NOORUL ISLAM CENTRE FOR HIGHER EDUCATION

(Deemed to be University Under Section 3 of the UGC Act, 1956)
Kumaracoil, Thuckalay

DEPARTMENT OF INFORMATION TECHNOLOGY

M.E. CYBER SECURITY

CURRICULUM AND SYLLABI

REGULATION 2023

NOORUL ISLAM CENTRE FOR HIGHER EDUCATION, Kumaracoil

Regulation: 2023

Curriculum and Syllabi

M.E Degree Programme

DEPARTMENT OF INFORMATION TECHNOLOGY

M.E. CYBER SECURITY

Vision of the University

To be recognized by the Government and society at large as an institution able to deliver excellence with relevance in the field of higher education and research focusing on the needs of the nation in tune with the technological revolution to cope with the knowledge explosion and global competence.

Mission of the University

To develop the institution as a Centre of Excellence, keeping pace with the advances in the field, so as to provide quality higher education to the students and instill in them high standards of discipline and ethics so that they become enlightened individuals in the service of humanity and to carry out focused research in the frontier areas of science and technology.

Faculty of Information and Computer Engineering

Department of Information Technology

Vision of the Department

Outstand in the field of cyber security education and research by providing a more conducive environment for quality oriented learning and research, with an aim of betterment of society.

Mission of the Department

1. Provide a solid foundation in key technology areas related to security.
2. Enable students to be technically competent, socially responsible and ethically realizable professionals.
3. Extend students their technical and programming skills to handle enterprise security challenges.
4. Make students perceive the latest trends and issues in the field of cyber security.
5. Mold the students into information security professionals through continuous team work by a group of committed faculty.
6. Provide a pathway to research in the field of cyber security.

Description of the programme

Studying cyber security equips you with various skills, including threat detection and analysis, network security, cryptography, ethical hacking, and risk management. These skills are valuable not only in the cyber security field but also in IT and related industries.

Programme Educational Objectives - PEO	
PEO-01	Provide a strong basic knowledge in key technology areas of security with a focus on both theoretical aspects and practical approaches of computation to implement and manage advanced safety protocols and risk mitigation strategies to protect individuals, communities, and ecosystems in high stake engineering areas.
PEO-02	Enable students to understand various tools and techniques to overcome the security challenges, master advanced engineering principles and apply them to design, analyze, and innovate systems that can address the present and emerging global challenges across diverse industries.
PEO-03	Develop skills and expertise to identify, analyze, and remediate computer and network security breaches by identifying opportunities for technological advancements and also by contributing original ideas that push the boundaries of engineering knowledge.
PEO-04	Enable students to learn investigation tools and techniques, technical aspects and legal aspects related to cyber crime and forensics by adapting ethical decisions in complex engineering contexts and apply interdisciplinary approaches with legal experts to solve problems of society.
PEO-05	Learn to stay updated on rapidly changing technology and prepare students with the technical, conceptual, and practical skills needed for a professional career in cyber security by adopting global engineering standards and practices, addressing international challenges and cultural sensitivities in engineering projects to make a broader societal impact.
PEO-06	Enable students to solve security issues by integrating data, techniques, perspectives, and concepts from interdisciplinary sciences like biometrics, image processing etc. with Interdisciplinary Collaboration, leveraging knowledge from multiple fields to solve complex, large-scale engineering problems that necessitate adoption of comprehensive and innovative solutions.
PEO-07	Make students practice ethical, legal and social implications throughout their profession by making informed ethical decisions taking into account the societal needs, environmental implications, and the long-term consequences of engineering practices.

PEO-08	Prepare students to analyze and identify the limitations of the existing literature and propose innovative and research oriented solutions by staying ahead of technological trends and exhibit agility in learning new tools and techniques to ensure continuous professional growth. The students will also learn about data-driven decision making tools by adopting machine learning, deep learning methodologies, analytics to make better engineering solutions.
PEO-09	Develop postgraduates to identify, analyze, and solve problems as an individual and as a team and cultivate an entrepreneurial mindset by translating engineering innovations to viable products, services leading towards commercialization by ensuring right societal impact.

Graduate Attributes-GA	
GA-1	**Advanced Engineering Expertise** Master advanced engineering principles and apply them to design, analyze, and innovate systems that address both present and emerging global challenges across diverse industries.
GA-2	**Leadership in Research and Innovation** Lead groundbreaking research and foster innovation by identifying opportunities for technological advancements, contributing original ideas that push the boundaries of engineering knowledge.
GA-3	**Sustainable Engineering Practices** Develop and implement engineering solutions that integrate sustainability, environmental stewardship, and resource efficiency, ensuring the long-term impact and responsibility of all projects.
GA-4	**Ethical and Strategic Decision-Making** Make informed, ethical decisions in complex engineering contexts, considering societal needs, environmental implications, and the long-term consequences of engineering practices.
GA-5	**Global Competence in Engineering Solutions** Exhibit a deep understanding of global engineering standards and practices, addressing international challenges and cultural sensitivities in engineering projects to make a broader societal impact.
GA-6	**Technological Agility and Lifelong Learning** Stay ahead of technological trends and exhibit agility in learning new tools, methodologies, and technologies, ensuring continuous professional growth in a rapidly evolving engineering landscape.
GA-7	**Interdisciplinary and Collaborative Innovation** Excel in multidisciplinary collaborations, leveraging knowledge from multiple fields to solve complex, large-scale engineering problems that require comprehensive and innovative solutions.

GA-8	**Data-Driven Decision Making** Employ advanced data analytics, machine learning, and computational tools to derive insights and make informed engineering decisions that improve performance, efficiency, and sustainability.
GA-9	**Entrepreneurial Mindset and Innovation Leadership** Cultivate an entrepreneurial mindset, translating engineering innovations into viable products, solutions, or services, and leading teams toward commercialization and societal impact.
GA-10	**Safety, Risk, and Crisis Management** Implement and manage advanced safety protocols and risk mitigation strategies to protect individuals, communities, and ecosystems in engineering practices, particularly in high-stakes and crisis environments.

Programme Outcome – POs

Programme Outcome– PO	
PO-A	Students gain knowledge about the basic concepts of cyber security needs of an organization and effectively apply this basic knowledge of security needs and principles to solve technical problems.
PO-B	Enable students to acquire knowledge about threats, how they materialize, typical attacks and how those attacks exploit vulnerabilities which mainly affect the organizational processes and decision-making.
PO-C	Make students to create, select and apply appropriate tools, techniques, resources and skills to complex engineering activities and to solve the various cyber security challenges in the society in a global and social context.
P0-D	Help students to understand the different investigation and forensics tools, techniques and to apply the ethical principles related with cyber crime.
PO-E	Enable students to function effectively as an individual or as member in teams and have the ability to engage in continuous learning in the broadest context of technological change.
PO-F	Enable students to utilize research-based knowledge and formulate research problems in the cyber security field.
PO-G	Drive students through technology innovation by means of scientific and social advancements.
PO-H	Make students to apply the foundational knowledge of cyber crimes, threats, vulnerabilities, biometric concepts to network systems of varying complexity.

Mapping of Graduate Attributes and Programme Educational Objectives(PEO)

GAs / PEOs	G A-01	GA-02	GA-03	GA-04	GA-05	GA-06	GA-07	GA-08	GA-09	GA-10
PEO-01	H	A	H	A	H	A	H	H	A	H
PEO-02	H	A	H	A	H	A	H	H	A	H
PEO-03	H	A	A	A	A	H	H	H	A	H
PE0-04	A	A	A	H	A	H	H	A	A	A
PEO-05	A	H	A	A	H	H	A	A	A	H
PEO-06	A	A	A	A	A	A	H	A	A	H
PEO-07	A	A	A	H	H	A	H	H	H	A
PEO-08	H	H	A	A	A	A	H	A	H	A
PEO-09	A	H	A	H	A	A	H	A	H	A

H- Highly Associated A- Associated Not – Not Associated

Mapping of Graduate Attributes and Programme Outcomes (PO)

GAs / POs	G A-01	GA-02	GA-03	GA-04	GA-05	GA-06	GA-07	GA-08	GA-09	GA-10
PO-A	A	A	A	A	A	A	A	A	A	A
PO-B	A	A	A	H	A	H	H	A	A	A
PO-C	A	A	A	H	H	H	A	H	H	A
P0-D	A	A	A	H	A	H	A	H	A	A
PO-E	A	A	A	A	A	A	A	A	A	A
PO-F	A	H	A	A	A	A	H	A	A	A
PO-G	H	A	A	A	A	A	H	A	H	A
PO-H	A	A	A	A	A	A	A	A	A	A

H- Highly Associated A- Associated Not – Not Associated

Mapping of Programme Educational Objective (PEOs) and Programme Outcomes (POs)

PEO / PO	PEO-01	PEO-02	PEO-03	PEO-04	PEO-05	PEO-06	PEO-07	PEO-08	PEO-09
PO-A	A	A	A	A	A	A	A	A	A
PO-B	A	A	A	A	A	A	A	A	A
PO-C	A	H	A	H	A	A	A	A	A
P0-D	A	A	A	H	A	A	A	A	A
PO-E	A	A	A	A	A	A	A	A	A

PO-F	A	A	A	A	A	A	A	A	A
PO-G	A	H	A	A	A	A	A	H	A
PO-H	A	A	A	A	A	A	A	A	A

H- Highly Associated A- Associated Not – Not Associated

Duration of the programme: 2 Years/ 4 Semesters
Total credits : 67

CURRICULUM & SYLLABI

SEMESTER I

Sl. No	Course Code	Course Title	L	T	P	C
THEORY						
1.	MA4505	Applied Probability and Statistics	3	1	0	4
2.	CY4501	Advanced Data Structures and Algorithms	3	0	0	3
3.	CY4502	Advanced Operating System and Security	3	0	0	3
4.	CY4503	Cryptography and Cyber Security	3	0	0	3
5.	OE35D1	Research Methodology and IPR	2	0	0	2
6.	PEC	Elective I	3	0	0	3
PRACTICAL						
7.	CY4571	Advanced Operating System and Data Structures Laboratory	0	0	2	1
TOTAL			**17**	**1**	**2**	**19**

SEMESTER II

Sl. No	Course Code	Course Title	L	T	P	C
THEORY						
1.	CY4504	Cyber Crime Investigations and Digital Forensics	3	0	0	3
2.	CY4505	Database Design and Security	3	0	0	3
3.	CY4506	Cyber Law and Security Policies	3	0	0	3
4.	CY4507	Advanced Network Security	3	0	0	3

5.	PEC	Elective II	3	0	0	3
6.	PEC	Elective III	3	0	0	3
PRACTICAL						
7.	CY4572	Database and Cyber Security Laboratory	0	0	2	1
TOTAL			**18**	**0**	**2**	**19**

SEMESTER III

Sl. No	**Course Code**	**Course Title**	**L**	**T**	**P**	**C**
THEORY						
1.	PEC	Elective IV	3	0	0	3
2.	OEC	Open Elective II	3	0	0	3
PRACTICAL						
3.	CY4573	Cyber Crime Investigations Laboratory	0	0	2	1
4.	CY45P1	Project work – Phase I	0	0	12	6
TOTAL			**6**	**0**	**14**	**13**

SEMESTER IV

Sl. No	**Course Code**	**Course Title**	**L**	**T**	**P**	**C**
1.	CY45P2	Project work – Phase II	0	0	32	16
TOTAL			**0**	**0**	**32**	**16**

PROFESSIONAL ELECTIVE COURSES

SI. NO	COURSE CODE	COURSE TITLE	L	T	P	C
1.	CY45A1	Ethical Hacking	3	0	0	3
2.	CY45A2	Biometric Security	3	0	0	3
3.	CY45A3	Forensics and Incident Response	3	0	0	3
4.	CY45A4	IOT Security	3	0	0	3
5.	CY45A5	Cyber Forensics	3	0	0	3
6.	CY45A6	Malware Forensics	3	0	0	3
7.	CY45A7	OS Forensics	3	0	0	3
8.	CY45A8	Virtual Forensics	3	0	0	3
9.	CY45A9	Security Policies and Governance	3	0	0	3
10.	CY45B1	Intrusion Detection and Prevention System	3	0	0	3
11.	CY45B2	Cyber Warfare	3	0	0	3

OPEN ELECTIVES

SI.No.	SUBJECT CODE	SUBJECT NAME	L	T	P	C
1.	OE35D1	Research Methodology and IPR	2	0	0	2
2.	OE35D2	Business Analytics	3	0	0	3
3.	OE35D3	Industrial Safety	3	0	0	3
4.	OE35D4	Operations Research	3	0	0	3
5.	OE35D5	Composite Materials	3	0	0	3
6.	OE35D6	Waste to Energy	3	0	0	3

Syllabus Format

SEMESTER I

Sl. No	Course Code	Course Title	L	T	P	C
THEORY						
1.	MA4505	Applied Probability and Statistics	3	1	0	4
2.	CY4501	Advanced Data Structures and Algorithms	3	0	0	3
3.	CY4502	Advanced Operating System and Security	3	0	0	3
4.	CY4503	Cryptography and Cyber Security	3	0	0	3
5.	OE35D1	Research Methodology and IPR	2	0	0	2
6.	PEC	Elective I	3	0	0	3
PRACTICAL						
7.	CY4571	Advanced Operating System and Data Structures Laboratory	0	0	2	1
TOTAL			**17**	**1**	**2**	**19**

MA4505	APPLIED PROBABILITY AND STATISTICS	L	T	P	C
		4	**1**	**0**	**4**

OBJECTIVE

To encourage students to develop knowledge in the concepts of probability and random variables. To apply the small and large sample tests and solve problems through testing of hypothesis. To enable the students to understand the properties of standard distributions and solve simulation problems.

