats, vulnerabilities and monitor network security implementations
3	Implement industry standard secure servers side managed operations as well as clients.

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Gain knowledge about OS Security and access control
CO-2	Apply principles, generalizations, or theories that govern security in different Operating Systems
CO-3	Analyze the Verifiable security and Secure Communications processor
CO-4	Apply the Secure Capability Systems and Secure Virtual Machine Systems

UNIT – I

Fundamentals- OS Processes, Synchronization, Memory Management, File Systems, Trusted Operating Systems, Assurance in Trusted Operating Systems, Virtualization Techniques.
Secure operating systems- Security goals, Trust model, Threat model.
Access Control Fundamentals – Protection system – Lampson's Access Matrix, Mandatory protection systems, Reference monitor. Multics – Multics system, Multics security, Multics vulnerability analysis.

UNIT – II

Unix and Linux Security: Basic Unix Security, Protecting User Accounts and Strengthening Authentication, Reducing Exposure to Threats by Limiting Super user Privileges, Eliminating the Security Weakness of Linux and Unix Operating systems: Hardening Linux and Unix, Proactive Defense for Linux and Unix.

UNIT– III

Security in OS: Unix, Windows, Verifiable security goals – Information flow, Denning's Lattice model, Bell-Lapadula model, Biba integrity model, Covert channels.
Security Kernels – Secure Communications processor, Securing Commercial OS

UNIT – IV

Secure Capability Systems: Fundamentals, Security, Challenges , Secure Virtual Machine Systems .Case study - Linux kernel, Android, DVL, Solaris Trusted Extensions

UNIT –V
Security Kernels, Building a Secure Operating System for Linux: Linux Security Modules, Security-Enhanced Linux. Secure Capability Systems: Capability System Fundamentals, Capability Security, Challenges in Secure Capability Systems, Building Secure Capability Systems

Suggested Reading:

1	Andrew S. Tanenbaum, Modern Operating Systems, Third Edition, Prentice Hall, 2007.
2	Abraham Silberschatz, Peter Baer Galvin and Greg Gagne, *Operating System Concepts with JAVA*", 8th Edition, Wiley, 2008
3	Trent Jaeger, Operating System Security, Synthesis Lectures on Information Security . Privacy and Trust, Morgan and Claypool
4	C. P. Pfleeger and S. L. Pfleeger, Security in Computing, Prentice Hall Professional, 2003.
5	W. Mauerer, Professional Linux Kernel Architecture, Wiley, 2008.
6	D. P. Bovet and M.Cesati, Understanding the Linux Kernel, 3rd Edition, O'Reilly Media, Inc., 2005

CS 513	**FIREWALL AND VPN SECURITY**					
PROGRAM ELECTIVE-I						
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Learn the concepts security components and TCP/IP Basics
2	Understand the technologies including NAT, PAT, ACL construction, application gateways, stateful packet inspection, application layer and URL filtering.
3	Learn the configuration and management of firewall and VPN technologies.

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Configure and test VPN connection for remote access and site-to-site connections.
CO-2	Apply the concepts security components and TCP/IP Basics
CO-3	Implement and Configure the gateways, stateful packet inspection, application layer and URL filtering.
CO-4	Use the IDS, Snort and Bro IDS tools and VPN technologies.

UNIT – I

Fundamentals of Network Security: Introduction, network Security, Seven Domains of a Typical IT Infrastructure, Goals of Network Security, Measure the Success of Network Security, Network Security Policies Important, Internal and External Network Issues, Common Network Security Components Used to Mitigate Threats, TCP/IP Basics.

Network Security Threats: Hackers and Their Motivation, Favorite Targets of Hackers, Threats from Internal Personnel and External Entities, The Hacking Process, Common IT Infrastructure Threats Malicious Code (Malware), Advanced Persistent Threat, Session Hijacking, Spoofing, and Man-in-the-Middle Attacks, Covert Channels, Hacker Tools, Social Engineering.

UNIT – II

Common Network Topologies and Infrastructures, Network Design Considerations, Firewall Fundamentals, Firewall Implementation, Firewall Deployment Considerations, Configuring Firewalls.

UNIT– III

Packet Filtering: Introduction, Understanding Packets and Packet Filtering, Packet-Filtering Methods, Setting Specific Packet Filter Rules, Hands-On Projects.

Working with Proxy Servers and Application-Level Firewalls: Proxy Servers, Benefits of Proxy Servers, Configuring Proxy Servers, Choosing a Proxy Server, Proxy Server-Based Firewalls Compared.

UNIT – IV
VPN Fundamentals, VPN Management, VPN Technologies, VPN Implementation, Firewall Security Management, Best Practices for Network Security Management Emerging Technology and Regulatory Considerations.

UNIT –V
IDS infrastructure: IDS Architecture, IDS/IPS Management and Architecture Issues with regard to deploying IDS/IPS systems, end point approach to security, system approach to security, IDS Interoperability models: CIDF (Common Intrusion Detection Framework), IDMEF (Intrusion Detection Message Exchange Format), IODEF (Incident Object Description Exchange Format), CVE (Common Vulnerabilities and Exposures), OVAL (Open Vulnerability and Assessment Language). IDS tools: Snort and Bro IDS tools, NIDS Evasion, Insertion, and Checksums to confuse NID systems, Snort Fundamentals and Configuration, Snort GUIs & Sensor Management, Snort Performance, Active Response & Tagging, Snort Rules, Stimulus Response, hosts response to both normal and abnormal traffic, Advanced Snort Concepts as rule ordering and reduction of false negatives and positives. Evaluation and tuning of IDS, Cross over Rate (CER) of IDS.

Suggested Readings:

1	Network Security, Firewall and VPNs, Third Edition. J. Michael Stewart, Denise Kinsey, 2020.
2	Guide to Firewalls and VPNs Michael E. Whitman, Herbert J. Mattord, Andrew Green, 2012.
3	Network Intrusion Detection, Stephen Narthcutt, 2002
4	CCNP Security: Intrusion Prevention and Intrusion Detection Systems, David Burns, Odunayo Adesina, Keith Barker, Cisco Press, 2012.

CS 514	**MALWARE ANALYSIS AND DETECTION**					
PROGRAM ELECTIVE-I						
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives:	
The course is taught with the objectives of enabling the student to:	
1	Fundamentals of malware and life cycle and Analysis setup
2	Learn about the malware components and distribution mechanism
3	Understand the static and dynamic analysis of malwares
4	Learn the malware detection and reverse engineering approaches

Course Outcomes:	
After the completion of this course, the students shall be able to:	
CO-1	Understand the malware and life cycle and Analysis setup
CO-2	Apply the distribution mechanism in malware analysis
CO-3	Discuss the static and dynamic analysis of malwares
CO-4	Analyze the malware detection methods and reverse engineering approaches

UNIT– I

Introduction: Types of Malware, Malware attack Life Cycle, Malware Business model, Malware Analysis setup, Operating Systems Files and File formats

UNIT – II

System Fundamentals: Virtual memory and Portable Executable Files, Windows Internals – Win32 API, Registry, Directories, Processes and services.

UNIT – III

Malware Components: Malware Components , Distribution mechanisms, Malware Packers, Persistence mechanism, Network Communication, Detecting Network Communication, Code Injection, Process Hollowing, API Hooking, Stealth techniques and Rootkits

UNIT – IV
Malware Analysis and Classification: Static Analysis, Dynamic Analysis , Memory Forensics with Volatility, Malware Payload dissection and Classification.

UNIT –V
Malware Reverse Engineering: Debuggers and disassembly, Debugging for unpacking malware and code injections, Armoring Techniques **Detection Engineering : Device** Analysis, Anti Virus Engines, IDS/IPS and Snort /Suricata rule writing, Malware Sandbox Internals, DBI for Malware analysis

Suggested Reading:

1	**Ahijit Mohanta, Anoop Saldanha** , *Malware Analysis and Detection Engineering: A Comprehensive Appraoch to Detect and Analyze Modern Malware,* Apress Berkeley, CA, **2020**
2	**Michael Sikorski and Andrew Honig**, "*Practical Malware Analysis : The Hands-On Guide to Dissecting Malicious Software*", No Starch Press, 2012

CS 515	**ETHICAL HACKING**					
PROGRAM ELECTIVE-I						
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
1	To understand the basics of computer based vulnerabilities.
2	To explore different foot printing, reconnaissance and scanning methods
3	To expose the enumeration and vulnerability analysis methods
4	To understand hacking options available in Web and wireless applications
5	.To explore the options for network protection.
6	To practice tools to perform ethical hacking to expose the vulnerabilities.

Course Outcomes :	
On completion of this course, the student will be able to:	
CO-1	: To express knowledge on basics of computer based vulnerabilities
CO-2	CO2: To gain understanding on different foot printing, reconnaissance and scanning methods.
CO-3	CO3 To demonstrate the enumeration and vulnerability analysis
CO-4	methods CO4: To gain knowledge on hacking options available in Web and wireless applications.
CO-5	CO5: To acquire knowledge on the options for network protection.
CO-6	CO6: To use tools to perform ethical hacking to expose the vulnerabilities.

UNIT– I

INTRODUCTION : Ethical Hacking Overview - Role of Security and Penetration Testers .- Penetration-Testing Methodologies- Laws of the Land - Overview of TCP/IP- The Application Layer - The Transport Layer - The Internet Layer - IP Addressing .- Network and Computer Attacks - Malware - Protecting Against Malware Attacks.- Intruder Attacks - Addressing Physical Security.

UNIT – II

FOOT PRINTING, RECONNAISSANCE AND SCANNING NETWORKS

Footprinting Concepts - Footprinting through Search Engines, Web Services, Social Networking Sites, Website, Email - Competitive Intelligence - Footprinting through Social Engineering - Footprinting Tools - Network Scanning Concepts - Port-Scanning Tools - Scanning Techniques - Scanning Beyond IDS and Firewall

UNIT – III
ENUMERATION AND VULNERABILITY ANALYSIS Enumeration Concepts - NetBIOS Enumeration – SNMP, LDAP, NTP, SMTP and DNS Enumeration - Vulnerability Assessment Concepts - Desktop and Server OS Vulnerabilities - Windows OS Vulnerabilities - Tools for Identifying Vulnerabilities in Windows- Linux OS Vulnerabilities- Vulnerabilities of Embedded Oss

UNIT– IV
UNIT IV SYSTEM HACKING Hacking Web Servers - Web Application Components- Vulnerabilities - Tools for Web Attackers and Security Testers Hacking Wireless Networks - Components of a Wireless Network – Wardriving- Wireless Hacking - Tools of the Trade –

UNIT –V
NETWORK PROTECTION SYSTEMS Access Control Lists. - Cisco Adaptive Security Appliance Firewall - Configuration and Risk Analysis Tools for Firewalls and Routers - Intrusion Detection and Prevention Systems - NetworkBased and Host-Based IDSs and IPSs - Web Filtering - Security Incident Response Teams – Honeypots.

Suggested Reading:

1	Michael T. Simpson, Kent Backman, and James E. Corley, Hands-On Ethical Hacking and Network Defense, Course Technology, Delmar Cengage Learning, 2010.
2	The Basics of Hacking and Penetration Testing - Patrick Engebretson, SYNGRESS, Elsevier, 2013.
3	The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Dafydd Stuttard and Marcus Pinto, 2011.

Reference Books:

1	Black Hat Python: Python Programming for Hackers and Pentesters, Justin Seitz , 2014.

CS 521	**THREAT INTELLIGENCE**					
	PROGRAM ELECTIVE-II					
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Identify sources of information about threats to an organization.
2	Conduct and analysis of the Intelligence-driven Incident Response process
3	Leverage intelligence to build profiles of different adversarial groups and analyse risks associated with different threat actors

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Identify sources of information to detect threats to an organization.
CO-2	Analyze the Intelligence-driven Incident Response process and generate reports
CO-3	Understand the threat Intelligence for Vulnerability Management
CO-4	Build profiles for adversial groups and risk assessments

UNIT – I

Threat Intelligence: Introduction, Types of Threat Intelligence, Operational, Strategic Threat Intelligence, The Role of Threat Data Feeds, The Role of Private Channels and the Dark Web.

The Threat Intelligence Lifecycle: Six Phases of the Threat Intelligence, Tools and People, Applications of Threat Intelligence, Threat Intelligence for Security Operations, Responsibilities of the SOC Team.

UNIT – II

Threat Intelligence for Incident Response, Continuing Challenges, A piecemeal approach, The Reactivity Problem, Minimizing Reactivity in Incident Response, Identification of probable threats, Prioritization, Strengthening Incident Response With Threat Intelligence, Threat Intelligence in Action, Use Cases. Essential Characteristics of Threat Intelligence for Incident Response. Cyber drills

UNIT– III

Threat Intelligence for Vulnerability Management, The Vulnerability Problem by the Numbers Zero day does not mean top priority, Time is of the essence, Assess Risk Based on Exploitability, Severity ratings can be misleading, The Genesis of Threat Intelligence:

Vulnerability Databases, Exploitability versus exploitation, Understanding the adversary, Sources of Intelligence. Use Cases.

UNIT – IV
Threat Intelligence for Security Leaders, Risk Management, Mitigation: People, Processes, and Tools, The Security Skills Gap. Threat Intelligence for Risk Analysis, The FAIR Risk Model, Measurements and transparency are key, Threat Intelligence and Threat Probabilities, Threat Intelligence and the Cost of Attacks Threat Intelligence for Fraud Prevention, Stand and Deliver, Criminal Communities and the Dark Web, Threat Intelligence for Reducing Third-Party Risk, Third-Party Risk Looms Large.

UNIT –V
Threat Intelligence for Digital Risk Protection, Types of Digital Risk, Your Threat Intelligence Program, Analytical Frameworks for Threat Intelligence, Flexibility, Challenges with the Diamond Model, Integrating threat intelligence with processes and infrastructure, Developing the Core Threat Intelligence Team, The role of intelligent machines.

Suggested Reading:

1	The Threat Intelligence Hand book, Second Edition Christopher Ahlberg, CyberEdge Press , 2018.
2	Practical Cyber Intelligence: How Action-based Intelligence Can be an Effective Response to Incidents, Wilson Bautista, 2018.
3	Cyber Threat Intelligence, Wiley Publications, Martin Lee, 2023

CS 522	**WEB APPLICATION SECURITY**					
PROGRAM ELECTIVE-II						
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Learn the fundamentals of web application and security principles
2	Understand the file security and database security principles
3	Learn the vulnerability detection and web application security controls

Course Outcomes :	
After the completion of this course, the students shall be able to:	
CO-1	Understand the concepts of web application architecture
CO-2	Apply the web application security controls
CO-3	Analyze the systematic vulnerability detection
CO-4	Apply the file security and database security principles

UNIT– I

Introduction: Introduction to Web Application Security, OWASP list, Security Fundamentals: Input Validation, Attack Surface Reduction, Classifying and Prioritizing Threats.

Web Application Security Principles: Authentication- Fundamentals, Two-factor and three-factor Authentication, Web Application Authentication, Securing password-based Authentication.

UNIT – II

Authorization: Access control methods, Session Management Fundamentals.

Database Security Principles: SQL Injection, Setting Database Permissions, Stored Procedure Security, Insecure Direct Object References

UNIT – III

File Security Principles: Keeping Your Secure Code Secret, Security Through Obscurity, Forceful Browsing, Directory Traversal

Secure Development Methodologies: Holistic Approach, Industry Standard Secure Development Methodologies and Maturity Models. DevSec Ops.

UNIT – IV
Web Application Reconnaissance, Structure of a Modern Web Application: REST APIs, SPA Frameworks, Finding Sub domains, API Analysis, Identifying third party dependencies and weak points in Application Architecture, web Application Firewall.

UNIT –V
Vulnerability Discovery and Management, Defending Against XSS Attacks, CSRF Attacks, Defending Against XXE, Defending Against Injection and DoS, Securing Third-Party Dependencies.

Suggested Reading:

1	Bryan Sullivan, Vincent Liu**, "***Web Application Security", McGraw Hill,* ***2012.***
2	Dafydd Stuttard Marcus Pinto, " The *Web Application Hacker's Handbook*", Wiley Publishing Inc., **2008.**

CS 523	**HARDWARE SECURITY**					
	PROGRAM ELECTIVE-II					
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Learn about the Physical Attacks and Tamper Resistance of SoC
2	Understand the Side Channel Attacks and Countermeasures.
3	How to verify the PCB Authentication and Integrity Validation

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Understand the Physical Attacks and Tamper Resistance of SoC
CO-2	Analyze the Side Channel Attacks and Countermeasures.
CO-3	Apply the PCB Authentication and Integrity Validation process

UNIT – I

Introduction to Hardware Security: Overview of a Computing System, Layers of a Computing System , What Is Hardware Security, Hardware Security vs. Hardware Trust, Attacks, Vulnerabilities, and Countermeasures , Conflict Between Security and Test/Debug, Evolution of Hardware Security

A Quick Overview of Electronic Hardware: Introduction, Nanoscale Technologies, Digital Logic, Circuit Theory , ASICs and FPGAs, Printed Circuit Board , Embedded Systems , Hardware-Firmware-Software Interaction .

System on Chip (SoC) Design and Test: Introduction , The IP-Based SoC Life-Cycle, SoCDesign Flow, SoCVerification Flow, SoC Test Flow, Design-for-Debug, Structured DFT Techniques Overview, At-Speed Delay Test. **Printed Circuit Board (PCB): Design and Test:** Introduction, Evolution of PCB and Components, PCB Life Cycle, PCB Assembly Process, PCB Design Verification.

UNIT – II

HARDWARE ATTACKS: ANALYSIS, EXAMPLES, AND THREAT MODELS

Hardware Trojans: Introduction , SoCDesign Flow, Hardware Trojans , Hardware Trojans in FPGADesigns, Hardware Trojans Taxonomy , Trust Benchmarks , Countermeasures Against Hardware Trojans.

Electronics Supply Chain: Introduction , Modern Electronic Supply Chain , Electronic

Components Supply Chain Issues, Security Concerns, Trust Issues, Potential Countermeasures.

Hardware IP Piracy and Reverse Engineering : Introduction, Hardware Intellectual Property (IP), Security Issues in IP-Based SoC Design, Security Issues in FPGA.

UNIT– III

Side-Channel Attacks: Introduction , Background on Side-Channel Attacks , Power Analysis Attacks , Electromagnetic (EM) Side-Channel Attacks , Fault Injection Attacks, Timing Attacks

Test-Oriented Attacks: Introduction, Scan-Based Attacks , JTAG-Based Attacks, Hands-on Experiment: JTAG Attack.

Physical Attacks and Countermeasures: Introduction Reverse Engineering, Probing Attack, Invasive Fault Injection Attack.

