PAAVAI ENGINEERING COLLEGE, NAMAKKAL – 637018

(AUTONOMOUS)

B.E – CYBER SECURITY

REGULATIONS 2019

CURRICULUM

(CHOICE BASED CREDIT SYSTEM)

(For the candidates admitted during the academic year 2020-2021)

SEMESTER V

S.No.	Category	Course Code	Course Title	L	T	P	C
Theory							
1.	PC	CY20501	Optimization Techniques	3	0	0	3
2.	PC	CY20502	Digital Forensics	3	0	0	3
3.	PC	CY20503	Operating Systems	3	0	0	3
4.	PC	CY20504	Design and Analysis of Algorithms	3	0	0	3
5.	PC	CY20505	Database Security	3	0	0	3
6.	PE	CY2015*	Professional Elective Course I	3	0	0	3
Practical							
7.	PC	CY20506	Operating Systems Laboratory	0	0	4	2
8.	PC	CY20507	Design and Analysis of Algorithms Laboratory	0	0	4	2
9.	EE	EN20501	Career Development Laboratory I	0	0	2	1
			TOTAL	**18**	**0**	**10**	**23**

SEMESTER VI

S.No.	Category	Course Code	Course Title	L	T	P	C
Theory							
1.	PC	CY20601	Software Engineering	3	0	0	3
2.	PC	CY20602	Artificial Intelligence	3	0	0	3
3.	PC	CY20603	Penetration Testing and Vulnerability Assessment	3	0	0	3
4.	PE	CY2025*	Professional Elective Course II	3	0	0	3
5.	OE	CY2090*	Open Elective I	3	0	0	3
Practical							
7.	PC	CY20604	Penetration Testing and Vulnerability Assessment Laboratory	0	0	4	2
8.	PC	CY20605	Artificial Intelligence Laboratory	0	0	4	2
9.	EE	EN20601	Career Development Laboratory II	0	0	2	1
			TOTAL	**15**	**0**	**10**	**20**

PROFESSIONAL ELECTIVE COURSES (PE I)

S.No.	Category	Course Code	Course Title	L	T	P	C
1.	PE	CY20151	Formal Language and Automated	3	0	0	3
2.	PE	CY20152	Cyber Physical Systems	3	0	0	3
3.	PE	CY20153	Data Warehousing and Data Mining	3	0	0	3
4.	PE	CY20154	Mobile and Wireless Security	3	0	0	3
			TOTAL	**12**	**0**	**0**	**12**

PROFESSIONAL ELECTIVE COURSES (PE II)

S.No.	Category	Course Code	Course Title	L	T	P	C
1.	PE	CY20251	Compiler Design	3	0	0	3
2.	PE	CY20252	Secure Coding	3	0	0	3
3.	PE	CY20253	Information Assurance and Security	3	0	0	3
4.	PE	CY20254	Operation System Security	3	0	0	3
			TOTAL	**12**	**0**	**0**	**12**

OPEN ELECTIVE COURSES (OE I)

S.No.	Category	Course Code	Course Title	L	T	P	C
1.	OE	CY20901	Information Security Risk Management	3	0	0	3
2.	OE	CY20902	Cyber Crime and Cyber Laws	3	0	0	3
			TOTAL	**6**	**0**	**0**	**6**

CY20501 **OPTIMIZATION TECHNIQUES** **3 0 0 3**

COURSE OBJECTIVES

To enable students to

- understand the need of using Optimization Techniques.
- able to formulate Linear Programing.
- evaluate Integer Programming problems, Transportation and Assignment Problems.
- obtain a solution to Network problems using CPM and PERT techniques.
- recognize fundamentals of Queuing model.

PRE-REQUISITES:LINEAR ALGEBRA

UNIT I INTRODUCTION **9**

Introduction to operation research - Features and Phases of operation research – Approach to Problem solving - Models and modelling in operations research – Advantages - Applications of model building-Methodology of operations research.

UNIT II LINEAR PROGRAMMING **9**

Structure of linear programming model - Advantages, Limitations and Applications of linear programming model- Mathematical formulation of LPP - Examples of Maximization, Minimization using Simplex Method and Two-Phase Method.

UNIT III INTEGER PROGRAMMING AND TRANSPORTATION PROBLEMS **9**

Classification of Linear Integer programming - Branch and bound method - Transportation Problem: Mathematical Model of Transportation Problem - Assignment problems: Mathematical Model of Assignment Problem -Solution Methods of Assignment Problem - Traveling Salesman Problem.

UNIT IV PROJECT SCHEDULING **9**

Project network -Diagram representation – Floats - Critical Path Method (CPM) – PERT- Cost considerations in PERT and CPM.

UNIT V QUEUING MODELS **9**

Structure of a Queuing system - Performance Measures of a Queuing System - Classification of Queuing model, Single server and Multi-server model.

TOTAL PERIODS: 45

COURSE OUTCOMES

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

- describe need of using Optimization Techniques.
- explain and formulate Linear Programing.
- summarize Integer Programming problems, Transportation and Assignment Problems.
- outline the solution to Network problems using CPM and PERT techniques.
- discuss fundamentals of Queuing model.

TEXTBOOKS

1. Hamdy A Taha, Operations Research: An Introduction, Pearson, 10th Edition, 2017.
2. J. K. Sharma, Operations Research Theory and Applications, Macmillan, 5th Edition, 2012.

REFERENCES

1. ND Vohra, Quantitative Techniques in Management, Tata McGraw Hill, 4th Edition, 2011.
2. Hiller F.S, Liberman G.J, Introduction to Operations Research, 10th Edition McGraw Hill, 2017.
3. Jit. S. Chandran, Mahendran P. Kawatra, KiHoKim, Essentials of Linear Programming, Vikas Publishing House Pvt.Ltd. New Delhi, 1994.
4. Ravindran A., Philip D.T., and Solberg J.J., Operations Research, John Wiley, 2nd Edition, 2007.

CO/PO MAPPING :

CO/PO Mapping (3/2/1 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak														
COs		Programmes Outcomes (POs)												
	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO1**	**PSO2**
CO1	3	2	1	1	1	1	-	-	-	1	1	2	3	2
CO2	2	2	1	1	1	1	-	-	-	1	1	1	3	2
CO3	3	2	3	1	1	1	1	-	1	1	-	1	2	1
CO4	2	2	3	2	1	1	1	-	1	1	-	1	2	3
CO5	3	2	2	1	1	1	1	-	1	1	-	2	1	1

CY20502 **DIGITAL FORENSICS** **3 0 0 3**

COURSE OBJECTIVES

To enable the students to

- understand Forensic science and Computer Forensic concepts.
- learn the various forensic Operandi and motive behind cyber-attacks.
- be familiar with the computer forensic process model and their legal perspective.
- learn the cybercrime tools and identify the digital pieces of evidence.
- gain knowledge about digital evidence used to commit cyber offences.

UNIT I INTRODUCTION **9**

Introduction - Computer Forensics Fundamentals, Types of Computer Forensics Technology, Types of Computer Forensics Systems; Vendor and Computer Forensics Services.

UNIT II COMPUTER FORENSICS EVIDENCE AND CAPTURE **9**

Computer forensics evidence and capture - Data Recovery - Evidence Collection and Data Seizure - Duplication and Preservation of Digital Evidence - Computer Image Verification and Authentication.

UNIT III COMPUTER FORENSIC ANALYSIS **9**

Discover of Electronic Evidence - Identification of Data, Reconstructing Past Events, Fighting against Macro Threats; Tactics of the Military - Tactics of Terrorist and Rogues, Tactics of Private Companies.

UNIT IV INFORMATION OPERATIONS **9**

Arsenal and Surveillance Tools - Hackers and Theft of Components, Contemporary Computer Crime, Identity Theft and Identity Fraud; Organized Crime &Terrorism - Applying the First Amendment to Computer Related Crime, The Fourth Amendment and other Legal Issues.

UNIT V DIGITAL FORENSIC CASES **9**

Developing Forensic Capabilities - Searching and Seizing Computer Related Evidence, Processing Evidence and Report Preparation, Future Issues.

TOTAL PERIODS 45

COURSE OUTCOMES

At the end this course, students will be able to

- describe Forensic science and Computer Forensic concepts.
- determine various digital forensic Operandi and motive behind cyber-attacks.
- interpret the cyber pieces of evidence, Tactics of the Military and their legal perspective.
- demonstrate various forensic tools to investigate the cybercrime and to identify the digital pieces of evidence.
- analyze the digital evidence used to commit cyber offences.

