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 2021

# NOORUL ISLAM CENTRE FOR HIGHER EDUCATION, Kumaracoil

## Regulation: 2021

## 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. Mould 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 : 71**

## CURRICULUM & SYLLABI

### SEMESTER I

| Sl. No | Course Code | Course Title | L | T | P | C |
|---|---|---|---|---|---|---|
| **THEORY** | | | | | | |
| 1. | MA3505 | Operation Research | 3 | 1 | 0 | 4 |
| 2. | CY3501 | Advanced Data Structures and Algorithms | 3 | 1 | 0 | 4 |
| 3. | CY3502 | Advanced Operating System and Security | 3 | 0 | 0 | 3 |
| 4. | CY3503 | Cyber Security Threats | 3 | 0 | 0 | 3 |
| 5. | PEC | Elective I | 3 | 0 | 0 | 3 |
| 6. | PEC | Elective II | 3 | 0 | 0 | 3 |
| **PRACTICAL** | | | | | | |
| 7. | CY3571 | Operating System and Data Structures Lab | 0 | 1 | 2 | 2 |
| **TOTAL** | | | **18** | **2** | **1** | **22** |

### SEMESTER II

| Sl. No | Course Code | Course Title | L | T | P | C |
|---|---|---|---|---|---|---|
| **THEORY** | | | | | | |
| 1. | CY3504 | Cybercrime Investigations and Digital Forensics | 3 | 0 | 0 | 3 |
| 2. | CY3505 | Database Design and Security | 3 | 1 | 0 | 4 |
| 3. | CY3506 | Cyber Law and Security Policies | 3 | 0 | 0 | 3 |
| 4. | CY3507 | Advanced Network Security | 3 | 1 | 0 | 3 |
| 5. | PEC | Elective III | 3 | 0 | 0 | 3 |
| 6. | PEC | Elective IV | 3 | 0 | 0 | 3 |
| **PRACTICAL** | | | | | | |
| 7. | CY3572 | Database and Cyber Security Lab | 0 | 1 | 2 | 2 |
| **TOTAL** | | | **18** | **1** | **2** | **21** |

## SEMESTER III

| Sl. No | Course Code | Course Title | L | T | P | C |
|---|---|---|---|---|---|---|
| **THEORY** | | | | | | |
| 1. | PEC | Elective V | 3 | 0 | 0 | 3 |
| 2. | OEC | Open Elective I | 3 | 0 | 0 | 3 |
| **PRACTICAL** | | | | | | |
| 3. | CY35P1 | Project work – Phase I | 0 | 0 | 12 | 6 |
| **TOTAL** | | | **8** | **0** | **12** | **12** |

## SEMESTER IV

| Sl. No | Course Code | Course Title | L | T | P | C |
|---|---|---|---|---|---|---|
| 1. | CY35P2 | Project work – Phase II | 0 | 0 | 32 | 16 |
| **TOTAL** | | | **0** | **0** | **32** | **16** |

## LIST OF ELECTIVES

| SI. NO. | COURSE CODE | COURSE TITLE | L | T | P | C |
|---|---|---|---|---|---|---|
| 1. | CY35A1 | Ethical Hacking | 3 | 0 | 0 | 3 |
| 2. | CY35A2 | Digital Watermarking and Steganography | 3 | 0 | 0 | 3 |
| 3. | CY35A3 | Biometric Security | 3 | 0 | 0 | 3 |
| 4. | CY35A4 | Intrusion Detection and Prevention System | 3 | 0 | 0 | 3 |
| 5. | CY35A5 | Forensics and Incident Response | 3 | 0 | 0 | 3 |
| 6. | CY35A6 | Pattern Recognition | 3 | 0 | 0 | 3 |
| 7. | CY35A7 | Biometric Image Processing | 3 | 0 | 0 | 3 |
| 8. | CY35A8 | Cyber Warfare | 3 | 0 | 0 | 3 |
| 9. | CY35A9 | Applied Cryptography | 3 | 0 | 0 | 3 |
| 10. | CY35B1 | Distributed Systems Security | 3 | 0 | 0 | 3 |
| 11. | CY35B2 | Cyber Criminology and Cyber Crimes | 3 | 0 | 0 | 3 |
| 12. | CY35B3 | Malware analysis | 3 | 0 | 0 | 3 |

## OPEN ELECTIVES

| | | |
|---|---|---|
| 1. GE35A1 | Business Analytics | 3 0 0 3 |
| 2. GE35A2 | Industrial Safety | 3 0 0 3 |
| 3. GE35A3 | Operations Research | 3 0 0 3 |
| 4. GE35A4 | Cost Management of Engineering Projects | 3 0 0 3 |
| 5. GE35A5 | Composite Materials | 3 0 0 3 |
| 6. GE35A6 | Waste to Energy | 3 0 0 3 |

**Syllabus format**

**SEMESTER I**

| Sl. No | Course Code | Course Title | L | T | P | C |
|---|---|---|---|---|---|---|
| **THEORY** | | | | | | |
| 1. | MA3505 | Operation Research | 3 | 1 | 0 | 4 |
| 2. | CY3501 | Advanced Data Structures and Algorithms | 3 | 1 | 0 | 4 |
| 3. | CY3502 | Advanced Operating System and Security | 3 | 0 | 0 | 3 |
| 4. | CY3503 | Cyber Security Threats | 3 | 0 | 0 | 3 |
| 5. | PEC | Elective I | 3 | 0 | 0 | 3 |
| 6. | PEC | Elective II | 3 | 0 | 0 | 3 |
| **PRACTICAL** | | | | | | |
| 7. | CY3571 | Operating System and Data Structures Lab | 0 | 1 | 2 | 2 |
| **TOTAL** | | | **18** | **2** | **1** | **22** |

| MA3505 | OPERATION RESEARCH | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | 1 | 0 | 4 |

**OBJECTIVE**

To develop mathematical skill to analyze various complex problems and to study the applications of operations research in functional areas of computing like network scheduling, queueing and simulation.

| Course Outcome | | Cognitive Skill |
|---|---|---|
| CO-01 | To formulate lpp, solve lpp using graphical method, simplex method, artificial variable technique, two phase method, to solve transportation and assignment problem. | U, R, A,E |
| CO-02 | To understand Bellman principles, characteristics of dynamic programming and solving by recursive method and application problems like allocation problems, cargo loading problems and shortest route problems. | U, R, A,E |
| CO-03 | Solving queuing problems in single and multi-server models by applying Littles formula. | U, R, A,E |

| | | |
|---|---|---|
| CO-04 | To solve network problems using critical path method and project evaluation and review techniques, solving shortest route problems, | U, R, A,E |
| CO-05 | Able to simulate real life problems using Monte Carlo simulation, generating random number using congruent techniques and apply simulation to solve queuing problems. | U, R, A,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: Linear Programming** **9**

Formulation Graphical solution Simplex method Artificial variable technique - Two Phase method - Transportation and Assignment problems.

**Unit II: Dynamic Programming** **9**

Bellmans principle of optimality Characteristics of the dynamic programming model The re-cursive equation - Backward and Forward approach Applications of Dynamic programming problem in Allocation problems, Shortest route problem and Cargo loading Problem.

**UnitIII: Queueing Models** **9**

Birth and Death Process - Poisson Process Markovian Queues Single Server Models Littles formula - Queues in Series Open Queueing Networks Closed Queueing networks.

**UnitIV: Network Model** **9**

Shortest Route, Minimal Spanning tree and Maximal flow models Critical Path Method Project Evaluation and Review Technique.

**UnitV: Simulation** **9**

Discrete Event Simulation Stochastic Simulation - Monte Carlo Simulation Generation of Ran- dom Numbers using Congruent method Applications to Queueing systems.