Attacks on PCB: Security Challenges and Vulnerabilities: Introduction , PCB Security Challenges: Attacks on PCB, Attack Models. Secure Element

UNIT – IV

COUNTER MEASURES AGAINST HARDWARE ATTACKS

Hardware Security Primitives: Introduction , Preliminaries, Physical Unclonable Function , True Random Number Generator, Design for Anti-Counterfeit , Existing Challenges and Attacks , Primitive Designs With Emerging Nano devices.

Security and Trust Assessment, and Design for Security: Introduction , Security Assets and Attack Models , Pre-silicon Security and Trust Assessment for SoCs, Post-silicon Security and Trust Assessment for ICs , Design for Security

Hardware Obfuscation: Introduction , Overview of Obfuscation Techniques , Hardware Obfuscation Methods, Emerging Obfuscation Approaches , Use of Obfuscation Against Trojan Attacks

UNIT –V

PCB Authentication and Integrity Validation : PCB Authentication , Sources of PCB Signature, Signature Procurement and Authentication Methods , Signature Assessment Metric, Emerging Solutions, PCB Integrity Validation

EMERGING TRENDS IN HARDWARE ATTACKS AND PROTECTIONS

System Level Attacks & Countermeasures, Introduction , Background on SoC Design, SoC Security Requirements , Security Policy Enforcement, Secure SoC Design Process, Threat Modeling , Hands-on Experiment: SoC Security Policy. STQC Specifications.

Suggested Reading:

1	Hardware Security: A Hands-On Learning Approach, Mark Tehranipoor and Swarup Bhunia, 2018.
2	Hardware Security: Design, Threats, and Safeguards, Debdeep Mukhopaday, Rajat Subhra Chakaraborthy, 2014.

CS 524	**AUDITING IT INFRASTRUCTURES FOR COMPLIANCE**					
PROGRAM ELECTIVE-II						
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Learn the principles, approaches and methodologies in auditing information systems.
2	Understand the processes and procedures in compliance with pertinent laws and regulatory provisions in the context of information systems security (ISS).
3	Secure business and consumer privacy data, an explanation of compliancy laws, and the process and legal requirements for conducting IT infrastructure compliance audits.

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Apply the principles, approaches and methodologies in auditing information systems.
CO-2	Analyze the procedures in compliance with pertinent laws and regulatory provisions in the context of information systems security (ISS).
CO-3	Apply the legal requirements for conducting IT infrastructure compliance audits.

UNIT – I
Foundations For IT Audit: Audit Overview, Information Technology Environment and IT Audit, Legislation Relevant to Information Technology, The IT Audit Process, Tools and Techniques Used in Auditing IT.

UNIT – II
Auditing Techniques: Auditing Entity-Level Controls, Auditing Cyber security Programs, Auditing Data Centers and Disaster

UNIT– III
Auditing Networking Devices, Auditing Windows Servers, Auditing Unix and Linux Operating Systems, Auditing Web Servers and Web Applications, Auditing Databases.

UNIT – IV
Auditing Big Data and Data Repositories, Auditing Storage, Auditing Virtualized Environments, Auditing End-User Computing Devices, Auditing Applications.

UNIT –V
Auditing Cloud Computing and Outsourced Operations, Auditing Company Projects, Auditing

New/Other Technologies, Frameworks and Standards, Regulations, Risk Management, Auditing Standards, ISACA Standards, Auditor empanelment Requirements.

Suggested Reading:

1	IT Auditing using controls to protect information assets, Chris Davis, Mike Schiller and Kevin Wheeler, 3rd Edition, McGraw Hill, 2011
2	Information Technology Control and audit, Sandra Senft, Frederick Gallegos, Aleksandra Davis, 2016.

CS 525	**BLOCKCHAIN TECHNOLOGIES**					
	PROGRAM ELECTIVE-II					
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	To Introduce the Theoretical Foundations of blockchain through bitcoin.
2	To Introduce Hash functions and Transactions.
3	To Study Algorithms for Mining and Consensus implementation.
4	To Study Ethereum and Smart contracts concepts.
5	To Learn the concepts of Oracles and Decentralized Applications (DApps).

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Understand the principles of blockchain technologies and bitcoin
CO-2	Be familiar with hash functions with wallets
CO-3	Understand mining and consensus strategies
CO-4	Understand Ethereum and tokens

UNIT– I

Introduction

What is Bitcoin, Bitcoin Uses, Users ,Getting Started ,Getting your first bitcoins ,Sending and receiving bitcoins, Transactions, Blocks, Mining, The Genesis Block, Merkle Trees, Block Header Hash and the Blockchain .

Keys, Addresses, Wallets : Introduction of Crptography, Public key cryptography and crypto-currency ,Private and Public Keys , Elliptic Curve Cryptography Explained Generating a public key , Bitcoin Addresses, Base58 and Base58Check Encoding Key Formats ,Implementing Keys and Addresses ,Wallets ,Non-Deterministic (Random) Wallets ,Deterministic (Seeded) Wallets ,Mnemonic Code Words ,Hierarchical Deterministic Wallets (BIP0032/BIP0044), Advanced Keys and Addresses , Encrypted Private Keys (BIP0038) ,Pay To Script Hash (P2SH) and Multi-Sig Addresses ,Vanity Addresses ,Paper Wallets

UNIT – II

Transactions: Introduction of Transaction Lifecycle ,Creating Transactions ,Broadcasting Transactions to the Bitcoin Network ,Propagating Transactions on the Bitcoin Network ,Transaction Structure ,Transaction Outputs and Inputs ,Transaction Outputs ,Transaction Inputs ,Transaction Fees, Adding Fees to Transactions, Transaction Chaining and Orphan Transactions ,Transaction Scripts and Script Language ,Script Construction (Lock + Unlock) ,Scripting Language ,Turing Incompleteness ,Stateless Verification ,Standard Transactions ,Pay to Public Key Hash (P2PKH) ,Pay-to-Public-Key ,Multi-Signature ,Data

Output (OP_RETURN) Pay to Script Hash (P2SH)
Mining and Consensus: De-centralized Consensus ,Independent Verification of Transactions ,Mining Nodes ,Aggregating Transactions into Blocks ,Transaction Age, Fees, and Priority ,The Generation Transaction ,Coinbase Reward and Fees ,Structure of the Generation Transaction ,Coinbase Data ,Constructing the Block Header ,Mining the Block ,Proof-of-Work Algorithm ,Difficulty Representation ,Difficulty Target and Re-Targeting ,Successfully Mining the Block ,Validating a New Block ,Assembling and Selecting Chains of Blocks ,Blockchain Forks ,Mining and the Hashing Race ,The Extra Nonce Solution ,Mining Pools ,Consensus Attacks

UNIT – III
Ethereum: Compared to Bitcoin, Ether Currency Units ,Choosing an Ethereum Wallet Control and Responsibility ,Getting Started with MetaMask, Creating a Wallet Switching Networks ,Getting Some Test Ether ,Sending Ether from MetaMask Exploring the Transaction History of an Address ,Introducing the World Computer Externally Owned Accounts (EOAs) and Contracts ,A Simple Contract: A Test Ether Faucet.
Cryptography Ethereum‟s Cryptographic Hash Function: Keccak-256 , Ethereum Addresses ,Ethereum Address Formats ,Inter Exchange Client Address Protocol, Hex Encoding with Checksum in Capitalization (EIP-55)
The Ethereum Virtual Machine : EVM, Comparison with Existing Technology, The EVM Instruction Set (Bytecode Operations) , Ethereum State , Compiling Solidity to EVM Bytecode , Contract Deployment Code , Disassembling the Bytecode

UNIT – IV
Transactions Transmitting Value to EOAs and Contracts, Transmitting a Data Payload to an EOA or Contract, Special Transaction: Contract Creation ,Digital Signatures ,The Elliptic Curve Digital Signature Algorithm ,How Digital Signatures Work ,Verifying the Signature ,ECDSA Math ,Transaction Signing in Practice ,Raw Transaction Creation and Signing ,Raw Transaction Creation with EIP-155 ,The Signature Prefix Value (v) and Public Key Recovery ,Separating Signing and Transmission (Offline Signing) ,Transaction Propagation ,Recording on the Blockchain , Multiple-Signature (Multisig) Transactions
Tokens How Tokens Are Used, Tokens and Fungibility, Counterparty Risk, Tokens and Intrinsicality, Using Tokens: Utility or Equity, ERC223: A Proposed Token Contract Interface Standard ,ERC777: A Proposed Token Contract Interface Standard, ERC721: Non-fungible Token (Deed) Standard

UNIT–V
Oracles Why Oracles Are Needed, Oracle Use Cases and Examples, Oracle Design, Patterns Data

Authentication ,Computation Oracles ,Decentralized Oracles, Oracle Client Interfaces in Solidity
Decentralized Applications (DApps): DApp, Backend (Smart Contract) , Frontend (Web User Interface) , Data Storage, Decentralized Message Communications Protocols , A Basic DApp Example: Auction DApp , Auction DApp: Backend Smart Contracts ,Auction DApp: Frontend User Interface ,Further Decentralizing the Auction DApp ,Storing the Auction DApp on Swarm ,Preparing Swarm ,Uploading Files to Swarm ,The Ethereum Name Service (ENS) , History of Ethereum Name Services ,The ENS Specification ,Bottom Layer: Name Owners and Resolvers ,Middle Layer: The .eth Nodes ,Top Layer: The Deeds, Registering a Name, Managing Your ENS Name ,ENS Resolver, Resolving a Name to a Swarm Hash (Content) , From App to DApp

Suggested Reading:

1	Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder, **Bitcoin and Cryptocurrency Technologies,** Princeton University Press and Oxford, 2016
2	Andreas M. Antonopoulos**, Mastering Bitcoin: Programming the Open Blockchain,** O‟Reilly, 2017.
3	Dr. Gavin Wood, Andreas M. Antonopoulos**, Mastering Ethereum: Building Smart Contracts and Dapps,** O‟Reilly, 2018.

CS 531	**BAYESIAN METHODS FOR HACKERS**					
PROGRAM ELECTIVE-III						
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Learn the Bayesian methods including Bayesian model specification, Bayesian posterior inference, and model assessment
2	Develop and estimate linear and nonlinear Bayesian models
3	Understand the knowledge of distribution methods

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Acquire a good understanding of Bayesian methods including Bayesian model specification, Bayesian posterior inference, and model assessment.
CO-2	Use the acquired knowledge of Bayesian statistics to develop and estimate linear and nonlinear Bayesian models as well as have enough exposure to MCMC (Markov Chain Monte Carlo) computation.
CO-3	Deploy this knowledge in analyzing the various distribution methods

UNIT – I

The Philosophy of Bayesian Inference: Introduction, Our Bayesian Framework, Probability Distributions, Using Computers to Perform Bayesian Inference. Inferring Behavior from Text-Message Data. PyMC: Introduction, Parent and Child Relationships, PyMC Variables, Observations in the Model, Modeling Approaches, Model Appropriate, Separation Plots

UNIT – II

Opening the Black Box of MCMC, The Bayesian Landscape, Exploring the Landscape Using MCMC, Algorithms to Perform MCMC, Other Approximation Solutions to the Posterior, Unsupervised Clustering Using a Mixture Model, Posterior Samples, Using MAP to Improve Convergence, Diagnosing Convergence, Autocorrelation , Thinning, pymc.Matplot.plot(), MCMC, Intelligent Starting Values, Priors, The Folk Theorem of Statistical Computing.

UNIT– III

The Greatest Theorem Never Told : Introduction, The Law of Large Numbers, Intuition, Example: Convergence of Poisson Random Variables, Compute Var (Z), Expected Values and Probabilities , Bayesian Statistics, The Disorder of Small Numbers, Sorting, Derivation of Sorting Comments Formula.

UNIT – IV
Introduction, Loss Functions, Loss Functions in the Real World, Optimizing for the Showcase on The Price Is Right, Machine Learning via Bayesian Methods, Financial Prediction, Kaggle Contest on Observing Dark Worlds, The Data, Priors, Training and PyMC Implementation.

UNIT –V
Getting Our Priorities Straight: Introduction, Subjective versus Objective Priors, Decisions, Empirical Bayes, The Gamma Distribution, The Wishart Distribution, The Beta Distribution, Bayesian Multi-Armed Bandits, Applications, Trial Roulette Method, Conjugate Priors, Jeffreys Priors, Effect of the Prior as N Increases. Bayesian Perspective of Penalized Linear Regressions.

Suggested Reading:

1	Bayesian Methods for hackers Willey publications, Cameron Davidson-Pilon, 2015.
2	Bayesian Methods for Statistical Analysis , Australian Nat University Press, Borek Puza · 2015.
3	Bayesian Reasoning and Machine Learning, Cambridge University Press, David Barber · 2012.

CS 532	**INTERNET OF THINGS SECURITY**					
PROGRAM ELECTIVE-III						
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Learn the IOT architectures and Vulnerability issues
2	Understand the importance of privacy and security issues
3	Learn the security mechanisms

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Identify and describe the variety of IoT systems architectures, essential components and challenges specific to IoT systems.
CO-2	Interpret information privacy and data protection requirements in regards to IoT products design.
CO-3	Apply appropriate security mechanisms for IoT to real-world problems.

UNIT – I

IOT-SECURITY OVERVIEW: IoT, Architecture of IoTs, IoT Security Requirements (Privacy preservation, Device security, authentication, confidentiality and integrity), Benefits & Applications of IoT, IoT Attack Surface, Industrial Standards and Evolution. Device security, Gateway security, IoT Privacy Concerns, Privacy by Design, Conducting a Privacy Impact Assessment, Case Study: The Connected Barbie.

UNIT – II

IOT- SECURITY & VULNERABILITY ISSUES: IoT Vulnerabilities -Secret-Key, Authentication/Authorization for Smart Devices, Constrained, System Resources, Device Heterogeneity, Fixed Firmware. Attack Models - Layer-wise Attack model, Attacks to Sensors in IoTs, Attacks to RFIDs in IoTs, Attacks to Network Functions in IoTs, Attacks to Back-end Systems, Security in Front-end Sensors and Equipment. IoT Attacks - Side-channel Attacks, Spoofing Attack, Sniffing Attack, Rogue Devices Attack, Man-in-Middle Attack, DDoS Attack, Sensor base Attack.

UNIT– III

Securing internet of things environments: Networking Function Security - IoT Networking Protocols, Layering Architecture, Secure IoT Lower Layers, Secure IoT Higher Layers, Secure Communication Links in IoTs, Back-end Security- Secure Resource Management, Secure IoT

Databases.

UNIT – IV
IoT Hardware -Test Device Range, Latency and Capacity, Manufacturability Test, Secure from Physical Attacks. IoT Software -Trusted IoT Application Platforms, Secure Firmware Updating, Network Enforced Policy, Secure Analytics Visibility and Control.

UNIT –V
IoT attacks- case study: MIRAI Botnet Attack, Iran's Nuclear Facility Stuxnet Attack, Tesla Crypto jacking Attack, The Spam-haus attack, Traffic Light Hacks, DDoS spoofing attack against American health insurance provider.

Suggested Reading:

1	Fei HU, *Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations* , CRC Press, 2016.
2	Ollie Whitehouse, *Security of Things: An Implementers' Guide to Cyber-Security for Internet of Things Devices and Beyond NCC Group*, 2014.
3	Russell, Brian and Drew Van Duren, *Practical Internet of Things Security* , Packet Publishing, 2016.

CS 533	**PENETRATION TESTING AND VULNERABILITY ASSESSMENTS**					
PROGRAM ELECTIVE-III						
Pre-requisites	Computer Networks		**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Learn the theoretical basis for cyber threats and penetration testing phases and vulnerabilities
2	Perform protocol analysis using packet captures and analysis data using a sniffer
3	Apply testing methodologies using tools such as Wireshark, Nmap, Snort, Metasploit and related applications and platforms.

Course Outcomes :	
After the completion of this course, the students shall be able to:	
CO 1	Apply the theoretical concepts to identify cyber threats and vulnerabilities
CO 2	Identify and exploit various vulnerabilities in web applications.
CO 3	Apply testing methodologies using tools such as Wireshark, Nmap, Snort, Metasploit and related applications and platforms.

UNIT– I
Introduction - Terminologies - Categories of Penetration Testing - Phases of Penetration Test - Penetration Testing Reports - Information Gathering Techniques - Active, Passive and Sources of Information Gathering - Approaches and Tools - Traceroutes, Neotrace, Whatweb, Netcraft, Xcode Exploit Scanner and NSlookup. Target Enumeration and Port scanning techniques - Host discovery - Scanning for open ports and services, Port scanning.

UNIT – II
Vulnerability Scanner Function, pros and cons - Vulnerability Assessment with NMAP - Testing SCADA environment with NMAP – Nessus, Vulnerability Scanner - Safe check - Silent dependencies - Port Range Vulnerability Data Resources, Network Sniffing, Shodan

UNIT – III
Network Sniffing, Remote Exploitation, Capturing traffic: Networking for Capturing Traffic, Using Wireshark, ARP Cache Poisoning, DNS Cache Poisoning, SSL Attacks, SSL Stripping, Exploitation.

UNIT – IV
Password Attacks: Password Management, Online Password Attacks, Offline Password Attacks. Client Side Exploitation and Post Exploitation

UNIT –V
Windows Exploit Development Basics, Wireless Hacking and Attacks, Web hacking , Mobile Hacking.

Suggested Reading:

1	Rafay Baloch *"Ethical Hacking and Penetration Testing Guide"*, CRC Press, **2015**.
2	Georgia Weidman, "*Penetration Testing: A Hands-On Introduction to Hacking"*, **2014.**
3	Wil Allsopp, *" Advanced Penetration Testing, Wiley*, **2017.**

CS 111	**SENTIMENT ANALYSIS**					
	PROGRAM ELECTIVE - III					
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
1	Understand the introducing real time problems related to sentiment extraction with an aim to bridge the gap between unstructured and structured data
2	To facilitate qualitative and quantitative analysis of opinions
3	To discuss the existing techniques for solving real time sentiment extraction problems.

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Understand the problem of sentiment analysis and opinion summarization as mini NLP.
CO-2	Use text classification and ML techniques for sentiment classification of documents.
CO-3	Use rules of sentiment composition in aspect-based sentiment analysis and aspect extraction.
CO-4	Generate sentiment lexicons and analyse comparative opinions.
CO-5	Understand the problem of Intension mining, classification, and able to detect opinion spams.