TEXTBOOKS

1. John R. Vacca, "Computer Forensics: Computer Crime Scene Investigation", Cengage Learning, 2nd Edition, 2005.
2. Marjie T Britz, "Computer Forensics and Cyber Crime: An Introduction", Pearson Education, 2nd Edition, 2008.

REFERENCES

1. Cyber security – Understanding of cybercrimes, computer forensics and Legal perspectives by Nina Godbole and Sunit Belapure – Wiley India Publication 2019.
2. The basics of digital Forensics (Latest Edition) – The primer for getting started in digital forensics by John Sammons – Elsevier Syngress Imprint 2015.
3. Practical Digital Forensics – Richard Boddington [PACKT] Publication, Open-source community 2010.
4. Majid Yar, "Cybercrime and Society", SAGE Publications Ltd, Hardcover, 2nd Edition, 2013.

CO-PO MAPPING:

Mapping of Course Outcomes with Programme Outcome (3/2/1 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak														
COs	**Programme Outcomes(POs)**												**Programme Specific Outcomes (PSOs)**	
	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO1**	**PSO2**
CO1	3	2	1	1	1	1	2	-	2	1	1	2	3	2
CO2	2	2	1	1	1	1	-	-	-	1	1	1	3	2
CO3	3	2	3	1	1	1	1	1	1	1	-	1	2	1
CO4	2	2	3	2	1	1	1	-	1	1	1	1	2	3
CO5	3	2	2	1	1	1	1	-	1	1	1	2	1	1

CY20503 **OPERATING SYSTEMS** **3 0 0 3**

COURSE OBJECTIVES

To enable the students to

- understand the basic concepts and functions of operating systems.
- interpret processes, threads, scheduling algorithms and concept of deadlocks.
- analyze various memory management schemes.
- associate file system interfaces and implementation process.
- acquire the knowledge of i/o streams and mass storage management.

UNIT I INTRODUCTION TO OPERATING SYSTEMS **9**

Introduction - Computer system organization, Introduction to operating systems, operating system structures, Services; System calls; System programs; Processes - Process concept - Process control block,Operations on Processes - Cooperating processes, Inter process communication; Threads-Multi - threadingmodels, Threading issues.

UNIT II PROCESS MANAGEMENT AND DEADLOCK **10**

CPU Scheduling - Scheduling criteria, Scheduling algorithms, Multiple processor scheduling, Real time scheduling, Algorithm Evaluation; Process Synchronization - The critical section problem, Synchronization hardware, Semaphores, Classic problems of synchronization, Monitors; Deadlock-System model, Deadlock Characterization, Methods for handling deadlocks, Deadlock prevention, Deadlock avoidance, Deadlock detection, Recovery from deadlock.

UNIT III MEMORY MANAGEMENT **9**

Main Memory - Background, Swapping, Contiguous memory allocation, Paging, Segmentation, Segmentation with paging; Virtual Memory - Background, Demand paging, Page replacement, Allocationof frames; Thrashing.

UNIT IV FILE SYSTEMS **9**

File System Interface - File concept, Access methods, Directory structure, File system mounting, File sharing, Protection; File System Implementation-Directory implementation, Allocation methods, Free - space management, efficiency and performance, recovery, Network file systems.

UNIT V I/O SYSTEMS AND MASS STORAGE MANAGEMENT **8**

I/O Systems - I/O Hardware, Application I/O interface, kernel I/O subsystem, streams, performance; Mass Storage Structure - Disk attachment, Disk scheduling, Disk management; Swap space management, RAID, stable storage; **CASE STUDY** - LINUX system.

TOTAL PERIODS 45

COURSE OUTCOMES

Upon the completion of this course, the students will be able to

- analyze various scheduling algorithms.
- use algorithms to prevent, avoid and solve deadlock situation.
- compare and contrast various memory management schemes.
- analyze the functionality of file systems.
- implement various disk scheduling algorithms.

TEXTBOOKS

1. Silberschatz, Galvin, and Gagne, "Operating System Concepts", Tenth Edition, Wiley India Pvt Ltd, 2018.
2. William Stallings, "Operating Systems – internals and design principles", Prentice Hall, 7thEdition, 2011.

REFERENCES

1. Andrew S. Tanenbaum, "Modern Operating Systems", Fourth Edition, Pearson Education, 2014.
2. Harvey M. Deital, "Operating Systems", Third Edition, Pearson Education, 2007.
3. Andrew S. Tannenbaum& Albert S. Woodhull, "Operating System Design and Implementation", Prentice Hall, 3rd Edition, 2006.
4. AchyutS. "Godbole, AtulKahate Operating Systems", McGram Hill Education,2016.

CO/PO MAPPING

Mapping of Course Outcomes with Programme Outcome (3/2/1 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak														
COs	**Programme Outcomes (POs)**												**Programme Specific Outcomes (PSOs)**	
	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO1**	**PSO2**
CO1	1	3	-	2	3	2	2	-	1	1	-	2	2	1
CO2	3	3	3	3	3	3	3	2	1	3	-	1	2	1
CO3	2	3	3	2	3	2	2	1	1	2	1	2	2	1
CO4	2	3	3	2	3	2	2	-	1	2	2	3	2	1
CO5	3	3	-	3	-	3	3	1	3	3	2	3	1	3

CY20504 DESIGN AND ANALYSIS OF ALGORITHMS 3 0 0 3

COURSE OBJECTIVES

To enable the students to

- identify the various algorithm designs.
- know the importance of computational complexity of the algorithm.
- become familiar with dynamic programming and greedy techniques.
- understand various design techniques to solve the problem.
- study about techniques in backtracking and branch, bound algorithms.

UNIT I INTRODUCTION 9

Notion of Algorithm - Fundamentals of algorithmic problem solving, important problem types; Fundamentals of the Analysis of Algorithm Efficiency- Analysis framework, asymptotic notations and its properties, mathematical analysis of recursive and non-recursive relations (insertion sort, bubble sort, selection sort, towers of hanoi).

UNIT II BRUTE FORCE AND DIVIDE-AND-CONQUER 9

Brute Force- Closest - pair and convex - hull problems, exhaustive search, travelling salesman problem, knapsack problem, assignment problem; Divide and Conquer Methodology - Merge sort, quick sort, binarysearch, multiplication of large integers, strassen's matrix multiplication, closest pair problem and convexhull problem.

UNIT III DYNAMIC PROGRAMMING AND GREEDY TECHNIQUE 9

Dynamic Programming - Computing a binomial coefficient, warshall's and floyd's algorithm, optimal binary search trees, 0/1 knapsack problem and memory functions; Greedy Technique - Prim's algorithm, kruskal's algorithm, dijikstra's algorithm, huffman trees.

UNIT IV ITERATIVE IMPROVEMENT 9

The Simplex Method - The maximum flow problem; Maximum Matching in Bipartite Graphs - The stablemarriage problem.

UNIT V ALGORITHM DESIGN TECHNIQUE AND ITS LIMITATIONS 9

Backtracking - N-Queen problem, hamiltonian circuit problem, subset sum problem; Branch and Bound - Assignment problem, knapsack problem, travelling salesman problem.

TOTAL PERIODS 45

COURSE OUTCOMES

Upon the completion of the course, the students will be able to

- understand the significance of algorithms in problem solving process.
- analyse algorithms and estimate their best-case, worst-case and average-case behavior.
- identify various algorithms design techniques for different problems.
- design efficient algorithms for new situations, using as building blocks the techniques learned.
- differentiate algorithms of backtracking and branch-and-bound.

TEXTB O O K S

1. Anany Levitin, "Introduction to the Design and Analysis of Algorithms", Third Edition, Pearson Education, 2014.
2. Ellis Horowitz, Sartaj Sahni and Sanguthevar Rajasekaran, Computer Algorithms/ C++, Second Edition, Universities Press, 2007.

REFERENCES

1. Thomas H.Cormen, Charles E.Leiserson, Ronald L. Rivest and Clifford Stein, Introduction to Algorithms, Third Edition, PHI Learning Private Limited, 2012.
2. Alfred V. Aho, John E. Hopcroft and Jeffrey D. Ullman, —Data Structures and Algorithms, Pearson Education, Reprint 2006.
3. Harsh Bhasin, —"Algorithms Design and Analysis", Oxford university press, 2016.
4. S. Sridhar, —"Design and Analysis of Algorithms", Oxford university press, 2014.