Course Outcome		Cognitive Skill
CO-01	Use the ideas of probability and random variables in solving engineering problems. To apply Baye's theorem and to find the moments and moment generating functions	R, U, A, E, An
CO-02	Gather knowledge of the standard distributions such as binomial, poisson and normal distribution. To understand the functions of random variable and apply central limit theorem	R, U, A, E, An
CO-03	Be familiar with some of the commonly encountered two dimensional random variables and to obtain Marginal and conditional distributions. Also to find the regression curve and correlation between variables	R, U, A, E, An
CO-04	Use statistical tests in testing hypotheses on data. To know the type I and type II errors and to analyse small and large samples using tests based on normal, t, Chi square and F distributions for testing of mean , variance and proportions	R, U, A, E, An
CO-05	Understand the types of simulation such as discrete event simulation and stochastic simulation. Apply Monte Carlo simulation techniques and generation random numbers using congruent method .	R, U, A, E, An

R-Remember,U-Understand,A-Apply,An-Analyze,E-Evaluate, S-Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	S	M	M	M	L	S	S	S
CO-02	M	S	M	S	S	L	M	M
CO-03	M	S	S	M	L	L	L	M
CO-04	S	S	M	M	L	L	L	L
CO-05	M	S	S	S	L	L	L	L

S-Strong, M-Medium,L-Low,N-Not relevant

Unit I: Probability and Random Variables **9**

Probability – Axioms of probability – Conditional probability – Baye's theorem – Random variables – Probability function – Moments – Moment generating functions and their properties

Unit II: Standard Distributions **9**

Binomial, Poisson, Geometric, Uniform, Exponential, Gamma and Normal distributions – Function of a random variable- Central Limit Theorem

Unit III: Two Dimensional Random Variables **9**

Joint distributions – Marginal and conditional distributions – Functions of two dimensional random variables – Regression curve – Correlation.

Unit IV: Testing of Hypothesis **9**

Sampling distributions – Type I and Type II errors – Small and Large samples – Tests based on Normal, t, Chi square and F distributions for testing of mean , variance and proportions – Tests for independence of attributes and goodness of fit.

Unit IV: Simulation **9**

Discrete Event Simulation – Stochastic Simulation - Monte Carlo Simulation – Generation of Random Numbers using Congruent method – Applications to inventory and queueing models.

L: 45 + T: 15, TOTAL: 60 HOURS

REFERENCES

1. Ross, "A first course in Probability", Sixth Edition, Pearson Education, Delhi, 2011.
2. Richard A. Johnson and Dean W. Wichern, "Applied multivariate statistical Analysis", Pearson Education, Fifth Edition, 6th Edition, New Delhi, 2013.
3. Taha, H.A., "Operations Research – An Introduction", Seventh Edition, Pearson Education, Delhi, 2002.
4. Oliver C. Ibe, "Fundamentals of Applied probability and Random Processes", Academic Press, Boston, 2014.
5. Johnson R. A. and Gupta C.B., "Miller and Freund's Probability and Statistics for Engineers", Pearson India Education, Asia, 9th Edition, New Delhi, 2017.

CY4501	ADVANCED DATA STRUCTURES AND ALGORITHMS	L	T	P	C
		3	0	0	3

OBJECTIVES

- To understand the usage of algorithms in computing.
- To learn and use hierarchical data structures and its operations
- To learn the usage of graphs and its applications.
- To select and design data structures and algorithms that is appropriate for problems.

Course Outcome – Cos		Cognitive Skill
CO-01	Student will be able to design and analyse programming problem statements.	An
CO-02	Student will be able to choose and implement efficient data structures and apply them to solve problems.	A
CO-03	Student will be able to learn various tree structures.	U
CO-04	Student will be able to design one's own algorithm for an unknown problem.	A
CO-05	Student will be able to summarize searching and sorting techniques and apply suitable design strategy for problem solving.	A

R- Remember, U-Understand, A-Apply, An-Analyse, E-Evaluate, S- Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	S	S	S	M	S	S	S	L
CO-02	S	S	S	M	S	S	S	L
CO-03	S	S	S	M	S	S	S	L
CO-04	S	S	S	M	S	S	S	L
CO-05	S	S	S	M	S	S	S	L

S-Strong, M-Medium,L-Low,N-Not relevant

Unit I: Role of Algorithms in Computing **9**

Algorithms – Algorithms as a Technology-Analysing Algorithm – Designing algorithms-Growth of Functions: Asymptotic Notation – Standard Notations and Common functions-Recurrences: The Substitution Method – The Recursion-Tree Method.

Unit II : Basic Data Structures **8**

ADT - List (Singly, Doubly and Circular) Implementation - Array, Pointer, Cursor Implementation- Stacks and Queues – ADT, Implementation and Applications- Trees – General, Binary tree.

Unit III: Hierarchical Data Structures **9**

Binary Search Trees: Basics – Querying a Binary search tree – Insertion and Deletion- Red Black trees: Properties of Red-Black Trees – Rotations – Insertion – Deletion -B-Trees:

Definition of B -trees – Basic operations on B-Trees – Deleting a key from a B-Tree- Heap – Heap Implementation – Disjoint Sets - Disjoint-set operations- Fibonacci Heaps: structure – Mergeable-heap operations-Decreasing a key and deleting a node-Bounding the maximum degree.

Unit IV: Graphs **10**

Elementary Graph Algorithms: Representations of Graphs – Breadth-First Search – Depth-First Search – Topological Sort – Strongly Connected Components- Minimum Spanning Trees– Kruskal and Prim- Single-Source Shortest Paths: The Bellman-Ford algorithm – Single-Source Shortest paths in Directed Acyclic Graphs – Dijkstra's Algorithm; All-Pairs Shortest Paths: Shortest Paths and Matrix Multiplication – The Floyd Warshall Algorithm.

Unit V : Searching, Sorting and Design Techniques **9**

Searching Techniques, Sorting – Internal Sorting – Bubble Sort, Insertion Sort, Quick Sort, Heap Sort, Bin Sort, Radix Sort – External Sorting – Merge Sort, Dynamic Programming: Matrix-Chain Multiplication – Elements of Dynamic Programming – Longest Common Subsequence- Greedy Algorithms: – Elements of the Greedy Strategy- An Activity-Selection Problem - Huffman Coding.

TOTAL: 45 HOURS

REFERENCES

1. Mark Allen Weiss, "Data Structures and Algorithm Analysis in C++", 4th Edition, Pearson Education, 2014.
2. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein, Introduction to Algorithms‖, Third Edition, Prentice-Hall, 2011.
3. Alfred V. Aho, John E. Hopcroft, Jeffrey D. Ullman, ―Data Structures and Algorithms, Pearson Education, Reprint 2006.
4. Robert Sedgewick and Kevin Wayne, ―ALGORITHMS‖, Fourth Edition, Pearson Education, 2011.
5. S.Sridhar,Design and Analysis of Algorithms‖, First Edition, Oxford University Press. 2014.
6. E. Horowitz, S. Sahni and S. Rajasekaran, "Fundamentals of Computer Algorithms", University Press, 2nd Edition, 2008.

CY4502	ADVANCED OPERATING SYSTEM AND SECURITY	L	T	P	C
		3	0	0	3

OBJECTIVES

- To get an overview of operating system and concept of virtual machines.
- To learn about distributed operating system.
- To learn embedded and cloud operating systems.
- To study about IOT, mobile operating systems, and security in operating system design.
- To learn about operating system security and case studies.

Course Outcome		Cognitive Skill
CO-01	Student will be able to get an overview of operating system and deep insight into the concept of virtual machines.	U
CO-02	Student will be able to understand and analyze the concepts and techniques of distributed operating system.	U, An
CO-03	Student will gain in-depth knowledge on embedded and cloud operating systems.	U, An
CO-04	Student will gain insight into IOT and mobile operating systems, and security in operating system design.	U, An
CO-05	Student will be able to gain knowledge on operating system security and case studies related to Windows and Linux operating system.	U, A

R-Remember,U-Understand,A-Apply,An-Analyze,E-Evaluate, S-Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	S	L	S	L	M	S	M	L
CO-02	M	M	S	L	M	S	S	L
CO-03	M	M	S	L	M	S	S	L
CO-04	L	M	S	L	M	S	S	L
CO-05	S	M	S	M	M	S	S	M

S-Strong, M-Medium,L-Low,N-Not relevant

Unit I: Operating System Overview and Virtual Machines 9

Overview -Operating System Objectives and Functions - The Evolution of Operating Systems - Major Achievements - Developments Leading to Modern Operating Systems -Fault Tolerance - OS Design Considerations for Multiprocessor and Multicore - Virtual Machines - Overview - History - Benefits and Features - Building Blocks - Types of VMs and Their Implementations - Virtualization and Operating System Components - Examples

Unit II: Distributed Operating System **9**

Distributed Systems -Advantages of Distributed Systems - Network Structure - Communication Structure - Network and Distributed Operating Systems - Design Issues in Distributed Systems - Distributed File Systems - DFS Naming and Transparency - Remote File Access - Distributed Process Management -Process Migration - Distributed Global States - Distributed Mutual Exclusion - Distributed Deadlock

Unit III: Embedded and Cloud Operating Systems **9**

Embedded Systems - Characteristics of Embedded Operating Systems - Embedded Linux - Tinyos - Cloud Computing- Cloud Operating Systems

Unit IV: IOT, Mobile Operating Systems, Security in OS Design **9**

The Internet of Things- IoT Operating Systems- Mobile OS- Android - Design Goals- Android Architecture- Android Applications- Security - Security in Operating Systems- Security in the Design of Operating Systems- RootKit- Cryptography as a Security Tool -User Authentication - Implementing Security Defenses

Unit V: Operating System Security and Case Studies **9**

Intruders and Malicious Software- Buffer Overflow- Access Control- Unix Access Control- Operating Systems Hardening- Security Maintenance- Windows Security- Linux/Unix Security- Virtualization Security

TOTAL: 45 HOURS

REFERENCES

1. William Stallings, "Operating Systems: Internals and Design Principles", Pearson India, 9th Edition, 2017
2. Abraham Silberschatz, Peter Baer Galvin and Greg Gagne, "Operating System Concepts", John Wiley and Sons Inc., 10th Edition, 2018.
3. Lawrie Brown , William Stallings, "Computer Security: Principles and Practice", Pearson Education, Fourth Edition, 2017
4. Michael Palmer, Guide to Operating Systems Security", Course Technology – Cengage Learning, New Delhi, 2008
5. Charles P. Pleeger, "Security in Computing", Prentice Hall, New Delhi, Fifth Edition, 2018

CY4503	CRYPTOGRAPHY AND CYBER SECURITY	L	T	P	C
		3	0	0	3

OBJECTIVES

- Learn to analyse the security of in-built cryptosystems.
- Know the fundamental mathematical concepts related to security
- Develop cryptographic algorithms for information security.
- Comprehend the various types of data integrity and authentication schemes
- Understand cyber-crimes and cyber security.

Course Outcome		Cognitive Skill
CO-01	Understand the fundamentals of networks security, security architecture, threats and vulnerabilities	U
CO-02	Apply the different cryptographic operations of symmetric cryptographic algorithms	A
CO-03	Apply the different cryptographic operations of public key cryptography	A
CO-04	Apply the various Authentication schemes to simulate different applications.	A
CO-05	Understand various cyber-crimes and cyber security.	U

R-Remember,U-Understand,A-Apply,An-Analyze,E-Evaluate, S-Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	S	S	S	S	M	S	M	S
CO-02	S	S	S	S	M	S	M	S
CO-03	S	S	S	S	M	S	M	S
CO-04	S	S	S	S	S	S	M	S
CO-05	S	S	S	S	S	S	M	M

S-Strong, M-Medium,L-Low,N-Not relevant

Unit I: Introduction to Security **9**

Computer Security Concepts – The OSI Security Architecture – Security Attacks – Security Services and Mechanisms – A Model for Network Security – Classical encryption techniques: Substitution techniques, Transposition techniques, Steganography – Foundations of modern cryptography: Perfect security – Information Theory – Product Cryptosystem – Cryptanalysis.

Unit II: Symmetric Ciphers **9**

Number theory – Algebraic Structures – Modular Arithmetic - Euclid's algorithm – Congruence and matrices – Group, Rings, Fields, Finite Fields SYMMETRIC KEY CIPHERS: SDES – Block Ciphers – DES, Strength of DES – Differential and linear cryptanalysis – Block cipher design principles – Block cipher mode of operation – Evaluation criteria for AES – Pseudorandom Number Generators – RC4 – Key distribution.

Unit III: Asymmetric Cryptography **9**

Mathematics of Asymmetric Key Cryptography: Primes – Primality Testing – Factorization – Euler's totient function, Fermat's and Euler's Theorem – Chinese Remainder Theorem – Exponentiation and algorithm ASYMMETRIC KEY CIPHERS: RSA cryptosystem – Key distribution – Key management – Diffie Hellman key exchange -– Elliptic curve arithmetic – Elliptic curve cryptography.

Unit IV: Integrity and Authentication Algorithms **9**

Authentication requirement – Authentication function – MAC – Hash function – Security of hash function: HMAC, CMAC – SHA – Digital signature and authentication protocols – DSS – Schnorr Digital Signature Scheme – ElGamal cryptosystem – Entity Authentication: Biometrics, Passwords, Challenge Response protocols – Authentication applications – Kerberos MUTUAL TRUST: Key management and distribution – Symmetric key distribution using symmetric and asymmetric encryption – Distribution of public keys – X.509 Certificates.

Unit V: Cyber Crimes and Cyber Security **9**

Cyber Crime and Information Security – classifications of Cyber Crimes – Tools and Methods – Password Cracking, Keyloggers, Spywares, SQL Injection – Network Access Control – Cloud Security – Web Security – Wireless Security.

TOTAL: 45 HOURS

REFERENCES

1. William Stallings, "Cryptography and Network Security - Principles and Practice", Seventh Edition, Pearson Education, 2017.
2. Nina Godbole, Sunit Belapure, "Cyber Security: Understanding Cybercrimes, Computer Forensics and Legal Perspectives", First Edition, Wiley India, 2011.
3. Behrouz A. Ferouzan, Debdeep Mukhopadhyay, "Cryptography and Network Security", 3rd Edition, Tata Mc Graw Hill, 2015.
4. Charles Pfleeger, Shari Pfleeger, Jonathan Margulies, "Security in Computing", Fifth Edition, Prentice Hall, New Delhi, 2015.