UNIT– I
Introduction: Sentiment Analysis Applications, Sentiment Analysis Research, Sentiment Analysis as mini NLP.
The Problem of Sentiment Analysis: Definition of Opinion, Opinion Summarization, Affect, Emotion and Mood, Different Types of Opinions.
Document Sentiment Classification: Supervised Sentiment Classification, Unsupervised Sentiment Classification, Sentiment Rating Prediction

UNIT – II
Document Sentiment Classification: Cross-Domain Sentiment Classification, Cross-Language Sentiment Classification, Emotion classification of Documents.
Sentence Subjectivity and Sentiment Classification: Subjectivity, Sentence Sentiment Classification, Dealing with Conditional Sentences, Dealing with Sarcastic Sentences, Crosslanguage Subjectivity and Sentiment Classification, Using Discourse Information for Sentiment Classification, Emotion classification of sentences.

UNIT – III

Aspect-based Sentiment Analysis: Aspect Sentiment Classification, Rules of sentiment Composition, Negation and Sentiment
Aspect and Entity Extraction: Aspect Extraction, Entity, Opinion Holder and Time Extraction, Coreference Resolution and Word Sense Disambiguation.

UNIT – IV
Sentiment Lexicon Generation: Dictionary-based Approach, Corpus-based Approach, Desirable and Undesirable Facts.
Analysis of Comparative Opinions: Problem Definitions, Identifying the Preferred Entity Set, Entity and Aspect Extraction.
Opinion Summarization and Search: Aspect based opinion summarization, Contrastive view summarization.

UNIT –V
Opinion Summarization and Search: Summarization of Comparative Opinions, Opinion Search, Existing Opinion retrieval Techniques.
Mining Intentions: Problem of Intention Mining, Intention Classification, Fine-Grained Mining of Intentions.
Opinion Spam Detection: Types of Spam and Spamming, Supervised Spam Detection, Unsupervised Spam Detection, Group Spam Detection.

Suggested Reading:

1	Sentiment Analysis – Mining Opinions, Sentiments, and Emotions in Text, Bing Liu, Cambridge University Press, 2015.
2	Sentiment Analysis and Opinion Mining, Bing Liu, Morgan and Claypool Publishers, 2012.
3	Sentiment Analysis in Social Networks by Federico Alberto Pozzi, Elisabetta Fersini, Enza Messina, Bing Liu, Morgan Kaufmann publications, 2017.
4	Foundations of Statistical Natural Language Processing 1st Edition, by Christopher D. Manning, Hinrich Schütze, The MIT Press Cambridge, Massachusetts London, England, 1999
5	Natural Language Processing with Python, by Steven Bird, Ewan Klein and Edward Loper.

CS 301	**MACHINE LEARNING**					
PROGRAM ELECTIVE-III						
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Learn basic concepts of machine learning and range of problems that can be handled by machine learning
2	Understand the instance based learning and decision tree induction
3	Learn the concepts of linear separability ,Perceptron and SVM
4	Learn the probabilistic inference, graphical models and evolutionary learning.
5	Understand the ensemble learning, dimensionality reduction and clustering.

Course Outcomes :	
After the completion of this course, the students shall be able to:	
CO-1	Identify the strengths and weakness of different machine learning techniques.
CO-2	Select suitable model parameter for different machine learning technique
CO-3	Design & implement various machine learning algorithms to a wide range of real world applications
CO-4	Evaluate available learning methods to develop the research based solutions in different domains.

UNIT– I

Introduction: Learning, Types of Machine Learning, Machine Learning Examples, Decision Tree Learning
Concept learning: Introduction, Version Spaces and the Candidate Elimination Algorithm.
Learning with Trees: Decision Tree Learning, the Big Picture
Linear Discriminants: Learning Linear Separators , The Perceptron Algorithm , Margins

UNIT – II

Estimating Probabilities from Data, Bayes Rule, MLE, MAP
Naive Bayes: Conditional Independence, Naive Bayes: Why and How, Bag of Words
Logistic Regression : Maximizing Conditional likelihood, Gradient Descent
Kernels: Kernalization Algorithm, Kernalizing Perceptoron,
Discriminants: The Perceptron, Linear Separability, Linear Regression
Multilayer Perceptron (MLP): Going Forwards, Backwards, MLP in practices, Deriving back Propagation.

UNIT – III
Support Vector Machines: Geometric margins, Primal and Dual Forms, Kernalizing SVM **Generalization & Overfitting:** Sample Complexity, Finite Hypothesis classes, VC Dimension Based Bounds **Some Basic Statistics:** Averages, Variance and Covariance, The Gaussian, The Bias-Variance Tradeoff Bayesian learning: Introduction, Bayes theorem. Bayes Optimal Classifier, Naive Bayes Classifier. **Graphical Models:** Bayesian networks, Approximate Inference, Making Bayesian Networks, Hidden Markov Models, The Forward Algorithm.

UNIT – IV
Model Selection & Regularization: Structural Risk Minimization, Regularization, k-Fold Cross validation **Linear Regression:** Linear regression, minimizing squared error and maximizing data Likelihood **Neural Networks**: Back Propagation, **Deep Neural Networks:** Convolution, Convolution Neural Networks, LeNet-5 architecture **Boosting:** Boosting Accuracy, Ada Boosting, Bagging

UNIT –V
Clustering: Introduction, Similarity and Distance Measures, Outliers, Hierarchical Methods, Partitional Algorithms, Clustering Large Databases, Clustering with Categorical Attributes, Comparison. **Dimensionality Reduction:** Linear Discriminant Analysis, Principal Component Analysis **Interactive Learning:** Active Learning, Active Learning, Common heuristics, Sampling bias , Safe Disagreement Based Active Learning Schemes **Semi-Supervised Learning:** Semi-supervised Learning, Transductive SVM, Co-training **Reinforcement Learning:** Markov Decision Processes, Value Iteration, Q-Learning

Suggested Reading:

1	Tom M. Mitchell, *Machine Learning*, Mc Graw Hill, 1997
2	Chistopher Bishop, Pattern recognition & Machine Learning, Springer 2006.
3	Margaret H Dunham, *Data Mining*, Pearson Edition., 2003.
4	Stephen Marsland, *Machine Learning - An Algorithmic Perspective*, CRC Press, 2009
5	Galit Shmueli, Nitin R Patel, Peter C Bruce, *Data Mining for Business Intelligence*, Wiley India Edition, 2007
6	Rajjan Shinghal, *Pattern Recognition*, Oxford University Press, 2006.
	Jerry Zhu, *Encyclopedia of Machine Learning*,
7	Margaret H Dunham, *Data Mining*, Pearson Edition., 2003.

CS 161	SECURITY LAB - I					
LAB – I						
Pre-requisites			L	T	P	C
			-	-	2	1
Evaluation	SEE	--	CIE		50 Marks	

PART-A

1. Install wireshark and explore the various protocols
   A. Analyze the difference between HTTP vs HTTPS
   B. Analyze the various security mechanisms embedded with different protocols
2. Identify the vulnerabilities using OWASP ZAP tool
3. Create simple REST API using python for following operation
   A.GET
   B.PUSH
   C.POST
   D.DELETE
4. Install Burp Suite explore the vulnerabilities:
   A.SQL injection
   B. cross-site scripting (XSS)
5. Attack the website using Social Engineering method

PART-B

1. Install Kali or Backtrack Linux / Metasploitable/ Windows XP
2. Practice the basics of reconnaissance.
3. Using FOCA / Search Diggity tools, extract metadata and expanding the target list.
4. Aggregates information from public databases using online free tools like Paterva‟s Maltego.
5. Information gathering using tools like Robtex.
6. Scan the target using tools like Nessus.
7. View and capture network traffic using Wireshark.
8. Automate dig for vulnerabilities and match exploits using Armitage

PART-C

1. Install Kali Linux on Virtual box

2. Explore Kali Linux and bash scripting

3. Perform open source intelligence gathering using Netcraft, Whois Lookups, DNS Reconnaissance, Harvester and Maltego

4. Understand the nmap command d and scan a target using nmap

5. Install metasploitable2 on the virtual box and search for unpatched vulnerabilities

6. Use Metasploit to exploit an unpatched vulnerability

7. Install Linux server on the virtual box and install SSH

8. Use Fail2banto scan log files and ban Ips that show the malicious signs

9. Launch brute-force attacks on the Linux server using Hydra.

10. Perform real-time network traffic analysis and data pocket logging using Snort

CS 561	**SECURITY LAB - II**					
Workshop						
Pre-requisites			**L**	**T**	**P**	**C**
			-	**-**	**2**	**1**
Evaluation	**SEE**	**--**	**CIE**		**50 Marks**	

- Software Security
- Buffer-overflow attacks in the light of stack protection mechanisms
- Return-to-libc attack
- Format string vulnerabilities
- Race condition vulnerabilities
- Environment variables and Set-UID
- Shellshock attack
- Dirty COW
- Web Security
- Cross-Site Scripting and XSS worm propagation
- Cross-Site Request Forgery
- SQL Injection Attack
- Network Security
- Packet sniffing and spoofing
- Attacks on the TCP protocol
- Firewalls
- DNS Attacks
- Virtual Private Networks
- PKI
- Transport Layer Security
- Heartbleed Attack
- Cryptography
- Attacks on encryption, signatures, and hash functions
- PKI and Man-In-The-Middle Attacks
- System Security
- Side-channel attacks with respect to CPU caching (Meltdown/Spectre)
- Mobile Security
- Reverse engineering of Android applications
- Android rooting

SEMESTER –II

CS 502	DIGITAL FORENSICS					
	CORE-IV					
Pre-requisites	Information Security, Operating Systems, Computer Networks		**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Understand the basic digital forensics and techniques for conducting the forensic examination on different digital devices.
2	Learn to examine digital evidences like data acquisition and identification analysis

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Apply memory analysis tools and file system analysis techniques to detect anti forensics.
CO-2	Understand privacy issues and able to use live/Online forensic tools.
CO-3	Analyze windows registry, Linux server configurations and Apache server to identify incidents.
CO-4	Analyze SQL databases and reconstruct activities by using SQL server toolkits.
CO-5	Use Network Traffic analysis tools and collect evidences from network devices.

UNIT – I
File Systems: FAT/NTFS file systems, Parsing FAT/NTFS file systems, Pre fetch and Super fetch, Shortcuts and Jumplists
Adversary and Malware hunting: Malware detection, Malware analysis
Memory Forensics: Memory acquisition, Memory analysis, memory analysis tools, Advanced Recycle bin, Server Logs, Google forensics.
Anti-Forensics Detection: detection methodologies, Volume shadow copy, ESE databases, Advanced Registry, Thumbnail cache.

UNIT – II
Computer Crime and legal issues: Privacy issues, Intellectual property
Incident Response: Threat and Adversary Intelligence, Financial crime analysis
Live/Online Forenics: Live Digital Forensics Investigation.
Tools: BitTorrent, Sleuthkit toolset, Windows Forensics. Tool chest Moot court: Moot court case.

UNIT– III
Networking overview: Windows Networks, Users and Groups, Introduction to Network

Investigations
Windows and Linux servers: Server roles, Server analysis, Windows Registry, Event logs
Linux Forensics: Linux File systems, Linux server configurations, Linux artifacts, Apache server forensics, LAMP forensics, SMB and Linux file shares.

UNIT – IV
IIS and Microsoft Exchange server: IIS server, Mail server, Windows rootkits, Compromised server analysis
SQL server and Data bases: Microsoft SQL server, SQL server permission and encryption,
SQL server Forensics Acquisition and analysis: SQL server forensics and traditional windows forensics, SQL server artifacts, Resident and non-resident artifact‟s Collecting SQL data bases, Creating an analysis database, Importing evidence, Activity Reconstruction, Data recovery, SQL server rootkits

UNIT –V
Network Traffic Analysis: Network addressing, DNS poisoning, ARP table analysis, DHCP analysis, Wire shark analysis.
Network Device Forensics: management of switches and routers, Diagramming physical networks, Securing and isolating physical devices, Collecting Volatile/Non-volatile evidences from the routers, Volatile/Non-volatile.

Suggested Reading:

1	H. Carvey, “Windows Forensics Analysis DVD Toolkit”, Syngress publishers 2009.
2	S. Anson, S. Bunting, R. Johnson, S. Perason, “Mastering Windows Network Forensics and Investigations”, Sybex publishers K. Fowler, SQL Server Forensic Analysis, Addison Wesley 2012.
3	K. Mandia, M. Pepe , J. Luttgens, “Incident Response & Computer Forensics”, Third Edition 2014.
4	M.H. Ligh, A. Case, J. Levy, A. waters, “The art of memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory”, Wiley 2014.
5	S. Davidoff, J. Ham, “Network Forensics: Tracking Hackers through Cyberspace”, Prentice Hall 2012.

CS 503	**CRYPTOGRAPHY -II**					
CORE- V						
Pre-requisites	Cryptography - I		**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives:	
The course is taught with the objectives of enabling the student to:	
1	Understand how to Assess / Evaluate the security deployed by cryptographic schemes
2	Learn how to prove or disprove security and learn cryptographic schemes and Implement attacks
3	Learn basics of lattice-based cryptography, Construction of Fully Homomorphic Encryption and Partial Homomorphic Encryption

Course Outcomes:	
On completion of this course, the student will be able to:	
CO-1	Assess / Evaluate the security deployed by cryptographic schemes
CO-2	Prove or disprove security and Justify the elements of cryptographic schemes
CO-3	Analyze cryptographic schemes and Implement attack methods
CO-4	Identify the importance of lattice-based cryptography

UNIT – I

Randomness and Computation: Probability Theory – Three Inequalities, Computational Models and Complexity classes, Some Basic Cryptographic Settings.
The Foundations of Modern Cryptography: Introduction, Classical Cryptography: Hidden Writing, Central Paradigms, Pseudo-randomness, Zero-Knowledge, : Provable Security, Shannon‟s Treatment of Provable Secrecy. Encryption, Signatures, Cryptographic Protocols.

UNIT – II

Computational Hardness: Efficient Computation and Efficient Adversaries, One-Way Functions, Multiplication, Primes, and Factoring, Hardness Amplification, Collections of One-Way Functions, Basic Computational Number Theory, Factoring-based Collection of OWF, Discrete Logarithm-based Collection, RSA Collection, One-way Permutations, Trapdoor Permutations, Rabin collection, A Universal One Way Function. The Basics of Provable Security.

UNIT– III

Indistinguishability & Pseudo-Randomness: Computational Indistinguishability, Pseudo-randomness, Pseudo-random generators, Hard-Core Bits from Any OWF, Secure Encryption,

An Encryption Scheme with Short Keys, Multi-message Secure Encryption, Pseudorandom Functions, Construction of Multi-message Secure Encryption, Public Key Encryption , El-Gamal Public Key Encryption scheme, A Note on Complexity Assumptions.
Knowledge: When Does a Message Convey Knowledge, A Knowledge-Based Notion of Secure Encryption, Zero-Knowledge Interactions, Interactive Protocols, Interactive Proofs, Zero-Knowledge Proofs , Zero-knowledge proofs for NP, Proof of knowledge, Applications of Zero-knowledge.

UNIT – IV

Authentication: Message Authentication, Message Authentication Codes, Digital Signature Schemes, A One-Time Signature Scheme for $\{0,1\}^n$, Collision-Resistant Hash Functions, One-Time Digital Signature Scheme for $\{0,1\}^n$, Signing Many Messages, Constructing Efficient Digital Signature, Zero-knowledge Authentication.
Computing on Secret Inputs: Secret Sharing, Yao Circuit Evaluation, Secure Computation.
Composability: Composition of Encryption Schemes, Composition of Zero-knowledge Proofs, Composition Beyond Zero-Knowledge Proofs.

UNIT –V

Simulation, Secure Computation: Semantic security and equivalence to IND-based security, Zero-knowledge. Definition. Protocols for graph 3-coloring, Multi-party Computation. Semi-honest and malicious security, Yao's garbled circuits. 2-party computation, Secret sharing. General multiparty computation. Fully Homomorphic Encryption (FHE): Basics of lattice-based cryptography. Construction of FHE from Learning with Errors. Partial Homomorphic Encryption

Suggested Reading:

1	A Course on Cryptography Rafael pass Lecture notes Cornell university
2	Modern Cryptography Volume 1, A Classical Introduction to Informational and Mathematical Principle. Zhiyong Zheng, 2022
3	Modern Cryptography Volume 2, A Classical Introduction to Informational and Mathematical Principle. Zhiyong Zheng, 2022

CS 504	**SECURE SYSTEM DEVELOPMENT**					
CORE-VI						
Pre-requisites	Data Structures		**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Learn the software security vulnerabilities and techniques to prevent
2	Understand wide-ranging technical and conceptual security skills to the software development lifecycle
3	Learn the complexity of contemporary software vulnerabilities and the techniques to discover and mitigate.

Course Outcomes :	
After the completion of this course, the students shall be able to:	
CO-1	Analyse software security vulnerabilities and apply best-practice practical techniques to prevent
CO-2	Apply wide-ranging technical and conceptual security skills to the software development lifecycle
CO-3	Demonstrate awareness of the complexity of contemporary software vulnerabilities and the techniques to discover and mitigate them.
CO-4	Demonstrate a systematic approach to problem solving and security planning

UNIT– I
Introduction: Intersection of Security and Reliability , Understanding adversaries. Designing Systems: Case Study Safe Proxies, Design Tradeoffs, Design for Least Privilege.

UNIT – II
Design for Understandability, Design for Changing Landscape, Design for Resilience, Design for recovery, Mitigating Denial-of-service Attacks

UNIT – III
Implementing Systems: Designing, Implementing and Maintaining a publicly Trusted CA, Writing Code and Testing Code

UNIT – IV
Deploying Code and Investigating Systems. Maintaining Systems: Disaster Planning, Crisis Management , Recovery and Aftermath

UNIT –V

Organization and Culture: Case study: Chrome Security Team, Understanding Roles and Responsibilities , Building a Culture of Security and Reliability.

Suggested Reading:

1	Ana Oprea , Betsy Beyer , Paul Blankinship Heather Adkins , Piotr Lewandowski , Adam Stubblefield, *"Building Secure and Reliable Systems: Best Practices for Designing, Implementing, and Maintaining Systems"*, O'Reilly; Edition **2020.**
2	Julia H Allen, Sean J Barnum, Robert J Ellison, Gary McGraw, Nancy R Mead, *"Software Security Engineering: A Guide for Project Managers"*, *Addison Wesley, **2008.***

CS 541	**POST QUANTUM CRYPTOGRAPHY**					
PROGRAM ELECTIVE -IV						
Pre-requisites	Fundamentals of Cryptography		**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Learn basics of quantum computing, speedups offered by quantum algorithms
2	Understand how attacks takes place on cryptography using quantum computers
3	Design cryptosystems resilient to quantum attacks and cryptographic protocols using quantum key distribution.

Course Outcomes :	
After the completion of this course, the students shall be able to:	
CO-1	Understand the concepts of quantum computing, speedups offered by quantum algorithms
CO-2	Analyze the attacks on cryptography using quantum computers
CO-3	Analyze the cryptographic protocols using quantum key distribution.