CO/PO MAPPING

Mapping of Course Outcomes with Programme Outcome (3/2/1 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak														
COs	**Programme Outcomes (POs)**												**Programme Specific Outcomes (PSOs)**	
	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO1**	**PSO2**
CO1	3	3	-	2	1	2	2	1	1	1	2	3	1	1
CO2	3	3	1	2	2	1	2	-	-	2	2	3	2	1
CO3	3	3	1	2	2	2	2	2	2	2	2	3	2	2
CO4	3	3	1	2	2	-	2	2	2	2	2	3	2	1
CO5	3	3	1	2	2	-	2	2	2	-	2	3	2	1

CY20505 **DATABASE SECURITY** **3 0 0 3**

COURSE OBJECTIVES

To enable the students to

- understand the fundamentals of security, and how it relates to information systems.
- identify risks and vulnerabilities in operating systems from a database perspective.
- learn good password policies, and techniques to secure passwords in an organization.
- understand the various database security models and their advantages or disadvantages.
- learn to implement privacy preserving data mining algorithms.

UNIT I **SECURITY ARCHITECTURE & OPERATING SYSTEM SECURITY FUNDAMENTAL'S INTRODUCTION** **9**

Security Architecture – Introduction, Information Systems, Information Security Architecture; Database Security – Asset Types and value, Security Methods; Operating System Security Fundamentals - Security Environment, Components, Authentication Methods, Vulnerabilities, E-mail Security.

UNIT II **ADMINISTRATION OF USERS & PROFILES, PASSWORD POLICIES, PRIVILEGES AND ROLES** **9**

Administration of Users - Introduction-Authentication, Creating Users, SQL Server User, Removing, Modifying Users, Default, Remote Users; Database Links - Linked Servers, Remote Servers; Practices for Administrators and Managers - Best Practices Profiles, Password Policies.

Privileges and Roles – Introduction, Defining and Using Profiles, Designing and Implementing Password Policies; Granting and Revoking User Privileges - Creating, Assigning and Revoking User Roles, Best Practices.

UNIT III **DATABASE APPLICATION SECURITY MODELS & VIRTUAL PRIVATE DATABASES** **9**

Database Application Security Models – Introduction, Types of Users, Security Models, Application Types, Application Security Models; Data Encryption Virtual Private Databases – Introduction, Overview of VPD, Implementation of VPD using Views; Application Context in Oracle - Implementing Oracle VPD, Viewing VPD Policies and Application contexts using Data Dictionary, Policy Manager Implementing Row and Column level Security with SQL Server.

UNIT IV **AUDITING DATABASE ACTIVITIES** **9**

Auditing Database Activities - Using Oracle Database Activities, Creating DLL Triggers with Oracle, Auditing Database Activities with Oracle, Auditing Server Activity with SQL Server 2000, Security and Auditing Project Case Study.

UNIT V **PRIVACY PRESERVING DATA MINING TECHNIQUES** **9**

Privacy Preserving Data Mining Techniques – Introduction, Privacy Preserving Data Mining Algorithms, General Survey, Randomization Methods, Group Based Anonymization, Distributed Privacy Preserving Data Mining, Curse of Dimensionality, Application of Privacy Preserving Data Mining.

TOTAL PERIODS **45**

COURSE OUTCOMES

Upon the completion of the course, the students will be able to

- ensure the data confidentiality.
- prove that the data integrity is preserved.
- prove that only authorized user has access to the data.
- identify security threats in database systems.
- design and implement secure database systems.

TEXTB O O K S

1) Hassan A. Afyouni, "Database Security and Auditing", Third Edition, Cengage Learning, 2009.
2) Charu C. Aggarwal, Philip S Yu, "Privacy Preserving Data Mining": Models and Algorithms,Kluwer Academic Publishers, 2008.

REFERENCES

1) Ron Ben Natan, "Implementing Database Security and Auditing", Elsevier Digital Press, 2005.
2) Alfred Basta, Melissa Zgola, "Database Security", 1st Edition, 2012.
3) Michael Gertz Sushil Jajodia, "Database Security Applications and Trends", Springer, 2008 Edition.
4) Herbert J. Mattord, "Principles of Information Security", 5th Edition, 2015.

CO/PO MAPPING

Mapping of Course Outcomes with Programme Outcome
(3/2/1 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

COs	Programme Outcomes (POs)												Programme Specific Outcomes (PSOs)	
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	1	1	1	1	-	-	-	1	1	2	3	2
CO2	2	2	1	1	1	1	-	-	-	1	1	1	3	2
CO3	3	2	3	1	1	1	1	-	1	1	-	1	2	1
CO4	2	2	3	2	1	1	1	-	1	1	-	1	2	3
CO5	3	2	2	1	1	1	1	-	1	1	-	2	1	1

CY20506 **OPERATING SYSTEMS LABORATORY** **0 0 4 2**

COURSE OBJECTIVES

To enable the students to

- execute shell programming and the use of filters in the unix environment.
- be exposed to programming in c using system calls and to process creation and inter process communication.
- implement file system related system calls.
- be familiar with implementation of CPU scheduling algorithms, page replacement algorithms and deadlock avoidance.

LIST OF EXPERIMENTS

1. Basics of UNIX commands.
2. Shell Programming.
3. Implement the following CPU scheduling algorithms.
   a) FCFS b) SJF c) Priority d) Round Robin
4. Implement the following file allocation strategies.
   a) Sequential b) Indexed c) Linked
5. Implement Semaphores.
6. Implement Bankers Algorithm for Dead Lock Avoidance and Deadlock Detection.
7. Implement the following page replacement algorithms.
   a) FIFO b) LRU c) Optimal
8. Implement Paging Technique of memory management.
9. Implement Shared memory and IPC.
10. Study of hardware and Software requirements of different operating systems
    a) Linux b) UNIX c) WINDOWS XP d) WINDOWS 7/8

TOTAL PERIODS 60

COURSE OUTCOMES

Upon the completion of the course, the students will be able to

- implement deadlock avoidance and detection algorithms.
- compare the performance of various CPU scheduling algorithms.
- critically analyze the performance of the various page replacement algorithms.
- create processes and implement IPC.

CO/PO MAPPING

Mapping of Course Outcomes with Programme Outcome
(3/2/1 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

COs	Programme Outcomes (POs)												Programme Specific Outcomes (PSOs)	
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	-	2	3	-	2	1	1	1	2	3	1	1
CO2	3	3	1	2	3	1	2	2	2	2	2	3	2	1
CO3	3	3	2	2	3	2	2	2	-	2	2	3	2	2
CO4	3	3	1	2	3	-	2	2	2	2	2	3	2	1

CY20507 DESIGN AND ANALYSIS OF ALGORITHMS LABORATORY 0 0 4 2

COURSE OBJECTIVES

To enable students to

- learn complexities of various sorting and searching algorithms.
- get familiarized with dynamic programming and greedy techniques.
- learn to find shortest path and minimum spanning tree techniques for a given graph.
- be familiar with various branch/bound and backtracking algorithms.

LIST OF EXPERIMENTS

1. Implementation of quick sort and merge sort algorithms.
2. Implementation of selection sort algorithm.
3. Implementation of linear search algorithm.
4. Compute transitive closure of a given directed graph using warshall's and floyd's algorithm.
5. Implement 0/1 Knapsack problem using dynamic programming.
6. Find the shortest paths to other vertices using dijikstra's algorithm.
7. Find the minimum cost spanning tree of a given undirected graph using Prim's and Kruskal's algorithm.
8. Implement N-Queens problem using backtracking.
9. Find all Hamiltonian cycles in a connected undirected graph of n vertices using backtracking.
10. Implement assignment problem using branch and bound strategy.
11. Case Study on Greedy Algorithm

    George is owner of an automobile spare-part shop. He wants to buy some accessories for his shop. The store in the market has, say, a total of, T types of accessories, and every jthaccessor costs j dollars ($1 \leq j \leq T$). Let the store has an unlimited supply of each accessory. George's profit depends directly upon how much money he spends during a purchase trip. George wants to purchase a total of N accessories according to the following rule: Any M-element subset of the purchased items should contain at least D distinct types of accessories. For example if George want to buy 7 accessories ($N = 7$), the shop has a total of 10 types of them($T = 10$),given the value of $M = 4$,and $D = 2$, he must choose 7 accessories such that, any subset of 4 accessories from 7 will contain at least 2 distinct types of items. Given input of N, T, M and D, find the maximum amount of money that George can spend around the trip; if it's not possible for George to make a purchase during a certain trip, return False instead.

TOTAL PERIODS 60

COURSE OUTCOMES

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

- program, execute, understand the complexity of various sorting and searching algorithms.
- design and execute problems related to dynamic and greedy technique.
- depict graph related algorithms such as shortest path and minimum spanning tree.
- design various backtracking and branch/ bound algorithms.