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

**REFERENCES**


1. Taha, H.A. Operations Research: An Introduction, Ninth Edition, Pearson Education Edition, Asia, New Delhi, 2002.
2. Robertazzi. T.G. Computer Networks and Systems Queuing Theory and Performance Evaluation, Third Edition, Springer, 2002 Reprint.
3. S.S. Rao Optimization Techniques Prentice Hall of India , 2004.
4. J.K Sharma Operations Research Macmillan, 2003


| CY3501 | ADVANCED DATA STRUCTURES AND ALGOROTHMS | 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 | | Cognitive Skill |
|---|---|---|
| CO-01 | Student will be able to design and analyze programming problem statements. | An |
| CO-02 | Student will be able to choose appropriate data structures and algorithms, understand the ADTs, and use it to design algorithms for a specific problem. | A |
| CO-03 | Student will be able to learn various tree structures. | U |
| CO-04 | Student will be able to design algorithms using graph structures to solve real-life problems. | 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-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 | 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-Analyzing 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: Tree Structures** **9**

Binary search trees-AVL trees-Red-Black trees-B-Trees-Splay trees, HEAP STRUCTURES: Min/Max heaps-Leftist Heaps-Binomial Heaps-Fibonacci Heaps.

**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: 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, Multi-way Merge Sort, Polyphase Sorting - Design Techniques - Divide and Conquer - Dynamic Programming - Greedy Algorithm – Backtracking - Local Search Algorithms.

**TOTAL: 45 HOURS**

**REFERENCES**


1. Mark Allen Weiss, "Data Structures and Algorithm Analysis in C++", 4th Edition, Pearson Education, 2014.
2. Alfred V. Aho, John E. Hopcroft, Jeffrey D. Ullman, ―Data Structures and Algorithms, Pearson Education, Reprint 2006.
3. Robert Sedgewick and Kevin Wayne, ―ALGORITHMS‖, Fourth Edition, Pearson Education.
4. S.Sridhar,Design and Analysis of Algorithms‖, First Edition, Oxford University Press. 2014.
5. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein, Introduction to Algorithms‖, Third Edition, Prentice-Hall, 2011.
6. Horowitz, Sahni, Rajasekaran, "Computer Algorithms", Galgotia, 2000.

| CY3502 | ADVANCED OPERATING SYSTEM AND SECURITY | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | 0 | 0 | 3 |

**OBJECTIVES**

- To study the basic concepts and functions of operating system.
- To learn about processes, threads and scheduling algorithms.
- To learn the various memory management techniques and the related security schemes.
- To study about I/O management, file systems and its security.
- To study the security models and the concept of security evaluation.

| Course Outcome | | Cognitive Skill |
|---|---|---|
| CO-01 | Student will be able to learn the fundamentals of Operating Systems | U |
| CO-02 | Student will be able to understand and analyze the concepts and techniques in Process management that includes process scheduling, threads and inter process communication. | U, An |
| CO-03 | Student will gain in-depth knowledge on various mechanisms involved in memory management and on memory and address protection techniques. | U, An |
| CO-04 | Student will gain insight into various devices and file management techniques and file protection mechanisms. | U, An |
| CO-05 | Student will be able to gain knowledge on various security models and on the concept of security evaluation. | 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: Introduction** **9**

Operating System concepts – Functions – Structure of Operating system – Types of Operating System.

**Unit II: Process Management** **9**

Introduction to processes – Process Scheduling - Threads-CPU Scheduling objectives, criteria – Types of scheduling algorithms – Performance comparison – Inter process Communications-Synchronization – Semaphores – Dead lock Prevention, Recovery, Detection and Avoidance

**Unit III: Memory Management** **9**

Single contiguous allocation – Partitioned allocation – Paging – Virtual memory concepts – Swapping – Demand paging – Page Replacement Algorithms – Segmentation- protected objects and methods of protection – memory and address protection

**Unit IV: Device and File Management** **9**

Principles of I/O hardware – I/O software – Disks – Disk Scheduling Algorithms--File Systems - Files and Directories- File System Implementation - Allocation Methods, File Recovery-– control of access to general objects – file protection Mechanisms.

**Unit V: Security models and Security Evaluation** **9**

System Security Planning - Operating Systems Hardening -Application Security -Security Maintenance - Windows Security - Virtualization Security - The Bell-LaPadula Model for Computer Security - Other Formal Models for Computer Security -The Concept of Trusted Systems - Trusted Computing and the Trusted Platform Module - Common Criteria for Information Technology Security Evaluation - Assurance and Evaluation

**TOTAL: 45 HOURS**

**REFERENCES**


1. Silberschatz A, Galvin P, Gagne G, "Operating Systems Concepts", John Wiley & Sons, Singapore, 2013.
2. Michael Palmer, Guide to Operating Systems Security", Course Technology – Cengage Learning, New Delhi, 2008
3. Charles P. Pleeger, "Security in Computing", Prentice Hall, New Delhi, 2009
4. Deitel H M, "Operating Systems ", PHI/ Pearson Education, New Delhi, 2004.
5. Lawrie Brown, William Stallings, Computer Security: Principles and Practice, Third Edition, Pearson Education, 2015


| CY3503 | CYBER SECURITY THREATS | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | 0 | 0 | 3 |

**OBJECTIVES**

- To study various cybercrimes and cyber security threats.
- To understand the network threats and their vulnerabilities.
- To analyze the security threats and forensic analysis.
- To analyze the security elements and procedures.
- To evaluate the threat assessment and management techniques.

| Course Outcome | | Cognitive Skill |
|---|---|---|
| CO-01 | Students will understand the nature of cybercrimes, different types of crimes etc. | U |
| CO-02 | Students will get an idea about the network threats, their sources and consequences and vulnerabilities to assets. | U |
| CO-03 | Students can analyze security threats, correlation and awareness measures. | An |
| CO-04 | Students can analyze the various security elements, security policy requirements and procedures. | An |
| CO-05 | Can able to evaluate threat assessment and management techniques and also about critical infrastructure protection. | 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 | M | S | S | M | S |
| **CO-02** | S | M | M | S | M | S | S | M |
| **CO-03** | M | S | S | L | N | M | L | S |
| **CO-04** | S | M | M | S | S | L | M | S |
| **CO-05** | S | M | S | M | N | N | S | S |

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

**Unit I: Cyber Security Threats** **9**

Introduction to Cyber Crime – Cybercriminals - Classifications of Cyber Crime - Categories of Cyber Crime – Criminals plan on Attacks - Social Engineering - Cyber stalking – Botnets – Attack Vector

**Unit II: Network Threats** **9**

Password Cracking – Keyloggers and Spywares – Virus and Worms – Trojan Horses and Backdoors – Steganography – DoS and DDoS Attacks – SQL Injection – Buffer Overflow – Attacks on Wireless Networks – Phishing – Identity Theft

**Unit III: Security Threats** **9**

Introduction: Security threats - Sources of security threats - Security Threat Motives - Security Threat Management: Risk Assessment - Forensic Analysis - Security Threat Correlation – Security Threat Awareness – Sources of Vulnerabilities – Vulnerability Assessment

**Unit IV: Security Elements** **9**

Access Rights – Access Control Systems – Authorization – Types of Authorization Systems – Authorization Principles – Authorization Granularity – Authentication – Authentication Elements – Types of Authentication – Authentication Methods.

**Unit V: Threat Management and Critical Infrastructure** **9**

System Security Policy – Building a Security Policy - Security Requirements Specifications - Threat identification - Threat Analysis - Vulnerability Identification and Assessment – Security Certification – Security Monitoring and Auditing - Critical Infrastructure Protection.