UNIT I

Introduction to post-quantum cryptography- Introduction and challenges
Quantum computing: Classical and quantum Computing, Computation model, The quantum Fourier transform, The hidden subgroup problem, Search algorithms

UNIT II

Hash-based Digital Signature Schemes: Hash based one-time signature schemes, Merkle‟s tree authentication scheme, One-time key-pair generation using an PRNG, Authentication path computation, Tree chaining, Distributed signature generation, Security of the Merkle Signature Scheme

UNIT III

Code-based cryptography: Introduction, Cryptosystems, The security of computing syndromes as one-way function, Codes and structures, Practical aspects.

UNIT IV

Lattice-based Cryptography: Introduction, Preliminaries, Finding Short Vectors in Random q-ary Lattices, Hash Functions, Public Key Encryption Schemes, Digital Signature Schemes, Other Cryptographic Primitives.

UNIT V
Multivariate Public Key Cryptography: Introduction, The Basics of Multivariate PKCs, Examples of Multivariate PKCs, Basic Constructions and Variations, Standard Attacks. **Isogeney based Cryptography**: Supersigular Isogeny based Key Exchange (SIKE), Digital Signature Algorithm based on Isogeny.

Suggested Readings:

1	Daniel J. Bernstein · Johannes Buchmann Erik Dahmen, *"Post-Quantum Cryptography"*, Springer Verilag, **2009.**
2	NIST Post Quantum Standardization- Specification document of the post-quantum secure algorithms https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions

CS 542	**CYBER FORENSIC, AUDIT AND INVESTIGATION**					
PROGRAM ELECTIVE -IV						
Pre-requisites	Fundamentals of Cryptography		**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives:	
The course is taught with the objectives of enabling the student to:	
1	Learn the file system structures and forensic tools
2	Understand the lossless and lossy data compression and Network Forensics
3	Collect and analyze computer forensic evidence

Course Outcomes:	
After the completion of this course, the students shall be able to:	
CO-1	Analyze the file system structures and demonstrate the forensic tools
CO-2	Apply the lossless and lossy data compression algorithms and Network Forensics
CO-3	Know how to collect the computer forensic evidence and submit the investigation reports

UNIT I

File systems, Microsoft file structure, Examining NTFS disks, Microsoft BitLocker, Third-Party Disk Encryption Tools, Windows Registry, Startup Tasks, Virtual Machines, Macintosh file structure and boot process, UNIX and Linux disk structures and boot processes. Other Disk structures (CD, SCSI, IDE and SATA devices)

UNIT II

Commercial Forensic Tools (Encase, FTK), Advanced Features of forensic tools (search, encryption and decryption, data carving), windows registry, memory analysis, advanced file system analysis (deleted and hidden data, metadata, temporary file, unknown\executable file analysis), applied decryption.

UNIT III

Graphic files: recognition, lossless and lossy data compression, locating and recovering graphic files, Identifying unknown file formats.

UNIT IV

Virtual Machines, Network Forensics, Network tools, E-mail Investigation, E-mail forensics tools, Mobile Device Forensic.

UNIT V
Computer Investigation, Evidence acquisition, Processing crime and Incidence scene, Preserving, Analysis, Digital forensic investigation procedures, Report writing, Ethics

Suggested Readings:

1	Computer Evidence - Collection and Preservation, Christopher L. T. Brown, Cengage Learning, 2009
2	Guide to Computer Forensics And Investigations Nelson, Bill ; Phillips, Amelia; Enfinger, Frank; Steuat, Christopher Thomson Course Technology, 2008.
3	Computer Forensics – Computer Crime Scene Investigation.Vacca, John R. Charles River Media, Laxmi Publications Pvt Limited, 2009
4	Prosise, Chris, Kevin Mandia, Incident Response: Computer Forensics, McGraw Hill Professional, 2003

CS 543	**SECURE MULTIPARTY COMPUTATION**					
PROGRAM ELECTIVE -IV						
Pre-requisites	Fundamentals of Cryptography		**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Learn the concepts of Secure Multi-party computation
2	Understand the Semi-honest Adversaries, Sigma Protocols and Efficient Zero-Knowledge protocols
3	Learn the concepts of Convert Adversaries and Secure Database Search

Course Outcomes *:*	
After the completion of this course, the students shall be able to:	
CO-1	Know about the Secure Multi-party computation methods
CO-2	Analyze the Semi-honest Adversaries, Sigma Protocols and Efficient Zero-Knowledge protocols
CO-3	Apply the Convert Adversaries and Secure Database Search

UNIT I

Secure Multiparty Computation : Introduction, Preliminaries, Security in the presence of Semi-honest Adversaries, Security in the presence of Malicious Adversaries, Security in the presence of covert Adversaries , Restricted Versus General Functionalities, Non-Simulation Based Definitions.

UNIT II

Semi-honest Adversaries: Tools, Garbled Circuit Construction, Yao‟s Two-party Protocol and efficiency.

Malicious Adversaries: Overview, Protocol, Proof of Security, Implementation of Different Primitives and efficiency.

UNIT III

Sigma Protocols and Efficient Zero-Knowledge: Definition and properties, Proof of Knowledge, Proving Compound Statements, Zero-Knowledge from Σ-Protocols, Efficient Commitment Schemes from Σ-Protocols.

UNIT IV
Convert Adversaries: Oblivious Transfer, Secure Two-party Computation and Efficiency Oblivious Transfer and Applications: Privacy, One-sided Simulation, Full Simulation, Secure Pseudorandom Function Evaluation, UPI Payments Architecture and Case study.

UNIT V
The k^{th}-Ranked Element: Background, Computing the Median – Semi-honest, Malicious, Search Problems :Introduction, Secure Database Search, Secure Document Search . Implementing Functionality FCPRP with Smartcards, Secure Text Search (Pattern Matching)

Suggested Readings:

1	Carmit Haza, Yehuda Lindell, *" Efficient Secure Two-Party Protocols Techniques and Constructions", Springer Series,* **2010**.
2	Ronald Cramer, Ivan Bjerre Damgard, Jesper Buus Nielsen, " *Secure Multiparty Computation and Secret Sharing", Cambridge University Press,* ***2015***

CS 544	**SOCIAL MEDIA ANALYTICS**					
PROGRAM ELECTIVE-IV						
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Understand the basics of online social media and networks on the Internet.
2	Learn the usage and impacts of Social Medial Websites like Facebook, YouTube, LinkedIn, Twitter, Flicker, Instagram, Google+, Four Square, Pinterest, Tinder
3	Learn the privacy and security issues on online social media.

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Appreciate various privacy and security concerns (spam, phishing, fraud nodes, identity theft) on Online Social Media
CO-2	Collect Data from OSM, analyze and visualize the Data
CO-3	Clearly articulate one or two concerns comprehensively on Online Social Media,

UNIT – I
Introduction - Types of social networks (e.g., Twitter, Facebook), Measurement and Collection of Social Network Data, Social Networks - Basic Structure and Measures, Basics of Text Processing over Social Data, Entity linking and entity resolution for Social data.

UNIT – II
Characteristics of OSNs, Information Diffusion, Experimental studies over OSNs, Sampling Social network Analysis, Social network and its representation, Graph-Matrix representation of social network, Inferential methods in Social Network Analysis.

UNIT – III
Fundamentals of Social Data Analytics, Topic Models, Random Walks, Heterogeneous Information Networks

UNIT – IV
Applied Social Data Analytics, Recommendation Systems, Community identification and link prediction, Digital Media Marketing.

UNIT –V
Online experiments for Computational Social Science, Big Data Sampling, Social Engineering Attacks, Data Leakage Prevention. Case Study : Exploring Twitter‟s API and Cookbook , Google+, Face book and LinkedIn

Suggested Reading:

1.	Song Yang and Franziska B Keller, " Social Network Analysis", ", Sage Publishers, 2017.
2.	Mathew A Russel, "Minig the Social Web ", Orielly Publishers, 2nd Edition 2013.
3	Analyzing Social Media Networks with NodeXL Insights from a Connected World Derek Hansen, Ben Shneiderman, Marc A. Smith, 2010.
4	Online Social Networks Security Principles, Algorithm, Applications, and Perspectives, Brij B. Gupta, Somya Ranjan Sahoo, CRC Press, 2021

CS 141	CYBER SYSTEMS SECURITY					
PROGRAM ELECTIVE - IV						
Pre-requisites			L	T	P	C
			3	-	-	3
Evaluation	SEE	60 Marks	CIE		40 Marks	

Course Objectives:	
1	To learn basic cyber security concepts
2	To learn social engineering attacks and countermeasures.
3	To learn about Malware and Kernel Debugging
4	To learn basic concepts of digital forensic practices
5	To introduce legal and compliance issues

Course Outcomes:	
On completion of this course, the student will be able to:	
CO-1	Understand different layers of security, vulnerabilities and threats
CO-2	Analyse vulnerabilities and apply counter measures for social engineering attacks
CO-3	Use kernel debugging, log analysis and network monitoring tools
CO-4	Analyse the forensic tools for evidence collection and Analysis.
CO-5	Understand IT Act and conduct compliance auditing

UNIT– I

Introduction to Cyber Security: Basic Cyber Security Concepts, layers of security, Vulnerability, threat, Harmful acts, Internet Governance – Challenges and Constraints, Computer Criminals, CIA Triad, Assets and Threat, motive of attackers, active attacks, passive attacks, Software attacks, hardware attacks, Cyber Threats-Cyber Warfare, Cyber Crime, Cyber terrorism, Cyber Espionage, etc., Comprehensive Cyber Security Policy.

UNIT – II

Social Engineering attacks and countermeasures. Password attacks, Privilege Escalation and Executing Applications, Network Infrastructure Vulnerabilities, IP spoofing, DNS spoofing, Wireless Hacking: Wireless footprint, Wireless scanning and enumeration, Gaining access (hacking 802.11), WEP, WPA, WPA2. **DoS attacks**. Web server and application vulnerabilities, SQL injection attacks, Vulnerability Analysis and Reverse Engineering, Buffer overflow attacks. Client-side browser exploits, Exploiting Windows Access Control Model for Local Elevation Privilege. Exploiting vulnerabilities in Mobile Application.

UNIT – III
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. Networking: Socket module, Port Scanning, Packet Sniffing, Traffic Analysis, TCP Packet Injection, Log analysis. HTTP Communications with Python built in Libraries, Web communications with the Requests module, Forensic Investigations with Python: geo-locating, recovering deleted items, examining metadata and windows registry

UNIT – IV
Introduction to Digital forensics, Forensic software and handling, forensic hardware and handling, analysis and advanced tools, forensic technology and practices, Biometrics: face, iris and fingerprint recognition, Audio-video evidence collection, Preservation and Forensic Analysis.

UNIT –V
Ethics, Policies and IT Act Basics of Law and Technology, Introduction to Indian Laws, Scope and Jurisprudence, Digital Signatures, E Commerce-an Introduction, possible crime scenarios, law coverage, data interchange, mobile communication development, smart card and expert systems Indian Laws, Information Technology Act 2000, Indian Evidence Act, India Technology Amendment Act 2008, Indian Penal Code, Computer Security Act 1987, National Information Infrastructure Protection Act 1996, Fraud Act 1997, Children Online Protection Act 1998, Computer Fraud and Abuse Act 2001, Intellectual Property, IP Theft, Copyright, Trademark, Privacy and Censorship, Introduction to Cyber Ethics, rights over intellectual property, Corporate IT Policy Formulations, Compliance Auditing.

Suggested Reading:

1	Baloch, R., Ethical Hacking and Penetration Testing Guide, CRC Press, 2015.
2	Michael Sikorski, Andrew Honig ―Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software‖ publisher Williampollock
3	Nina Godbole and SunitBelpure, Cyber Security Understanding Cyber Crimes,Computer Forensics and Legal Perspectives,Wiley
4	Chalie Kaufman, Radia Perlman, Mike Speciner, ―Network Security: Private Communication in a Public Network‖, Pearson Education, New Delhi, 2004.
5	Neal Krawetz, ‖Introduction to Network Security‖, Thomson Learning, Boston, 2007
6	Bruce Schneier, ―Applied Cryptography‖, John Wiley & Sons, New York, 2004.

CS 551	**DATABASE SECURITY**					
PROGRAM ELECTIVE-V						
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Learn the data base security principles and Role based access
2	Understand the data privacy methods and insider threats
3	Learn the Differential Privacy principles and online learning

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Demonstrate the data base security principles and Role based access methods
CO-2	Apply the data privacy methods and protection methods to address insider threats
CO-3	Explain the Differential Privacy principles and online learning

UNIT – I

Introduction, Design Principles, Discretionary Access Control, Virtual Private Database, Mandatory Access Control, Oracle Label Security.

UNIT – II

Role-based Access , Database as a Service I – Query, Encrypted Domain Keyword Search, Database as a Service II – Encryption-based, Executing SQL over encrypted data in the database-service-provider model, Efficient Execution of Aggregation Queries over Encrypted Relational Databases. Database Encryption.

UNIT– III

Data Privacy: Review **,** Achieving k-anonymity privacy protection using generalization and suppression. Differential Privacy. Privacy in Location Based Service, Review, Steganographic File Systems, Insider Threat: Detecting anomalous access patterns in relational databases. Design and Implementation of an Intrusion Response System for Relational Databases.

UNIT – IV

The Promise of Differential Privacy: Privacy-preserving data analysis, **Basic Terms,** The model of computation, Towards defining private data analysis, Formalizing differential privacy.

Basic Techniques and Composition Theorems: Useful probabilistic tools, Randomized response, The laplace mechanism, The exponential mechanism, Composition theorems, The sparse vector technique. **Releasing Linear Queries with Correlated Error:** An offline algorithm: SmallDB, An online mechanism: private multiplicative weights. **Generalizations:** Mechanisms via _-nets, The iterative construction mechanism, Connections.

UNIT –V

Boosting for Queries: The boosting for queries algorithm, Base synopsis generators. When Worst-Case Sensitivity is Atypical: Subsample and aggregate, Propose-test-Release, Stability and privacy. Lower Bounds and Separation Results: Reconstruction attacks, Lower bounds for differential privacy.

Differential Privacy and Computational Complexity: Polynomial time curators, Some hard-to-Syntheticize distributions, Polynomial time adversaries. Differential Privacy and Mechanism Design: Differential privacy as a solution concept, Differential privacy as a tool in mechanism design, Mechanism design for privacy aware agents

Differential Privacy and Machine Learning: The sample complexity of differentially private machine learning, Differentially private online learning, Empirical risk minimization.

Suggested Reading:

1	Christopher Diaz, Database Security: Problems and Solutions, Mercury Learning and Information, 2022
2	Cynthia Dwork, Aaron Roth , The Algorithmic Foundations of Differential Privacy , Now Publishers, 2014
3	Elisa Bertino, Ravi S. Sandhu: Database Security-Concepts, Approaches, and Challenges. IEEE Trans. Dependable Sec. Computing, VOL. 2, NO. 1, JANUARY-MARCH 2005
4	L. Sweeney: k-anonymity: a model for protecting privacy. Int. Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5):557-570, 2002.
5	A. Kamra, E. Terzi, E. Bertino: Detecting anomalous access patterns in relational databases. VLDB J. 17(5): 1063-1077 (2008)

CS552	**CLOUD SECURITY**					
PROGRAM ELECTIVE- V						
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Learn the concepts of distributed systems, algorithms and protocols
2	Understand the security in the cloud-infrastructure and analyze various attacks on cloud computing
3	Learn various cloud services and key management problems in cloud storage

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Understanding the distributed systems, algorithms and protocols
CO-2	Evaluate Security in the cloud-infrastructure and analyze various attacks on cloud computing
CO-3	Understanding various cloud services and key management problems in cloud storage

UNIT – I
Cloud Computing Architectural Framework: Cloud Benefits, Business scenarios, Cloud Computing Evolution, cloud vocabulary, Essential Characteristics of Cloud Computing, Cloud deployment models, Cloud Service Models, Multi- Tenancy, Approaches to create a barrier between the Tenants, cloud computing vendors, Cloud Computing threats, Cloud Reference Model, The Cloud Cube Model, Security for Cloud Computing, How Security Gets Integrated.

UNIT – II
Compliance and Audit: Cloud customer responsibilities, Compliance and Audit Security Recommendations. Portability and Interoperability: Changing providers reasons, Changing providers expectations, Recommendations all cloud solutions, IaaS Cloud Solutions, PaaS Cloud Solutions, SaaS Cloud Solutions.

UNIT– III
Traditional Security, Business Continuity, Disaster Recovery, Risk of insider abuse, Security baseline, Customers actions, Contract, Documentation, Recovery Time Objectives (RTOs), Customers responsibility, Vendor Security Process (VSP).

UNIT – IV

Data Center Operations, Security challenge, Implement Five Principal Characteristics of Cloud Computing, Data center Security Recommendations. Encryption and Key Management: Encryption for Confidentiality and Integrity, Encrypting data at rest, Key Management Lifecycle, Cloud Encryption Standards, Recommendations.

UNIT –V
Identity and Access Management in the cloud, Identity and Access Management functions, Identity and Access Management (IAM) Model, Identity Federation, Identity Provisioning Recommendations, Authentication for SaaS and Paas customers, Authentication for IaaS customers, Introducing Identity Services, Enterprise Architecture with IDaaS , IDaaS Security Recommendations. **Virtualization:** Hardware Virtualization, Software Virtualization, Memory Virtualization, Storage Virtualization, Data Virtualization, Network Virtualization, Virtualization Security Recommendations.

Suggested Reading:

1	Practical Cloud Security *A Guide for Secure Design and Deployment O'reilley Chris Dotson, 2012*
2	Cloud Computing Security: Foundations and Challenges, 2nd Edition
3	Securing The Cloud: Cloud Computing Security Techniques and Tactics by Vic (J.R.) Winkler, 2019
4	Ronald L. Krutz, Russell Dean Vines, "Cloud Security: A Comprehensive Guide to Secure Cloud Computing", Wiley Publishing, 2010.

CS 553	**PROGRAMMING FOR QUANTUM COMPUTERS**					
PROGRAM ELECTIVE-V						
Pre-requisites	Python Programming		**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Learn basic quantum operations and arithmetic logic
2	Quantum Fourier Transform and its applications
3	Quantum Principal Component Analysis and Quantum Machine Learning

Course Outcomes :	
After the completion of this course, the students shall be able to:	
CO-1	Understand the basic quantum operations and arithmetic logic
CO-2	Apply Quantum Fourier Transform and its applications
CO-3	Analyze the Quantum Principal Component Analysis and Quantum Machine Learning

UNIT I

Introduction: Introduction to Quantum Computing, Qubits, Operators and Measurements, Complexity theory, QPU Vs GPU, Programming for a QPU: Qubit, QPU operations, QPU instructions, Multiple Qubits , Quantum Teleportations

UNIT II

Quantum Primitives: Quantum Arithmetic Logic- Arithmetic on QPU, adding two quantum bits, Negative integers, reversibility and scratch Qubits, Mapping Boolean logic to QPU operations.