CO/PO MAPPING

Mapping of Course Outcomes with Programme Outcome (3/2/1 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak														
COs	**Programme Outcomes (POs)**												**Programme Specific Outcomes (PSOs)**	
	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO 1**	**PSO2**
CO1	3	3	3	2	3	3	2	1	1	1	2	3	1	-
CO2	3	3	2	2	2	3	2	-	2	-	2	3	2	-
CO3	3	3	3	2	1	3	2	2	2	2	2	3	2	2
CO4	3	3	3	2	3	3	2	2	-	2	2	3	2	1

EN20501 **CAREER DEVELOPMENT LABORATORY I** **0 0 2 1**

COURSE OBJECTIVES

To enable students to

- enhance their Writing Skills.
- evaluate their Presentation Skill to face the corporate world.
- solve the quantitative aptitude problems and improve their Mental ability.
- improve their reasoning skills.

UNIT I WRITING SKILLS **6**

Writing Skills: The Essentials of Writing – The Importance of Structure – Types of Writing – Common Mistakes in Writing.

Activities: Email Writing - Paragraph writing – Report Writing – Story Writing - Story Telling Session: 2 – JAM Session 1.

UNIT II PRESENTATION SKILLS & GROUP DISCUSSION **6**

Presentation Skills: Types of Presentation– Methods of Delivering Presentation –Ways to improve the Presentation – Presentation Aids: Group Discussion: Introduction –Types & Importance – Why GD – Types of GD- Evaluation Criteria – Do's & Don'ts of GD.

Activities: Presentation Session I, Group Discussion Session I, Role Play Session (Team): Level II – Personality Profile Session II – Company Profile Analysis Session II.

UNIT III QUANTITATIVE APTITUDE **6**

Simplification – Cubes & Cube Roots – Squares & Square Roots – Boats & Streams – Trains – Profit & Loss – Pipes & Cisterns.

UNIT IV LOGICAL REASONING - I **6**

Series Completion – Letter Series – Symbol Series – Number Series – Arithmetic Reasoning.

UNIT V LOGICAL REASONING - II **6**

Blood Relations – Seating Arrangement - Character Puzzle.

TOTAL PERIODS: 30

COURSE OUTCOMES

Upon completion of the course, the students will be able to

- excel in drafting mails and speaking
- demonstrate the participative skills in the group discussions
- solve problems based on quantitative aptitude
- enhance the logical and verbal reasoning

TEXTBOOKS

1. Agarwal, R.S." a modern approach to Verbal & Non Verbal Reasoning", S.Chand& Co Ltd, new delhi
2. Agarwal, R.S. "Objective General English", S.Chand&Co

REFERENCES

1. Abhijit Guha, "Quantitative Aptitude ", Tata-Mcgraw Hill.
2. Word Power Made Easy By Norman Lewis ,Wr.Goyal Publications.
3. Johnson, D.W. Reaching out – Interpersonal Effectiveness and self actualization. Boston: Allyn And Bacon.
4. Infosys Campus Connect Program – students' guide for soft skills.

CO/PO MAPPING

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) (1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak														
CO's	**Programme Outcomes (PO's)**													
	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO1**	**PSO2**
CO1	3	2	2	3	3	1	1	1	2	-	-	1	3	2
CO2	2	2	3	1	2	2	2	-	3	2	1	2	3	2
CO3	3	2	2	2	2	2	1	-	2	2	2	2	2	3
CO4	3	2	2	1	1	1	-	-	2	3	2	3	2	3
CO5	2	3	3	2	1	3	3	1	3	1	2	1	2	3

SEMESTER VI

CY20601	SOFTWARE ENGINEERING	3	0	0	3

COURSE OBJECTIVES

To enable the students to

- understand the phases in a software project development process.
- acquire knowledge on fundamental concepts of requirements engineering and analysis modeling.
- categorize the major considerations for enterprise integration and deployment.
- analyze various testing and maintenance measures.
- estimate and manage software projects.

UNIT I SOFTWARE PROCESS 9

Introduction to Software Engineering - The nature of software, software process; The Process Framework - Umbrella activities, software process models; Prescriptive Process Models - Specialized process models, the unified process, Agile development; Introduction to Agility- Agile process, extreme programming.

UNIT II SOFTWARE REQUIREMENTS AND MODELING 9

Understanding Requirements - Establishing the groundwork, eliciting requirements, building the analysis model; Requirements Modeling - Scenario-based methods, class-based methods, requirements modeling for web and mobile apps.

UNIT III SOFTWARE DESIGN 9

Design Concepts - The design process, design concepts; The Design Model - Architectural design, component level design, designing class-based components; User Interface Design - Interface analysis, interface design, interface design steps, pattern-based design, pattern-based software design.

UNIT IV SOFTWARE TESTING STRATEGIES 9

A Strategic Approach to Software Testing- Test strategies for conventional software, test strategies for object-oriented software, system testing; testing conventional applications- white-box testing; Black-Box Testing; Testing Object Oriented Applications - Testing OOA and OOD models, object-oriented testing strategies, object-oriented testing method.

UNIT V MANAGING SOFTWARE PROJECTS 9

Project Management Concepts - Estimation for Software Projects - Software project estimation; Decomposition Techniques - Empirical Estimation Models - Project Scheduling - Basic concepts, scheduling; Risk Management - risk identification, projection, risk refinement; Maintenance and Reengineering- software maintenance, software reengineering, reverse engineering, restructuring, forward engineering.

TOTAL PERIODS 45

COURSE OUTCOMES

Upon the completion of the course, the students will be able to

- compare different software development process models.
- design the software model based on the requirement analysis.
- identify the software design in managing a software project.
- analyze various testing and maintenance for a given software project.
- incorporate various software project management concepts during software development.

TEXTB O O K S

1. Rogers. Pressman Software Engineering: A Practitioner's Approach, McGraw Hill International edition, Eighth edition, 2015.
2. Ian Sommerville, Software Engineering, 9 th Edition, Pearson Education,2011.

REFERENCES

1. Rajib Mall, "Fundamentals of Software Engineering", Third Edition, PHI Learning Private Limited,2009.
2. PankajJalote, "Software Engineering, A Precise Approach", Wiley India, 2010.
3. Kelkar S.A., "Software Engineering", Prentice Hall of India Pvt Ltd,2007.
4. Stephen R.Schach, "Software Engineering", Tata McGraw-Hill Publishing Company Limited,2007.

CO-PO MAPPING

Mapping of Course Outcomes with Programme Outcome

(1,2,3 indicates the strength of correlation) 3 – Strong, 2 – Medium, 1 - Less

CO	PO												PSO	
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	1	1	-	-	3	-	-	1	-	-	2	2
CO2	3	3	2	1	1	2	3	2	1	2	2	1	1	1
CO3	3	3	2	2	1	2	3	3	1	-	1	2	1	2
CO4	3	3	3	3	2	1	3	3	1	1	1	2	1	3
CO5	3	3	3	3	3	1	3	1	1	-	1	2	1	3

CY20602 **ARTIFICIAL INTELLIGENCE** **3 0 0 3**

COURSE OBJECTIVES

To enable the students to

- acquire a knowledge of various methods of different problem solving and searching.
- understand the concepts of knowledge representation.
- understand about inference and how to solve the problems using various inference technique.
- realize the concepts of planning and learning.
- design various AI systems.

UNIT I INTRODUCTION **9**

Introduction to AI - Problem formulation, Problem Definition, Production systems, Control strategies, Search strategies; Problem characteristics - Production system characteristics - Specialized productions system - Problemsolving methods - Problem graphs - Matching - Indexing and Heuristic functions - Hill Climbing - Depth first and Breath first - Constraints satisfaction - Related algorithms - Measure of performance and analysis of search algorithms.

UNIT II REPRESENTATION OF KNOWLEDGE **9**

Game playing - Knowledge representation - Knowledge representation using Predicate logic, Introduction to predicate calculus, Resolution, Use of predicate calculus; Knowledge representation using other - Structured representation of knowledge.

UNIT III KNOWLEDGE INFERENCE **9**

Knowledge representation - Production based system - Frame based system - Inference - Backward logic chaining, Forward chaining; Rule value approach - Fuzzy reasoning.

UNIT IV PLANNING AND EXPERT SYSTEM **9**

Basic plan generation systems - Strips, Advanced plan generation systems, K strips; Strategic explanations - Why, Why not and how explanations; Expert systems - Architecture of expert systems, Roles of expert systems, Knowledge Acquisition, Typical expert systems Applications; MYCIN - DART - XOON.