CY4571	ADVANCED OPERATING SYSTEM AND DATA STRUCTURES LABORATORY	L	T	P	C
		0	0	2	1

OBJECTIVES

- To learn to program in C++
- To efficiently implement the different data structures
- To efficiently implement solutions for specific problems

Course Outcome		Cognitive Skill
CO-01	Ability to identify the appropriate data structure for given problem	A
CO-02	Ability to implement basic data structures like arrays, linked list, stack, queue and its applications.	A
CO-03	Ability to apply sorting and searching techniques in real life applications	A
CO-04	Ability to design advance data structures using non-linear data structures.	A
CO-05	Ability to understand and implement principle requirements of memory management, CPU scheduling and memory partitioning concepts.	A

R-Remember,U-Understand,A-Apply,An-Analyze,E-Evaluate, S-Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	S	S	S	S	S	S	S	S
CO-02	S	M	S	S	M	S	S	S
CO-03	S	M	S	M	S	M	M	M
CO-04	S	S	S	M	S	M	M	M
CO-05	S	S	M	M	M	M	M	M

S-Strong, M-Medium,L-Low,N-Not relevant

List of Experiments

1. Implementation of Stack and Infix to postfix conversion.
2. Implementation of Queue, Circular Queue
3. Implementation of Linked list and Double Linked List.
4. Implementation of Binary Tree, Traversal Techniques and BST.
5. Implementation of Prim's algorithm and Kruskal's algorithm
6. Implementation of Merge Sort and Quick Sort
7. Implementation of Red-Black tree
8. Fibonacci Heap Implementation
9. Shortest Path Algorithms (Dijkstra's algorithm, Bellman Ford Algorithm)
10. Implementation of Matrix Chain Multiplication
11. Implement the following CPU Scheduling Algorithms.
    a. i) FCFS ii) Round Robin iii) Shortest Job First.
12. Implement Best fit, First Fit Algorithm for Memory Management.
13. Implement FIFO page Replacement Algorithm.
14. Implement LRU page Replacement Algorithm.
15. Implement the creation of Shared memory Segment.
16. Implement File Locking.

TOTAL: 45 HOURS

REFERENCES

1. Silberschatz, Galvin, Gagne "Operating System Concepts" Sixth Edition, 2003
2. Mark Allen Weiss, "Data Structures and Algorithm Analysis in C++", Pearson Education, 2002.
3. K.R Venugopal, Rajkumar Buyya, T. Ravishankar, "Mastering C++", TMH 2003.

SEMESTER II

Sl. No	Course Code	Course Title	L	T	P	C
THEORY						
1.	CY4504	Cyber Crime Investigations and Digital Forensics	3	0	0	3
2.	CY4505	Database Design and Security	3	0	0	3
3.	CY4506	Cyber Law and Security Policies	3	0	0	3
4.	CY4507	Advanced Network Security	3	0	0	3
5.	PEC	Elective II	3	0	0	3
6.	PEC	Elective III	3	0	0	3
PRACTICAL						
7.	CY4572	Database and Cyber Security Laboratory	0	0	2	1
TOTAL			**18**	**0**	**2**	**19**

CY4504	CYBER CRIME INVESTIGATIONS AND DIGITAL FORENSICS	L	T	P	C
		3	**0**	**0**	**3**

OBJECTIVES

- To understand the cyber-crime investigation process and laws related to cyber crime
- To learn the different types of hacking and attacks.
- To study various investigation methods, digital evidence collection and preservation techniques.
- To learn digital forensic concepts and tools.
- To study the various current cyber forensics tools

Course Outcome		Cognitive Skill
CO-01	Students should be able to understand cybercrime issues and related laws.	R
CO-02	Students should be able to analyze various cybercrimes.	U
CO-03	Students should be able to investigate cybercrimes using tools and techniques.	A
CO-04	Students should be able to explore methodology of incident responses and various security issues in the internet world and identify digital forensics for data.	An
CO-05	Students should be able to understand the importance of current digital forensics tools for analysis.	E

R-Remember,U-Understand,A-Apply,An-Analyze,E-Evaluate, S-Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	S	S	L	M	S	S	L	S
CO-02	S	L	M	L	M	L	M	N
CO-03	S	L	M	M	S	N	S	L
CO-04	M	L	S	S	S	S	S	M
CO-05	M	S	L	L	M	M	L	L

S-Strong, M-Medium,L-Low,N-Not relevant

Unit I: Introduction **8**

Introduction and Overview of Cyber Crime, Digital laws and legislation, Law Enforcement Roles and Responses, Social engineering, Policies followed in cybercrime investigations.

Unit II: Cyber Crime Issues **9**

Unauthorized Access to Computers, Computer Intrusions, White collar Crimes, Viruses and Malicious Code, Internet Hacking and Cracking, Virus Attacks, Pornography, Software Piracy, Intellectual Property, Mail Bombs, Exploitation, Stalking and Obscenity in Internet.

Unit III: Investigation **9**

Introduction to Cyber Crime Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IPTracking, E-Mail Recovery, Hands on Case Studies. Encryption and Decryption Methods, Search and Seizure of Computers, Recovering Deleted Evidences, Password Cracking.

Unit IV: Digital Forensics **9**

Introduction to Digital Forensics, Forensic Software and Hardware, Analysis and Advanced Tools, Forensic Technology and Practices, Forensic Ballistics and Photography, Face, Iris and Fingerprint Recognition, Audio Video Analysis.

Unit V: Current Computer Forensic Tools **10**

Evaluating computer forensic tool needs, computer forensic software tools, computer forensic hardware tools, validating and testing forensic software. E-mail investigations: Exploring the role of email in investigations, exploring the role of client and server in email, investigating email crimes and violations, understanding email servers, using specialized email.

TOTAL: 45 HOURS

REFERENCES

1. Nelson Phillips and EnfingerSteuart, "Computer Forensics and Investigations", Cengage Learning, New Delhi, 2009.
2. Kevin Mandia, Chris Prosise, Matt Pepe, "Incident Response and Computer Forensics ", Tata McGraw -Hill, New Delhi, 2006.
3. Computer Forensics, Computer Crime Investigation by John R,Vacca, Firewall Media,New Delhi.
4. Robert M Slade," Software Forensics", Tata McGraw - Hill, New Delhi, 2005.
5. Bernadette H Schell, Clemens Martin, "Cybercrime", ABC – CLIO Inc, California, 2004.
6. " Understanding Forensics in IT ", NIIT Ltd, 2005.

CY4505	DATABASE DESIGN AND SECURITY	L	T	P	C
		3	1	0	4

OBJECTIVES

- To learn about the database systems and the related concepts
- To understand the design constraints and to implement them
- To deal with concurrent executions in databases
- To gain knowledge about the database security
- To learn and implement the security techniques in databases.

Course Outcome		Cognitive Skill
CO-01	Understanding the basics of database systems and the related concepts	U
CO-02	To get a deep insight of Object Oriented DB and to work with MongoDB and NoSQL.	U,A
CO-03	Gaining knowledge of database security , the related concepts and analyzing the requirements to provide secure database systems	U, An
CO-04	Implementing the various techniques for database security	A
CO-05	Applying the auditing process to ensure safety and security of the database systems	A

R-Remember,U-Understand,A-Apply,An-Analyze,E-Evaluate, S-Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	S	M	S	M	S	M	S	S
CO-02	S	S	M	S	S	S	S	S
CO-03	S	L	M	M	M	M	M	M
CO-04	S	S	S	S	S	S	S	S
CO-05	S	S	S	S	S	S	S	S

S-Strong, M-Medium,L-Low,N-Not relevant

Unit I: Introduction **9**

Database- Data models, Database Design, component of database management system, Database languages- DDL, DML, SQL standard, Relational databases – design guidelines-normalization, Integrity constraints, Authorization, Query processing and optimization.

Unit II: Object Oriented Databases and Document Oriented Databases **9**

Object oriented database system – Need for OO databases - OODBMS Architectures Approaches – Advantages and disadvantages of OODBMS – Document oriented databases – Need for document databases – MongoDB- data model-working with data–NoSQL

Unit III: Database Security **9**

Introduction to database security, security models, security requirements, reliability and integrity, sensitive data, inference, multilevel databases and multilevel security, access control- mandatory, discretionary and role based.

Unit IV: Implementing Database Security **9**

Hardening database environment – patching database – securing services from network attacks – firewalls- VPN – authentication options – strong passwords – account lockout- password profiles- obfuscating application code – securing from SQL injection attacks – secure replication mechanisms- securing data sources and sinks, encrypting data-in-transit and data-at-rest

Unit V: Database Auditing **9**

Database auditing – auditing process, auditing classification and types, auditing categories - Audit- logon/logoff, sources, usage and errors, changes, auditing architectures - external audit system architecture, archive and secure auditing information, auditing the audit system.

TOTAL: 45 HOURS

REFERENCES

1. Abraham Silberschatz, Hanry F Korth, Sudarshan S, "Database Systems Concepts", McGraw Hill, 2007.
2. Ron Ben Natan, "Implementing database security and auditing", Elsevier publications, 2005.
3. Hassan A. Afyouni, "Database Security and Auditing", Course Technology – Cengage Learning, NewDelhi, 2009.
4. Thomas Connolly, Carolyn Begg,Database Systems: A Practical Approach to Design, Implementation, and Management, 6th Edition**,** Pearson Education, 2015**.**
5. RamezElmasri, Shamkant B. Navathe , "Fundamentals of Database System" Addison Wesley, New Delhi/Fourth Edition 2004
6. M. Gertz, and S. Jajodia, Handbook of Database Security- Application and Trends, 2008, Springer.
7. Charles P, Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, Security in Computing, 5th Edition, PH, 2015
8. Osama S. Faragallah, El-Sayed M. El-Rabaie, Fathi E. Abd El-Samie, Ahmed I. Sallam, and Hala S. El-Sayed,Multilevel security for relational databases, CRC press, 2015.
9. David Hows, Peter Membrey, EelcoPlugge, Tim Hawkins, 'The Definitive Guide to MongoDB',APress, 2015.
10. Pramod J. Sadalage and MartinFowler,'NoSQL Distilled', Addison Wesley, 2012.

CY4506	CYBER LAW AND SECURITY POLICIES	L	T	P	C
		3	0	0	3

OBJECTIVES

- To explore the various security policies and procedures.
- To understand the fundamentals of asset classification policies and several typical policies.
- To understand the fundamentals of information security and its tools.
- To be familiar with the organization and the information security standards and procedures.
- To realize the importance of internet ethics, IT Act and its legal procedures.

Course Outcome		Cognitive Skill
CO-01	Student will be able to gain basic knowledge on security policies	R
CO-02	Student will be able to understand asset classification policies	R
CO-03	Student will gain insight into typical policies and information security concepts	U
CO-04	Student will gain knowledge on Internet Ethics, Information Technology Act And Legal Frame Work	U
CO-05	Students will gain knowledge on copyright law and contract law	An

R-Remember,U-Understand,A-Apply,An-Analyze,E-Evaluate, S-Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	S	S	S	M	M	M	S	S
CO-02	S	S	S	M	M	M	S	S
CO-03	S	S	S	M	M	M	S	S
CO-04	S	S	S	M	M	M	S	S
CO-05	S	S	S	M	M	M	S	S

S-Strong, M-Medium,L-Low,N-Not relevant

Unit I: **Introduction** **9**

Corporate Policies- Organization wide Policies- Organization wide Policy Document -Legal Requirements- Duty of Loyalty- Duty of Care- Other Laws and Regulations-Business Requirements - Developing Policies- Implementation of Information Security Policy -Some Major Points for Establishing Policies - Policy Key Elements-Policy Format-Additional Hints-Pitfalls to Avoid.

Unit II: Asset Classification Policy **9**

Information Classification - Confidential Information-Employee Responsibilities-Classification Examples-Declassification or Reclassification of Information- Records Management Policy-Information Handling Standards Matrix-Information Classification Methodology-Authorization for Access

Unit III: Information Security Policies and Standards and Procedures and Secure Information Processing **9**

Typical Tier 1 Policies -Typical Tier 2 Policies-Tools of Information Security -Information Processing- Information Security Program Administration, Orange Book and Red Book. Developing Standards-Introduction- Overview- Sample Information Security Manual-Developing Procedures-Important Procedure Requirements-Key Elements in Procedure Writing-Procedure Checklist- Procedure Styles- Procedure Development Review-Observations.

Unit IV: Cyber Laws **9**

Ethics and the Internet - Ethics Online - Information Technology Law : Need of Legal Protection -Information Technology Act 2000: Objectives - Scope - Applicability - Information Technology (Amendment) Act, 2008 - Data - Privacy of Data - Requirements and mandates for data privacy, Data Privacy Act, Recompense - Limitation -Legal Protection against Cyber Crimes: Criminal Liabilities under Information Technology Act, 2000 - Common Cyber Crimes and Applicable Legal Provisions- Civil Liabilities under Information Technology Act, 2000 - Civil Liability for Corporate- Cyber Crimes under IPC and Special Laws 80 - The Indian Penal Code - Cyber Crimes under the Special Acts- Cyber Laws: Recent Trends.

Unit V: Copyright Law **9**

Introduction to Intellectual property, Scope of copyright law, Copyright notice, Copyright registration, Copyright Duration, Digital Millennium Copyright Act, Copyright infringement, International Enforcement of copyright, Sources of contract law, Electronic Signatures in Global and National Commerce Act, Principles of the Law of Software Contracts, Fundamental principles of contract law, E-Commerce law.

TOTAL: 45 HOURS

REFERENCES

1. Thomas R. Peltier, “Information Security policies and procedures: A Practitioner’s Reference”, 2nd Edition Prentice Hall, 2004.
2. Cybercrime Law and Practice, the Institute of Company Secretaries of India, 2016.