UNIT III

Amplitude Amplification, Quantum Fourier Transform-QFT, DFT, FFT, Frequencies to QPU Register, Quantum phase Estimation

UNIT IV

QPU Applications- Real data- Non integer data, QRAM, Vector Encodings, Matrix Encodings , Quantum Search, Phase logic, Solving Logic puzzles and Satisfiability and Quantum Supersampling , Mathematical tools for Vector operations, Boolean Functions and Matrix operations

UNIT V

Shor's Factoring algorithm-quantum approach, Quantum Machine Learning- solving systems of linear equations, Quantum Principal Component Analysis and Support Vector Machines.

Suggested Readings:

1.	**Eric R. Johnston, Nic Harrigan, Mercedes Gimeno-Segovia "** *Programming Quantum Computers Essential Algorithms and Code Samples",* O'Reilly Media, Incorporated, 2019.
2.	**Jack D. Hidary** "*Quantum Computing: An applied Approach",* Springer International Publishers, 2021.
3.	*Robert Hundt "Quantum Computing for Programmers", Cambridge University Press, 2022*

CS 554	**GAME THEORY BASED NETWORK SECURITY**					
PROGRAM ELECTIVE-V						
Pre-requisites	Computer Networks		**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Learn the Security concepts, threats and attacks
2	Understand the Stochastic Security games with limitations
3	Understand the Security attack and intrusion detection

Course Outcomes :	
After the completion of this course, the students shall be able to:	
CO-1	Analyze the security threats and games in wireless networks
CO-2	Analyze the Stochastic Security games with limitations
CO-3	Apply the intrusion detection mechanism for various attacks

UNIT- I

Introduction: Introduction, Network Security Concepts: threats, Attacks, Defenders and their motives, Defense mechanisms, Security trade-offs and risk management.

UNIT- II

Security games: Deterministic Security games: Security game model, Intrusion detection games, Sensitivity analysis, Modeling malicious behavior in social networks, Security games for vehicular networks, Security games in wireless networks, Revocation games

Stochastic Security games: Markov Security games, Stochastic Intrusion detection game, Security of Interconnected systems, Malware filter placement game.

UNIT- III

Security games with information limitations: Bayesian security games, Security games with observation and decision errors.

Security risk-management: Quantitative risk-management, Security investment games, Cooperative games for security risk-management.

UNIT- IV

Resource allocation for security: An optimization approach to malware filtering, a robust control framework for security response, Optimal and robust epidemic response. **Usability, trust, and privacy:** Security and Usability, Digital trust online communities, Location privacy in mobile networks.

UNIT- V
Security attack and intrusion detection: Machine learning for intrusion and anomaly detection: Intrusion and anomaly detection, Machine learning for security, Distributed machine learning. **Hypothesis testing for attack detection**: Hypothesis testing and network security, hypothesis testing, Decentralized hypothesis testing with correlated observations, majority votes and optimal threshold.

Suggested Readings:

1	Tansu Alpcan and Tamer Basar "*Network theory: A Decision and Game-theoretic Approach"* Cambridge University Press, **2011**
2	Sungwook Kim, "*Game Theory Applications in Network Design"*, Information Sciences, **2014.**

CS 153	**STORAGE MANAGEMENT**					
	PROGRAM ELECTIVE-V					
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	The evolution of storage and implementation models
2	Storage devices principles including structure, host I/O processing & core algorithms
3	Storage classes (SAN, NAS. CAS), interconnection protocols, and management principles
4	Storage network design principles, Networked storage capabilities (Snaps, mirroring, virtualization)
5	Backup, Business Continuity, and Disaster Recovery principles

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Search, retrieve and synthesize information from a variety of systems and sources.
CO-2	Evaluate systems and technologies in terms of quality, functionality, cost-effectiveness and adherence to professional standards.
CO-3	Integrate emerging technologies into professional practice. Apply theory and principles to diverse information contexts.

UNIT – I
Introduction to Information Storage and Management, Storage System Environment, Intelligent Storage System.

UNIT – II
Direct-Attached Storage and Introduction to SCSI, Storage Area Networks, Network-Attached Storage.

UNIT – III
IP SAN, Content-Addressed Storage, Storage Virtualization.

UNIT – IV
Introduction to Business Continuity, Backup and Recovery, Local Replication.

UNIT –V
Remote Replication, Securing the Storage Infrastructure, Managing the Storage Infrastructure.

Suggested Reading:

1	G. Somasundaram, Alok Shrivastava, Information Storage and Management, Wiley Publishing Inc., 2009.
2	Raplh H. Thornburgh, Burry J Schoenborn, Storage Area Networks, Prentice-Hall, 2000.

OE 941 BM	**MEDICAL ASSISTIVE DEVICES**					
	OPEN ELECTIVE					
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	To extend knowledge of the amputee, of lost and remaining functions affecting locomotion, and to collect information on the best possible medical treatment.
2	To improve fitting techniques and practices, including training, so that existing devices might be used with greater comfort and function.
3	To develop improved lower-extremity devices

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Apply fundamental knowledge of engineering in rehabilitation
CO-2	Apply analytical skills to assess and evaluate the need of the end-user
CO-3	Develop self-learning initiatives and integrate learned knowledge for problem solving
CO-4	Understand the basics of robotics and apply their principles in developing prosthetics
CO-5	Apply the knowledge of computers in solving rehabilitation problems

UNIT – I
Introduction to Rehabilitation Engineering, Measurement and analysis of human movement, Disability associated with aging in the workplace and their solutions, clinical practice of rehabilitation engineering.

UNIT – II
Assistive Technology, Seating Biomechanics and systems. Wheeled Mobility: Categories of Wheelchairs. Wheelchair Structure and Component Design. Ergonomics of Wheel chair propulsion. Power Wheelchair Electrical Systems. Control. Personal Transportation. Auxiliary devices and systems.

UNIT – III
Sensory augmentation and substitution: Visual system: Visual augmentation. Tactual vision substitution, Auditory vision substitution; Auditory system: Auditory augmentation. Cochlear implantation, Visual auditory substitution, Tactual auditory substitution, Tactual system: Tactual augmentation. Tactual substitution. Measurement tools and processes: fundamental principles, structure, function; performance and behavior. Subjective and objective measurement methods.

UNIT – IV
Rehabilitation Robotics, Major Limb Prosthetic Devices, Orthotic Devices, Types of orthotics and prosthetics, Intelligent prosthetic Knee, Prosthetic Hand, Controlled orthotics and prosthetics FES system, Restoration of Hand function, Restoration of standing and walking, Myo-electric Hand.

UNIT – V
Augmentative and Alternative communication technology, Computer applications in Rehabilitation Engineering, telecommunications, and Web Accessibility.

Suggested Reading:

1	Robinson C.J., *Rehabilitation Engineering*, CRC Press, 1995.
2	Ballabio E., et al., *Rehabilitation Technology*, IOS Press, 1993.
3	Rory A Cooper, Hisaichi Ohnabe, Douglas A. Hobson, *Series in medical physis and biomedical engineering: An introduction to rehabilitation engineering*, Taylor and Francis Group, London, 2007.
4	Joseph D. Bronzino *The biomedical engineering handbook -biomedical engineering fundamentals*, 3rdEd., CRC Press, Taylor & Francis Group, London, 2006.

OE 942 BM	**MEDICAL IMAGING TECHNIQUES**					
OPEN ELECTIVE						
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	To familiarize the students with various medical imaging modalities.
2	To make learners understand the principles, detectors and operating procedures of X-ray, CT, MRI, ultrasound, PET and SPECT.
3	To make the students learn the advantages, disadvantages and hazards of various medical imaging equipment.

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Interpret the working principle and operating procedure and applications of X-ray equipment.
CO-2	Understand the image reconstruction techniques and applications of CT.
CO-3	Summarize the image acquisition and reconstruction techniques in MRI.
CO-4	Comprehend the working principle, modes and medical applications of ultrasound imaging.
CO-5	Examine the operation and applications of PET, SPECT and radio nuclide instrumentation.

UNIT – I

X ray Imaging: Electromagnetic spectrum, Production of X-rays, X-ray tubes- Stationary and Rotating Anode types, Block diagram of an X-Ray Machine, Collimators and Grids, Timing and Exposure controls. X-Ray Image visualization-Films, Fluorescent screens, Image Intensifiers.

Dental X-Ray machines, Portable and mobile X-Ray units, Mammographic X-Ray equipment,

Digital Radiography and flat panel detectors.

Radiation safety, ALARA principle, Dose units and dose limits, Radiation dosimeters and detectors.

UNIT – II

Computed Tomography: Basic principles, CT number scale, CT Generations. Major sub systems- Scanning system, processing unit, viewing unit, storage unit. Need and Principle of sectional imaging, 2D image reconstruction techniques - Iteration and Fourier methods. Applications of CT - Angio, Osteo, Dental, Perfusion (Body & Neuro), Virtual Endoscopy, Coronary Angiography.

UNIT – III
Magnetic Resonance Imaging: Principles of NMR imaging systems, Image reconstruction techniques-Relaxation processes, imaging/ pulse sequences. Sub systems of an NMR imaging system, NMR detection system, types of coils, biological effects and advantages of NMR imaging. Functional MRI - The BOLD effect, intra and extra vascular field offsets, source of T2* effects, Creating BOLD contrast sequence optimization sources and dependences of physiological noise in fMRI.

UNIT – IV
Ultrasound Imaging: - Principles of image formation -Imaging principles and instrumentation of A-mode, B-Mode, Gating Mode, Transmission mode and M-mode. Basics of multi-element linear array scanners, Digital scan conversion. Doppler Ultrasound and Colour Doppler imaging, Image artifacts, Biological effects, Ultrasound applications in diagnosis, therapy and surgery.

UNIT – V
Nuclear Medicine–Radioisotopes in medical diagnosis, Basic instrumentation- Radiation detectors, Pulse height analyzer, Rectilinear scanner, Gamma camera. Emission Computed Tomography (ECT), Principle and instrumentation of Single Photon Emission Computed Tomography(SPECT) and Positron Emission Tomography (PET). Comparison of SPECT, PET and combined PET/ X-ray CT.

Suggested Reading:

1	Khandpur R.S., *Handbook of Biomedical Instrumentation*, Tata McGraw Hill, 2016.
2	S Webb, "*The Physics of Medical Imaging*", Adam Highler, Bristol Published by CRC Press, 1988.
3	A C Kak, "*Principle of Computed Tomography*", IEEE Press New York, 1988.
4	Hykes, Heorick, Starchman, *Ultrasound physics and Instrumentation* MOSBY year book, 2nd Ed. 1992.
5	Stewart C. Bushong, *Magnetic Resonance Imaging- physical and biological principles*, MOSBY, 2nd Ed., 1995.

OE 941 CE	**GREEN BUILDING TECHNOLOGY**					
OPEN ELECTIVE						
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Exposure to the green building technologies and their significance.
2	Understand the judicial use of energy and its management.
3	Educate about the Sun-earth relationship and its effect on climate.
4	Enhance awareness of end-use energy requirements in the society.
5	Develop suitable technologies for energy management

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Understand the fundamentals of energy use and energy processes in building.
CO-2	Identify the energy requirement and its management.
CO-3	Know the Sun-earth relationship vis-a-vis its effect on climate.
CO-4	Be acquainted with the end-use energy requirements.
CO-5	Be familiar with the audit procedures of energy

UNIT – I

Overview of the significance of energy use and energy processes in building - Indoor activities and environmental control - Internal and external factors on energy use and the attributes of the factors - Characteristics of energy use and its management - Macro aspect of energy use in dwellings and its implications.

UNIT – II

Indoor environmental requirement and management - Thermal comfort - Ventilation and air quality – Air-conditioning requirement - Visual perception - Illumination requirement - Auditory requirement.

UNIT – III

Climate, solar radiation and their influences - Sun-earth relationship and the energy balance on the earth's surface - Climate, wind, solar radiation, and temperature - Sun shading and solar radiation on surfaces - Energy impact on the shape and orientation of buildings.

UNIT – IV
End-use, energy utilization and requirements - Lighting and day lighting - End-use energy requirements - Status of energy use in buildings Estimation of energy use in a building. Heat gain and thermal performance of building envelope - Steady and non-steady heat transfer through the glazed window and the wall - Standards for thermal performance of building envelope - Evaluation of the overall thermal transfer.

UNIT – V
Nuclear Medicine–Radioisotopes in medical diagnosis, Basic instrumentation- Radiation Energy management options - Energy audit and energy targeting - Technological options for energy management.

Suggested Reading:

1	Bryant Edwards, Natural Hazards, Cambridge University Press, 2005.
2	Carter, W. Nick, Disaster Management, Asian Development Bank, Manila, 1991
3	Sahni, Pardeep et.al., Disaster Mitigation Experiences and Reflections, Prentice Hall of India, New Delhi, 2002.

OE 942 CE	**COST MANAGEMENT OF ENGINEERING PROJECTS**					
OPEN ELECTIVE						
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Introduce the concepts of cost management
2	Fundamentals of cost overruns
3	Introduce the concepts of Quantitative techniques for cost management Linear Programming, PERT/CPM.

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Understanding of strategic cost management process, control of cost and decision making based on the cost of the project.
CO-2	Ability to appreciative detailed engineering activities of the project and execution of projects
CO-3	Preparation of project report and network diagram
CO-4	Able to plan Cost Behavior , Profit Planning , Enterprise Resource Planning, Total Quality Management.
CO-5	Applications of various quantitative techniques for cost management

UNIT – I

Introduction and Overview of the Strategic Cost Management Process-Cost concepts in decision-making; relevant cost, Differential cost, Incremental cost and Opportunity cost. Objectives of a Costing System- Inventory valuation- Creation of a Database for operational control; Provision of data for Decision-Making.

UNIT – II

Project: meaning, Different types, why to manage, cost overruns centres, various stages of project execution: conception to commissioning- Project execution as conglomeration of technical and non- technical activities- Detailed Engineering activities.

UNIT – III

Pre project execution main clearances and documents Project team: Role of each member. Importance Project site: Data required with significance. Project contracts. Types and contents. Project execution Project cost control. Bar charts and Network diagram. Project commissioning: mechanical and process.

UNIT – IV
Cost Behavior and Profit Planning Marginal Costing; Distinction between Marginal Costing and Absorption Costing; Break-even Analysis, Cost-Volume-Profit Analysis. Various decision-making problems- Standard Costing and Variance Analysis. Pricing strategies: Pareto Analysis. Target costing, Life Cycle Costing. Costing of service sector- Just-in-time approach, Material Requirement Planning, Enterprise Resource Planning, Total Quality Management and Theory of constraints- Activity-Based Cost Management, Bench Marking; Balanced Score Card and Value-Chain Analysis. Budgetary Control; Flexible Budgets- Performance budgets- Zero-based budgets. Measurement of Divisional profitability pricing decisions including transfer pricing.

UNIT – V
Quantitative techniques for cost management, Linear Programming, PERT/CPM,- Transportation problems, Assignment problems, Simulation, Learning Curve Theory.

Suggested Reading:

1	Cost Accounting A Managerial Emphasis, Prentice Hall of India, New Delhi
2	Charles T. Horngren and George Foster, Advanced Management Accounting
3	Robert S Kaplan Anthony A. Alkinson, Management & Cost Accounting
4	Ashish K. Bhattacharya, Principles & Practices of Cost Accounting A. H. Wheeler publisher
5	N.D. Vohra, Quantitative Techniques in Management, Tata McGraw Hill Book Co. Ltd.

OE942CE	**BUSINESS ANALYTICS**					
OPEN ELECTIVE						
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Understanding the basic concepts of business analytics and applications
2	Study various business analytics methods including predictive, prescriptive and prescriptive analytics
3	Prepare the students to model business data using various data mining, decision making methods

Course Outcomes :	
After the completion of this course, the students shall be able to:	
CO-1	To understand the basic concepts of business analytics
CO-2	Identify the application of business analytics and use tools to analyze business data
CO-3	Become familiar with various metrics, measures used in business analytics
CO-4	Illustrate various descriptive, predictive and prescriptive methods and techniques
CO-5	Model the business data using various business analytical methods and techniques

UNIT– I
Introduction to Business Analytics: Introduction to Business Analytics, need and science of data driven (DD) decision making, Descriptive, predictive, prescriptive analytics and techniques, Big data analytics, Web and Social media analytics, Machine Learning algorithms, framework for decision making, challenges in DD decision making and future.

UNIT – II
Descriptive Analytics: Introduction, data types and scales, types of measurement scales, population and samples, measures of central tendency, percentile, decile and quadrille, measures of variation, measures of shape-skewness, data visualization.

UNIT – III
Forecasting Techniques: Introduction, time-series data and components, forecasting accuracy, moving average method, single exponential smoothing, Holt‟s method, Holt-Winter model, Croston‟s forecasting method, regression model for forecasting, Auto regression models, auto-
regressive moving process, ARIMA, Theil‟s coefficient

UNIT – IV
Decision Trees: CHAID, Classification and Regression tree, splitting criteria, Ensemble and method and random forest. **Clustering**: Distance and similarity measures used in clustering Clustering algorithms, K-Means and Hierarchical algorithms, **Prescriptive Analytics**- Linear Programming (LP) and LP model building.

UNIT –V
Six Sigma: Introduction, introduction, origin, 3-Sigma Vs Six-Sigma process, cost of poor quality, sigma score, industry applications, six sigma measures, DPMO, yield, sigma score, DMAIC methodology, Six Sigma toolbox.

Suggested Reading:

1	U Dinesh Kumar, ―Data Analytics‖, Wiley Publications, 1st Edition, 2017
2	Marc J. Schniederjans, Dara G. Schniederjans, Christopher M. Starkey, ―Business analytics Principles, Concepts, and Applications with SAS‖, Associate Publishers, 2015
3	S. Christian Albright, Wayne L. Winston, ―Business Analytics - Data Analysis and Decision Making‖, 5th Edition, Cengage, 2015

OE 941 EC	**ELEMENTS OF EMBEDDED SYSTEMS**					
OPEN ELECTIVE						
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Understanding various Embedded Design strategies
2	Designing Micro controller based Embedded Systems
3	Designing FPGA Based Embedded Systems

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Understand Embedded Design Strategies and architecture of Arduino Board
CO-2	Program using various onboard components of Arduino
CO-3	Design real time interfacing with Arduino
CO-4	Understand Design Flow of FPGA, programming FPGA using Verilog HDL
CO-5	Implement combinational and sequential circuits using verilog HDL

UNIT – I
Embedded Systems Design Strategies: Micro Controller, DSP, FPGA, Introduction to Arduino (Micro controller Board), Components of Arduino, Architecture and Pin Configuration of ATMega328, Ports of ATMega328.