UNIT V AI APPLICATIONS **9**

AI Applications - Language Models - Information Retrieval - Information Extraction - Natural Language Processing - Machine Translation - Speech Recognition - Robot – Hardware, Perception, Planning, Moving.

TOTAL PERIODS **45**

COURSE OUTCOMES

At the end of the course, the students will be able to

- demonstrate awareness of intelligent agents and problem solving using uninformed, informed and local search methods.
- develop knowledge about usage of propositional logic and first order logic for making inferences.
- use the knowledge and the process of inference to derive new facts.
- describe the use of planning and explain about various expert systems.
- design and develop various AI systems.

TEXTBOOKS

1. Kevin Night and Elaine Rich, Nair B, "Artificial Intelligence", 3rd edition, McGraw Hill- 2017.
2. Stuart Russel and Peter Norvig, "AI -A Modern Approach", 3rd Edition, Pearson Education 2015.

REFERENCES

1. Lavika Goel "Artificial Intelligence Concepts and Applications", Wiley 2021.
2. Dan W. Patterson, "Introduction to AI and ES", Pearson Education, 2015.
3. Deepak Khemani, "Artificial Intelligence", Tata McGraw Hill Education 2013.
4. Patrick H. Winston, "Artificial Intelligence", Third Edition, Pearson Education, 2006.

CO-PO MAPPING

Mapping of Course Outcomes with Programme Outcome
(3/2/1 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

COs	Programme Outcomes (POs)												Programme Specific Outcomes (PSOs)	
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	1	1	1	1	-	1	-	1	1	2	3	2
CO2	2	2	1	1	1	1	-	1	-	1	1	1	3	2
CO3	3	2	3	1	1	1	1	1	1	1	-	1	2	1
CO4	2	2	3	2	1	1	1	-	1	1	2	1	2	3
CO5	3	2	2	1	1	1	1	-	1	1	-	2	1	1

CY20603 PENETRATION TESTING AND VULNERABILITY ASSESSMENT 3 0 0 3

COURSE OBJECTIVES

To enable the students to

- impart the fundamental aspects and principles of security protocols
- learn about the cross-site scripting
- understand the SQL injection concepts
- gain the knowledge of web environment vulnerability
- understand the xml attacks

UNIT I INTRODUCTION 9

Penetration Testing phases - Testing Process, types and Techniques, Blue/Red Teaming, Strategies of Testing, Non-Disclosure Agreement Checklist, Phases of hacking, Open source/proprietary Pentest Methodologies.

UNIT II INFORMATION GATHERING AND SCANNING 9

Information gathering methodologies - Foot printing, Competitive Intelligence DNS Enumerations, Social Engineering attacks; Port Scanning - Network Scanning Vulnerability Scanning, NMAP scanning tool , OS Fingerprinting , Enumeration

UNIT III SYSTEM HACKING 9

Password cracking techniques - Key loggers; Escalating privileges - Hiding Files, Double Encoding, Steganography technologies and its Countermeasures. Active and passive sniffing, ARP Poisoning, MAC Flooding, SQL Injection, Error based, Union - based, Time-based, Blind SQL, Out-of-band. Injection Prevention Techniques.

UNIT IV ADVANCED SYSTEM HACKING 9

Broken Authentication - Sensitive Data Exposure, XML External Entities, Broken Access Code; XSS - Stored, Reflected, DOM Based.

UNIT V WIRELESS PENTEST 9

Wi-Fi Authentication Modes - Bypassing WLAN Authentication, Types of Wireless Encryption, WLAN Encryption Flaws, AP Attack, Attacks on the WLAN Infrastructure, DoS-Layer1, Layer2, Layer 3, DDoS Attack, Client Mis association, Wireless Hacking Methodology, Wireless Traffic Analysis.

TOTAL PERIODS 45

COURSE OUTCOMES

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

- analyse the basic protocols
- understand the cross-site scripting
- solve SQL vulnerability
- analyze the file upload vulnerabilities
- perform the evaluation of xml attacks

TEXTBOOKS

1. Prakhar Prasad," Mastering Modern Web Penetration Testing " , Packt Publishing, October 2016.
2. Wolf Halton, Bo Weaver, "Kali Linux 2: Windows Penetration Testing ", Packt Publishing June 2016.

REFERENCES

1. Robert Svensson, From Hacking to Report Writing: An Introduction to Security and Penetration Testing 2016, ISBN 978-1-4842-2282-9
2. Georgia Weidman," Penetration Testing: A Hands On Introduction to Hacking", No Startch Press, First Edition 2014. ISBN-13: 978-1593275648 ISBN-10: 1593275641
3. B.Singh, H.Joseph and Abhishek Singh,"Vulnerability Analysis and Defense for the Internet, Springer, 2008 Edition. ISBN-10: 0387743898 ISBN-13: 978-0387743899.
4. Rafay Baloch, "Ethical Hacking and Penetration Testing Guide",CRC Press, 2015,ISBN 78-1-4822-3161-8.

CO-PO MAPPING

Mapping of Course Outcomes with Programme Outcome (3/2/1 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

COs	Programme Outcomes (POs)												Programme Specific Outcomes (PSOs)	
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	1	1	1	1	-	1	-	1	1	2	3	2
CO2	2	2	1	1	1	1	-	1	-	1	1	1	3	2
CO3	3	2	3	1	1	1	1	1	1	1	-	1	2	1
CO4	2	2	3	2	1	1	1	-	1	1	2	1	2	3
CO5	3	2	2	1	1	1	1	-	1	1	-	2	1	1

CY20604	PENETRATION TESTING AND VULNERABILITY ASSESSMENT LABORATORY	0	0	4	2

COURSE OBJECTIVES

To enable students to

- Introduce the methodologies framework tools of penetration testing to get awareness in enhancing the security.
- get knowledge on various attacks and their directions
- get knowledge on root kits
- get knowledge on Nmap Scanner

LIST OF EXPERIEMENTS

1. Setup a honey pot and monitor the honey pot on network
2. Write a script or code to demonstrate SQL injection attacks
3. Create a social networking website login page using phishing techniques
4. To encrypt and decrypt passwords using RC4 algorithm in CRYPT TOOL.
5. Traceroute, ping, ifconfig, netstat Command
6. Using Nmap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAS.
7. Wireshark sniffer to capture network traffic and analyze.
8. Simulate persistent Cross Site Scripting attack.
9. Create a simple keylogger using python
10. Study of Techniques uses for Web Based Password Capturing.
11. Write a code to demonstrate DoS attacks
12. Install rootkits and study variety of options

TOTAL PERIODS 60

COURSE OUTCOMES

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

- gain the knowledge of the use and availability of tools to support an ethical hack
- gain the knowledge of interpreting the results of a controlled attack
- gain knowledge on rootkits
- gain knowledge on Nmap Scanner

CO-PO MAPPING

Mapping of Course Outcomes with Programme Outcome (3/2/1 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak														
COs	**Programme Outcomes (POs)**												**Programme Specific Outcomes (PSOs)**	
	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO1**	**PSO2**
CO1	3	2	1	1	1	1	-	-	-	1	1	2	3	2
CO2	2	2	1	1	1	1	-	-	-	1	1	1	3	2
CO3	3	2	3	1	1	1	1	-	1	1	2	1	2	1
CO4	2	2	3	2	1	1	1	-	1	1	-	1	2	3

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
AUTONOMOUS

CY20605 **ARTIFICIAL INTELLIGENCE LABORATORY** **0 0 4 2**

COURSE OBJECTIVES

To enable the students to

- provide a strong foundation of fundamental concepts in artificial intelligence.
- enable the students to apply ai techniques in applications which involve perception, reasoning, and learning.
- empowering humans to perform collaborative activities in complex and dynamic settings.
- exploiting and integrating information coming from different (and possibly heterogeneous) information sources.

LIST OF EXPERIMENTS USING C/C++, PERFORM THE FOLLOWING EXPERIMENTS

1. Depth first search.
2. Breadth first search.
3. Best first search.
4. Travelling sales man problem.
5. Water jug problem.
6. Tower of Hanoi problem.
7. Eight puzzle problem.
8. A* search.
9. AO* search.
10. Design Expert System.

TOTAL PERIODS 60

COURSE OUTCOMES

Upon the completion of the course, students will be able to

- demonstrate the use of different search techniques for problem solving.
- develop solutions for some ai problems.
- demonstrate the use of "prolog" for predicate logic applications.
- design an expert system.