3. Cyberlaw: The Law of the Internet and Information Technology" by Brian Craig
4. Rick Lehtinen and G.T. Gangemi, "Computer Security Basics (Paperback)", 2ndEdition, O' Reilly Media, 2006.
5. Economic Laws Practice, 2017
6. PavanDuggal," Cyber Laws", Universal Law Publishing, 2016
7. Deborah G Johnson, Computer Ethics, Pearson Education, 2009
8. Thomas R Peltier, Justin Peltier and John blackley," Information Security Fundamentals", Prentice Hall, 2004

CY4507	ADVANCED NETWORK SECURITY	L	T	P	C
		3	0	0	3

OBJECTIVES

- To understand the basic concepts of IP security and to protect the data in Web.
- To identify various kinds of security breaches and security vulnerability attacks in wireless networks.
- To describe the process of Bluetooth security architecture and threats to Bluetooth security.
- To gain fundamental knowledge on applications of system security.
- To study various Internet security applications.

Course Outcome		Cognitive Skill
CO-01	Understand the basic concepts of IP security and to protect the data in Web.	U
CO-02	Identify various kinds of security breaches and security vulnerability attacks in wireless networks.	An
CO-03	Illustrate the process of Bluetooth security architecture and threats to Bluetooth security.	U
CO-04	Apply modern cryptographic techniques to enhance overall system security.	A
CO-05	Interpret the various Internet security applications.	A

R-Remember,U-Understand,A-Apply,An-Analyze,E-Evaluate, S-Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	S	M	M	M	S	S	S	S
CO-02	S	S	M	M	S	S	S	S
CO-03	S	S	M	M	S	S	S	S
CO-04	S	S	M	M	S	S	S	S
CO-05	S	S	M	M	S	S	S	S

S-Strong, M-Medium,L-Low,N-Not relevant

Unit I: IP & Web Security **9**

IP security: Overview - Architecture – Authentication Header - Encapsulating Security Payload - Key management – Web security: Secure Socket Layer and Transport Layer Security – HTTPS - Secure Shell (SSH) – Electronic Mail Security- Pretty Good Privacy, Secure/Multipurpose Internet Mail Extension.

Unit II: Wireless Security **9**

Kinds of security breaches - Eavesdropping - Communication Jamming - RF interference - Covert wireless channels - DOS attack – Spoofing - Theft of services - Traffic Analysis - Cryptographic threats - Wireless security Standards - Wireless Network Security.

Unit III: Bluetooth Security **9**

Basic specifications – Pico nets and Scatter nets – Bluetooth Protocol architecture – Bluetooth security architecture – Security at the baseband layer and link layer – Frequency hopping – Security manager – Authentication – Encryption – Threats to Bluetooth security.

Unit IV: System Security **9**

Intruders – Intrusion detection – Password management – Malicious Software: Viruses and related threats – Virus countermeasures – Firewalls: Firewall design principles – Firewall configurations – Trusted System - Network storage devices - SIEM.

Unit V: Network and Internet Security **9**

Network Access Control - Cloud Security - Secure electronic transaction - Blockchain: The growth of blockchain technology - Types, Consensus, and Mining Task – Platforms, Cryptocurrency, Bitcoin. - Introduction to quantum cryptography.

TOTAL: 45 HOURS

REFERENCES

1. William Stallings, “Cryptography and Network Security”, Seventh Edition, Pearson Education, June 2017.
2. Shari Lawrence Pfleeger, Charles P. Pfleeger, Jonathan Margulies "Security in Computing", Pearson, January 2015.
3. Nichols and Lekka, “Wireless Security-Models, Threats and Solutions”, Tata McGraw – Hill, New Delhi, 2006.
4. Merritt Maxim and David Pollino, “Wireless Security”, Osborne/McGraw Hill, New Delhi, 2005.
5. Behrouz A Forouzan and Debdeep Mukhopadhyay, “Cryptography and Network Security”, Second Edition, Tata McGraw Hill Education Pvt. Ltd., New Delhi, 2010.
6. Chalie Kaufman, Radia Perlman, Mike Speciner, “Network Security: Private Communication in a Public Network”, Pearson Education, New Delhi, 2004.
7. AtulKahate, “Cryptography and Network Security”, Tata McGraw Hill Ltd., New Delhi, 2013.
8. Hans, Knebl, Helmut, Delfs , "Introduction To Cryptography Principles And Applications", 3rd Edition, Springer- Verlag, Berlin Heidelberg, 2015.
9. Imran Bashir, "Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained", 7 th Edition, Packt Publishing Ltd, 2018.

CY4572	DATABASE AND CYBER SECURITY LABORATORY	L	T	P	C
		0	0	2	1

OBJECTIVES

- To create database environment
- To set up integrity constraints
- To grant, revoke authentication
- To implement standard security mechanisms

Course Outcome		Cognitive Skill
CO-01	Able to create database environment	A
CO-02	Able to set up integrity constraints	A
CO-03	Able to implement authentication mechanisms	A
CO-04	Able to implement standard security mechanisms	A
CO-05	Hiding confidential information within image	A

R-Remember,U-Understand,A-Apply,An-Analyze,E-Evaluate, S-Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	M	S	M	M	S	S	M	S
CO-02	M	M	S	S	S	S	S	S
CO-03	M	S	S	M	S	S	S	S
CO-04	M	M	S	S	S	S	S	S
CO-05	M	S	S	S	S	S	S	S

S-Strong, M-Medium,L-Low,N-Not relevant

List of Experiments

1. Creating a database for an application using DDL.
2. Setting up of integrity constraints.
3. Data manipulation using DML queries.
4. Use Rollback, commit, save point, grant and revoke commands.
5. Creation, deletion and modification of users and implementing authentication mechanisms for different users.
6. Designing and implementing password policies.
7. Implementation of Substitution and Transposition ciphers
8. Implementation of Data Encryption Standard
9. Implementation of Advanced Encryption Standard
10. Implementation of RSA Algorithm
11. Implementation of Digital Signature Standard
12. Hiding of confidential information within Image

TOTAL: 45 HOURS

SEMESTER III

Sl. No	Course Code	Course Title	L	T	P	C
THEORY						
1.	PEC	Elective IV	3	0	0	3
2.	OEC	Open Elective II	3	0	0	3
PRACTICAL						
3.	CY4573	Cyber Crime Investigations Laboratory	0	0	2	1
4.	CY45P1	Project work – Phase I	0	0	12	6
TOTAL			**6**	**0**	**14**	**13**

CY4573	CYBER CRIME INVESTIGATIONS LABORATORY	L	T	P	C
		0	**0**	**2**	**1**

OBJECTIVES

- Illustrates the digital forensics and relate it to an investigative process.
- Elucidates the legal issues of preparing for and performing digital forensic analysis based on the investigator's position and duty.
- Demonstrate the use of digital forensics tools.
- Guide a digital forensics exercise.

Course Outcome		Cognitive Skill
CO-01	Facilitate students to be aware of the advanced scanning techniques and identify malicious activity if any.	An
CO-02	Students should be made to be knowledgeable in information gathering techniques.	U, An
CO-03	Enable students to acquire knowledge about the different cyber forensics tools.	U,A

CO-04	Enable students to be familiar with the forensics tools to collect evidence from devices such as hard drives and smartphones	An
CO-05	Students will gain practical proficiency in using PSTools for efficient and effective system administration troubleshooting, and remote management tasks in a Windows environment.	U,A

R-Remember,U-Understand,A-Apply,An-Analyze,E-Evaluate, S-Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	S	M	M	S	S	N	L	S
CO-02	S	S	S	M	M	N	M	S
CO-03	M	S	S	S	M	M	M	M
CO-04	S	S	S	S	S	M	S	M
CO-05	M	S	S	M	M	M	M	S

S-Strong, M-Medium,L-Low,N-Not relevant

List of Experiments

1. Analysis of Network Traffic using Packet Sniffing Tool.
2. Capture and Analyze network traffic using Wireshark
3. Use Google and Whois for Reconnaissance.
4. Perform real-time data mining and information gathering using Maltego.
5. Perform port scanning.
6. Imaging and analyzing a disk using Disk forensics tools.
7. Analysis of Network using Network Forensic tools.
8. Familiarization of NeSA (Network Packet Analysis) Tool
9. Acquire the Image of a Mobile phone and analyze it using MobileCheck.
10. Live Forensic evidence extraction and analysis using Win-LiFT.
11. Capture the physical memory of a suspect's computer using MAGNET RAM Capture
12. Perform various administrative tasks using PSTools.

TOTAL: 45 HOURS

PROFESSIONAL ELECTIVE COURSES

SI. NO	COURSE CODE	COURSE TITLE	L	T	P	C
1.	CY45A1	Ethical Hacking	3	0	0	3
2.	CY45A2	Biometric Security	3	0	0	3
3.	CY45A3	Forensics and Incident Response	3	0	0	3
4.	CY45A4	IOT Security	3	0	0	3
5.	CY45A5	Cyber Forensics	3	0	0	3
6.	CY45A6	Malware Forensics	3	0	0	3
7.	CY45A7	OS Forensics	3	0	0	3
8.	CY45A8	Virtual Forensics	3	0	0	3
9.	CY45A9	Security Policies and Governance	3	0	0	3
10.	CY45B1	Intrusion Detection and Prevention System	3	0	0	3
11.	CY45B2	Cyber Warfare	3	0	0	3

CY45A1	ETHICAL HACKING	L	T	P	C
		3	0	0	3

OBJECTIVES

- To prepare ethical hacking plan, find out different hacking methodologies, relate law related to the attack and perform vulnerability and penetration testing.
- To work with foot printing tools and to identify different social engineering techniques to gather information.
- To work with port scanning, enumerations tools and analyze gathered information.
- To explore hacking in web server and wireless network.
- To identify the vulnerabilities and hack different operating system such as windows, Linux.

Course Outcome		Cognitive Skill
CO-01	Students will be able to prepare ethical hacking plan, find out different hacking methodologies and relate law related to the attack and understand vulnerability and penetration testing.	R
CO-02	Students will be able to work with foot printing tools and identify different social engineering techniques to gather information.	U
CO-03	Students will be able to understand port scanning, enumeration tools, system hacking, malware threats and analyze gathered information.	A
CO-04	Students will be able to explore hacking web servers and wireless networks.	An
CO-05	Students will be able to identify the vulnerabilities and hack different operating systems such as windows, Linux.	E

R-Remember,U-Understand,A-Apply,An-Analyze,E-Evaluate, S-Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	S	S	S	S	L	M	M	S
CO-02	M	S	S	S	L	M	L	M
CO-03	M	S	S	S	L	M	M	L
CO-04	M	S	S	S	L	M	L	L
CO-05	M	M	S	S	L	M	M	M

S-Strong, M-Medium,L-Low,N-Not relevant

Unit I: Ethical Hacking Overview **9**

Introduction - Certified Ethical Hackers – Network and Computer Attacks – Ethical Hacking Plan – Hacking Methodology. Legal Issues and Law Enforcement- Vulnerability and Penetration Testing- Developing Security Testing Plan

Unit II: Footprinting and Social Engineering **9**

Footprinting Concepts - Footprinting Methodology -Foot printing Tools – Conducting Competitive Intelligence - DNS Zone Transfers – Introduction to Social Engineering – Performing Social Engineering Attacks - Social Engineering Countermeasures.

Unit III: Service Scanning **9**

Introduction to Port Scanning – Types of Port Scan – Port Scanning Tools - Conducting Ping Sweeps - Shell Scripting. Enumeration: Introduction - Enumerating Windows- System Hacking- Online tool for default passwords- Rainbow Table using Winrtgen tool- Malware Threats-Introduction- Trojan Concept- Virus and Worms Concepts- Malware Reverse Engineering

Unit IV: Hacking Networks **9**

Hacking Web Servers: Web Application – Web Application Vulnerabilities – Tools for Web Attackers and Security Testers. Hacking Wireless Network- Wireless Technology – Wireless Network Standards – Authentication – War driving – Wireless Hacking – Protecting Networks with Security Devices- Encryption Attacks- Authentication Attacks

Unit V: Hacking Operating Systems **9**

Hacking Windows- Overview- Unauthenticated Attacks- Authenticated Attacks- Windows Security Features- Hacking UNIX- The Quest for Root- Remote Access- Local Access- Rootkit Recovery- Embedded Operating Systems- Introduction-Vulnerabilities of Embedded OS

TOTAL: 45 HOURS

REFERENCES

1. Michael T. Simpson, "Ethical Hacking and Network Defense", Cengage Learning, New Delhi, 2010.
2. Stuart McClure, Joel Scambray, George Kurtz, "Hacking Exposed 7: Network Security Secrets & Solutions ", McGraw-Hill publishing, 7th Edition, July 2012
3. The Certified Ethical Hacker CEH V10, Complete Hacking Guide
   Kevin Beaver, "Hacking for Dummies", Wiley Publication, India, 5th Edition, 2016.
4. AnkitFadia, "Unofficial Guide to Ethical Hacking", Macmillan Company, New Delhi, 2006.
5. SanjibSinha, "Beginning Ethical Hacking with Python", Apress, 2017

CY45A2	BIOMETRIC SECURITY	L	T	P	C
		3	0	0	3

OBJECTIVES

- To have a thorough understanding of the basic concepts of biometrics and various performance measures.
- To discuss in detail about the physiological biometrics authentication techniques.
- To discuss in detail about the behavioral biometrics authentication techniques.
- To expose how to apply biometric technologies in various applications.
- To familiarize the students to handle privacy, risks and standards in biometrics.