**TOTAL: 45 HOURS**

**REFERENCES**


1. Nina Godbole, SunitBelapure, Cyber Security – Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley India Pvt. Ltd, 2011.
2. Joseph M Kizza, "Computer Network Security", Springer Verlag, 2005.
3. BernadetteH Schell, Clemens Martin, "Cyber Crime", ABC-CLIO Inc, California, 2004.
4. Swiderski, Frank and Syndex, "Threat Modeling", Microsoft Press, 2004.
5. William Stallings and Lawrie Brown, "Computer Security: Principles and Practice", Prentice Hall, Fourth Edition, 2018.
6. Thomas Calabres and Tom Calabrese, "Information Security Intelligence: Cryptographic Principles & Application", Thomson Delmar Learning, 2004.


| CY3571 | OPERATING SYSTEM AND DATA STRUCTURES LAB | L | T | P | C |
|---|---|---|---|---|---|
| | | 0 | 1 | 2 | 2 |

**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, De queue and Priority 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.
6. Implementation of Sort using Divide Conquer Method.
7. Implementation of Quick, Bubble, Radix and Heap Sort.
8. Implementation of Linear and Binary search.
9. Implement the following CPU Scheduling Algorithms.
    a. i) FCFS ii) Round Robin iii) Shortest Job First.
10. Implement Best fit, First Fit Algorithm for Memory Management.
11. Implement FIFO page Replacement Algorithm.
12. Implement LRU page Replacement Algorithm.
13. Implement the creation of Shared memory Segment.
14. 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. | CY3504 | Cybercrime Investigations and Digital Forensics | 3 | 0 | 0 | 3 |
| 2. | CY3505 | Database Design and Security | 3 | 1 | 0 | 4 |
| 3. | CY3506 | Cyber Law and Security Policies | 3 | 0 | 0 | 3 |
| 4. | CY3507 | Advanced Network Security | 3 | 1 | 0 | 3 |
| 5. | PEC | Elective III | 3 | 0 | 0 | 3 |
| 6. | PEC | Elective IV | 3 | 0 | 0 | 3 |
| **PRACTICAL** | | | | | | |
| 7. | CY3572 | Database and Cyber Security Lab | 0 | 1 | 2 | 2 |

| CY3504 | CYBERCRIME INVESTIGATIONS AND DIGITAL FORENSICS | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | 0 | 0 | 3 |

**OBJECTIVES**

- To learn cybercrime issues and related laws.
- To analyze various cybercrimes.
- To investigate cybercrimes using tools and techniques.
- To explore methodology of incident response and various security issues in internet world, and identify digital forensic tools for data collection.
- To recognize the importance of digital forensic tools for analysis to achieve adequate perspectives of digital forensic investigation in various applications devices like Windows/Unix system.
- To generate legal evidence and supporting investigation reports and use various digital forensic tools.
- To apply the knowledge of intrusion detection system to secure network and performing router and network analysis.

| Course Outcome | | Cognitive Skill |
|---|---|---|
| CO-01 | Students should able to understand cybercrime issues and related laws. | U |
| CO-02 | Students should able to analyze various cyber crimes. | An |
| CO-03 | Students should able to investigate cyber crimes using tools and techniques. | A |
| CO-04 | Students should able to explore methodology of incident response and various security issues in internet world, and identify digital forensic tools for data collection. | S |
| CO-05 | Students should able to recognize the importance of digital forensic tools for analysis to achieve adequate perspectives of digital forensic investigation in various applications /devices like Windows/Unix system. | 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** **9**

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, IP Tracking, 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. Drone forensics.

**Unit V: OPERATING SYSTEM FORENSICS** **9**

Windows System Forensics, Linux System Forensics, MAC system forensics, Mobile Phone OS Forensics: Android, IOS,Windows OS, BlackBerry, Network Forensics, Wireless Forensics, Bluetooth Forensics, Live Acquisitions.

**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. Robert M Slade," Software Forensics", Tata McGraw - Hill, New Delhi, 2005.
4. Bernadette H Schell, Clemens Martin, "Cybercrime", ABC – CLIO Inc, California, 2004.
5. "Understanding Forensics in IT ", NIIT Ltd, 2005.
6. John Sammons, "The Basics of Digital Forensics", 2nd Edition, Syngress,2014
7. Khalifa Al-Room , "Drone Forensics: A Case Study of Digital Forensic Investigations Conducted on Common Drone Models" , 2021,IGI Global Publications.


| CY3505 | DATABASE DESIGN AND SECURITY | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | 0 | 0 | 3 |

**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**

Authentication – password security, application security – securing database to database communications – secure replication mechanisms, encryption.

**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, Prentice Hall, Jan 14, 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.

| CY3506 | CYBER LAW AND SECURITY POLICIES | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | 0 | 0 | 3 |

**OBJECTIVES**

The students should be able:

- 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 standards and procedures | U |
| CO-05 | Student will gain knowledge on Internet Ethics, Information Technology Act And Legal Frame Work | 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 and Policies** **9**

Typical Tier 1 Policies -Typical Tier 2 Policies-Tools of Information Security -Information Processing- Information Security Program Administration

**Unit IV: Standards And Procedures** **9**

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 V: 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 -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

**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. Rick Lehtinen and G.T. Gangemi, "Computer Security Basics (Paperback)”, 2ndEdition, O’ Reilly Media, 2006.
4. Economic Laws Practice, 2017
5. PavanDuggal,” Cyber Laws”, Universal Law Publishing, 2016
6. Deborah G Johnson, Computer Ethics, Pearson Education, 2009
7. Thomas R Peltier, Justin Peltier and John blackley,” Information Security Fundamentals”, Prentice Hall, 2004


| CY3507 | 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 study various security services for Electronic Mail.
- 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.

| Course Outcome | | Cognitive Skill |
|---|---|---|
| CO-01 | Understand the basic concepts of IP security and to protect the data in Web. | U |
| CO-02 | Interpret the various security services for Electronic Mail. | U |
| CO-03 | Identify various kinds of security breaches and security vulnerability attacks in wireless networks. | An |
| CO-04 | Illustrate the process of Bluetooth security architecture and threats to Bluetooth security. | U |
| CO-05 | Apply modern cryptographic techniques to enhance overall system security. | 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: Web security considerations – Secure Socket Layer and Transport Layer Security – Secure electronic transaction – Bitcoin.

**Unit II: Electronic Mail Security** **9**

Store and forward – Security services for e-mail – Establishing keys – Privacy – Authentication of the Source – Message Integrity – Non-repudiation – Proof of submission and delivery - Pretty Good Privacy – Secure/Multipurpose Internet Mail Extension.

**Unit III: 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.

**Unit IV: 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 V: System Security** **9**

Intruders – Intrusion detection – Password management – Malicious Software: Viruses and related threats – Virus countermeasures – Firewalls: Firewall design principles – Firewall configurations – Trusted systems.