UNIT – II
Interfacing: Interfacing Switches, LEDs, Analog to Digital Converter, Digital to Analog Converter, Interfacing and Programming I2C, SPI

UNIT – III
Real Time Programming: Interfacing Key Pad, 7-segment display, LCD, Interfacing Sensors, Interfacing Stepper Motor**,** USB programming

UNIT – IV
FPGA Based Embedded Design: FPGA Design flow, Introduction to Verilog HDL**,** Basic building blocks, Data types of Verolog HDL, Behavioral Modelling, Data Flow Modelling, Structural Modelling, Hierarchal Structural Modelling, Case Studies on Verilog HDL descriptions of Basic Circuits

UNIT – V
Modelling of Circuits: Verilog HDL Implementation of Combinational MSI Circuits, Verilog HDL Implementation of Sequential MSI Circuits, Finite Sate Machine Design, Tasks and Functions, Introduction to Test Benches

Suggested Reading:

1	Ming-Bo Lin, Digital System Designs and Practices Using Verilog HDL and FPGAs, Wiley India, 2008
2	Samir Palnitkar, Verilog HDL: A Guide to Digital Design and Synthesis, Pearson Education, 2005
3	Simon Monk, Programming Arduino: Getting Started with sketches, Mc.Hill, 2016

OE 941 EE	**WASTE TO ENERGY**					
OPEN ELECTIVE						
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	To know the various forms of waste
2	To understand the processes of Biomass Pyrolysis.
3	To learn the technique of Biomass Combustion.

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Understand the concept of conservation of waste
CO-2	Identify the different forms of wastage.
CO-3	Chose the best way for conservation to produce energy from waste.
CO-4	Explore the ways and means of combustion of biomass.
CO-5	Develop a healthy environment for the mankind.

UNIT – I
Introduction to Energy from Waste: Classification of waste as fuel – Agro based, Forest residue, Industrial waste - MSW – Conversion devices – Incinerators, gasifiers, digestors

UNIT – II
Biomass Pyrolysis: Pyrolysis – Types, slow fast – Manufacture of charcoal – Methods Yields and application – Manufacture of pyrolytic oils and gases, yields and applications.

UNIT – III
Biomass Gasification: Gasifiers – Fixed bed system – Downdraft and updraft gasifiers Fluidized bed gasifiers – Design, construction and operation – Gasifier burner arrangement for thermal heating – Gasifier engine arrangement and electrical power – Equilibrium and kinetic consideration in gasifier operation.

UNIT – IV
Biomass Combustion: Biomass stoves – Improved chullahs, types, some exotic designs, Fixed bed combustors, Types, inclined grate combustors, Fluidized bed combustors, Design, construction and operation - Operation of all the above biomass combustors.

UNIT – V
Biogas: Properties of biogas (Calorific value and composition) - Biogas plant technology and status - Bio energy system - Design and constructional features - Biomass resources and their classification - Biomass conversion processes - Thermo chemical conversion - Direct combustion - biomass gasification - pyrolysis and liquefaction - biochemical conversion anaerobic digestion - Types of biogas Plants – Applications - Alcohol production from biomass Bio diesel production - Urban waste to energy conversion - Biomass energy programme in India.

Suggested Reading:

1	Non Conventional Energy, Desai, Ashok V., Wiley Eastern Ltd., 1990.
2	Biogas Technology - A Practical Hand Book - Khandelwal, K. C. and Mahdi, S. S., Vol. I & II, Tata McGraw Hill Publishing Co. Ltd., 1983.
3	Food, Feed and Fuel from Biomass, Challal, D. S., IBH Publishing Co. Pvt. Ltd., 1991.
4	Biomass Conversion and Technology, C. Y. WereKo-Brobby and E. B. Hagan, John Wiley & Sons, 1996.

OE 942 EE	**POWER PLANT CONTROL AND INSTRUMENTATION**					
OPEN ELECTIVE						
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Learn of different types of power plants.
2	Learn basic working principle of instruments for measurement of electrical and non-electrical quantities like Temperature Pressure flow level measurements.
3	Understand the instrumentation and protection systems applied in thermal power plant.
4	Learn control techniques employed for the operation of modern power generation plant

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Explain the different methods of power generation. Along with Piping and Instrumentation diagram of boiler.
CO-2	Select various measurements involved in power generation for measuring electrical and non-electrical parameters.
CO-3	Identify the different types of analyzers used for scrutinizing boiler steam and water.
CO-4	Model different types of controls and control loops in boilers.
CO-5	Illustrate the methods of monitoring and control of different parameters like speed, vibration of turbines

UNIT – I
Brief survey of methods of power generation, hydro, thermal, nuclear, solar and wind power, importance of instrumentation in power generation, thermal power plants, block diagram, details of boiler processes, Piping and Instrumentation diagram of boiler, cogeneration.

UNIT – II
Electrical measurements, current, voltage, power, frequency, power factor etc, non-electrical parameters, flow of feed water, fuel, air and steam with correction factor for temperature, steam pressure and steam temperature, drum level measurement, radiation detector, smoke density measurement, dust monitor.

UNIT – III
Flue gas oxygen analyzer: Analysis of impurities in feed water and steam, dissolved oxygen analyzer. Chromatography, pH meter, fuel analyzer, pollution monitoring instruments.

UNIT – IV
Combustion control, air / fuel ratio control, furnace draft control, drum level control, main steam and reheat steam temperature control, super heater control, air temperature, distributed control system in power plants, interlocks in boiler operation.

UNIT – V
Speed, vibration, shell temperature monitoring and control, steam pressure control, lubricant oil temperature control, cooling system.

Suggested Reading:

1	Sam G. Dukelow, The Control of Boilers, Instrument Society of America, 2nd Edition, 2010.
2	P.K. Nag, „Power Plant Engineering“, Tata McGraw-Hill, 1st Edition, 2001.
3	S.M. Elonka and A.L. Kohal, “Standard Boiler Operations”, Tata McGraw-Hill, 1st Edition, 1994.
4	R K Jain, “Mechanical and Industrial Measurements”, Khanna Publishers, 1st Edition, 1995.
5	E Al Wakil, “Power Plant Engineering”, Tata McGraw-Hill, 1st Edition, 1984.

OE 941 ME	**OPERATIONS RESEARCH**					
OPEN ELECTIVE						
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60Marks	**CIE**		40Marks	

Course Objectives:	
The course is taught with the objectives of enabling the student to:	
1	Understand the dynamic programming to solve problems of discrete and continuous variables
2	Apply the concept of non-linear programming and carry out sensitivity analysis
3	Understand deterministic and probabilistic inventory control models.

Course Outcomes:	
After the completion of this course, the students shall be able to:	
CO-1	Understand the basics of OR, including mathematical modeling, feasible solutions and optimization.
CO-2	Able to carry out sensitivity analysis.
CO-3	Apply PERT/CPM in project management.
CO-4	Select appropriate inventory control model.
CO-5	Able to apply dynamic programming and understand the concept of non-linear programming.

UNIT–I
Development, Different Phases, Characteristics, Operations Research models and applications. Linear Programming Problem: Introduction, Basic Assumptions, Formulation, graphical method, simplex method: Big M and Two Phase method.

UNIT–II
DUALITY: Duality theory, primal-dual relationships, Economic interpretation, Dual simplex method, Post optimal or sensitivity analysis.

UNIT–III
Project Management: Introduction to PERT and CPM, critical Path calculation, float calculation and its importance. Cost reduction by Crashing of activity. Inventory models – Economic order quantity models – Quantity discount models – Stochastic inventory models – Multi product models – Inventory control models in practice.

UNIT–IV
Sequencing Models: Introduction, General assumptions, processing n jobs through 2 machines, processing „n‟ jobs through m machines. Game Theory: Introduction, Characteristics of Game Theory, Dominance theory, Mixed strategies (2 x 2, m x 2), Algebraic and graphical methods. Nonlinear programming problem: - Kuhn-Tucker conditions.

UNIT–V
Queuing models - Queuing systems and structures – Notation parameter – Single server and multi server models – Poisson arrivals – Exponential service times – with finite population – Infinite population. Dynamic Programming: Characteristics, principle of optimality, deterministic problems.

Suggested Reading:

1	H.A.Taha, Operations Research, An Introduction, PHI,2008
2	H.M.Wagner, Principles of Operations Research, PHI,Delhi,2010
3	J.C.Pant,IntroductiontoOptimization:OperationsResearch,JainBrothers,Delhi, 2008.
4	Frederick S. Hillier, Gerald J. Lieberman, Operations Research, 10thEdition, McGraw Hill Pub. 2017.
5	Pannerselvam, Operations Research: Prentice Hall of India, 2010.
6	Ronald L. Rardin, Optimization in Operations Research, First Indian Reprint, Pearson Education Asia. 2002,

OE 942 ME	**COMPOSITE MATERIALS**					
OPEN ELECTIVE						
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Study the concepts of composite construction.
2	Learn analysis and designs of composite beams, floors, columns and trusses as per the recommendations of IS codes of practice.
3	Apply the concepts for design of multi-storey composite buildings.
4	Scope of analysis is restricted to skeletal structures subjected to prescribed dynamic loads.

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Understand the fundamentals of composite construction, and analysis and designs of composite beams.
CO-2	Analyse and design the composite floors
CO-3	Select suitable materials for composite columns,
CO-4	Analyse composite trusses and understand connection details.
CO-5	Analyse and design the multi-storey composite buildings

UNIT – I
Introduction of composite constructions: Benefits of composite construction - Introduction to IS - BS and Euro codal provisions. Composite beams: Elastic behaviour of composite beams - No and full interaction cases - Shear connectors - Ultimate load behaviour - Serviceability limits - Effective breadth of flange - Interaction between shear and moment - Basic design consideration and design of composite beams.

UNIT – II
Composite floors: Structural elements - Profiled sheet decking - Bending resistance - Shear resistance - Serviceability criterion - Analysis for internal forces and moments - Design of composite floors.

UNIT – III
Composite columns: Materials - Concrete filled circular tubular sections - Non-dimensional

slenderness - Local buckling of steel sections - Effective elastic flexural stiffness - Resistance of members to axial compressions - Composite column design - Fire resistance.

UNIT – IV
Composite trusses: Design of truss - Configuration - Truss members - Analysis and design of composite trusses and connection details.

UNIT – V
Design of multi-storey composite buildings: Design basis - Load calculations - Design of composite slabs with profile decks - Composite beam design - Design for compression members - Vertical cross bracings - Design of foundation.

Suggested Reading:

1	R.P. Johnson, "Composite Structures of Steel and Concrete - Beams, Slabs, Columns and Frames in Buildings", Blackwell Publishing, Malden, USA, 2004.
2	"INSDAG Teaching Resources for Structural Steel Design", Vol-2, Institute for Steel Development and Growth Publishers, Calcutta, India.
3	"INSDAG Handbook on Composite Construction – Multi-Storey Buildings", Institute for Steel Development and Growth Publishers, Calcutta, India.
4	"INSDAG Design of Composite Truss for Building", Institute for Steel Development and Growth Publishers, Calcutta, India.
5	"INSDAG Handbook on Composite Construction – Bridges and Flyovers", Institute for Steel Development and Growth Publishers, Calcutta, India.
6	IS: 11384-1985, "Code of Practice for Composite Construction in Structural Steel and Concrete", Bureau of Indian Standards, New Delhi, 1985.

OE 943 ME	**INDUSTRIAL SAFETY**					
OPEN ELECTIVE						
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Identify the causes for industrial accidents and preventive steps to be taken.
2	Learn fundamental concepts of Maintenance Engineering.
3	Learn About wear and corrosion along with preventive steps to be taken
4	Learn the basic concepts and importance of fault tracing.
5	Learn steps involved in carrying out periodic and preventive maintenance of various equipments used in industry

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Identify the causes for industrial accidents and suggest preventive measures.
CO-2	Identify the basic tools and requirements of different maintenance procedures.
CO-3	Apply different techniques to reduce and prevent Wear and corrosion in Industry.
CO-4	Identify different types of faults present in various equipments like machine tools, IC Engines, boilers etc.
CO-5	Apply periodic and preventive maintenance techniques as required for industrial equipments like motors, pumps and air compressors and machine tools etc

UNIT – I
Industrial safety: Accident, causes, types, results and control, mechanical and electrical hazards, types, causes and preventive steps/procedure, describe salient points of factories act 1948 for health and safety, wash rooms, drinking water layouts, light, cleanliness, fire, guarding, pressure vessels, etc, Safety color codes, Fire prevention and firefighting, equipment and methods.

UNIT – II
Fundamentals of Maintenance Engineering: Definition and aim of maintenance engineering, Primary and secondary functions and responsibility of maintenance department, Types of maintenance, Types and applications of tools used for maintenance, Maintenance cost & its relation with replacement economy, Service life of equipment.

UNIT – III
Wear and Corrosion and their Prevention: Wear- types, causes, effects, wear reduction methods, lubricants-types and applications, Lubrication methods, general sketch, working and applications of Screw down grease cup, Pressure grease gun, Splash lubrication, Gravity lubrication, Wick feed lubrication, Side feed lubrication, Ring lubrication, Definition of corrosion, principle and factors affecting the corrosion, Types of corrosion, corrosion prevention methods.

UNIT – IV
Fault Tracing: Fault tracing-concept and importance, decision tree concept, need and applications, sequence of fault finding activities, show as decision tree, draw decision tree for problems in machine tools, hydraulic, pneumatic, automotive, thermal and electrical equipment‟s like, any one machine tool, Pump, Air compressor, Internal combustion engine, Boiler, Electrical motors, Types of faults in machine tools and their general causes.

UNIT – V
Periodic and Preventive Maintenance: Periodic inspection-concept and need, degreasing, cleaning and repairing schemes, overhauling of mechanical components, overhauling of electrical motor, common troubles and remedies of electric motor, repair complexities and its use, definition, need, steps and advantages of preventive maintenance. Steps/procedure for periodic and preventive maintenance of Machine tools, Pumps, Air compressors, Diesel generating (DG) sets, Program and schedule of preventive maintenance of mechanical and electrical equipment, advantages of preventive maintenance. Repair cycle concept and importance.

Suggested Reading:

1	H. P. Garg, “Maintenance Engineering”, S. Chand and Company
2	Audels, “Pump-hydraulic Compressors”, Mcgraw Hill Publication
3	Higgins & Morrow, “Maintenance Engineering Handbook”, Da Information Services.
4	Winterkorn, Hans, “Foundation Engineering Handbook”, Chapman & Hall London

OE 941 LA	**INTELLECTUAL PROPERTY RIGHTS**					
OPEN ELECTIVE						
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Acquaint the students with basics of intellectual property rights with special reference to Indian Laws and its practices.
2	Compare and contrast the different forms of intellectual property protection in terms of their key differences and similarities.
3	Provide an overview of the statutory, procedural, and case law underlining these processes and their interplay with litigation.

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Understand the concept of intellectual property rights.
CO-2	Develop proficiency in trademarks and acquisition of trade mark rights.
CO-3	Understand the skill of acquiring the copy rights, ownership rights and transfer.
CO-4	Able to protect trade secrets, liability for misappropriations of trade secrets.
CO-5	Apply the patents and demonstration of case studies.

UNIT – I
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.

UNIT – II
Trade Marks: Purpose and function of trademarks, acquisition of trade mark rights, protectable matter, selecting, and evaluating trade mark, trade mark registration processes.

UNIT – III
Law of copy rights: Fundamental of copy right law, originality of material, rights of reproduction, rights to perform the work publicly, copy right ownership issues, copy right

registration, notice of copy right, international copy right law. Law of patents: Foundation of patent law, patent searching process, ownership rights and transfer**.**

UNIT – IV

Trade Secrets: Trade secrete law, determination of trade secrete status, liability for misappropriations of trade secrets, protection for submission, trade secrete litigation. Unfair competition: Misappropriation right of publicity, false advertising.

UNIT – V

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.

Suggested Reading:

1	Halbert, "Resisting Intellectual Property", Taylor & Francis Ltd, 2007.
2	"Mayall, "Industrial Design", McGraw Hill,1992
3	"Niebel, "Product Design", McGraw Hill,1974.
4	"Asimov, "Introduction to Design", Prentice Hall,1962.
5	"Robert P. Merges, Peter S. Menell, Mark A. Lemley, "Intellectual Property in New Technological Age",2016.
6	T. Ramappa, "Intellectual Property Rights Under WTO", S. Chand,2008

CS 562	DIGITAL FORENSICS LAB					
	LAB – II					
Pre-requisites			**L**	**T**	**P**	**C**
			-	-	2	1
Evaluation	**SEE**	--	**CIE**		**50 Marks**	

LIST OF EXPERIMENTS

1. Study of Computer Forensics and different tools used for forensic investigation
2. How to Recover Deleted Files using Forensics Tools
3. How to make the forensic image of the hard drive using EnCase Forensics.
4. How to Collect Email Evidence in Victim PC
5. How to Extracting Browser Artifacts
6. Find Last Connected USB on your system (USB Forensics)
7. Live Forensics Case Investigation using Autopsy
8. Capturing and analyzing network packets using Wireshark
9. Analyze the packets provided in lab and solve the questions using Wireshark
   a) What web server software is used by www.uceou.com
   b) About what cell phone problem is the client concerned?
   c) How many webservers are running in Apache webserver.
10. Using Sysinternals tools for Network Tracking and Process Monitoring
    - Check Sysinternals tools
    - Monitor Live Processes
    - Capture RAM
    - Capture TCP/UDP packets
    - Monitor Hard Disk
    - Monitor Virtual Memory
    - Monitor Cache Memory
11. Email Forensics
    - Mail Service Providers
    - Email protocols
    - Recovering emails
    - Analyzing email header
12. Analyzing data of android mobile using MOBILedit.