Course Outcome		Cognitive Skill
CO-01	Understand the basic concepts of Biometrics and various performance measures.	U
CO-02	Acquire knowledge about psychological biometric authentication techniques.	U
CO-03	Acquire knowledge about Behavioural biometric authentication techniques.	U
CO-04	Apply Biometric technologies in various applications.	A
CO-05	Develop simple applications for privacy.	An

R-Remember,U-Understand,A-Apply,An-Analyze,E-Evaluate, S-Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	S	S	M	L	S	M	M	L
CO-02	S	S	M	L	S	M	M	L
CO-03	S	S	M	L	S	M	M	L
CO-04	S	S	M	L	S	M	M	L
CO-05	S	S	M	L	S	M	M	L

S-Strong, M-Medium,L-Low,N-Not relevant

Unit I: Introduction **9**

Biometric fundamentals-Need for Biometrics- Biometrics Vs traditional techniques – Benefits of Biometrics Vs traditional -Authentication methods– Benefits of biometrics in identification system-fraud detection-fraud deterrence- Characteristics of a good biometric system-Biometrics systems–Design cycle of Biometric Systems- Key biometric processes: verification, identification and biometric matching – Performance measures in biometric systems: FAR, FRR, FTE rate, EER and ATV rate.

Unit II: Physiological Biometrics **9**

Leading technologies: Finger-scan – Facial-scan – Iris-scan – Voice-scan – components, working principles, competing technologies, strengths and weaknesses – Other physiological biometrics: Hand-scan, Retina-scan – components, working principles, competing technologies, strengths and weaknesses – Automated fingerprint identification systems, Multimodal Biometrics.

Unit III: Behavioural Biometrics **9**

Leading technologies: Signature-scan – Keystroke scan – components, working principles, strengths and weaknesses, Human identification based on gait – Speaker recognition- Gesture recognition.

Unit IV: Biometric Applications **9**

Categorizing biometric applications – Citizen-facing applications-criminal identification- - citizen identification- surveillance-Employee-facing applications- PC/network access- Customer-facing applications-E-commerce/Telephony- retail/ATM/Point of sale- costs to deploy – other issues in deployment

Unit V: Privacy Enhancement and Multimodal Biometrics **9**

Privacy concerns associated with biometric developments – Identity and privacy – Privacy concerns – biometrics with privacy enhancement – Comparison of various biometrics in terms of privacy – Soft biometrics - Introduction to biometric cryptography – General purpose cryptosystem – Modern cryptography and attacks – Symmetric key ciphers – Cryptographic algorithms – Introduction to multimodal biometrics – Basic architecture using face and ear – Characteristics and advantages of multimodal biometrics characters – AADHAAR : An Application of Multimodal Biometrics.

TOTAL: 45 HOURS

REFERENCES

1. Samir Nanavati, Michael Thieme, Raj Nanavati, “Biometrics – Identity Verification in a Networked World”, Wiley-dreamtech India Pvt Ltd, New Delhi, 2003.
2. G R Sinha and Sandeep B. Patil, Biometrics: Concepts and Applications, Wiley, 2013
3. James wayman,Anil k.Jain ,Arun A.Ross ,Karthik Nandakumar, ―Introduction to Biometrics, Springer, 2011.
4. John D Woodward, Jr.; Nicholas M Orlans; Peter T Higgins, Biometrics – The Ultimate Reference, Wiley Dreamtech.College Publications, 2015.
5. Anil K Jain, Patrick Flynn, Arun A Ross, “Handbook of Biometrics”, Springer, 2008.
6. David D. Zhang, “AUTOMATED BIOMETRICS Technologies and Systems”, Springer Science Business Media, LLC, 2000.
7. Mohammad S Obaidat, Issa Traore and Isacc Woungang, “Biometric-based physical and cyber security systems”, Springer 2019.
8. Paul Reid, “Biometrics for Network Security”, Pearson Education, New Delhi, 2004.
9. John R Vacca, “Biometric Technologies and Verification Systems”, Elsevier Inc, 2007.

CY45A3	FORENSICS AND INCIDENT RESPONSE	L	T	P	C
		3	0	0	3

OBJECTIVES

- To know the real world incidents.
- To make the pre- incident preparation.
- To understand about incident detection and characterization.
- To gain knowledge on data collection and the duplication process.
- To know the data analysis techniques.

Course Outcome		Cognitive Skill
CO-01	Learn the fundamental concepts of incident response and the incident response process.	U
CO-02	Understand the methods to handle incidents and prepare the organization and infrastructure for incident response.	U, An
CO-03	Gain knowledge on how to detect the incidents, what are the proofs and how to resolve them.	U, An
CO-04	Able to know how to collect live data, the different toolkits for collecting data for response and forensic duplication process.	U, An
CO-05	Learn the analysis methodology and able to investigate the OS and applications for incidents.	U, An

R-Remember,U-Understand,A-Apply,An-Analyze,E-Evaluate, S-Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	S	S	S	S	M	M	M	L
CO-02	S	S	S	S	M	M	M	L
CO-03	S	S	S	S	M	M	M	L
CO-04	S	S	S	S	M	M	M	L
CO-05	S	S	S	S	M	M	M	L

S-Strong, M-Medium,L-Low,N-Not relevant

Unit I: Real-World Incidents **8**

Introduction to Incident - Incident Response Methodology – Steps - Activities in Initial Response Phase after detection of an incident.

Unit II: Pre-Incident Preparation **9**

Preparing the Organization for Incident Response, Identifying Risk, Policies That Promote a Successful IR, Working with Outsourced IT, Thoughts on Global Infrastructure Issues, Educating Users on Host-Based Security, Preparing the IR Team, Preparing the Infrastructure for Incident Response, Computing Device Configuration, Network Configuration.

Unit III: Incident detection and Characterization **9**

Collecting Initial Facts, Checklists, Maintenance of Case Notes, Building an Attack Timeline, Understanding Investigative Priorities, Elements of Proof, Setting Expectations with Management, Initial Development of Leads, Defining Leads of Value, Acting on Leads, Turning Leads into Indicators, The Lifecycle of Indicator Generation, Resolving Internal Leads, Resolving External Leads.

Unit IV: Forensic Data Collection and Duplication **9**

Live Data Collection, Live Data Collection on Microsoft Windows Systems, Live Data Collection on Unix-Based Systems, Android systems, IoS phones, Live Response Toolkits, Forensic Image Formats, Traditional Duplication, Live System Duplication, Duplication of Enterprise Assets, Duplication of Virtual Machines, Authentication of Evidence.

Unit V: Forensic Data Analysis **10**

Analysis methodology, Investigating Windows Systems, Linux Systems, Android systems, IoS Phones Investigating Mac OS X Systems, Investigating Applications, Malware handling.

TOTAL: 45 HOURS

REFERENCES

1. Kevin Mandia, Mathew Pepe, Jason Luttgens, “Incident Response and Computer Forensics”, 3rd Edition, McGraw-Hill Osborne Media, 2014.
2. Kevin Mandia, Chris Prosise , “Incident Response and computer forensics”, Tata McGrawHill, 2006.
3. Eoghan Casey, "Handbook Computer Crime Investigation's Forensic Tools and Technology", Academic Press.
4. Skoudis. E., Perlman. R. Counter Hack, “A Step-by-Step Guide to Computer Attacks and Effective Defenses”, Prentice Hall Professional Technical Reference.
5. Norbert Zaenglein, “Disk Detective: Secret You Must Know to Recover Information From a Computer”, Paladin Press.
6. Bill Nelson, Amelia Philips and Christopher Steuart, “Guide to computer forensics and investigations”, Cengage Learning.

CY45A4	IOT SECURITY	L	T	P	C
		3	0	0	3

OBJECTIVE

To provide knowledge about security risks IoT domain faces and countermeasures available for the known issues

Course Outcome		Cognitive Skill
CO-01	Students will be able to analyze, select, and apply appropriate IoT protocols for different layers	U, An
CO-02	Students will be able to understand vulnerabilities, attacks defend against different types of IoT attacks	U
CO-03	students will be able to analyse security in IoT systems	An
CO-04	Students will be able to analyse the IoT security lifecycle.	U, A
CO-05	Students will be able to analyze the role of cryptography for securing IoT	U, A

R-Remember,U-Understand,A-Apply,An-Analyze,E-Evaluate, S-Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	M	L	L	M	L	L	L	M
CO-02	S	M	M	M	M	M	M	M
CO-03	M	M	L	M	M	L	M	M
CO-04	L	N	N	M	L	M	L	L
CO-05	S	M	S	S	M	M	S	S

S-Strong, M-Medium,L-Low,N-Not relevant

Unit I: Introduction to Internet of Things **9**

Introduction, Definition and characteristics of IoT, Physical design of IoT-Things in IoT, IoT Protocols-Link Layer, Network/Internet Layer, Transport Layer, Application Layer. Logical design of IoT. IoT Communication models.

Unit II: Vulnerabilities, Attacks and Countermeasures **9**

The classic pillars of information assurance, Threats, Vulnerability, Risks, Primer on attacks and countermeasures -Common IoT attack types, Attack Trees-Fault Trees and CPS. Today's IoT Attacks-Wireless reconnaissance and mapping, Security protocol attacks, Physical security attacks, Application security attacks. Threat modeling an Iot System.

Unit III: IOT Security **9**

Building security into design and development, Secure design - Safety and security design, Processes and agreements. Technology selection – IoT Device and hardware, selecting RTOs, security products and services. IoT relationship platforms, Cryptographic security APIs, Authentication/Authorization

Unit IV: The IOT Security Lifecycle **9**

The secure IoT system implementation lifecycle, Implementation and integration, IoT security CONOPS document, Network and security integration, planning for updates to existing network and security infrastructures, System security verification and validation (V&V), Security training, Secure configurations. Operations and Maintenance-Managing identities, roles, and attributes, Security Monitoring, Penetration testing, Compliance monitoring, Asset and configuration management, Incident management, Forensics. Dispose-Secure device disposal and zeroization, Data purging, Inventory control, Data archiving and records management

Unit V: Cryptographic Fundamentals for IOT Security Engineering **9**

Cryptography and its role for securing IoT, Types and uses of cryptographic primitives in the IoT, Encryption and decryption, Hashes, Digital Signatures, Cryptographic Module Principles, Cryptographic Key Management fundamentals, Examining Cryptographic controls for IoT protocols, Future directions of the IoT and Cryptography.

TOTAL: 45 HOURS

REFERENCES

1. Russell, Brian and Drew Van Duren, “Practical Internet of Things Security”, Packt Publishing, 2016.
2. "Internet of Things: A Hands-on Approach", by ArshdeepBahga and Vijay Madisetti (Universities Press)

CY45A5	CYBER FORENSICS	L	T	P	C
		3	0	0	3

OBJECTIVES

- Gain a comprehensive understanding of the field of computer forensics, including its history, legal aspects, and professional conduct, as well as the process of conducting computer investigations and establishing a forensic lab.
- Develop skills in data acquisition
- Acquire knowledge and proficiency in working with Windows and DOS systems

Course Outcome		Cognitive Skill
CO-01	Students will be able to effectively conduct computer investigations by applying a systematic approach.	U, A
CO-02	Students will be able to effectively acquire and process digital evidence by applying appropriate storage formats, selecting and utilizing acquisition methods and tools	R, A
CO-03	Students will be able to effectively work with Windows and DOS systems	U, An
CO-04	Students will be able to effectively analyze and validate forensic data by generating reports.	U, A
CO-05	Students will be able to investigate email crimes.	U, A

R-Remember,U-Understand,A-Apply,An-Analyze,E-Evaluate, S-Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	M	L	L	M	L	L	L	M
CO-02	S	M	M	M	M	M	M	M
CO-03	M	M	L	M	M	L	M	M
CO-04	L	N	N	M	L	M	L	L
CO-05	S	M	S	S	M	M	S	S

S-Strong, M-Medium,L-Low,N-Not relevant

Unit I: Introduction to Cyber Forensics **9**

Computer Forensics: history of computer forensics, understanding case law, developing computer forensics resources, preparing for computer investigations, understanding law enforcement agency investigations and corporate investigations, maintaining professional conduct. Understanding Computer Investigations -Preparing a computer investigation, taking a systematic approach, procedures for corporate high tech investigations, understanding data recovery workstations and software, conducting an investigation, completing the case, Requirements for Forensic Lab certification, determining the physical requirements for a CF lab, selecting a basic forensic workstation, building a business case for developing a forensic lab

Unit II: Data Acquisition **9**

Data Acquisition - storage formats for digital evidence, determining the best acquisition method, contingency planning for image acquisitions, using acquisition tools, validating data acquisitions, performing RAID data acquisitions, using remote network acquisition tools, using other forensic acquisition tools, Processing Crime and Incident Scene - Identifying digital evidence, collecting evidence in private sector incident scenes, processing law enforcement crime scenes, preparing for a search, securing a computer incident or crime scene . Seizing digital evidence at the scene, storing digital evidence, obtaining a digital hash.

Unit III: Windows and Dos Systems **9**

Working with windows and DOS systems- file systems, exploring Microsoft file structures, examining NTFS disks, whole disk encryption, the windows registry, Microsoft and MS-DOS start up tasks, virtual machines, Evaluating Computer Forensics Tool needs, computer forensics software and hardware tools, validating and testing forensics software. Examining UNIX and LINUX disk structures and boot processes, examining CD data structures, examining SCSI Disk, examining IDE/EIDE and SATA devices

Unit IV: Analysis and Reporting **9**

Analysis and validation -determining what data to collect and analyze, validating forensic data, addressing data -hiding techniques.Report writing for High-Tech Investigations-Understanding the importance of reports-Limiting a report to specifics, Types of reports-Guidelines for writing reports –What to include in written preliminary reports, Reports structure, Writing reports clearly, Designing the layout and presentation of reports-Generating report findings with Forensics Software tools.

Unit V: **Email Investigations** **9**

Email Investigations-role of E-mail in investigations, exploring the roles of the client and server, investigating E-mail crimes and violations, understanding E-mail servers, specialized E-mail forensic tools. Cell Phone and Mobile Device forensics- Mobile device forensics, acquisition procedures for cell phones and mobile devices. Report writing for high tech investigations, Expert Testimony in High Tech Investigations.