**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. Neal Krawetz, “Introduction to Network Security”, Thomson Learning, Boston, 2007.
8. https://bitcoin.org/bitcoin.pdf

| CY3572 | DATABASE AND CYBER SECURITY LAB | L | T | P | C |
|---|---|---|---|---|---|
| | | 0 | 1 | 2 | 2 |

**OBJECTIVES**

- To implement the Relational Database Management System concepts
- To make use of the aggregate functions and group functions to summarize data
- To implement access control methods
- To use the cryptographic algorithms to protect database
- To use digital signatures and hash functions to secure database

| Course Outcome | | Cognitive Skill |
|---|---|---|
| CO-01 | Implement basic DDL, DML and DCL commands | A |
| CO-02 | Use aggregate and group functions to summarize data | A |
| CO-03 | Design and implement access control rules to assign privileges and protect data in databases | A |
| CO-04 | Master the concepts of secret and public key cryptographic techniques | An |
| CO-05 | Understand how digital signatures are performed and the role of digital certificates in providing security | 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 | S | S | S | M |
| **CO-02** | S | S | S | S | S | S | S | M |
| **CO-03** | S | S | S | S | S | S | S | M |
| **CO-04** | S | S | S | S | S | S | S | M |
| **CO-05** | S | S | S | S | S | S | S | M |

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 International Data Encryption Algorithm
10. Implementation of Advanced Encryption Standard
11. Implementation of RSA Algorithm
12. Implementation of Diffie-Hellman Key Exchange
13. Implementation of Message Authentication Codes
14. Implementation of Hash functions
15. Implementation of Digital Signature Standard
16. 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 V | 3 | 0 | 0 | 3 |
| 2. | OEC | Open Elective I | 3 | 0 | 0 | 3 |
| **PRACTICAL** | | | | | | |
| 3. | CY35P1 | Project work – Phase I | 0 | 0 | 12 | 6 |
| **TOTAL** | | | **8** | **0** | **12** | **12** |

## SEMESTER IV

| Sl. No | Course Code | Course Title | L | T | P | C |
|---|---|---|---|---|---|---|
| 1. | CY35P2 | Project work – Phase II | 0 | 0 | 32 | 16 |
| **TOTAL** | | | **0** | **0** | **32** | **16** |

## LIST OF ELECTIVES

| SI. NO. | COURSE CODE | COURSE TITLE | L | T | P | C |
|---|---|---|---|---|---|---|
| 13. | CY35A1 | Ethical Hacking | 3 | 0 | 0 | 3 |
| 14. | CY35A2 | Digital Watermarking and Steganography | 3 | 0 | 0 | 3 |
| 15. | CY35A3 | Biometric Security | 3 | 0 | 0 | 3 |
| 16. | CY35A4 | Intrusion Detection and Prevention System | 3 | 0 | 0 | 3 |
| 17. | CY35A5 | Forensics and Incident Response | 3 | 0 | 0 | 3 |
| 18. | CY35A6 | Pattern Recognition | 3 | 0 | 0 | 3 |
| 19. | CY35A7 | Biometric Image Processing | 3 | 0 | 0 | 3 |
| 20. | CY35A8 | Cyber Warfare | 3 | 0 | 0 | 3 |
| 21. | CY35A9 | Applied Cryptography | 3 | 0 | 0 | 3 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 22. | CY35B1 | Distributed Systems Security | 3 | 0 | 0 | 3 |
| 23. | CY35B2 | Cyber Criminology and Cyber Crimes | 3 | 0 | 0 | 3 |
| 24. | CY35B3 | Malware analysis | 3 | 0 | 0 | 3 |

## OPEN ELECTIVES

| | | |
|---|---|---|
| 1. GE35A1 | Business Analytics | 3 0 0 3 |
| 2. GE35A2 | Industrial Safety | 3 0 0 3 |
| 3. GE35A3 | Operations Research | 3 0 0 3 |
| 4. GE35A4 | Cost Management of Engineering Projects | 3 0 0 3 |
| 5. GE35A5 | Composite Materials | 3 0 0 3 |
| 6. GE35A6 | Waste to Energy | 3 0 0 3 |

## ELECTIVES

| **CY25A1** | **ETHICAL HACKING** | **L** | **T** | **P** | **C** |
|---|---|---|---|---|---|
| | | **3** | **0** | **0** | **3** |

**OBJECTIVES**

- To prepare ethical hacking plan, find out different hacking methodologies and relate law related to the attack.
- To work with foot printing tools and 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 should able to prepare ethical hacking plan, find out different hacking methodologies and relate law related to the attack. | R |
| CO-02 | Students should able to work with foot printing tools and identify different social engineering techniques to gather information. | U |
| CO-03 | Students should able to work with port scanning, enumeration tools and analyze gathered information. | A |
| CO-04 | Students should able to explore hacking in web server and wireless network. | An |
| CO-05 | Students should able to identify the vulnerabilities and hack different operating system 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, Python 3 and Ethical Hacking.

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

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, Java OS, Android and NetWare Operating Systems.

**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.

**Unit V: Hacking Operating Systems** **9**

Windows: Vulnerabilities – Choosing Tools – Information Gathering – RPC – Null Sessions – Share Permissions – Hardcore Vulnerability Exploitation. Linux: Vulnerabilities – Information Gathering – Unconnected Services - .rhosts and hosts.equiv Files – NFS – File Permissions – Buffer Overflow. Hacking Applications**:** Messaging Systems – Web Applications – Mobile Applications - Databases - Reporting Results.

**TOTAL: 45 HOURS**

**REFERENCES**


1. Michael T. Simpson, "Ethical Hacking and Network Defense", Cengage Learning, New Delhi, 2010.
2. Kevin Beaver, "Hacking for Dummies", Wiley Publication, India, 2007.
3. AnkitFadia, "Unofficial Guide to Ethical Hacking", Macmillan Company, New Delhi, 2001.
4. SanjibSinha, "Beginning Ethical Hacking with Python", Apress, 2017


| CY35A2 | DIGITAL WATERMARKING AND STEGANOGRAPHY | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | 0 | 0 | 3 |

**OBJECTIVES**

- To learn the basic concepts of watermarking and steganography
- To understand embedding information and analysing its performance
- To learn various watermarking approaches and find the impact of attack
- To study the various type of steganography techniques and steganalysis

| Course Outcome | | Cognitive Skill |
|---|---|---|
| CO-01 | Discuss the need of watermarking. | U |
| CO-02 | Embedding information and analyzing errors. | An |
| CO-03 | Elaborate various watermarking approaches and find the impact of attack. | A |
| CO-04 | Apply various type of steganography techniques and steganalysis algorithms. | A, An |
| CO-05 | Practice steganography and find its impact | A.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 | M | L | M | M | S |
| **CO-02** | S | S | S | M | L | M | M | S |
| **CO-03** | S | S | S | M | L | M | S | S |
| **CO-04** | S | S | S | M | L | M | M | S |
| **CO-05** | S | S | S | S | L | M | S | M |

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

**Unit I: Watermarking Models & Message Coding** **9**

Introduction-Information Hiding, Steganography and Watermarking – History of watermarking – Importance of digital watermarking – Applications – Properties – Evaluating watermarking systems. Notation – Communications – Communication based models – Geometric models – Mapping messages into message vectors – Error correction coding – Detecting multi-symbol watermarks

**Unit II: Watermarking With Side Information & Analyzing Errors** **9**

Informed Embedding – Informed Coding – Structured dirty-paper codes - Message errors – False positive errors – False negative errors – ROC curves – Effect of whitening on error rates.

**Unit III: Perceptual Models** **9**

Evaluating perceptual impact – General form of a perceptual model – Examples of perceptual models – Robust watermarking approaches - Redundant Embedding, Spread Spectrum Coding, Embedding in Perceptually significant coefficients. Watermark Security & Authentication: Security requirements – Watermark security and cryptography – Attacks – Exact authentication – Selective authentication – Localization – Restoration.

**Unit IV: Introduction to Digital Steganography** **9**

Types of Steganography, Technical Steganography, Linguistic Steganography, Digital Steganography, Applications of Steganography, Cover Communication, One-Time Pad Communication, Embedding Security and Imperceptibility, Examples of Steganographic Software, S-Tools, StegoDos, EzStego, Jsteg-Jpeg.