CO-PO MAPPING

Mapping of Course Outcomes with Programme Outcome (3/2/1 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

COs	Programme Outcomes (POs)												Programme Specific Outcomes (PSOs)	
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO 2
CO1	3	2	1	1	1	1	-	-	-	1	1	2	3	2
CO2	2	2	1	1	1	1	-	-	-	1	1	1	3	2
CO3	3	2	3	1	1	1	1	-	1	1	-	1	2	1
CO4	2	2	3	2	1	1	1	-	1	1	-	1	2	3

EN20601 CAREER DEVELOPMENT LABORATORY II 0 0 2 1

COURSE OBJECTIVES

To enable students to

- draft resume and enhance their skills to manage stress to survive in corporate world.
- excel in interview skills.
- solve the quantitative aptitude problems and improve their problem-solving skills.
- improve their reasoning skills to get placed in reputed companies.

UNIT I RESUME WRITINGS 6

Resume Writing Skills: Curriculum Vitae and Resume – Things to do while writing a Resume – Mistakes and Pitfalls to Avoid- Cover Letter: General Guidelines – The Content - Stress Management – Dressing Etiquette

Activities: Corporate Resume Building Session I – JAM Session: Level III – Role Play Session (Individual): Level III - Company Profile Analysis Session III – Personality Profile Analysis Session III

UNIT II INTERVIEW SKILLS 6

Interview Skills: Introduction – Before the Interview – During the Interview – After the Interview – Types of Interview

Activities: Presentation Session: Level II- Group Discussion Session: Level III ,Mock Interview Practice Session, Corporate Resume Building Session II

UNIT III QUANTITATIVE APTITUDE 6

Permutation and Combination – Probability: Dice, Colours, Coin, Cards ; Partnership – Ages – Calendars

UNIT IV LOGICAL REASONING -I 6

Making Judgments – Matching Definitions – Cause and Effect

UNIT V LOGICAL REASONING II 6

Directions – Syllogism – Analogy – Statements and Arguments

TOTAL PERIODS 30

COURSE OUTCOMES

Upon completion of the course, the students will be able to

- write resume and enhance their etiquettes.
- demonstrate the interpersonal skills in group discussions.
- compute problems based on quantitative aptitude.
- reveal their logical and verbal reasoning by scoring the expected percentage to get placed in reputed companies.

TEXTBOOKS

- Agarwal, R.S." a modern approach to Verbal & Non Verbal Reasoning", S.Chand& Co Ltd, new delhi.2015.
- Agarwal, R.S. " Objective General English", S.Chand&Co.2016.

REFERENCES

- Abhijit Guha, "Quantitative Aptitude ", Tata-Mcgraw Hill.2015.
- Word Power Made Easy By Norman Lewis ,Wr.Goyal Publications.2016.
- Johnson, D.W. Reaching out – Interpersonal Effectiveness and self actualization. Boston: Allyn And Bacon.2019.
- Infosys Campus Connect Program – students' guide for soft skills.2015.

CO/PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) (1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak														
CO's	Programme Outcomes (PO's)													
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	2	3	3	1	-	-	-	-	-	-	3	2
CO2	-	2	3	-	2	-	2	-	-	-	-	-	3	2
CO3	3	2	2	2	-	-	1	-	-	-	-	-	2	3
CO4	3	2	2	-	-	1	-	-	-	-	2	-	2	3
CO5	2	3	3	2	1	3	3	1	-	1	2	-	2	3

PROGRAM ELECTIVE - 1

CY20151 **FORMAL LANGUAGES AND AUTOMATA** **3 0 0 3**

COURSE OBJECTIVES

To enable the students to

- provide introduction to some of the central ideas of theoretical computer science from the Perspective of formal languages and understand deterministic and non-deterministic machines
- introduce the fundamental concepts of regular expression and finite automata.
- introduce the fundamental concepts of context free grammar.
- employ push down automata to solve problems in computing.
- understand Turing machines and the differences between decidability and undecidability.

UNIT I INTRODUCTION TO FINITE AUTOMATA 9

Introduction to finite automata structural representations - the central concepts of automata theory, alphabets, strings, languages, problems; Nondeterministic finite automata - formal definition, finite automata with epsilon, transitions; Deterministic finite automata - definition of DFA, DFA process strings, language of DFA, conversion of NFA with ε-transitions to NFA without ε transitions; conversionof NFA to DFA.

UNIT II REGULAR EXPRESSIONS 9

Regular expressions - finite automata and regular expressions - applications of regular expressions algebraic laws for regular expressions - properties of regular languages pumping lemma for regular languages - applications of the pumping lemma - closure properties of regular languages - decision properties of regular languages; equivalence and minimization of automata.

UNIT III CONTEXT FREE GRAMMAR 9

Context-Free Grammars - definition of context - free grammars; Derivations using a grammar - leftmost and right most derivations, the language of a grammar, sentential forms, parse trees; Applications of context - free grammars, ambiguity in grammars and languages; Normal forms for context free grammars - eliminating useless symbols; Eliminating - productions; Chomsky normal form griebach normal form; Pumping lemma for context - free languages, statement of pumping lemma, applications Closure properties of CFL's, decision Properties of CFL's.

UNIT IV PUSH DOWN AUTOMATA 9

Push Down Automata - definition of the pushdown automaton, languages of a PDA, equivalence of PDA's and CFG's, acceptance by final state, acceptance by empty stack; deterministic pushdown automata;CFG to PDA, PDA to CFG.

UNIT V TURING MACHINE 9

Introduction to turning machine - Formal Description, Instantaneous description, the language of Turing machine and halting Undecidability, A language that is Not Recursively Enumerable, An Undecidable Problem that is RE, undecidable Problems about Turing machines, Recursive Languages, Properties of recursive languages, Post's Correspondence Problem.

TOTAL PERIODS 45

COURSE OUTCOMES

At the end this course, students will be able to

- understand the concept of finite automata and to recognize the languages.
- convert regular expression to finite automata and minimize the DFA
- design context free grammars for formal language
- know the concept of PDA and its conversions.
- gain proficiency with Turing machine and distinguish between decidability and undecidability.

TEXTBOOKS

1. "Introduction to Automata Theory, Languages and Computations", Third Edition, J.E.Hopcroft, R.Motwani and J.D Ullman, Pearson Education.
2. "Introduction to the Theory of Computation", Micheal Sipser, 3rd edition, Cengage Learning.

REFERENCES

1. "Introduction to Languages and the Theory of Computation", John C.Martin, Fourth Edition, Tata McGraw Hill.
2. "Introduction to Computer Theory, Daniel I.A.Cohen, John Wiley.
3. Hopcroft J.E., Ullman J.D Introduction to Automata Theory, Languages, and Computation (3rd Edn). Reading, MA: Addison-Wesley. (2006).
4. Eitan G An Introduction to the "Theory of Computation". Computer Science Press. (1989).

CO/PO MAPPING

Mapping of Course Outcomes with Programme Outcome (3/2/1 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak														
COs	**Programme Outcomes (POs)**												**Programme Specific Outcomes (PSOs)**	
	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO1**	**PSO2**
CO1	3	2	1	1	1	1	-	1	-	1	1	2	3	2
CO2	2	2	1	1	1	1	-	1	-	1	1	1	3	2
CO3	3	2	3	1	1	1	1	1	1	1	-	1	2	1
CO4	2	2	3	2	1	1	1	-	1	1	-	1	2	3
CO5	3	2	2	1	1	1	1	-	1	1	-	2	1	1

CY20152 CYBER PHYSICAL SYSTEMS 3 0 0 3

COURSE OBJECTIVES

To enable the students to

- understand the basics of cyber physical systems.
- design synchronous models for Real Time applications.
- design Asynchronous models for Real Time applications.
- develop Deep Understanding on selection of hardware and software's for designing dynamical systems.
- design and implement cyber physical system and address the problems and limitations for real world problems.

UNIT I INTRODUCTION TO CYBER PHYSICAL SYSTEMS 9

Introduction To Cyber - Physical Systems, Cyber-Physical Systems Design Recommendations, Cyber-Physical System Requirements ; Requirements Engineering, Interoperability, Real Time System - GPU Computing, Internet Of Things (IOT) , Radio Frequency Identification Technology; Wireless Sensor Networks Technology, Powerline Communication, Smart Cities And Internet of Everything; Ubiquitous Computing Fundamentals - Core Properties Of Ubiquitous Computing, Smart Devices Components And Services, Autonomous Systems In Ubiquitous Computing; CASE STUDY: Cyber Physical Vehicle Tracking System.