TOTAL: 45 HOURS

REFERENCES

1. Bill Nelson, Amelia Phillips, Chris Steuart, "Guide to Computer Forensics and Investigations", Sixth edition, 2018
2. John R,Vacca, "Computer Forensics, Computer Crime Investigation", Firewall Media, New Delhi
3. Eoghan Casey, "Digital Evidence and Computer Crime" Edition 3, Academic Press,2011
4. MarjieBritz, "Computer Forensics and Cyber Crime : An Introduction",Edition 2, Prentice Hall, 2008
5. David Benton and Frank Grindstaff,"Practical guide to Computer Forensics", Book Surge Publishing,2006
6. Christopher L.T Brown Charles,"Computer Evidence: Collection & Preservation" River Media publishing, Edition 1, 2005
7. Elizabeth Bauchner,"Computer Investigation" (Forensics, the Science of crime-solving) , Mason Crest Publishers, 2005
8. Keith J. Jones, Richard Bejtlich and Curtis W. Rose, "Real Digital Forensics" Addison-Wesley publishers, 2005
9. Thomas A. Johnson,"Forensic Computer Crime Investigation" (International Forensic Science and Investigation), CRC Press, 2005 Publishing Co. Beijing, 1999.
10. S. K. Basu, "Design Methods and Analysis of Algorithms", Prentice Hall India, 2005.

CY45A6	MALWARE FORENSICS	L	T	P	C
		3	0	0	3

OBJECTIVES

- To understand the working of malware programs
- To find the malware artifacts from a live Windows and Linux system
- To analyze the suspect files affected by malwares
- To learn how to extract the malware artifacts

Course Outcome		Cognitive Skill
CO-01	Students will be able to effectively respond to malware incidents by employing appropriate methodologies	U, A
CO-02	Students will be proficient in memory forensics by utilizing appropriate methodologies, tools, and techniques	R, A
CO-03	Students will be equipped with the knowledge and skills to perform post-mortem forensics	U, An
CO-04	Students will be proficient in file identification and profiling.	U, A
CO-05	Students will be able to effectively analyze and counter file obfuscation techniques	U, A

R-Remember,U-Understand,A-Apply,An-Analyze,E-Evaluate, S-Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	M	L	L	M	L	L	L	M
CO-02	S	M	M	M	M	M	M	M
CO-03	M	M	L	M	M	L	M	M
CO-04	L	N	N	M	L	M	L	L
CO-05	S	M	S	S	M	M	S	S

S-Strong, M-Medium,L-Low,N-Not relevant

Unit I: Malware Incident **9**

Malware Incident response: Volatile Data Collection and Examination on a Live Windows / Linux System-Volatile Data collection methodology-Preservation of volatile data, Collecting Subject System details, Identifying Users logged into the system, Inspect Network Connections and activity, Current and recent network connections, Collecting process information, Process to executable program mapping , Dependencies loaded by running processes, Correlate open ports with running processes and programs, Identifying servers and drivers, Determining scheduled tasks, Collecting Clipboard contents, Non-volatile Data collection from a live Windows system, Forensic duplication of storage media on a live Windows system, Forensic preservation of Select Data on a Live Windows System, Incident Response Tool Suites for Windows, Assess Security configuration, Collect Logon and System Logs

Unit II: Memory Forensics **9**

Memory Forensics: Analyzing Physical and Process Dumps for Malware Artifacts- Memory Forensics methodology, Old School Memory Analysis, Windows Memory Forensics Tools, Active, Inactive and Hidden Processes, How Windows Memory Forensics Tools work, Process Memory Dumping and Analysis on a Live Windows System, Capturing Process and Analyzing Memory, Linux Memory Forensics Tools, How Linux Memory Forensics Tools work, Process Memory Dumping and Analysis on a Live Linux System, Capturing and Examining Process Memory in Linux System.

Unit III: Post-Mortem Forensics **9**

Post-Mortem Forensics: Discovering and Extracting Malware and Associated Artifacts from Windows Systems and Linux systems Forensic Examinations of Compromised Windows / Linux Systems, Functional Analysis Resuscitating a Windows / Linux Computer, Malware Discovery and Extraction from a Windows/ Linux system, inspect services, Drivers Auto-starting Locations, and scheduled jobs. Legal considerations- Framing the issues, Sources of

Investigative authority, Statutory limits of authority, protected data, Tools for acquiring data, acquiring data across Borders, Involving Law Enforcement, Improve chances for admissibility

Unit IV: File Identification **9**

File Identification and profiling: Initial Analysis of a suspect file on a Windows system-Overview of the File Profiling process, Working with Executables-Compilation, Linking-Static, Dynamic, System details, Hash values, File similarity indexing, File signature identification and classification- File types, Tools, Embedded artifact extraction, Symbolic and Debug information.

Unit V: **File Obfuscation** **9**

File Obfuscation: Packing and Encryption Identification-Packers, Cryptors, Wrappers, Elf File structure, Analysis of a suspect program: Windows- Analysis Goals, Guidelines for examining a malicious executable program, establishing the environment baseline, Pre -execution preparation: system and network monitoring, Observing, File system, Embedded Artifact Extraction revisited, Exploring and verifying specimen functionality and purpose, Event reconstruction and artifact review: File system, Registry, Process and Network Activity Post-run Data analysis.

TOTAL: 45 HOURS

REFERENCES

1. Malware Forensics Investigating and Analyzing Malicious code-James M. Aquilina, EoghanCasey,Cameron H. Malin, Syngress Publishing, 2008
2. Malware Analyst's Cookbook Tools and Techniques for fighting malicious code-Michael Hale Ligh, Steven Adair, Blake Hartstein, Matthew Richard, Wiley Publishing Inc, 2011
3. Unix and Linux Forensic Analysis DVD ToolKit - Chris Pogue, Cory Altheide, Todd Haverkos, Syngress Inc. , 2008
4. Windows Forensic Analysis DVD Toolkit- Harlan Carvey, Edition 2, Syngress Inc. , 2007
5. Windows Forensic Analysis- Harlan Carvey , Dave Kleiman, Syngress Inc. , 2007
6. Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry – Harlan Carvey, SyngressInc, Feb 2011
7. File System Forensic Analysis- Brian Carrier, Addison Wesley, Edition 1, 2005
8. Handbook of Digital Forensics and Investigation- Eoghan Casey, Academic Press,2009
10. Digital Forensics with Open Source Tools- Cory Altheide, Harlan Carvey, SyngressInc, Edition1, April 2011

CY45A7	OS FORENSICS	L	T	P	C
		3	0	0	3

OBJECTIVE

To understand how data acquisition is done from different operating Systems.

Course Outcome		Cognitive Skill
CO-01	Students will acquire the necessary skills to perform live response investigations in Windows environments	U, A
CO-02	Students will gain proficiency in conducting in-depth analysis of Windows systems by effectively analyzing memory dumps	R, A
CO-03	Students will acquire advanced skills in iOS Forensics Analysis.	U, A
CO-04	Students will able to perform Linux forensic analysis, including live response data collection, data analysis techniques	U, A
CO-05	Students will acquire advanced skills in Linux file analysis	U, A

R-Remember,U-Understand,A-Apply,An-Analyze,E-Evaluate, S-Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	M	L	L	M	L	L	L	M
CO-02	S	M	M	M	M	M	M	M
CO-03	M	M	L	M	M	L	M	M
CO-04	L	N	N	M	L	M	L	L
CO-05	S	M	S	S	M	M	S	S

S-Strong, M-Medium,L-Low,N-Not relevant

Unit I: Windows Forensic Analysis **9**

Windows Forensic Analysis- Live Response: Data Collection- Introduction, Locard's Exchange Principle, Order of Volatility, When to Perform Live Response ,What Data to Collect- System Time, Logged-on Users , Open Files, Network Information ,Network Connections ,Process Information, Process-to-Port Mapping, Process Memory, Network Status, Nonvolatile Informations. Live-Response Methodologies: Data Analysis, Agile Analysis.

Unit II: Windows Memory Analysis **12**

Windows Memory Analysis-Collecting Process Memory, Dumping Physical Memory, Alternative Approaches for Dumping Physical Memory, Analyzing a Physical Memory Dump. Registry Analysis, RegRipper, System Information, Autostart Locations, USB Removable Storage Devices, Mounted Devices, Portable Devices, Finding Users, Tracking User Activity, Redirection, Virtualization, Deleted Registry Keys. Windows File Analysis-Log Files, Event Logs, Recycle Bin, XP System Restore Points, Vista Volume Shadow Copy Service, File Metadata, File Signature Analysis, NTFS Alternate Data Streams, Alternative Methods of Analysis, Executable File Analysis- Static Analysis, Dynamic Analysis

Unit III: iOS Forensic Analysis **6**

History of Apple Mobile Devices, iOS Operating and File System Analysis - The iOS File System, HFS+ File System, HFSX, iPhone Partition and Volume Information, OS Partition, iOS System Partition, iOS Data Partition, SQLite Databases - iPhone Logical Acquisition, Logical Data Analysis

Unit IV: Linux Forensic Analysis **9**

Linux Forensic Analysis- Live Response Data Collection- Prepare the Target Media, Format the Drive, Gather Volatile Information, Acquiring the Image, Initial Triage and Live Response: Data Analysis- Log Analysis, Keyword Searches, User Activity, Network Connections, Running Processes, Open File Handlers, The Hacking Top Ten, Reconnaissance Tools

Unit V: Linux File Analysis **9**

The /Proc File System- Introduction, Process IDs, File Analysis- The Linux Boot Process, System and Security Configuration Files- Users, Groups, and Privileges, Cron Jobs , Log Files, Identifying Other Files of Interest- . SUID and SGID Root Files, Recently Modified/Accessed/Created Files, Modified System Files, Out -of-Place inodes, Hidden Files and Hiding Places.

TOTAL: 45 HOURS

REFERENCES

1. Unix and Linux Forensic Analysis DVD ToolKit - Chris Pogue, Cory Altheide, ToddHaverkos, Syngress Inc. , 2008
2. Windows Forensic Analysis DVD Toolkit- Harlan Carvey, Edition 2, Syngress Inc.,2009
3. Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry - Harlan Carvey, SyngressInc, Feb 2011
4. File System Forensic Analysis- Brian Carrier, Addison Wesley, Edition 1, 2005
5. Handbook of Digital Forensics and Investigation- Eoghan Casey, Academic Press, 2009
6. Digital Forensics with Open Source Tools- Cory Altheide, Harlan Carvey, SyngressInc, Edition 1, April 2011
7. "iOS Forensic Analysis: for iPhone, iPad, and iPod Touch" - Sean Morrissey, 2010
8. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=6766b849a7a0c71accc8f5e02bc7106d2a88ebcc

CY45A8	VIRTUAL FORENSICS	L	T	P	C
		3	0	0	3

OBJECTIVES

Develop theoretical Foundations of virtualization, concepts and different categories of virtualization, fundamentals of investigating live virtual environments and the different challenges faced in virtualization

Course Outcome		Cognitive Skill
CO-01	Students will be able to effectively utilize virtualization technologies	U, A
CO-02	Students will be proficient in utilizing virtual desktops, virtual appliances, and virtualization hardware devices for forensic investigations	R, A
CO-03	students will possess the skills necessary to effectively investigate and analyze live virtual environments	U, An
CO-04	Students will be equipped with the expertise to effectively detect and handle rogue virtual machines and analyze virtual machine traces.	U, A
CO-05	Develop the knowledge and skills to analyze and address virtualization challenges	U, A

R-Remember,U-Understand,A-Apply,An-Analyze,E-Evaluate, S-Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	M	L	L	M	L	L	L	M
CO-02	S	M	M	M	M	M	M	M
CO-03	M	M	L	M	M	L	M	M
CO-04	L	N	N	M	L	M	L	L
CO-05	S	M	S	S	M	M	S	S

S-Strong, M-Medium,L-Low,N-Not relevant

Unit I: Virtualization **9**

Requirement of virtualization, How virtualization works- virtualizing operating systems, hardware platforms and servers, hypervisors- baremetal, embedded, hosted, categories of virtualization- full virtualization, para virtualization, hardware-assisted virtualization , operating system virtualization, application server virtualization , application virtualization , network virtualization , storage virtualization , service virtualization , benefits of virtualization, cost of virtualization, Purpose of server virtualization, server virtualization the bigger picture, differences between desktop and server virtualization, common virtual servers.

Unit II: Desktop Virtualization **9**

What is desktop virtualization, common virtual desktops, virtual appliances and forensics, virtual desktops as a forensic platform, portable virtualization-MajoPac, MokaFive, preconfigured virtual Environments, virtual appliance providers, Jumpbox virtual appliances, virtual Box, virtualization hardware devices, virtual privacy machine, virtual emulators. Investigating dead Virtual environments – Install files, Remnants, registry, Microsoft disk image format, data to look for

Unit III: Investigating Live Virtual Environments **9**

Fundamentals of investigating live virtual environments, artifacts, processes and ports, log files, VM memory usage, memory analysis, Microsoft analysis tools, trace collection for a virtual machine, separate swap files for different virtual machines in a host computer, profile based creation of virtual machine in a virtualization environment, system and methods for enforcing software license compliance with virtual machine as well as for improving memory locality of virtual machines, mechanisms for providing virtual machines for multiple users.

Unit IV: Rogue Virtual Machines **9**

Detecting Rogue virtual machines, alternate data streams and Rogue virtual machines, virtual machine traces- prefetch file, link files, registry files, imaging virtual machines, snapshots and snapshot files, VMotion, Identification and conversion tools, Environment to environment conversion. Virtual environment and compliance- standards, compliance, regulatory requirements, discoverability of virtual environment, legal and protocol document language, organizational chain of custody, data retention policies, backup and data recovery.

Unit V: **Virtualization Challenges** **9**

Virtualization challenges- Data Centers, Storage Area networks, Direct attached storage and network attached storage, cluster file systems, Analysis of cluster file systems, security considerations- technical guidance, VM threats, Hypervisors, virtual appliances, Malware and virtualization- detection, Red Pill, Blue Pill, No Pill, Other methods of finding VMs.