**Unit V: Steganography Communication** **9**

Notation and terminology – Information-theoretic foundations of steganography – Practical steganographic methods – Minimizing the embedding impact – Steganalysis.

**TOTAL: 45 HOURS**

**REFERENCES**


1. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, “Digital Watermarking and Steganography”, Margan Kaufmann Publishers, New York, 2008.
2. Michael T. Raggo, Chet Hosmer, “Data Hiding -Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices and Network Protocols”, Elsevier Science, 2012.
3. Neil F. Johnson, Zoran Duric, Sushil Jajodia, “Information Hiding: Steganography and Watermarking-Attacks and Countermeasures”,Springer Us, 2012.
4. Frank Y. Shih, “Digital Watermarking and Steganography - Fundamentals and Techniques”, CRC Press 2017.
5. Peter Wayner , "Disappearing Cryptography: Information Hiding, Steganography and Watermarking”, Elsevier Science, 2009.

| CY35A3 | 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 behavioural 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 | Handling privacy, risks and standards in biometrics. | 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 | L | M | S | M | S |
| **CO-02** | S | M | M | L | M | S | M | S |
| **CO-03** | S | M | M | L | M | S | M | S |
| **CO-04** | S | M | M | S | S | S | M | S |
| **CO-05** | S | S | M | M | S | M | M | M |

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

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

Biometric fundamentals – Biometric technologies – Biometrics Vs traditional techniques – Characteristics of a good biometric system – Benefits of biometrics – 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 – application areas: criminal and citizen identification, surveillance, PC/network access, e-commerce and retail/ATM – costs to deploy – other issues in deployment.

**Unit V: Privacy and Standards in Biometrics** **9**

Assessing the Privacy Risks of Biometrics – Designing Privacy-Sympathetic Biometric Systems – Need for standards – different biometric standards.

**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. James wayman,Anil k.Jain ,Arun A.Ross ,Karthik Nandakumar, ―Introduction to Biometrics, Springer, 2011.
3. Anil K Jain, Patrick Flynn, Arun A Ross, "Handbook of Biometrics", Springer, 2008.
4. David D. Zhang, "AUTOMATED BIOMETRICS Technologies and Systems", Springer Science+Business Media, LLC, 2000.
5. Mohammad S Obaidat, Issa Traore and Isacc Woungang, "Biometric-based physical and cyber security systems", Springer 2019.
6. Paul Reid, "Biometrics for Network Security", Pearson Education, New Delhi, 2004.
7. John R Vacca, "Biometric Technologies and Verification Systems", Elsevier Inc, 2007.


| CY35A4 | 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 | Interpret the mathematical foundations on various intrusion detection algorithms. | U |
| CO-03 | Gain knowledge about working principles of various architecture of intrusion detection. | U |
| CO-04 | Use intrusion detection system to protect information in a public institution and measure 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: 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 III: Architecture and Implementation** **9**

Centralized – Distributed – Cooperative Intrusion Detection - Tiered architecture.

**Unit IV: Justifying Intrusion Detection** **9**

Intrusion detection in security – Threat Briefing – Quantifying risk – Return on Investment (ROI)

**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", McGraw Hill, 2004
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.


| CY35A5 | FORENSICS AND INCIDENT RESPONSE | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | 0 | 0 | 3 |

**OBJECTIVES**

- To know the real world incidents.
- To make a 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 tool kits 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, 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, Investigating Mac OS X Systems, Investigating Applications, Malware handling.

**TOTAL: 45 HOURS**

**REFERENCES**


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


| CY35A6 | PATTERN RECOGNITION | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | 0 | 0 | 3 |

**OBJECTIVES**

- To understand the fundamental of pattern recognition and its application
- To learn pattern classification using supervised and unsupervised learning methods.
- To study the various pre-processing and feature selection methods
- To acquire knowledge in application of pattern recognition in different fields like image analysis, clustering and artificial neural networks.

| Course Outcome | | Cognitive Skill |
|---|---|---|
| CO-01 | Students should able to understand basic concept and mathematical model of pattern recognition. | R |
| CO-02 | Students should able develop pattern classification algorithm and analysis the result. | U |
| CO-03 | Students should able to write pattern classification algorithm using likelihood functions and analysis the results. | A |
| CO-04 | Students should able to work with pattern classification, pre-processing and feature selection using different algorithm. | An |
| CO-05 | Students should able to analyze case studies for clustering, artificial neural network and image 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 | M | M | N | M | S | L | M |
| **CO-02** | M | M | M | L | L | S | S | M |
| **CO-03** | M | M | M | L | L | S | S | L |
| **CO-04** | S | M | L | M | M | S | M | M |
| **CO-05** | M | M | S | L | M | M | S | M |

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

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

Basic Concepts of Pattern Recognition- Fundamental problems in Pattern Recognition System Design- Design Concepts and Methodologies – Examples of Automatic Pattern Recognition Systems

**Unit II: Pattern Classification by Distance Functions** **9**

Decision functions-Introduction, Linear Decision Functions, Generalized Decision Functions, Pattern Space and Weight Space Minimum Distance Pattern Classification – Cluster Seeking – Unsupervised Pattern Recognition.

**Unit III: Pattern Classification by Likelihood Functions** **9**

Introduction – Pattern Classification as a Statistical Decision Problem – Bayes Classifier for Normal Patterns- Nonparametric decision making

**Unit IV: Pattern Preprocessing and Feature Selection** **9**

Similarity and Distance – Clustering Transformations and Feature Ordering – Clustering in Feature Selection – Feature selection through Divergence Maximization – Binary Feature Selection

**Unit V: Case Studies in Pattern Recognition** **9**

Clustering – Artificial Neural Networks – Image Analysis

**TOTAL: 45 HOURS**

**REFERENCES**


1. Julius T. Tou and Rafael C. Gonzalez, "Pattern Recognition Principles", Addison Wesley, New Delhi, 1972.
2. Earl Gose, Richard Johnsonbaugh and Steve Jost,"Pattern Recognition and Image Analysis", Prentice Hall, New Delhi, 2005.
3. Wolff D D, Parsons M L, "Pattern Recognition Approach to Data Interpretation", Plenum Press, 1983.

4. Robert.J.Schalkoff, "Pattern recognition:Stastical Structural and Neural approaches",John Wiley & Sons,1992.
5. Richard O. Duda, Peter E. Hard , David G. Stork , "Pattern Recognition", 2ed, An Indian Adaptation Paperback, John Wiley, India, 2021.

| CY35A7 | BIOMETRIC IMAGE PROCESSING | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | 0 | 0 | 3 |

**OBJECTIVES**

The student should be made to:

- Learn digital image fundamentals.
- Be familiar with image enhancement and segmentation
- Be exposed to fingerprint biometrics and processing.
- Be familiar with face recognition and processing.
- Be familiar with iris biometrics and multibiometrics.

| Course Outcome | | Cognitive Skill |
|---|---|---|
| CO-01 | Know and understand the basics and fundamentals of digital image processing and image transforms. | U |
| CO-02 | Apply the enhancement and segmentation techniques to the digital images. | A,An |
| CO-03 | Apply the image processing techniques to fingerprint images. | A,An |
| CO-04 | Apply the image processing techniques to face images. | A,An |
| CO-05 | Apply the image processing techniques to iris images and learn the basics of multi biometrics. | A ,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 | S | S | S | S |
| **CO-02** | S | S | S | S | S | S | S | M |
| **CO-03** | S | S | M | S | L | M | S | S |
| **CO-04** | S | S | S | S | S | L | S | S |
| **CO-05** | S | S | S | S | M | S | S | S |

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

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

Digital Image representation - Fundamental steps in Image Processing – Components of Digital Image Processing Systems - Image Sampling and Quantization - Some Basic Relationships

between Pixels – Some Basic Intensity Transformation Functions, The Discrete Fourier Transform-Properties of 2D Discrete Fourier Transform.