UNIT II SYNCHRONOUS MODEL 9

Reactive Components - Variables, Valuations, And Expression, Execution, Extended, State Machines; Properties of Components, Finite State Components, Combinational Components, Event, Triggered Components, Nondeterministic Components, Input Enabled Components, Task Graphs and Await Dependencies; Composing Components - Block Diagrams Input / Output Variable Renaming, Parallel Composition, Output Hiding, Synchronous Designs - Synchronous Circuits, Cruise Control Systems, Synchronous Networks.

UNIT III ASYNCHRONOUS MODEL 9

Asynchronous Process - States, Internal Actions, Executions, Extended State Machines, Operation on Process; Asynchronous Design Primitives - Blocking Vs Non-Blocking Synchronization, Deadlocks, Shared Memory, Fairness Assumptions; Asynchronous Coordination Protocols, LeaderElection, Reliable Transmission - Wait Fee Consensus, Safety Specifications, Invariants of Transition Systems, Safety Monitors.

UNIT IV DYNAMICAL SYSTEM 9

Continuous Time Model - Continuously Evolving Inputs and Outputs, Models with Disturbance, Composing Components Stability; Linear Systems Linearity, Solutions of Linear Differential Equations Stability; Designing Controllers - Open Loop Vs Feedback Controller, Stabilizing Controller, PID Controllers; Analysis Techniques - Numerical Solutions; Barrier Certificates.

UNIT V HYBRID SYSTEMS 9

Hybrid Dynamical Model - Hybrid Process, Process Composition, Zeno Behavior, Stability; Designing Hybrid Systems - Automated Guided Vehicle, Obstacle Avoidance with Multi Robot Coordination, Multi Hop Control Networks, Linear Hybrid Automata, Example Pursuit Game - Formal Model; Symbolic Reachability Analysis; Timed Automata Model of Timed Automata.

TOTAL PERIODS 45

COURSE OUTCOMES

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

- understand the basics of cyber physical systems.
- design synchronous models for Real Time applications.
- design Asynchronous models for Real Time applications.
- develop Deep Understanding on selection of hardware and software's for designing dynamical systems
- come up with cost effective, reliable, robust and feasible designs for real world problems.

TEXTBOOKS

1. Rajeev Alur, Principles of Cyber Physical Systems, 1st Edition, MIT Press 2015.
2. E. A. Lee and S. A. Seshia, Introduction to Embedded Systems – A Cyber-Physical Systems Approach, Lulu.com, First Edition, Jan 2013.

REFERENCES

1. Raj Rajkumar, "Cyber Physical Systems," 2nd Edition, Elsevier 2015.
2. Edward D Lamie, "Computing Fundamentals Of Cyber Physical Systems " , 2nd Edition,Newnes Elsevier Publication.
3. Sang C.Suh , U.JohnTanik and John N.Carbone , Applied Cyber-Physical systems, Springer,2014.
4. Hespanha, Joao P. Linear systems theory. Princeton university press, 2009.

CO/PO MAPPING

Mapping of Course Outcomes with Programme Outcome (3/2/1 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak														
COs	**Programme Outcomes (POs)**												**Programme Specific Outcomes (PSOs)**	
	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO1**	**PSO 2**
CO1	3	3	3	3	3	3	-	3	3	3	3	3	3	3
CO2	3	3	3	2	3	3	2	3	2	2	2	3	3	2
CO3	2	3	3	3	3	3	-	3	3	3	3	3	3	3
CO4	2	3	2	3	2	2	1	2	3	2	3	2	2	3
CO5	3	3	3	3	3	3	-	3	2	3	2	3	3	3

CY20153 **DATA WAREHOUSING AND DATA MINING** **3 0 0 3**

COURSE OBJECTIVES

To enable the students to

- understand the design and implementation of a data store
- acquire knowledge on data and various preprocessing techniques
- analyze the various correlation based frequent patterns mining in large data sets
- learn various classifiers in data mining
- understand the data mining techniques and methods to be applied on large data sets.

UNIT I DATA WAREHOUSING **9**

Data warehouse - Basic Concepts, Modeling, Design, and usage; Implementation - Data cube Computation Methods; Data Generalization by Attribute Oriented Induction approach.

UNIT II DATA MINING **9**

Introduction - Kinds of Data and Patterns, Major Issues in Data Mining, Statistical Description of Data, Measuring Data Similarity and Dissimilarity; Data preprocessing - Data Cleaning, Data Integration, Data Transformation, Data Reduction - Data Discretization Concept Hierarchy Generation.

UNIT III ASSOCIATION RULE MINING **9**

Basic concepts - Frequent Item set Mining Methods - Apriori algorithm, A Pattern Growth Approach for Mining Frequent Item sets, Mining Various Kinds of Association Rules, Correlation Analysis; Constraint Based Association Mining.

UNIT IV CLASSIFICATION **9**

Basic Concepts - Decision Tree Induction - Bayes Classification Methods - Rule Based Classification- Classification by Back propagation - Support vector machines - Associative Classification - Lazy Learners - Other Classification Methods - Prediction.

UNIT V CLUSTERING AND DATA MINING APPLICATIONS **9**

Cluster analysis - Partitioning Methods - Hierarchical Methods - Density Based Methods - Grid Based Methods - Model Based Clustering Methods - Clustering High Dimensional Data - Constraint Based Clustering Analysis - Outlier Analysis - Data Mining Applications - Financial Data Analysis, Science and Engineering, Intrusion Detection and Prevention.

TOTAL PERIODS **45**

COURSE OUTCOMES

At the end of the course, the students will be able to

- understand the design of a data warehouse
- apply preprocessing techniques
- identify frequent patterns in large data sets
- compare and contrast the various classifiers
- apply clustering techniques and methods to large data sets

TEXTBOOKS

1. Jiawei Han and Micheline Kamber, —Data Mining Concepts and Techniques, Third Edition, Elsevier, 2012.
2. Alex Berson and Stephen J.Smith, —Data Warehousing, Data Mining & OLAP‖, Tata McGraw – Hill Edition, 35th Reprint 2016.

REFERENCES

1. Alex Berson and Stephen J.Smith, —Data Warehousing, Data Mining & OLAP‖, Tata McGraw – Hill Edition, 35th Reprint 2016.
2. K.P. Soman, Shyam Diwakar and V. Ajay, —Insight into Data Mining Theory and Practice, Eastern Economy Edition, Prentice Hall of India, 2006.
3. Ian H.Witten and Eibe Frank, —Data Mining: Practical Machine Learning Tools and Techniques, Elsevier, Second Edition.
4. Agile Data Warehouse Design: Collaborative Dimensional Modeling, from Whiteboard to Star Schema.

CO/PO MAPPING

Mapping of Course Outcomes with Programme Outcome
(3/2/1 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

COs	Programme Outcomes (POs)												Programme Specific Outcomes (PSOs)	
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	1	1	1	1	-	-	-	1	1	2	3	2
CO2	2	2	1	1	1	1	-	1	-	1	1	1	3	2
CO3	3	2	3	1	1	1	1	3	1	1	3	1	2	1
CO4	2	2	3	2	1	1	1	3	1	1	3	1	2	3
CO5	3	2	2	1	1	1	1	2	1	1	2	2	1	1

CY20154 MOBILE AND WIRELESS SECURITY 3 0 0 3

COURSE OBJECTIVES

To enable the students to

- study salient features of various wireless and mobile technology.
- understand the need of security at mobile device, network, server levels
- explain the security issues in cellular networks.
- know about various types of threats for MANET applications.
- learn security challenges and attacks over mobile commerce services

UNIT I SECURITY ISSUES IN MOBILE COMMUNICATION 9

Mobile Communication History - Security – Wired Vs Wireless, Security Issues in Wireless and Mobile Communications, Security Requirements in Wireless and Mobile Communications, Security for Mobile Applications, Advantages and Disadvantages of Application-level Security.

UNIT II SECURITY OF DEVICE, NETWORK, AND SERVER LEVELS 9

Mobile Devices Security Requirements - Mobile Wireless network level Security, Server Level Security; Application - Level Security in Wireless Networks - Application of WLANs, Wireless Threats, Some Vulnerabilities and Attach Methods over WLANs, Security for 1G Wi-Fi Applications, Security for 2GWi-Fi Applications, Recent Security Schemes for Wi-Fi Applications.

UNIT III APPLICATION-LEVEL SECURITY IN CELLULAR NETWORKS 9

Generations of Cellular Networks - Security Issues and attacks in cellular networks - GSM Security for applications - GPRS Security for applications - UMTS security for applications - 3G security for applications - Some of Security and authentication Solutions.