TOTAL: 45 HOURS

REFERENCES

1. Diane Barrett, Greg Kipper, "Virtualization and Forensics: A Digital Forensic Investigator's Guide to Virtual Environments", Elsevier Science & Technology, 2010
2. Introduction to Virtualization e-book
3. Venkata Josyula, Malcolm Orr & Greg Page,"Cloud Computing: Automating the Virtualized Data Center", Cisco Press, 2011
4. Dr Kumar Saurabh,"Cloud Computing : Insights into new- era infra structure", Wiley Publishers, April 2011
5. Hoff Christofer, Mogull Rich & Balding Craig, "Hacking Exposed: Virtualization & Cloud Computing: Secrets& Solutions", McGraw Hill,

CY45A9	SECURITY POLICIES AND GOVERNANCE	L	T	P	C
		3	0	0	3

OBJECTIVES

- To understand Information security concepts, risk management and its role in the organization.
- To explore about the security standards, regulations and laws.
- To learn how to develop, implement and maintain various types of Information Security policies.
- To know how to manage the security related aspects.
- To be familiar the role of Information Security governance and planning within the organizational context.

Course Outcome		Cognitive Skill
CO-01	Identify the roles of individuals in securing an organization's information assets and apply risk management to identify and reduce security risks.	U, A
CO-02	Analyze security policy terms and concepts and the state of an organization in respect to information security governance.	An
CO-03	Understands the process of developing, implementing and maintaining various types of Information Security Policies	U
CO-04	Develop policies stating management views on ethical and cultural standards and procedures within laws and regulations.	A
CO-05	Gains knowledge on the importance, benefits and desired outcomes of Information Security Governance	E

R-Remember,U-Understand,A-Apply,An-Analyze,E-Evaluate, S-Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	S	S	S	S	M	M	S	S
CO-02	S	M	M	S	S	M	M	M
CO-03	M	S	M	L	S	N	L	M
CO-04	S	M	L	S	L	S	N	S
CO-05	S	S	M	M	N	S	M	S

S-Strong, M-Medium,L-Low,N-Not relevant

Unit I: Information Security Overview **9**

Importance of Information Protection – Evolution of Information Security – Justifying Security Investment – Security Methodology – Building a Security Program - Risk Analysis: Threat Vectors, Sources and Targets – Types of Attacks – Risk Analysis.

Unit II: Compliance with Standards, Regulations and Laws **9**

Information Security Standards – Regulations affecting Information Security Professionals – Laws affecting Information Security Professionals – Secure Design Principles: The CIA Triad – Defense Models – Zones of Trust – Best Practices for Network Defense.

Unit III: Security Policies and Standards **9**

Security policies – Security Awareness – Enforcement – Computer and Network policies – Data privacy and Integrity policies – Personnel and Security Management Policies – Physical Security Policies – Security Standards – Security Procedures –Security Guidelines.

Unit IV: Security Management **9**

Security Leaders Library – Seven Competencies for Effective Security Leadership – Security Functions – Assessing Risk – Implement policies and Control Functions – Promote Awareness Functions – Monitor and Evaluate Functions – Security Council – Risk Management Process – Risk Mitigation Options.

Unit V : Security Governance **9**

Security Control Frameworks – Security Control Frameworks and Standards – Managerial Controls – Technical Controls – Operational Controls – End user Security Awareness Training – Delivering the Message – The Law and Information Security – Recent Security Incidents.

TOTAL: 45 HOURS

TEXTBOOKS

1. Todd Fitzgerald, "Information Security Governance Simplified: From the Boardroom to the Keyboard, CRC Press, Taylor & Francsis Group, 2012.
2. Mark Rhodes–Ousley, "Information Security-The Complete Reference", The McGraw Hill Companies, Second Edition, 2013.

REFERENCES

1. Alan Calder, Steve Watkins, "IT Governance - An International Guide to Data Security and ISO27001/ISO27002", KoganPage, Seventh Edition, 2020.
2. Sari Stern Greene, "Security Program and Policies, Principles and Practices", Pearson Education, 2014.
3. Harold F. Tipton, Micki Krause, "Information Security Management Handbook", Taylor & Francis Group, Sixth Edition, 2008.

CY45B1	INTRUSION DETECTION AND PREVENTION SYSTEM	L	T	P	C
		3	0	0	3

OBJECTIVES

- To understand the vulnerabilities and detection techniques of various attacks.
- To acquire fundamental knowledge on mathematical foundations on various intrusion detection algorithms.
- To study the working principles of various architecture of intrusion detection.
- To design a typical intrusion detection system.
- To apply intrusion detection tools to detect intrusion.

Course Outcome		Cognitive Skill
CO-01	Understand basics of intrusion detection and detection approaches.	U
CO-02	Learn the fundamental concepts of IDS technologies.	U
CO-03	Interpret the mathematical foundations on various intrusion detection algorithms.	A
CO-04	Gain knowledge about working principles of various architecture of intrusion detection and measure intrusion detection risk.	A
CO-05	Apply intrusion detection tools to detect intrusion and specify the law related to the attack.	A

R-Remember,U-Understand,A-Apply,An-Analyze,E-Evaluate, S-Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	S	S	M	M	S	S	S	S
CO-02	S	S	M	M	S	S	S	S
CO-03	S	S	M	M	S	S	S	S
CO-04	S	S	M	M	S	S	S	S
CO-05	S	S	M	M	S	S	S	S

S-Strong, M-Medium,L-Low,N-Not relevant

Unit I: Introduction **9**

Understanding Intrusion Detection – Intrusion Detection and Prevention basics – IDS and IPS analysis schemes, Attacks, Detection approaches –Misuse detection – anomaly detection – specification based detection – hybrid detection

Unit II: IDS Technologies **9**

Components and Architecture - Security capabilities - Information gathering capabilities, Logging capabilities, Detection and Prevention capabilities, Network based IDS -Components and Architecture, Host based IDS -Components and Architecture, Network Behavior Analysis System.

Unit III: Theoretical Foundations of Detection **9**

Taxonomy of anomaly detection system – fuzzy logic – Bayes theory – Artificial Neural networks – Support vector machine – Evolutionary computation – Association rules – Clustering

Unit IV: Architecture and Implementation **9**

Centralized – Distributed – Cooperative Intrusion Detection - Tiered architecture – Justifying Intrusion detection- Intrusion detection in security – Threat Briefing – Quantifying risk – Return on Investment.

Unit V: Applications and Tools **9**

Tool Selection and Acquisition Process - Bro Intrusion Detection – Prelude Intrusion Detection - Cisco Security IDS - Snorts Intrusion Detection – NFR security. Legal Issues and Organizations Standards: Law Enforcement / Criminal Prosecutions – Standard of Due Care – Evidentiary Issues, Organizations and Standardizations.

TOTAL: 45 HOURS

REFERENCES

1. Ali A. Ghorbani, Wei Lu, "Network Intrusion Detection and Prevention: Concepts and Techniques", Springer, 2010.
2. Carl Enrolf, Eugene Schultz, Jim Mellander, "Intrusion detection and Prevention", Tata McGraw Hill, 2006
3. Paul E. Proctor, "The Practical Intrusion Detection Handbook ", Prentice Hall, 2001.
4. AnkitFadia and MnuZacharia, "Intrusion Alert", Vikas Publishing house Pvt., Ltd, 2007.
5. Earl Carter, Jonathan Hogue, "Intrusion Prevention Fundamentals", Pearson Education, 2006.
6. Christopher Kruegel, Fredrik Valeur, Giovanni Vigna: ―Intrusion Detection and Correlation Challenges and Solutions‖, 1st Edition, Springer, 2005
7. Karen Scarfone, Peter Mell," Guide to Intrusion Detection and Prevention Systems (IDPS)", NIST special publication, 2007

CY45B2	CYBER WARFARE	L	T	P	C
		3	0	0	3

OBJECTIVES

- To attain idea on how to identify and defend the network against malicious attacks.
- To know about the relevant technical and factual information on cyber warfare strategies.
- To know about the ethics, laws and consequences of cyber war and how computer criminal law may change as a result.

- To know the participants, battlefields and the tools and techniques used into day's digital conflicts and how to detect and defend against espionage, hacktivism, insider threats and non-state actors such as organized criminals and terrorists.
- Tolearnsomeexamplesandreal-worldguidanceonhowtoidentifyanddefendanetwork against cyber-attacks.

Course Outcome		Cognitive Skill
CO-01	Able to understand the cyber warfare related concepts.	U, R
CO-02	Analyze and use various logical and physical tools.	A, An
CO-03	Obtain knowledge in computer network exploitation, attack and defense.	U , R
CO-04	Understand the legal and ethical systems and analyze how the current laws impact cyber warfare.	U, An
CO-05	Create solutions for cyber challenges.	S

R-Remember,U-Understand,A-Apply,An-Analyze,E-Evaluate, S-Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	S	S	M	M	S	S	M	S
CO-02	M	M	S	S	S	S	S	S
CO-03	M	S	S	M	S	S	S	S
CO-04	M	M	S	S	S	S	S	S
CO-05	M	S	S	S	S	S	S	S

S-Strong, M-Medium,L-Low,N-Not relevant

Unit I: Introduction **9**

Cyber Warfare, Cyber Threatscape –Attack Methodology, Threats and Major Categories of Threats, Defense in Depth. Cyberspace Battle Field – Boundaries, War-Fighting Domains,

Threat Actors. Cyber Doctrine– Strategy, Guidance and Directives, Operations. Cyber Warriors –Cyber Warfare Forces, Staffing for cyber war.

Unit II: Logical and Physical Weapons **9**

Logical Weapons –Reconnaissance Tools, Scanning Tools, Access and Escalation Tools, Exfiltration Tools, sustainment tools, Assault Tools, Obfuscation Tools. Physical Weapons – Infrastructure concerns, Supply Chain concerns, Tools for Physical Attack and Defense. Psychological –Social Engineering, Military Approaches and Defense against social Engineering.

Unit III: Computer Network in Warfare **9**

Computer network exploitation –Intelligence and counter intelligence, reconnaissance, surveillance. Computer network attack–waging war modes, attack processes. Computer Network Defense–security awareness and training, modes of defending against cyber attacks.

Unit IV: Legal and Ethical System **9**

Non-State Actors – Individual Actors, Corporations, Cyber Terrorism, Organized Cyber Crime, Autonomous Actors, Legal System Impacts- legal systems –privacy impacts, Digital Forensics, Ethics in Cyber Warfare -Just War Theory.

Unit V: Case Studies **9**

Cyber Space Challenges, Future of Cyber War, Unmanned Aerial Vehicle. Case Studies: Cyber Warfare against Industry, Cyber Attacks against Electrical Infrastructure, cyber attacks against Nuclear Facilities.

TOTAL: 45 HOURS

REFERENCES

1. Jason Andress, Steve Winterfeld and Lillian Ablon, “Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners”, Second Edition, Elsevier, 2014.
2. Mike Chapple and David Seidl, “Cyber warfare: Information Operations in a Connected World”, Jones & Bartlett Publishers, 2014.
3. Paulo Shakarian, Jana Shakarian and Andrew Ruef, “Introduction to Cyber-Warfare: A Multidisciplinary Approach”, Elsevier, 1st Edition, 2013.
4. George Loukas, “Cyber-Physical Attacks: A Growing Invisible Threat”, Elsevier, 2015.

OPEN ELECTIVES

SI.No.	SUBJECT CODE	SUBJECT NAME	L	T	P	C
1	OE35D1	Research Methodology and IPR	2	0	0	2
2	OE35D2	Business Analytics	3	0	0	3
3	OE35D3	Industrial Safety	3	0	0	3
4	OE35D4	Operations Research	3	0	0	3
5	OE35D5	Composite Materials	3	0	0	3
6	OE35D6	Waste to Energy	3	0	0	3

OE35D1	RESEARCH METHODOLOGY & IPR	L	T	P	C
		2	0	0	2

OBJECTIVE

To learn about the methodologies followed in research and to get aware of the intellectual property rights.

Course Outcome		Cognitive Skill
CO-01	Students are able to illustrate research problem formulation.	U
CO-02	Students are able to analyze research related information and research ethics.	An
CO-03	Students are able to Correlate the results of any research article with other published results and write a review article in the field of engineering.	A
CO-04	Students are able to explain why intellectual property rights (IPR) will play such a significant role in the development of people and nations, and briefly discuss the necessity to spread awareness of IPR among students in general and engineers in particular.	U
CO-05	Students are able to discuss how IPR protection encourages innovators to conduct additional research and invest in R & D, which results in the development of new and improved products, which in turn leads to economic growth and societal benefits.	U

R-Remember,U-Understand,A-Apply,An-Analyze,E-Evaluate, S-Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	S	M	M	M	S	S	S	M
CO-02	S	S	M	M	S	S	S	S
CO-03	S	S	S	M	S	S	S	S
CO-04	S	S	S	M	S	S	S	S
CO-05	S	S	S	M	S	S	S	S

S-Strong, M-Medium,L-Low,N-Not relevant

Unit I: Research Methodology **6**

Meaning of research problem, Sources of research problem, Criteria and Characteristics of a good research problem, Errors in selecting a research problem, Scope and objectives of research problem. Approaches of investigation of solutions for research problem, data collection, analysis, interpretation, Necessary instrumentations.

Unit II: Literature Survey and Ethics **6**

Effective literature studies approaches - analysis Plagiarism - Research ethics.

Unit III: Technical Writing **6**

Effective technical writing - how to write a manuscript/ responses to reviewers comments - preparation of research article/ research report - Writing a Research Proposal - presentation and assessment by a review committee.

Unit IV: Intellectual Property Rights **6**

Nature of Intellectual Property: Patents, Designs, Trade Mark and Copyright - Process of Patenting and Development: technological research, innovation, patenting & development - Procedure for grants of patents - Patenting under PCT.

Unit V: Patent Rights and New Developments in IPR **6**

Scope of Patent Rights - Licensing and transfer of technology - Patent information and databases - Geographical Indications - New Developments in IPR: Administration of Patent System - New developments in IPR - IPR of Biological Systems - Computer Software etc - Traditional knowledge.