**Unit II: Image Processing Methods** **9**

Image Enhancement: The Spatial Domain Methods, The Frequency Domain Methods - Image Segmentation: Pixel Classification by Thresholding, Histogram Techniques, Smoothing and Thresholding - Gradient Based Segmentation: Gradient Image, Boundary Tracking, Laplacian Edge Detection.

**Unit III: Fingerprint Biometrics** **9**

Fingerprint Patterns, Fingerprint Features, Fingerprint Image, width between two ridges - Fingerprint Image Processing - Minutiae Determination - Fingerprint Matching: Fingerprint Classification, Matching policies.

**Unit IV: Face Recognition** **8**

Detection and Location of Faces: Statistics-Based method, Knowledge-Based method - Feature Extraction and Face Recognition: Gray value Based method, Geometry Feature Based method, Neural Networks method.

**Unit V: Iris Biometrics** **10**

Iris System Architecture, Definitions and Notations - Iris Recognition: Iris location, Doubly Dimensionless Projection, Iris code, Comparison - Coordinate System: Head Tilting Problem, Basic Eye Model - Searching Algorithm - Texture Energy Feature. Fusion in Biometrics: Introduction to Multibiometrics - Information Fusion in Biometrics - Issues in Designing a Multibiometric System - Sources of Multiple Evidence - Levels of Fusion in Biometrics - Sensor level , Feature level, Rank level, Decision level fusion - Score level Fusion.

**TOTAL: 45 HOURS**

**REFERENCES**


1. Rafael C.Gonzalez, Richard E.Woods, "Digital Image Processing", Pearson Education, 4th Edition, New York, 2018.
2. Rafael C.Gonzalez, Richard E.Woods, "Digital Image Processing", Pearson Education, 3th Edition, New York, 2008.
3. David D. Zhang, "Automated Biometrics: Technologies and Systems", Kluwer Academic Publishers, New Delhi, 2000.
4. Arun A. Ross, Karthik Nandakumar, A.K.Jain, "Handbook of Multibiometrics", Springer, New Delhi, 2006.


| CY35A8 | 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, Corporations, Cyber Terrorism, Organized Cyber Crime, Autonomous Actors, Legal System Impacts, 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.


| CY35A9 | APPLIED CRYPTOGRAPHY | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | 0 | 0 | 3 |

**OBJECTIVES**

- To understand OSI security architecture and classical encryption techniques.
- To acquire fundamental knowledge on the concepts of finite fields and number theory.
- To study various symmetric and public key cryptosystems.
- To describe the principles of data authentication and hash functions.
- To gain knowledge on applications of digital signature in payments and cryptography tools.

| Course Outcome | | Cognitive Skill |
|---|---|---|
| CO-01 | Understand the basic concepts of network security and security architecture. | U |
| CO-02 | Interpret the fundamental knowledge on finite field and number theory. | U |
| CO-03 | Apply the different cryptographic operations of symmetric and public key cryptographic algorithms. | An |
| CO-04 | Employ the various Authentication schemes and digital signature to simulate different applications. | A |
| CO-05 | Apply cryptographic tools to enhance system security. | 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**

Cryptography and Cryptanalysis – OSI Security Architecture – Services, Mechanisms and Attacks – Historical Ciphers - Shift cipher, Affine cipher, Vignere cipher – Substitution and Transposition Techniques – Stream and Block Ciphers - Basic principles of modern cryptography.

**Unit II: Symmetric Techniques** **9**

Simplified DES - Data Encryption Standard - International Data Encryption Algorithm – Block cipher principles - Block cipher modes of operation - Advanced Encryption Standard - Blowfish - RC4 - Characteristics of good ciphers – Confidentiality using symmetric encryption.

**Unit III: Asymmetric Techniques** **9**

Number Theory concepts - Principles of Public Key Cryptosystems – The RSA Algorithm – Diffie Hellman Key Exchange – Finite Fields - Elliptic Curve Cryptography – Cryptography in Embedded Hardware – Key Management – Random Number Generation

**Unit IV: Data Authentication** **9**

Authentication requirements – Authentication functions – Message Authentication Codes (MAC) – Hash functions – Security of hash function and MAC - MD5 Message Digest Algorithm – Secure Hash Algorithm –RIPMED160 – HMAC.

**Unit V: Digital Signatures and Cryptography Tools** **9**

Digital Signatures - Digital Signature Standard (DSS) - Authentication Protocols – Authentication applications – Kerberos - Cryptography Tools: TrueCrypt- AxCrypt - Cryptography-Case Studies.

**TOTAL: 45 HOURS**

**REFERENCES**

1. William Stallings, “Cryptography and Network Security”, Seventh Edition, Pearson Education, June 2017.

2. Behrouz A Forouzan and Debdeep Mukhopadhyay, “Cryptography and Network Security”, Second Edition, Tata McGraw Hill Education Pvt. Ltd., New Delhi, 2010.
3. Bernard Menezes, “Network Security and Cryptography”, Cengage Learning, New Delhi, 2010.
4. Wenbo Mao, “Modern Cryptography – Theory and Practice”, Pearson Education, New Delhi, 2006.
5. Jonathan Katz, Yehuda Lindell, “Introduction to Modern Cryptography”, Chapman & Hall/CRC, New York, 2007.
6. Bruce Schneier, “Applied Cryptography”, John Wiley & Sons, New York, 2004.
7. http://www.truecrypt.org/docs/tutorial.
8. http://www.darknessgate.com/index.php/security-tutorials/using-encryption tools/axcrypt/

| CY35B1 | DISTRIBUTED SYSTEMS SECURITY | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | 0 | 0 | 3 |

**OBJECTIVES**

The students should be able:

1. To understand the fundamental concepts of distributed systems.
2. To acquire knowledge about the Infrastructure, grid, storage and network level threats and vulnerabilities.
3. To understand the different threats and vulnerabilities in application level and service level.
4. To analyze the importance of sandboxing and virtualization concepts and offer solutions to host level threats.
5. To learn about the various security solutions to service level threats and vulnerabilities.

| Course Outcome | | Cognitive Skill |
|---|---|---|
| CO-01 | Describe the main concepts, key technologies, strengths, and limitations of cloud computing and the possible applications for state-of-the-art cloud computing | U |
| CO-02 | Explain the architecture and infrastructure of cloud computing, including SaaS, PaaS, IaaS, public cloud, private cloud, hybrid cloud, etc. | U |
| CO-03 | Identify problems, and explain, analyze, and evaluate various cloud computing solutions. | An |
| CO-04 | Choose the appropriate technologies, algorithms, and approaches for the related issues. | An |
| CO-05 | Discover new ideas and innovations in cloud computing. | 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 | M | M | S | S | S |
| **CO-02** | S | S | S | M | L | N | M | M |
| **CO-03** | M | S | M | M | S | S | M | S |
| **CO-04** | S | M | S | S | M | L | N | M |
| **CO-05** | S | S | S | S | M | M | L | M |

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

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

Distributed Systems - Distributed Systems Security- Security in Engineering: Secure Development Lifecycle Processes - A Typical Security Engineering Process – Security Engineering Guidelines and Resources - Common Security Issues and Technologies: Security Issues - Common Security Techniques.