CS 563	SECURITY LAB - III					
LAB – III						
Pre-requisites			L	T	P	C
			-	-	2	1
Evaluation	SEE	--	CIE		50 Marks	

Module 1: Basics of Networking and Security Concepts

- Types of IP address
- How Computer Communication.
- Transport Protocol
- IP Planning.
- DNS Server and Various types of DNS records.
- Understanding of OSI model and Reference layer devices.
- TCP/IP Packet Understanding.
- 3 Ways Handshake.
- Router, Switches Understanding Of designing Corporate network etc.
- Understanding of Firewall. Web Application Firewall (WAF) Proxy
- Email Gateway (Email Security) IPS/IDS
- DLP
- End Point Security
- Ransomware Attack.
- DOS Attack.
- SQL Injection.
- Cross Sites Scripting.
- Malware Attacks & Phishing Attack

Module 2: Splunk Enterprise & Splunk Enterprise Security

- What is SIEM
- Logs, Events, Parsing, Normalization
- Selection Criteria of any SIEM
- Introduction of Splunk and its Components
- Detail understanding of various deployment Architectures of Splunk including Single instance Distributed and Cluster Architecture
- cSplunk Indexes, Buckets, Data Retention Policies
- Splunk Licensing, Search factor, Replication factor etc.
- Heavy Forwarders, Universals Forwarders, License Master, Master Node, Deployer, Deployment Server
- Splunk Solution Architect Scenario: Size and Design an Splunk Deployment Architecture for a Company, Calculate Storage, License, Resources requirement.
- Installing Splunk Enterprise
- Understanding various settings and options available in
- Splunk Web
- Splunk Apps and Addons

- Integration of various devices with Splunk such as
- Windows, Linux Firewall etc
- Installing Splunk Universal Forwarders
- Troubleshooting device integration Issues
- Installing Apps and Addons
- Deploying Apps using Deployment Server
- Configuration of Heavy Forwarder
- Splunk Directory hierarchy, Splunk Configuration Commands
- Understating of Splunk data Backup and Configuration
- backup requirement
- Understating Splunk Version Upgrade
- Splunk Field based Search
- Understanding logical operators
- Searching on Splunk using SPL
- Various Splunk SPL command which are required from Cyber Security Perspective
- Creating and Scheduling and Downloading Report
- Creating Dashboard
- Installing Splunk Enterprise Security App
- Understanding the use of various dashboard on Splunk Security App
- Creating and Managing Correlation Rules/Searches
- Fine tuning Correlation Rules
- SOC Incident Response
- Analyzing and investigating on the Real-time Incidents for True Positive or False Positive
- How to Create Incident on the Email and Tickets for True Positive cases
- Learning TOP 10 Incident Response Cases which commonly generated in the companies SIEM
- Shift Handover and Splunk SIEM Health Check
- Interview Preparation Session
- Resume Preparation Session
- LinkedIn Profile Preparation, Naukri Profile Key Skills
- Realtime Company Environment Scenario discussion, like Number of Devices, EPS, Locations, Licenses, number of Soc analyst etc.
- Type of SOC, Dedicated, MSSP etc.
- Roles of L1, L2, L3, Administrator etc.

Module 3: Phishing Email Analysis

- What is Phishing email
- Phishing email Analysis
- Email Header Analysis

Module 4: CrowdStrike EDR

- Understanding EDR
- EDR vs Anti Virus
- Understanding Fileless Malware
- Briefing on Pyramid of Pain
- Mitre attack frame work
- Falcon Platform Architecture Overview

- Falcon Platform Technical Fundamentals
- Falcon console overview
- Roles and access control & user Management
- Sensor installation and troubleshooting
- Falcon Fusion workflow & Policy briefing
- Dashboards and Reports creation
- On-demand Scans
- Investigation Fundamentals & Event Searches.
- Threat Intelligence & Sandboxing
- Falcon for responders & RTR fundamentals.
- Incident response using EDR
- USB Device Control management

Module 5: Cortex XSOAR

Domain 1: Knowing SOAR

- What is SOAR
- What does SOAR consist of
- What can be integrated with SOAR
- Benefits of SOAR in Today's SOC

Domain 2: Knowing Playbook

- Reference and manipulate context data to manage
- automation workflow
- Summarize inputs, outputs, and results for playbook tasks
- Differentiate among Playbook Task Types

- Manual
- Automated
- Conditional
- Data Collection
- Sub-Playbook

Domain 3: Automations, Integrations, and Related Concepts

- Playbook Tasks
- War Room
- Layouts (Dynamic Sections, Buttons)
- Jobs
- Field Trigger Scripts
- Pre/Post-Processing

Domain 4: UI Workflow, Dashboards, and Reports.

- Identify Methods for Querying Data

- Indicators
- Incidents
- Dashboards
- Global Search

- Interact with Layouts for Incident Management

- Sections
- Fields
- Buttons

- Summarize Tools used for Managing Incidents

- Bulk Incident Actions
- Table View versus Summary View
- Table Settings

Module 6: Vulnerability Management (Self-paced)

- Need for Vulnerability Assessment
- The life cycles of Vulnerability Assessment and Penetration Testing
- Introduction to Nmap (Discovery, Port scanning, Vulnerability scanning)
- Various features of Nmap
- Introduction to Nessus
- Installing Nessus on different platforms
- Scan prerequisites
- Scan-based target system admin credentials
- Direct connectivity without a firewall
- Backup of all systems including data and configuration
- Updating Nessus plugins
- Sufficient network bandwidth to run the scan
- Policy configuration
- Credential scan vs Non-Credential scan
- Removing False Positive from the Scan /Scan
- execution and results
- Preparing the report (Mitigation/Vulnerability Tracker)

CS 171	**MINI PROJECT**					
Mini project						
Pre-requisites	-		**L**	**T**	**P**	**C**
			-	-	4	2
Evaluation	**SEE**	-	**CIE**	**50 Marks**		

Course Objectives:	
The course is taught with the objectives of enabling the student to:	
1	To review available literature and formulate structural engineering problems
2	To learn the technique of writing reports and prepare presentation

Course Outcomes:	
On completion of this course, the student will be able to:	
CO-1	Identify engineering problems reviewing available literature
CO-2	Understand of contemporary / emerging technology for various processes and systems.
CO-3	Share knowledge effectively in oral and written form and formulate documents
CO-4	Present solution by using his/her technique applying engineering principles.
CO-5	Prepare technical report and presentation

Guidelines:

The students are required to search / gather the material / information on a specific topic comprehend it and present / discuss in the class. Students can take up small problems in the field of design engineering as mini project. It can be related to solution to an engineering problem, verification and analysis of experimental data available, conducting experiments on various engineering subjects, material characterization, studying a software tool for the solution of an engineering problem etc.

Mini Project will have mid semester presentation and end semester presentation. Mid semester presentation will include identification of the problem based on the literature review on the topic referring to latest literature available. End semester presentation should be done along with the report on identification of topic for the work and the methodology adopted involving scientific research, collection and analysis of data, determining solutions highlighting individuals ‘contribution. Continuous assessment of Mini Project at Mid Semester and End Semester will be monitored by the departmental committee.

SEMESTER –III

AC 040	**RESEARCH METHODOLOGY**					
AUDIT COURSE– I						
Pre-requisites			**L**	**T**	**P**	**C**
			3	-	-	3
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
1	To understand the research process
2	To solve unfamiliar problems using scientific procedures
3	To pursue ethical research
4	To use appropriate tools for documentation and analysis of data

Course Outcomes :	
On completion of this course, the student will be able to Implement:	
CO-1	Understand research problem formulation
CO-2	Design experiments
CO-3	Analyze research related information
CO-4	Write papers and thesis, Follow research ethics
CO-5	Use tools for analysis and thesis writing

UNIT – I

Research Process: Meaning of Research, Objectives and Motivation of Research, Technological Innovation, Types of Research, Research Vs Scientific method, Research Methodology vs Research Methods, Research process.

Research Problem Formulation: Problem solving in Engineering, Identification of Research Topic, Problem Definition, Literature Survey, Literature Review.

Research Design: Research Design: What it is?, Why we need Research Design? Terminology and Basic Concepts, Different Research Designs, Experimental Designs, Important Experimental Designs, Design of Experimental Setup, Use of Standards and Codes.

UNIT – II
Mathematical Modeling: Models in General, Mathematical Model, Model Classification, Modelling of Engineering Systems. **Probability and Distributions:** Importance of Statistics to Researchers, Probability Concepts, Probability Distributions, Popular Probability Distributions, Sampling Distributions. **Sample Design And Sampling:** Sample design, Types of sample designs, The Standard Error, Sample Size for Experiments, Prior Determination Approach, Use of Automatic Stopping Rule **Hypothesis Testing and ANOVA:** Formulation of Hypothesis, Testing of Hypothesis, Analysis of Variance.

UNIT – III
Design of Experiments and Regression Analysis: Design of Experiments, Planning of Experiments, Multivariate Analysis, Simple Regression and Correlation, Multiple Regression and Correlation **Analysis and Interpretation of Data:** Introduction, Data Checking, Data Analysis, Interpretation of Results, Guidelines in Interpretations. **Accuracy, Precision and Error Analysis:** Introduction, Repeatability and Reproducibility, Error Definition and Classification, Analysis of Errors, Statistical Analysis of Errors, Identification of Limitations

UNIT – IV
Writing of Papers and Synopsis: Introduction, Audience Analysis,, Preparing Papers for Journals, Preparation of Synopsis of Research Work **Thesis Writing Mechanics:** Introduction, Audience for Thesis Report, Steps in Writing the report, Mechanics of Writing, Presentation of graphs, figures and tables. **Structure of Thesis Report:** Suggested Framework of the Report, Preliminary Pages, Main Body of Thesis, Summary, Appendices, References, Glossary.

UNIT –V
Ethics in Research: Importance of Ethics in Research, Integrity in Research, Scientific Misconduct and Consequences. **Spreadsheet tool:** Introduction, Quantitative Data Analysis Tools, Entering and preparing your data, using statistical functions, Loading and using Data Analysis Tool Pack [Tools: Microsoft Excel / Open office] **Thesis writing & scientific editing tool [Tool: Latex]:** Introduction, Document Structure, Typesetting Text, Tables, Figures, Equations, Inserting References.

Suggested Reading:

1	R.Ganesan; Research Methodology for Engineers; MJP Publishers; Chennai, 2011
2	Paul R Cohen. Empirical Methods in AI. PHI, New Delhi, 2004
3	C.R.Kothari, Research Methodology, Methods & Technique; New age International Publishers, 2004
4	Kumar, Ranjit. Research Methodology-A Step-by-Step Guide for Beginners, Pearson Education, 2005
5	LaTEX for Beginners, Workbook, 5th Edition , March 2014.

AC 031	**ENGLISH FOR RESEARCH PAPER WRITING**					
AUDIT - II						
Pre-requisites			**L**	**T**	**P**	**C**
			2	-		0
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Understand that how to improve your writing skills and level of readability
2	Understand the nuances of language and vocabulary in writing a Research Paper.
3	Develop the content, structure, format of writing a research paper and produce original research papers without plagiarism

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Interpret the nuances of research paper writing.
CO-2	Differentiate the research paper format and citation of sources.
CO-3	To review the research papers and articles in a scientific manner.
CO-4	Avoid plagiarism and be able to develop their writing skills in presenting the research work.
CO-5	Create a research paper and acquire the knowledge of how and where to publish their original research papers

Unit – I
Academic Writing: Meaning & Definition of a research paper– Purpose of a research paper – Scope – Benefits, Limitations – outcomes.

Unit – II
Research Paper Format: Title – Abstract – Introduction – Discussion – Findings, Conclusion – Style of Indentation – Font size/Font types – Indexing – Citation of sources.

Unit – III
Research Methodology: Methods (Qualitative – Quantitative) Review of Literature. Criticizing, Paraphrasing & Plagiarism.

Unit – IV

Process of Writing a research paper: Choosing a topic - Thesis Statement – Outline – Organizing notes - Language of Research – Word order, Paragraphs – Writing first draft – Revising/Editing - The final draft and proof reading.

Unit – V
Research Paper Publication: Reputed Journals – National/International – ISSN No, No. of volumes, Scopus Index/UGC Journals – Free publications - Paid Journal publications – Advantages/Benefits *Presentation Skills:* Developing Persuasive Presentations, Structure of Presentation, Presentation Slides, Presentation Delivery, role of the audience, what to search and cite, how to establish credibility.

Suggested Reading:

1	C. R Kothari, Gaurav, Garg, "*Research Methodology Methods and Techniques*", 4/e, New Age International Publishers.
2	Day R, "*How to Write and Publish a Scientific Paper***",** Cambridge University Press, 2006
3	"*MLA Hand book for writers of Research Papers*", 7/e, East West Press Pvt. Ltd, New Delhi
4	Lauri Rozakis, Schaum‟s, "*Quick Guide to Writing Great Research Papers"*, Tata McGraw Hills Pvt. Ltd, New Delhi.

AC 032	**DISASTER MITIGATION AND MANAGEMENT**					
	AUDIT - II					
Pre-requisites			**L**	**T**	**P**	**C**
			2	-		0
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Introduction of various types of disasters and its effect on structures.
2	Learning of quality assurance and damage assessment of structures
3	Educate different types of repair, strengthening, rehabilitation and retrofitting techniques.
4	Awareness about flood characteristics and flood forecasting systems
5	Description of Flood mitigation, adjustment, and regulation

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Understand the fundamentals of disaster and seismic performance of buildings
CO-2	Able to assess various damages in structures and give assurance of quality of concrete
CO-3	Decide the appropriate repair, strengthening, rehabilitation and technique required for a case study of building.
CO-4	Applications of flood routing, flood forecasting and space time characteristics of rainfall.
CO-5	Advanced understanding of flood plain adjustments and employment of appropriate technologies for flood mitigation.

UNIT – I
Disaster: Classifications - Causes - Impacts including social, economical, political, environmental, health, psychosocial, etc.
Seismic performance of buildings: case studies of major earthquakes in the country, damage to buildings, damage patterns, performance of non-engineered buildings- Introduction to repair and rehabilitation of structures.

UNIT – II
Quality assurance for concrete – Strength, Durability and Thermal properties of concrete. Damage Assessment**:** - Condition assessment and distress, Purpose of assessment, Rapid assessment - diagnostic techniques, Investigation of damage, , Evaluation of surface and structural cracks, Damage assessment procedure, destructive, non-destructive and semi destructive testing systems, Procedure for evaluating damaged of structure.

UNIT – III
Repair, Rehabilitation And Retrofitting Techniques : Repair materials, Common types of repairs – Repair in concrete structures – Repairs in under water structures – Guniting – Shot create –Underpinning, Strengthening of Structural elements, Repair of structures distressed due to corrosion, fire, Leakage, earthquake, Retrofitting techniques

UNIT – IV
Introduction to Disasters: Hazard, Vulnerability, Resilience, Risks.-Disaster- Different types of cold wave-heat wave- droughts- floods-Effect of climate change on Processes.
Flood characteristics and forecasting: Measureable features of a flood (Elevation, discharge, volume, and duration), flood forecasting (unit hydrograph method, meteorological and snow data, and snow field air temperatures), operation of flood forecasting systems.
Space-time characteristics of rainfall: Policy criteria for design flood of a major and minor reservoir, spillways, diversion dams and barrages, design flood criteria for dams and other hydraulic structures (CWC recommendations).

UNIT – V
Flood Routing: Mathematics of flood routing, various methods of flood routing, Hydrologic and Hydraulic routing.
Flood mitigation: flood ways, channel improvement, evacuation and flood proofing, land management, flood plain management, estimating benefits of flood mitigation.
Flood plain adjustments and regulations: Results of controlling floods, alternatives to controlling floods, range of possible adjustments, practical range of choice, critical characteristics of flood hazards.

Suggested Reading:

1	Barry A. Richardson, “Defects and Deterioration in Buildings”, E &FN Spon Press, London, 1991.
2	J. H. Bungey, “Testing of Concrete in Structures”, Chapman and Hall,New York, 1989.
3	“A.R. Santakumar, “Concrete Technology”, Oxford University Press,New Delhi, 2006.
4	“Pankaj Agarwal and Manish Shrihkande (2006). “Earthquake Resistance Design of Structures.” Prentice Hall of India.
5	“Ravishankar.K., Krishnamoorthy.T.S, "Structural Health Monitoring, Repair and Rehabilitation of Concrete Structures", Allied Publishers, 2004. New Technological Age”,2016.
6	CPWD and Indian Buildings Congress, Hand book on Seismic Retrofit of Buildings, Narosa Publishers, 2008.

AC 033	**SANSKRIT FOR TECHNICAL KNOWLEDGE**					
AUDIT - II						
Pre-requisites			**L**	**T**	**P**	**C**
			2	-		0
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	*To get a working knowledge in illustrious Sanskrit, the scientific language in the world*
2	*To make the novice Learn the Sanskrit to develop the logic in mathematics, science & other subjects*
3	*To explore the huge knowledge from ancient Indian literature*

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	*Develop passion towards Sanskrit language*
CO-2	*Decipher the latent engineering principles from Sanskrit literature*
CO-3	*Correlates the technological concepts with the ancient Sanskrit history.*
CO-4	*Develop knowledge for the technological progress*
CO-5	*Explore the avenue for research in engineering with aid of Sanskrit*

Unit – I
Introduction to Sanskrit Language: Sanskrit Alphabets-vowels-consonants- significance of Amarakosa-parts of Speech-Morphology-creation of new words-significance of synonyms-sandhi-samasa-sutras-active and passive Voice-Past/Present/Future Tense-Syntax-Simple Sentences (elementary treatment only)

Unit – II
Role of Sanskrit in Basic Sciences: Brahmagupthas lemmas (second degree indeterminate equations), sum of squares of n-terms of AP- sulba, sutram or baudhayana theorem (origination of Pythagoras theorem)-value of pie-Madhava‟s sine and cosine theory (origination of Taylor's series). The measurement system-time-mass-length-temp, Matter elasticity-optics-speed of light (origination of Michaelson and Morley theory).

Unit – III
Role of Sanskrit in Engineering-I (Civil, Mechanical, Electrical and Electronics Engineering): Building construction-soil testing-mortar-town planning-Machine definition-crucible-

furnace-air blower- Generation of electricity in a cell-magnetism-Solar system-Sun: The source of energy, the earth-Pingala chandasutram (origination of digital logic system)

Unit – IV
*Role of Sanskrit in Engineering-II (Computer Science Engineering & Information Technology):*Computer languages and the Sanskrit languages-computer command words and the vediccommand words-analogy of pramana in memamsa with operators in computer language-sanskrit analogy of physical sequence and logical sequence, programming.

Unit – V
*Role of Sanskrit in Engineering-III (Bio-technology and Chemical Engineering):*Classification of plants- plants, the living-plants have senses-classification of living creatures, Chemical laboratory location and layout- equipment-distillation vessel-kosthiyanthram

Suggested Reading:

1	M Krishnamachariar, *"History of Classical Sanskrit Literature"*, TTD Press, 1937.
2	M.R. Kale, *"A Higher Sanskrit Grammar: For the Use of School and College Students*", Motilal Banarsidass Publishers, 2015.
3	Kapail Kapoor, *"Language, Linguistics and Literature: The Indian Perspective"*, ISBN- 10: 8171880649, 1994.
4	"*Pride of India*", Samskrita Bharati Publisher, ISBN: 81-87276 27-4, 2007.
5	Shri Rama Verma, *"Vedas the source of ultimate science"*, Nag publishers, 2005.