TOTAL: 30 HOURS

TEXT BOOKS

1. C.R.Kothari, "Research Methodology", 3rd Edition, New Age International, 2017.
2. Ranjit Kumar, "Research Methodology – A Step by Step for Beginner's", 2nd Edition, Pearson, Education, 2016.
3. Ann M. Korner, Guide to Publishing a Scientific paper, Bioscript Press 2004.
4. T. Ramappa, "Intellectual Property Rights Under WTO", S. Chand, 2008.
5. Kompal Bansal & Parshit Bansal, "Fundamentals of IPR for Beginner's", 1st Edition, BS Publications, 2016.

REFERENCES

1. Kothari, C. R. Research Methodology - Methods and Techniques, New Age International publishers, New Delhi, 2004.
2. Stuart Melville and Wayne Goddard, "Research methodology: an introduction for science & engineering students', Juta & Company, 1996.
3. Robert P. Merges, Peter S. Menell and Mark A. Lemley, "Intellectual Property in New Technological Age", Aspen Publishers, 2016.
4. Halbert, "Resisting Intellectual Property", Taylor & Francis Ltd ,2007.
5. Mayall , "Industrial Design", McGraw Hill, 1992.
6. Niebel , "Product Design", McGraw Hill, 1974. 7. Asimov , "Introduction to Design", Prentice Hall, 1962.

WEB RESOURCES

1. https://nptel.ac.in/courses/106/105/106105077/

OE35D2	BUSINESS ANALYTICS	L	T	P	C
		3	0	0	3

OBJECTIVE

To make students understandable about the Regression Analysis, Business analytics, forecasting and decision analysis.

Course Outcome		Cognitive Skill
CO-01	Analyze business data using statistical tools.	An
CO-02	Apply trend analysis and regression to make informed decisions.	A

CO-03	Design organizational structures for effective business analytics.	A
CO-04	Utilize forecasting techniques for prediction and decision-making.	U,A,An
CO-05	Employ decision analysis methods and stay updated on recent trends in business intelligence and data storytelling	A,An

R-Remember,U-Understand,A-Apply,An-Analyze,E-Evaluate, S-Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	M	M	S	M	S	S	S	M
CO-02	S	M	S	S	S	S	S	M
CO-03	M	M	S	M	S	S	S	M
CO-04	S	M	M	S	S	S	S	M
CO-05	M	M	S	S	S	S	S	M

S-Strong, M-Medium,L-Low,N-Not relevant

Unit I **9**

Business analytics: Overview of Business analytics, Scope of Business analytics, Business Analytics Process, Relationship of Business Analytics Process and organisation, competitive advantages of Business Analytics.

Statistical Tools: Statistical Notation, Descriptive Statistical methods, Review of probability distribution and data modelling, sampling and estimation methods overview.

Unit II **9**

Trendiness and Regression Analysis: Modelling Relationships and Trends in Data, simple Linear Regression.

Important Resources, Business Analytics Personnel, Data and models for Business analytics, problem solving, Visualizing and Exploring Data, Business Analytics Technology.

Unit III **9**

Organization Structures of Business analytics, Team management, Management Issues, Designing Information Policy, Outsourcing, Ensuring Data Quality, Measuring contribution of Business analytics, Managing Changes. Descriptive Analytics, predictive

analytics, predicative Modelling, Predictive analytics analysis, Data Mining, Data Mining Methodologies, Prescriptive analytics and its step in the business analytics Process, Prescriptive Modelling, nonlinear Optimization.

Unit IV **9**

Forecasting Techniques: Qualitative and Judgmental Forecasting, Statistical Forecasting Models, Forecasting Models for Stationary Time Series, Forecasting Models for Time Series with a Linear Trend, Forecasting Time Series with Seasonality, Regression Forecasting with Casual Variables, Selecting Appropriate Forecasting Models.
Monte Carlo Simulation and Risk Analysis: Monte Carle Simulation Using Analytic Solver Platform, New-Product Development Model, Newsvendor Model, Overbooking Model, Cash Budget Model.

Unit V **9**

Decision Analysis: Formulating Decision Problems, Decision Strategies with the without Outcome Probabilities, Decision Trees, The Value of Information, Utility and Decision Making, Recent Trends in : Embedded and collaborative business intelligence, Visual data recovery, Data Storytelling and Data journalism.

TOTAL: 45 HOURS

REFERENCES

1. Business analytics Principles, Concepts, and Applications by Marc J. Schniederjans, Dara G. Schniederjans, Christopher M. Starkey, Pearson FT Press.
2. Business Analytics by James Evans, persons Education.

OE35D3	INDUSTRIAL SAFETY	L	T	P	C
		3	0	0	3

OBJECTIVE

To make students understandable about the Industrial safety, Maintenance and fault tracing.

Course Outcome		Cognitive Skill
CO-01	Identify and mitigate industrial safety hazards effectively.	U,An,A
CO-02	Apply maintenance engineering principles to optimize equipment performance.	A
CO-03	Implement strategies for wear reduction and corrosion prevention.	A
CO-04	Utilize fault tracing techniques to diagnose equipment problems efficiently.	R,A,An
CO-05	Develop and execute periodic and preventive maintenance programs for machinery and equipment	A

R-Remember,U-Understand,A-Apply,An-Analyze,E-Evaluate, S-Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	S	M	S	M	S	M	S	M
CO-02	S	M	S	M	S	M	S	M
CO-03	M	L	S	M	S	M	S	M
CO-04	M	M	S	M	S	M	S	M
CO-05	M	M	S	M	S	M	S	M

S-Strong, M-Medium,L-Low,N-Not relevant

Unit I **9**

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 fire fighting, equipment and methods.

Unit II **9**

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 **9**

Wear and Corrosion and their prevention: Wear- types, causes, effects, wear reduction methods, lubricants-types and applications, Lubrication methods, general sketch, working and applications, i. Screw down grease cup, ii. Pressure grease gun, iii. Splash lubrication, iv. Gravity lubrication, v. Wick feed lubrication vi. Side feed lubrication, vii. Ring lubrication, Definition, principle and factors affecting the corrosion. Types of corrosion, corrosion prevention methods.

Unit IV **9**

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, I. Any one machine tool, ii. Pump iii. Air compressor, iv. Internal combustion engine, v. Boiler, vi. Electrical motors, Types of faults in machine tools and their general causes.

Unit V **9**

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: I. Machine tools, ii. Pumps, iii. Air compressors, iv. Diesel generating (DG) sets, Program and schedule of preventive maintenance of mechanical and electrical equipment, advantages of preventive maintenance. Repair cycle concept and importance.

TOTAL: 45 HOURS

REFERENCES

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

OE35D4	OPERATIONS RESEARCH	L	T	P	C
		3	0	0	3

OBJECTIVE

To make students understandable about the optimization techniques

Course Outcome		Cognitive Skill
CO-01	Students will be able to formulate and solve optimization problems using simplex method, sensitivity analysis, and parametric programming.	R,A
CO-02	Students will be able to apply linear programming to model real-world scenarios, understand duality theory, and analyze sensitivity.	A
CO-03	Students will be able to solve nonlinear programming problems with Kuhn-Tucker conditions.	U,A
CO-04	Students will be able to develop scheduling and sequencing models for resource utilization and inventory control.	A
CO-05	Students will be able to apply competitive modeling, dynamic programming, and game theory to optimize decision-making in various scenarios.	A

R-Remember,U-Understand,A-Apply,An-Analyze,E-Evaluate, S-Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	S	M	M	M	L	S	S	S
CO-02	M	S	M	S	S	L	M	M
CO-03	M	S	S	M	L	L	L	M
CO-04	S	S	M	M	L	L	L	L
CO-05	M	S	M	S	L	L	L	L

S-Strong, M-Medium,L-Low,N-Not relevant

Unit I **9**

Optimization Techniques, Model Formulation, models, General L.R Formulation, Simplex Techniques, Sensitivity Analysis, Inventory Control Models.

Unit II **9**

Formulation of a LPP - Graphical solution revised simplex method - duality theory - dual simplex method - sensitivity analysis - parametric programming.

Unit III **9**

Nonlinear programming problem - Kuhn-Tucker conditions min cost flow problem - max flow problem - CPM/PERT.

Unit IV **9**

Scheduling and sequencing - single server and multiple server models - deterministic inventory models - Probabilistic inventory control models - Geometric Programming.

Unit V **9**

Competitive Models, Single and Multi-channel Problems, Sequencing Models, Dynamic Programming, Flow in Networks, Elementary Graph Theory, Game Theory Simulation.

TOTAL: 45 HOURS

REFERENCES

1. H.A. Taha, Operations Research, An Introduction, PHI, 2008
2. H.M. Wagner, Principles of Operations Research, PHI, Delhi, 1982.
3. J.C. Pant, Introduction to Optimisation: Operations Research, Jain Brothers, Delhi, 2008
4. Hitler Libermann Operations Research: McGraw Hill Pub. 2009
5. Pannerselvam, Operations Research: Prentice Hall of India 2010
6. Harvey M Wagner, Principles of Operations Research: Prentice Hall of India 2010

OE35D5	COMPOSITE MATERIALS	L	T	P	C
		3	0	0	3

OBJECTIVE

To make students understandable about the material characteristics, processing and classifications of composite materials.

Course Outcome		Cognitive Skill
CO-01	Students will be able to understand the classification, characteristics, and advantages of composite materials, along with their applications in various industries.	U,R
CO-02	Students will be able to demonstrate knowledge of different reinforcements used in composites and their preparation methods, properties, and applications.	A
CO-03	Students will be able to gain proficiency in manufacturing metal matrix composites, ceramic matrix composites, and polymer matrix composites, including understanding the processes involved and their resulting properties.	R,U
CO-04	Students will be able to analyze the mechanical behavior and strength of composite materials, including failure criteria and design considerations for laminated structures.	An
CO-05	Students will be able to apply learned concepts to solve real-world problems related to the design, manufacturing, and application of composite materials in engineering projects.	A

R-Remember,U-Understand,A-Apply,An-Analyze,E-Evaluate, S-Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	S	M	M	M	L	S	S	S
CO-02	M	S	M	S	S	L	M	M
CO-03	M	S	S	M	L	L	L	M
CO-04	S	S	M	M	L	L	L	L
CO-05	M	S	M	S	L	L	L	L

S-Strong, M-Medium,L-Low,N-Not relevant

Unit I: Introduction **9**

Definition – Classification and characteristics of Composite materials. Advantages and application of composites. Functional requirements of reinforcement and matrix. Effect of reinforcement (size, shape, distribution, volume fraction) on overall composite performance.

Unit II: Reinforcements **9**

Preparation-layup, curing, properties and applications of glass fibers, carbon fibers, Kevlar fibers and Boron fibers. Properties and applications of whiskers, particle reinforcements. Mechanical Behavior of composites: Rule of mixtures, Inverse rule of mixtures. Isostrain and Isostress conditions.

Unit III: Manufacturing Of Metal Matrix Composites **9**

Casting – Solid State diffusion technique, Cladding – Hot isostatic pressing. Properties and applications. Manufacturing of Ceramic Matrix Composites: Liquid Metal Infiltration – Liquid phase sintering. Manufacturing of Carbon – Carbon composites: Knitting, Braiding, Weaving. Properties and applications.

Unit IV: Manufacturing Of Polymer Matrix Composites **9**

Preparation of Moulding compounds and prepregs – hand layup method – Autoclave method – Filament winding method – Compression moulding – Reaction injection moulding. Properties and applications.

Unit V: Strength **9**

Laminar Failure Criteria-strength ratio, maximum stress criteria, maximum strain criteria, interacting failure criteria, hygrothermal failure. Laminate first play failure-insight strength; Laminate strength-ply discount truncated maximum strain criterion; strength design using caplet plots; stress concentrations.

TOTAL: 45 HOURS

TEXT BOOKS

1. Material Science and Technology – Vol 13 – Composites by R.W.Cahn – VCH, West Germany.
2. Materials Science and Engineering, An introduction. WD Callister, Jr., Adapted by R. Balasubramaniam, John Wiley & Sons, NY, Indian edition, 2007.

REFERENCES

1. Hand Book of Composite Materials-ed-Lubin.
2. Composite Materials – K.K.Chawla.
3. Composite Materials Science and Applications – Deborah D.L. Chung.
4. Composite Materials Design and Applications – Danial Gay, Suong V. Hoa, and Stephen W. Tasi.

OE35D6	WASTE TO ENERGY	L	T	P	C
		3	0	0	3

OBJECTIVE

To make students understandable about the gasification process, bio materials and its design considerations.

Course Outcome		Cognitive Skill
CO-01	Students will be able to identify and classify waste types for energy generation.	U,A,An
CO-02	Students will be able to apply biomass pyrolysis and gasification techniques.	A
CO-03	Students will be able to understand biomass combustion principles and technologies.	U
CO-04	Students will be able to analyze biogas properties, plant technology, and applications.	An
CO-05	Students will be able to evaluate biomass conversion processes and related energy programs.	E

R-Remember,U-Understand,A-Apply,An-Analyze,E-Evaluate, S-Synthesis

Mapping of Course Outcome with Programme Outcome

PO / CO	PO-A	PO-B	PO-C	PO-D	PO-E	PO-F	PO-G	PO-H
CO-01	S	M	M	M	L	S	S	S
CO-02	M	S	M	S	S	L	M	M
CO-03	M	S	S	M	L	L	L	M
CO-04	S	S	M	M	L	L	L	L
CO-05	M	S	M	S	L	L	L	L

S-Strong, M-Medium,L-Low,N-Not relevant

Unit I: Introduction to Energy from Waste **9**

Classification of waste as fuel – Agro based, Forest residue, Industrial waste - MSW – Conversion devices – Incinerators, gasifiers, digestors.

Unit II: Biomass Pyrolysis **9**

Pyrolysis – Types, slow fast – Manufacture of charcoal – Methods - Yields and application – Manufacture of pyrolytic oils and gases, yields and applications.

Unit III: Biomass Gasification **9**

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 **9**

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 **9**

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.

TOTAL: 45 HOURS

REFERENCES

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.