**Unit II: Host and Infrastructure Level Threats and Vulnerabilities** **9**

Host-Level Threats and Vulnerabilities - Transient code Vulnerabilities and Resident Code Vulnerabilities - Malware – Eavesdropping – Overflow and Injection Attacks – Network-Level Threats and Vulnerabilities: Denial–of –Service Attacks – DNS Attacks – Routing Attacks – Wireless Security Vulnerabilities –Grid Computing Threats and Vulnerabilities: Architecture Related Issues – Management Related Issues -Storage Threats and Vulnerabilities

**Unit III: Application and Service Level Threats and Vulnerabilities** **9**

Application-Layer Vulnerabilities –Injection Vulnerabilities - Cross-Site Scripting (XSS) - Improper Session Management - Improper Error Handling - Improper Use of Cryptography - Insecure Configuration Issues - Denial of Service - Canonical Representation Flaws - Overflow Issues. Service-Level Threats and Vulnerabilities: SOA and Role of Standards - Service-Level Security Requirements - Service-Level Threats and Vulnerabilities - Service-Level Attacks: SQL Injection Attacks and Authentication Attacks

**Unit IV: Host and Infrastructure Level Solutions** **9**

Sandboxing – Virtualization - Resource Management - Proof-Carrying Code -Memory Firewall – Antimalware - Network-Level Solutions: Network Information Security Solutions – Denial of Service Solutions–Grid Level Solutions: Architecture Security Solutions – Grid management Solutions - Storage Level Solutions

**Unit V: Application and Service Level Solutions** **9**

Application-Level Solutions: Application-Level Security Solutions - Service Level Solutions: Services Security Policy - SOA Security Standards Stack – Standards in Depth - Deployment Architectures for SOA Security - Compliance in Financial Services: SOX Compliance – Multilevel Policy-Driven Solution Architecture - Future Directions

**TOTAL: 45 HOURS**

## REFERENCES


1. Abhijit Belapurakar, AnirbanChakrabarti and et al., "Distributed Systems Security: Issues. Processes and solutions", Wiley, Ltd., Publication, 2009.
2. Sukumar Ghosh, "Distributed Systems – An Algorithmic Approach", Second Edition, CRC Press, Taylor and Francis Group, 2014.
3. AbhijitBelapurkar, AnirbanChakrabarti, HarigopalPonnapalli, NiranjanVaradarajan, SrinivasPadmanabhuni and SrikanthSundarrajan, "Distributed Systems Security: Issues, Processes and Solutions", Wiley publications, 2009.
4. RachidGuerraoui and Franck Petit, "Stabilization, Safety, and Security of Distributed Systems", Springer, 2010.


| CY35B2 | CYBER CRIMINOLOGY AND CYBER CRIMES | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | 0 | 0 | 3 |

## OBJECTIVES

- To understand the fundamentals of Cybercrimes.
- To be familiar criminological theories and its importance.
- To understand the various terrorism activities.
- To know the online criminal activities
- To understand the different real time examples.

| Course Outcome | | Cognitive Skill |
|---|---|---|
| CO-01 | Students will be able to understand the basic concepts of cybercrimes. | U,R |
| CO-02 | Students will be able to understand the different cyber criminology theories and apply the knowledge gained in various applications. | U,A |
| CO-03 | Students will be able to understand the different cyber terrorism activities and analyze how these activities are employed by hackers. | U,A |
| CO-04 | Able to understand and analyze the impact of cyber criminal activities such as gambling and child pornography. | An,A |
| CO-05 | Able to understand and analyze the various real time examples. | 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** | M | L | M | L | M | S | M | L |
| **CO-02** | L | M | S | L | S | M | L | N |
| **CO-03** | M | M | S | N | L | L | S | L |
| **CO-04** | L | L | S | L | M | S | L | N |
| **CO-05** | S | M | S | M | N | N | S | M |

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

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

Cyber Crime: History & Evolution: Definition-History and Evolution of Cyber Crime- Legal and Policy Issues in Cyber Crime

**Unit II: Cyber Criminology** **9**

Cyber Criminology and Psychology- Criminological and Psychological Theories- Cyber Aggression and Cyber Bullying: Widening the Net-The Dark Web

**Unit III: Cyber Terrorism** **9**

Cyber Terrorism: Definition of Cyber Terrorism- Why Cyber Terrorism-Forms of Cyber Terrorism- Countering Cyber Terrorism- Terrorists use of Internet- Cyber Warfare : What is Cyber Warfare- Features of Cyber Warfare-Features of Cyber weapons-Cyber Bullying: Cyber Stalking: Sexting: Revenge Pornography, Sexting, Sextortion and Related Offences- Tackling Offences.

**Unit IV: Cyber Criminal Activities** **9**

Why cyber safety important? What are the threats? child pornography- The nature of child pornography- Adult sexual interest in children-The Internet, child pornography and adult sexual interest in children- Laws to ensure online safety of children: ITA Act 2008-other relevant provisions-Indian Penal code,1860-Protection of children from sexual offences Act,2012-Modes of registration of complaints-Guidelines for children: Do's and Don'ts-Guidelines for Parents-Guidelines for Teachers.

**Unit V: Case Studies** **9**

Cybercrime Detection: Predicting the Cyber Attackers-Crime Data Mining, Threat Analysis and Prediction-Education, Training and Awareness in Cybercrime Prevention:
Combating Cyber Victimization.

**TOTAL: 45 HOURS**

**REFERENCES**


1. Dr.Nagarathna.A, Jay Bhaskar Sharma and Sparsh Sharma, " Children & Cyber Safety:an e-book, Advanced Centre for Research, Developemnt and Training in cyber Laws and forensics",National Law School of India University, Bengaluru.
2. Max Taylor and Ethel Quayle, " Child Pornography: An Internet Crime", Brunner-Routledge, First Edition, Taylor & Francis Group,2003.
3. Hamid Jahankhani, " CyebrbCriminology", Springer, Advanced Sciences and Technologies for Security Applications, 2018.
4. K.JaiShankar, " Cyber Criminology: Exploring Internet Crimes and Criminal Behavior", First Edition,CRC Press, Taylor & Francis Group,2011.
5. Sunit Belapure and Nina Godbole, " Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", First Edition,Wiley India Pvt. Ltd., 2011.


| CY35B3 | MALWARE ANALYSIS | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | 0 | 0 | 3 |

**OBJECTIVES**

- To learn the malware fundamentals and its types.
- To understand the basic static and dynamic analysis techniques.
- To understand the advanced static and dynamic analysis techniques.
- To procure knowledge about the malware functionalities and behavior.
- To gain knowledge about the various malware detection and prevention techniques.

| Course Outcome | | Cognitive Skill |
|---|---|---|
| CO-01 | Students will learn about malware, its types, importance and techniques. | U,R |
| CO-02 | Students will learn about the analyzing different file formats, libraries VMware machine and sandboxing. | U, An |
| CO-03 | Students will learn about identifying the malicious windows programs and apply the knowledge gained in live systems. | U, A |
| CO-04 | Students gain knowledge about the functionalities of malware and analyze its behavior. | U, An |
| CO-05 | Students will learn to detect the malware and to how to prevent it in different applications and also gain knowledge about the different malware tools. | U, R |

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 | L | L | L |
| **CO-02** | L | N | N | N | L | S | S | M |
| **CO-03** | L | M | L | M | M | M | M | L |
| **CO-04** | M | S | S | S | S | L | S | M |
| **CO-05** | M | L | M | L | L | M | M | L |

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

**Unit I: Malware Fundamentals** **9**

Introduction: Malware threats- Evolution of Malware-Malware types- What is Malware Analysis? Why Malware Analysis? The Goals of Malware Analysis- Malware Sources-Malware Analysis Techniques: Basic static-Basic Dynamic-Advanced Static-Advanced Dynamic- General Rules for Malware Analysis-Method of Infection-Malware Propagation Techniques-Propagation Injection Vectors.