AC 034	**VALUE EDUCATION**					
AUDIT - II						
Pre-requisites			**L**	**T**	**P**	**C**
			2	-		0
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Understand the need and importance of Values for self-development and for National development.
2	Imbibe good human values and Morals
3	Cultivate individual and National character.

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Gain necessary Knowledge for self-development
CO-2	Learn the importance of Human values and their application in day to day professional life.
CO-3	Appreciate the need and importance of interpersonal skills for successful career and social life
CO-4	Emphasize the role of personal and social responsibility of an individual for all-round growth.
CO-5	Develop a perspective based on spiritual outlook and respect women, other religious practices, equality, non-violence and universal brotherhood.

Unit – I
Human Values, Ethics and Morals: Concept of Values, Indian concept of humanism, human values; Values for self-development, Social values, individual attitudes; Work ethics, moral and non- moral behaviour, standards and principles based on religion, culture and tradition.

Unit – II
Value Cultivation, and Self-management: Need and Importance of cultivation of values such as Sense-of Duty, Devotion to work, Self-reliance, Confidence, Concentration, Integrity & discipline, and Truthfulness.

Unit – III
Spiritual outlook and social values: Personality and Behavior, Scientific attitude and Spiritual (soul) outlook; Cultivation of Social Values Such as Positive Thinking, Punctuality, Love & Kindness, avoiding fault finding in others, Reduction of anger, forgiveness, Dignity of labour, True friendship, Universal brotherhood and religious tolerance.

Unit – IV
Values in Holy Books: Self-management and Good health; internal & external cleanliness, Holy books versus Blind faith, Character and Competence, Equality, Nonviolence, Humility, Role of Women.

Unit – V
Dharma, Karma and Guna: Concept of soul; Science of Reincarnation, Character and Conduct, Concept of Dharma; Cause and Effect based Karma Theory; The qualities of Devine and Devilish; Satwic, Rajasic and Tamasic gunas.

Suggested Reading:

1	Chakroborty, S.K., *"Values & Ethics for organizations Theory and practice*", Oxford University Press, New Delhi, 1998.
2	Jaya DayalGoyandaka, *"Srimad Bhagavad Gita with Sanskrit Text*", Word Meaning and Prose Meaning‖, Gita Press, Gorakhpur, 2017.

AC 035	**STRESS MANAGEMENT BY YOGA**					
	AUDIT - II					
Pre-requisites			**L**	**T**	**P**	**C**
			2	-		0
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Creating awareness about different types of stress and the role of yoga in the management of stress.
2	Promotion of positive health and overall wellbeing (Physical, mental, emotional, social and spiritual).
3	Prevention of stress related health problems by yoga practice.

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	To understand yoga and its benefits.
CO-2	Enhance Physical strength and flexibility.
CO-3	Learn to relax and focus.
CO-4	Relieve physical and mental tension through Asanas
CO-5	Improve work performance and efficiency.

Unit – I
Meaning and definition of Yoga - Historical perspective of Yoga - Principles of Astanga Yoga by Patanjali.

Unit – II
Meaning and definition of Stress - Types of stress - Eustress and Distress. Anticipatory Anxiety and Intense Anxiety and depression. Meaning of Management- Stress Management.

Unit – III
Concept of Stress according to Yoga - Stress assessment methods - Role of Asana, Pranayama and Meditation in the management of stress.

Unit – IV
Asanas- (5 Asanas in each posture) - Warm up - Standing Asanas - Sitting Asanas - Prone Asanas - Supine asanas - Surya Namaskar.

Unit – V
Pranayama- Anulom and Vilom Pranayama - Nadishudhi Pranayama – Kapalabhati-Pranayama - Bhramari Pranayama - Nadanusandhana Pranayama.
Meditation techniques: Om Meditation - Cyclic meditation : Instant Relaxation technique (QRT), Quick Relaxation Technique (QRT), Deep Relaxation Technique (DRT).

Suggested Reading:

1	"Yogic Asanas for Group Training - Part-I": Janardhan Swami Yogabhyasi Mandal, Nagpur
2	"Rajayoga or Conquering the Internal Nature" by Swami Vivekananda, Advaita Ashrama (Publication Department), Kolkata
3	Nagendra H.R nad Nagaratna R, "Yoga Perspective in Stress Management", Bangalore, Swami Vivekananda Yoga Prakashan

Web resource:

1	https://onlinecourses.nptel.ac.in/noc16_ge04/preview
2	https://freevideolectures.com/course/3539/indian-philosophy/11

AC 036	**PERSONALITY DEVELOPMENT THROUGH LIFE ENLIGHTENMENT SKILLS**					
AUDIT - II						
Pre-requisites			**L**	**T**	**P**	**C**
			2	-		0
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	*To learn to achieve the highest goal happily*
2	*To become a person with stable mind, pleasing personality and determination*
3	*To awaken wisdom in students*

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	*Develop their personality and achieve their highest goal of life.*
CO-2	*Lead the nation and mankind to peace and prosperity.*
CO-3	*To practice emotional self regulation.*
CO-4	*Develop a positive approach to work and duties.*
CO-5	*Develop a versatile personality.*

Unit – I
Neetisatakam – Holistic development of personality - Verses 19, 20, 21, 22 (Wisdom) - Verses 29, 31, 32 (Pride and Heroism) - Verses 26,28,63,65 (Virtue)

Unit – II
Neetisatakam – Holistic development of personality (cont‟d) - Verses 52, 53, 59 (dont‟s) - Verses 71,73,75 & 78 (do‟s) - Approach to day to day works and duties.

Unit – III
Introduction to Bhagavad Geetha for Personality Development - Shrimad Bhagawad Geeta: Unit 2 – Verses 41, 47, 48 - Unit 3 – Verses 13,21,27,35 - Unit 6 – Verses 5,13,17,23,35 - Unit 18 – Verses 45, 46, 48 Unit – 6: Verses 5, 13, 17, 23, 35; Unit – 18: Verses 45, 46, 48.

Unit – IV
Statements of basic knowledge - Shrimad Bhagawad Geeta: Unit 2- Verses 56, 62,68 - Unit 12 – Verses 13, 14, 15, 16, 17, 18 - Personality of Role model from Shrimad Bhagawat Geeta.

Unit – V
Role of Bahgavadgeeta in the present scenario - Unit 2 – Verses 17 – Unit 3 – Verses 36, 37, 42 - Unit 4 – Verses 18, 38, 39 - Unit 18 – Verses 37, 38, 63.

Suggested Reading:

1	"Srimad Bhagavad Gita" by Swami SwarupanandaAdvaita Ashram (Publication Department), Kolkata.
2	Bhartrihari"s Three Satakam (Niti-sringar-vairagya) by P.Gopinath, Rashtriya Sanskrit, Sansthanam, New Delhi.

Web resource:

1	NTPEL:http://nptel.ac.in/downloads/109104115

AC 037	**CONSTITUTION OF INDIA**					
	AUDIT - II					
Pre-requisites			**L**	**T**	**P**	**C**
			2	-		0
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	*The history of Indian Constitution and its role in the Indian democracy.*
2	*Address the growth of Indian opinion regarding modern Indian intellectuals' constitutional role and entitlement to civil and economic rights as well as the emergence of nationhood in the early years of Indian nationalism.*
3	*Have knowledge of the various Organs of Governance and Local Administration.*

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	*Understand the making of the Indian Constitution and its features.*
CO-2	*Understand the Rights of equality, the Right of freedom and the Right to constitutional remedies.*
CO-3	*Have an insight into various Organs of Governance - composition and functions*
CO-4	*Understand powers and functions of Municipalities, Panchayats and Co-operative Societies.*
CO-5	*Understand Electoral Process, special provisions.*

Unit – I
History of making of the Indian constitutions: History, Drafting Committee (Composition & Working). **Philosophy of the Indian Constitution**: Preamble, Salient Features.

Unit – II
Contours of Constitutional Rights and Duties Fundamental Rights, Right to Equality, Right to Freedom, Right against Exploitation, Right to Freedom of Religion, Cultural and Educational Rights, Right to Constitutional Remedies, Directive Principles of State Policy, Fundamental Duties

Unit – III
Organs of Governance": Parliament: Composition, Qualifications, Powers and Functions, Union executives : President, Governor, Council of Ministers, Judiciary, appointment and transfer of judges, qualifications, powers and functions.

Unit – IV
Local Administration - District‟s Administration head: Role and importance. Municipalities: Introduction, ayor and role of Elected Representative, CEO of Municipal Corporation. Panchayati Raj: Introduction, PRI: Zilla Panchayat, Elected Officials and their roles, CEO Zilla Panchayat: positions and role. Block level: Organizational Hierarchy (Different departments) Village level: role of elected and appointed officials. Importance of grass root democracy.

Unit – V
Election commission: Election Commission: Role and functioning, Chief Election Commissioner and Election Commissioners, State Election Commission :Role and functioning. Institute and Bodies for the welfare of SC/ST/OBC and women**.**

Suggested Reading:

1	The Constitution of India”, 1950 (Bare Act), Government Publication
2	Dr. S. N. Busi, Dr. B. R. Ambedkar, “Framing of Indian Constitution”, 1st Edition, 2015.
3	M. P. Jain, “Indian Constitution Law”, 7th Edn., Lexis Nexis, 2014
4	D.D. Basu, “Introduction to the Constitution of India”, Lexis Nexis, 2015.

Web resource:

1	http://www.nptel.ac.in/courses/103107084/Script.pdf

AC 038	**PEDAGOGY STUDIES**					
	AUDIT - II					
Pre-requisites			**L**	**T**	**P**	**C**
			2	-		0
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	*To present the basic concepts of design and policies of pedagogy studies.*
2	*To provide understanding of the abilities and dispositions with regard to teaching techniques, curriculum design and assessment practices and familiarize various theories of learning and their connection to teaching practice.*
3	*To create awareness about the practices followed by DFID, other agencies and other researchers and provide understanding of critical evidence gaps that guides the professional development*

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	*Illustrate the pedagogical practices followed by teachers in developing countries both in formal and informal classrooms.*
CO-2	*Examine the effectiveness of pedagogical practices.*
CO-3	*Understand the concept, characteristics and types of educational research and perspectives of research.*
CO-4	*Describe the role of classroom practices, curriculum and barriers to learning.*
CO-5	*Understand Research gaps and learn the future directions.*

Unit – I
Introduction and Methodology: Aims and rationale, Policy background, Conceptual framework and terminology - Theories of learning, Curriculum, Teacher education - Conceptual framework, Research questions, Overview of methodology and Searching.

Unit – II
Thematic Overview: Pedagogical practices followed by teachers in formal and informal classrooms in developing countries - Curriculum, Teacher education.

Unit – III
*Evidence on the Effectiveness of Pedagogical Practices***:** Methodology for the in depth stage: quality assessment of included studies - How can teacher education (curriculum and Practicum) and the school curriculum and guidance material best support effective pedagogy?

- Theory of change - Strength and nature of the body of evidence for effective pedagogical practices - Pedagogic theory and pedagogical approaches – Teachers attitudes and beliefs and pedagogic strategies.

Unit – IV
Professional Development: alignment with classroom practices and follow up support - Support from the head teacher and the community – Curriculum and assessment - Barriers to learning: Limited resources and large class sizes.

Unit – V
Research Gaps and Future Directions: Research design – Contexts – Pedagogy - Teacher education - Curriculum and assessment – Dissemination and research impact.

Suggested Reading:

1	Ackers J, Hardman F, *"Classroom Interaction in Kenyan Primary Schools, Compare*", 31 (2): 245 – 261, 2001.
2	Agarwal M, *"Curricular Reform in Schools: The importance of evaluation*", Journal of Curriculum Studies, 36 (3): 361 – 379, 2004.
3	Akyeampong K, "*Teacher Training in Ghana – does it count? Multisite teacher education research project (MUSTER)",* Country Report 1. London: DFID, 2003.
4	Akyeampong K, Lussier K, Pryor J, Westbrook J, *"Improving teaching and learning of Basic Maths and Reading in Africa: Does teacher Preparation count?"*International Journal Educational Development, 33 (3): 272- 282, 2013.
5	Alexander R J, *"Culture and Pedagogy: International Comparisons in Primary Education",* Oxford and Boston: Blackwell, 2001.
6	Chavan M, Read India: *"A mass scale, rapid, learning to read campaign",* 2003

AC 039	**E-WASTE MANAGEMENT**					
	AUDIT - II					
Pre-requisites			**L**	**T**	**P**	**C**
			2	-		0
Evaluation	**SEE**	60 Marks	**CIE**		40 Marks	

Course Objectives :	
The course is taught with the objectives of enabling the student to:	
1	Introduction to E-Waste management
2	Understanding on resource efficiency and circular economy
3	E-waste Management rules 2016
4	RoHS compliances/directives to EEE

Course Outcomes :	
On completion of this course, the student will be able to :	
CO-1	Complete understanding on E-Waste management
CO-2	Understanding on effective recycling methodologies for e-waste management
CO-3	Overall understanding about E-waste Management rules 2016 and strategies for e-waste management
CO-4	Understanding on RoHS compliances for EEE products

UNIT – I

Waste Electrical and Electronic Equipment (WEEE): Flows, Quantities and Management, a Global Scenario; The Importance of Waste Management; Types of Waste- Solid and Liquid; Criteria for EEE/E-Waste Classification; Multivariate Model for E-Waste Estimation; Environmental and Health Effects of Waste Management, Inventorisation of E-Waste and Emerging trends in E-waste disposal with bench marks for depollution - global scenario; Dumping, Burning and Landfill: Impact on the Environment

UNIT – II

Effective Waste Management and Disposal Strategies; Legislative Influence on Electronics Recycling; Waste Management Rules and Their Amendments; Extended Producer Responsibility (EPR) in E-Waste Management; The Role of Collective versus Individual Producer Responsibility in E-Waste Management

UNIT – III

Electronic Waste: Public Health Implications; Restriction of Hazardous Substances (RoHS) Directives in Electrical and Electronic Equipment; Materials Used in Manufacturing Electrical and Electronic Products

UNIT – IV
Recycling and Resource Management: Ecological and Economical Valuation; Life Cycle Assessment (LCA) Approach to Waste Management System; Environmental Incentives for Recycling and Life Cycle Analysis of Materials Recycling Electronic Waste: Challenges and Opportunities for Sustainable Management; Resource Recovery from E-waste: Efficiency and Circular Economy; Integrated Approach to E-Waste Recycling: Recycling and Recovery Technologies, Recycling and Recovery Technologies.

UNIT – V
Cases studies: E-waste Generation, collection and recycling

Suggested Reading:

1	Electronic Waste Management and Treatment Technology, Editors: MajetiNarasimhaVara Prasad MeththikaVithanage
2	Electronic Waste Management, Edited by R. E. Hester, R. M. Harrison, RSC Publishing 2009
3	Solid Waste Technology & Management, Christensen, T., Ed., Wiley and Sons., 2011
4	Electronics Waste Management: An India Perspective. Front Cover. Sandip Chatterjee. Lap Lambert Academic Publishing GmbH KG, 2010 - Electronic
5	Handbook of Electronic Waste Management, International Best Practices and Case studies, Elsevier, 2019
6	E-waste: Implications, regulations, and management in India and current global best practices. Author(s): RakeshJohri, TERI Press

CS 581	**DISSERTATION PHASE-I**					
Pre-requisites	-		**L**	**T**	**P**	**C**
			-	-	20	10
Evaluation	**SEE**	-	**CIE**	100 Marks		

Course Outcomes :	
At the end of the course, the student will be able to:	
CO-1	Synthesize knowledge and skills previously gained and apply them to new technical problem.
CO-2	Select from different methodologies, methods and analyses to produce a suitable research design, and justify their design.
CO-3	Present the findings of their technical solution in a written report.
CO-4	Presenting the work in International/ National conference or reputed journals.
CO-5	Develop oral and written communication skills to present and defend their work in front of technically qualified audience.

Guidelines:

The student shall identify the domain and define dissertation objectives. The referred literature should preferably include IEEE/IET/IETE/Springer/Science Direct/ACM journals in the areas of Computer Science, cyber security, parallel Algorithms and Artifical Intelligence and Machine Learning, Computing and Processing (Hardware and Software), NLP and Image Processing and Analysis and any other related domain. In case of industry sponsored projects, the relevant application notes, product catalogues should be referred and reported. The student is expected to detail out specifications, methodology, resources required, critical issues involved in design and implementation and phase wise work distribution, and submit the proposal within a month from the date of registration.

Evaluation for stage-I is based on mid semester presentation and end semester presentation. Mid semester presentation will include identification of the problem based on the literature review on the topic referring to latest literature available. End semester presentation should be done along with the report on identification of topic for the work and the methodology adopted involving scientific research, collection and analysis of data, determining solutions and must bring out individuals contribution. Continuous assessment of Project stage – I at Mid Semester and End Semester will be monitored by the departmental committee.

A document report comprising of summary of literature survey, detailed objectives, project specifications, paper and/or computer aided design, proof of concept/functionality, part results, record of continuous progress. In case of unsatisfactory performance, committee may recommend repeating the Phase-I work.

SEMESTER - IV

CS 582	**DISSERTATION PHASE-II**					
Pre-requisites	-		**L**	**T**	**P**	**C**
			-	-	32	16
Evaluation	**SEE**	100	**CIE**	100 Marks		

Course Outcomes :	
At the end of the course, the student will be able to:	
CO-1	Use different experimental techniques.
CO-2	Use different software/ computational/analytical tools.
CO-3	Design and develop an experimental set up/ equipment/test
CO-4	Conduct tests on existing set ups/equipments and draw logical conclusions from the results after analyzing them.
CO-5	Either work in a research environment or in an industrial environment.
CO-6	Present and convince their topic of study to the engineering community.

Guidelines:

Project stage – II will be extension of the work on the topic identified in Project stage – I. Student is expected to exert on design, development and testing of the proposed work as per the schedule.

Accomplished results/contributions/innovations should be published in terms of research papers in reputed journals and reviewed focused conferences OR IP/Patents.

The candidate has to prepare a detailed project report consisting of introduction of the problem, problem statement, literature review, objectives of the work, methodology (experimental set up or numerical details as the case may be) of solution and results and discussion.

The report must bring out the conclusions of the work and future scope for the study. A dissertation should be presented in standard format as provided by the department.

The candidate has to be in regular contact with his guide. Continuous assessment should be done of the work done by adopting the methodology decided involving numerical analysis/ conduct experiments, collection and analysis of data, etc. There will be pre-submission seminar at the end of academic term.

After the approval the student has to submit the detail report and external examiner is called for the viva-voce to assess along with guide.

****