**Unit II: Basic Malware Analysis Techniques** **9**

Basic Analysis: Basic Static Techniques-Antivirus Scanning-Hashing-Finding Strings-Packed and Obfuscated Malware-Portable Executable File Format- Linked Libraries and Functions-Static Analysis in Practice-The PE File Headers and Sections-Malware Analysis in Virtual Machines: Structure-Creating Malware Analysis Machine-VMware for Malware Analysis-Basic Dynamic Analysis: Sandboxes-Monitoring-Viewing Processes-Faking a Network.

**Unit III: Advanced Malware Analysis Techniques** **9**

Advanced Static Analysis: x86 Disassembly-IDA Pro-Recognizing C code Constructs in assembly-Analyzing Malicious Windows Programs-Advanced Dynamic Analysis: Debugging-OllyDbg-Kernel Debugging with WinDbg.

**Unit IV: Malware Functionalities and Behavior** **9**

Malware Functionality: What Malware Does Once It's Installed?- Identifying Installed Malware-Malware Behavior-Downloaders and Launchers-Backdoors-RATs-Botnets-Credential Stealers-Hash Dumping-Keystroke Logging-Persistence Mechanisms-Privilege Escalation- User-mode Rootkits-Ransomware- Pegasus(Spyware)

**Unit V: Malware Detection and Prevention Techniques** **9**

Malware Detection: Signature-based techniques-Non-signature based techniques-Malware Prevention: Rogue Software-Great Interface-Antivirus-Host Protection Systems- General Security Policies-Tools for Malware Analysis.

**TOTAL: 45 HOURS**

**REFERENCES**


1. Alexey Kleymenov and Amr Thabet, "Mastering Malware Analysis: The complete malware analyst's guide to combating malicious software, APT, cybercrime, and IOT attacks", Packt Publication, June 2019. Monnappa, " Learning Malware Analysis", Packt Publication, June 2018.
2. Christopher C. Elisan, " Advanced Malware analysis", McGraw Hill Education, First Edition, 2015.
3. Michael Sikorski and Andrew Honig, "Practical Malware Analysis: The Hands-on-Guide to Dissecting Malicious Software", William Pollock Publisher, 2012.
4. Michael A. Davis, Sean M.Bodmer and Aaron LeMasters, " Hacking Malware & Rootkits Exposed: Malware & Rootkits Secrets & Solutions", McGraw Hill Publications,2010.
5. https://www.drishtiias.com/daily-updates/daily-news-analysis/pegasus-spyware.


| G335A1 | 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 | Ability to understand the concepts of Business Analytics. | R,U |
| CO-02 | Can understand the factors of Trendiness and Regression analysis. | R,U |
| CO-03 | Students can understand about organization structures of business analytics. | R,U |
| CO-04 | One can understand the concepts of Forecasting Techniques. | R,U |
| CO-05 | Can understand the Decision analysis. | R,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** | 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: Business Analytics** **9**

Overview of Business analytics, Scope of Business analytics, Business Analytics Process, Relationship of Business Analytics Process and organization, competitive advantages of Business Analytics. Statistical Tools: Statistical Notation, Descriptive Statistical methods, Review of probability distribution and data modeling, sampling and estimation methods overview.

**Unit II: Trendiness and Regression Analysis** **9**

Modeling 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: Organization Structures of Business Analytics** **9**

Team management, Management Issues, Designing Information Policy, Outsourcing, Ensuring Data Quality, Measuring contribution of Business analytics, Managing Changes.
Descriptive Analytics, predictive analytics, predicative Modeling, Predictive analytics analysis, Data Mining, Data Mining Methodologies, Prescriptive analytics and its step in the business analytics Process, Prescriptive Modeling, nonlinear Optimization.

**Unit IV: Forecasting Techniques** **9**

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: Decision Analysis** **9**

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.


| G335A2 | 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 | Ability to understand the concepts of Industrial Safety. | R,U |
| CO-02 | Can understand the fundamentals of Maintenance Engineering. | R,U |
| CO-03 | Students can understand the ways to prevent from wear and corrosion. | R,U |
| CO-04 | One can understand the concepts of fault tracing. | R,U |
| CO-05 | Can understand the functions of periodic and preventive maintenance. | R,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 | 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 releva

**Unit I: Industrial Safety** **9**

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

**Unit II: Fundamentals of Maintenance Engineering** **9**

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

**Unit III: Wear and Corrosion and their Prevention** **9**

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: Fault Tracing** **9**

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: Periodic and Preventive Maintenance** **9**

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.

| G335A3 | 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 | Ability to understand the concepts of Optimization Techniques. | R,U |
| CO-02 | Can understand the fundamentals of LPP formulation. | R,U |
| CO-03 | Students can understand the Non-Linear Programming. | R,U |
| CO-04 | One can understand the concepts Scheduling and Sequencing. | R,U |
| CO-05 | Can understand the functions of Competitive models. | R,U |

S-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: Optimization Techniques** **9**

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

**Unit II: LPP Formulation** **9**

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

**Unit III: Nonlinear Programming** **9**

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

**Unit IV: Scheduling and Sequencing** **9**

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

**Unit V: Competitive Models** **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


| G335A4 | COST MANAGEMENT OF ENGINEERING PROJECTS | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | 0 | 0 | 3 |

**OBJECTIVE**

To make students understandable about the cost concepts in decision making and profit planning.

| Course Outcome | | Cognitive Skill |
|---|---|---|
| CO-01 | Ability to understand the strategic cost management. | R,U |
| CO-02 | Can understand the fundamentals of cost concepts in decision making. | R,U |
| CO-03 | Students can understand the process involved in project execution. | R,U |
| CO-04 | One can understand the concepts of cost behavior and profit planning. | R,U |
| CO-05 | Can understand the functions of quantitative techniques. | R,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 | 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: Strategic Cost Management** **9**

Introduction and Overview of the Strategic Cost Management Process.

**Unit II: Cost Concepts in Decision Making** **9**

Relevant cost, Differential cost, Incremental cost and Opportunity cost. Objectives of a Costing System; Inventory valuation; Creation of a Database for operational control; Provision of data for Decision-Making.

**Unit III: Project** **9**

Meaning, Different types, why to manage, cost overruns centres, various stages of project execution: conception to commissioning. Project execution as conglomeration of technical and nontechnical activities. Detailed Engineering activities. Pre project execution main clearances and documents Project team: Role of each member. Importance Project site: Data required with significance. Project contracts. Types and contents. Project execution Project cost control. Bar charts and Network diagram. Project commissioning: mechanical and process

**Unit IV: Cost Behavior and Profit Planning** **9**

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

**Unit V: Quantitative Techniques** **9**

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

**TOTAL: 45 HOURS**

**REFERENCES**


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


| G335A5 | 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 | Ability to understand the functional requirements of composite materials. | R,U |
| CO-02 | Can understand the properties and applications of reinforcements. | R,U |
| CO-03 | Students can understand the process involved in metal matrix composite fabrication. | R,U |
| CO-04 | One can understand the concepts of polymer matrix composites fabrication. | R,U |
| CO-05 | Can understand the physical characteristics of composite materials. | R,U |

S-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.

| G335A6 | 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 | Ability to understand the process of obtaining Energy from waste substances. | R,U |
| CO-02 | Can understand manufacturing of pyrolytic oils and gases, yields and applications. | R,U |
| CO-03 | Students can understand kinetic consideration in gasifier operation. | R,U |
| CO-04 | One can understand the Design, construction and operation of Bio Mass chamber. | R,U |
| CO-05 | Can understand the basic Properties of biogas | R,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 | 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.