UNIT IV APPLICATION-LEVEL SECURITY IN MANETS 9

MANETs-Applications of MANETs, MANET Features, Security Challenges in MANETs; Security Attacks on MANETs - External Threats for MANET applications, Internal threats for MANET Applications, Some of the Security Solutions; Ubiquitous Computing - Need for Novel Security Schemes for UC Security Challenges for UC, Security Attacks on UC networks, Some of the security solutions for UC.

UNIT V SECURITY FOR MOBILE COMMERCE APPLICATION 9

M-commerce Applications - M-commerce Initiatives - Security Challenges in Mobile E-commerce - Types of Attacks on Mobile E-commerce - A Secure M-commerce Model Based on Wireless LocalArea Network - Some of M-Commerce Security Solutions.

TOTAL PERIODS 45

COURSE OUTCOMES

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

- describe salient features of various wireless and mobile technology.
- explain the need of security at mobile device, network, server levels
- summarize the security issues in cellular networks.
- list the various types of threats for MANET applications.
- discuss security challenges and attacks over mobile commerce services

TEXTBOOKS

1. Pallapa Venkataram, Satish Babu,"Wireless and Mobile Network Security", 1st Edition, TataMcGraw Hill,2010.
2. Man Ho Au, Raymond Choo,"Mobile Security and Privacy",1st Edition , Syngress Publisher,2016

EFERENCES

1. Frank Adelstein, K.S.Gupta , "Fundamentals of Mobile and Pervasive Computing", 1st Edition, Tata McGraw Hill 2005.
2. Randall k. Nichols, Panos C. Lekkas , "Wireless Security Models, Threats and Solutions", 1st Edition, Tata McGraw Hill, 2006.
3. Bruce Potter and Bob Fleck , "802.11 Security" , 1st Edition, SPD O'REILLY 2005.
4. James Kempf, "Guide to Wireless Network Security, Springer. Wireless Internet Security – Architecture and Protocols", 1st Edition, Cambridge University Press, 2008.

CO-PO MAPPING

Mapping of Course Outcomes with Programme Outcome (3/2/1 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak														
COs	**Programme Outcomes (POs)**												**Programme Specific Outcomes (PSOs)**	
	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO1**	**PSO2**
CO1	3	2	3	2	3	2	3	2	3	2	3	2	3	2
CO2	2	2	2	3	2	3	2	2	2	2	2	2	2	2
CO3	3	2	3	2	3	2	3	2	2	2	2	2	2	2
CO4	2	2	3	2	2	3	2	3	2	2	2	2	2	3
CO5	3	2	2	2	3	2	3	2	2	2	2	2	2	2

PROFESSIONAL ELECTIVE COURSES (PE-II)

CY20251 **COMPILER DESIGN** **3 0 0 3**

COURSE OBJECTIVES

To enable the students to

- learn the design principles of a compiler
- understand the various parsing techniques
- learn different levels of translation
- learn to optimize machine codes
- learn to generate machine codes.

UNIT I INTRODUCTION TO COMPILERS **9**

Translators - Compilation and Interpretation - Language processors - The Phases of Compiler-Errors encountered in Different Phases - The Grouping of Phases - Compiler Construction Tools - ProgrammingLanguage basics.

UNIT II LEXICAL ANALYSIS **9**

Need and Role of Lexical Analyzer - Lexical Errors-Expressing Tokens by Regular Expressions - Converting Regular Expression to DFA - Minimization of DFA - Language for Specifying Lexical Analyzers - LEX-Design of Lexical Analyzer for a sample Language.

UNIT III SYNTAX ANALYSIS **9**

Need and Role of the Parser-Context Free Grammars - Top Down Parsing - General Strategies - Recursive Descent Parser Predictive Parser - LL (1) Parser-Shift Reduce Parser-LR Parser - LR (0)Item-Construction of SLR Parsing Table - Introduction to LALR Parser – Error Handling and Recovery in Syntax Analyzer - YACC-Design of a syntax Analyzer for a Sample Language.

UNIT IV SYNTAX DIRECTED TRANSLATION & RUN TIME ENVIRONMENT **9**

Syntax directed Definitions- Construction of Syntax Tree - Bottom-up Evaluation of S-Attribute Definitions - Design of predictive translator – Type Systems - Specification of a simple type of checker-Equivalence of Type Expressions-Type Conversions. RUN - TIME ENVIRONMENT - Source Language Issues - Storage Organization- Storage Allocation - Parameter Passing-Symbol Tables - Dynamic Storage Allocation - Storage Allocation in FORTAN.

UNIT V CODE OPTIMIZATION AND CODE GENERATION **9**

Principal Sources of Optimization – DAG - Optimization of Basic Blocks - Global Data Flow Analysis - Efficient Data Flow Algorithms - Issues in Design of a Code Generator - A Simple Code Generator Algorithm. Case Study - Single pass and two pass compilers.

TOTAL PERIODS 45

COURSE OUTCOMES

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

- design and implement a prototype compiler.
- use the knowledge of patterns, tokens & regular expressions for solving a problem in the field of datamining.
- apply the various optimization techniques
- develop the runtime structures used to represent constructs in typical programming languages
- use the different compiler construction tools.

TEXTBOOKS

1. Alfred V Aho, Monica S. Lam, Ravi Sethi and Jeffrey D Ullman, "Compilers – Principles, Techniques and Tools", 2nd Edition, Pearson Education, 2007
2. Steven S. Muchnick, "Advanced Compiler Design and Implementation, "Morgan Kaufmann Publishers -Elsevier Science, India, Indian Reprint 2003.

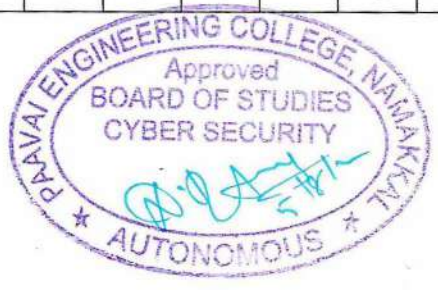
REFERENCES

1. Randy Allen, Ken Kennedy, "Optimizing Compilers for Modern Architectures: Dependence- based Approach", Morgan Kaufmann Publishers, 2002.
2. Keith D Cooper and Linda Torczon, "Engineering a Compiler", Morgan Kaufmann Publishers Elsevier Science, 2004.
3. Charles N. Fischer, Richard. J. LeBlanc, "Craftinga Compiler with C", Pearson Education, 2008.
4. A.V. Aho, Monica, R.Sethi, J.D.Ullman, "Compilers, Principles, Techniques and Tools", Second Edition, Pearson Education/Addison Wesley, 2009.

CO-PO MAPPING

Mapping of Course Outcomes with Programme Outcome
(3/2/1 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

COs	Programme Outcomes (POs)												Programme Specific Outcomes (PSOs)	
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	1	1	1	1	-	1	-	1	1	2	3	2
CO2	2	2	1	1	1	1	-	1	-	1	1	1	3	2
CO3	3	2	3	1	1	1	1	1	1	1	1	1	2	1
CO4	2	2	3	2	1	1	1	-	1	1	1	1	2	3
CO5	3	2	2	1	1	1	1	-	1	1	1	2	1	1



CY20252	SECURE CODING	3 0 0 3

COURSE OBJECTIVES

To enable the students to

- understand the various security attacks.
- know the secure software development cycle
- identify the concept of threats modeling process and security techniques.
- learn the different types of attacks and its security issues.
- apply the security tester and its applications.

UNIT I INTRODUCTION 9

Security - CIA Triad, Viruses, Trojans, and Worms in a Nutshell; Security Concepts - exploit, threat, vulnerability, risk, attack; Malware Terminology - Rootkits, Trapdoors, Botnets, Key loggers, Honeypots. Active and Passive Security Attacks; IP Spoofing - Tear drop, DoS, DDoS, XSS, SQL injection, Smurf, Man in middle, Format String attack.

UNIT II NEED FOR SECURE SYSTEMS 9

Proactive Security development process - Secure Software Development Cycle (S-SDLC) - Security issues while writing SRS, Design phase security; Development Phase - Test Phase, Maintenance Phase, Writing Secure Code.

UNIT III THREAT MODELLING PROCESS 9

Identifying the Threats by Using Attack Trees and rating threats using DREAD - Risk Mitigation Techniques and Security Best Practices - Security Techniques, Authentication, authorization, Defense in Depth and Principle of Least Privilege.

UNIT IV SECURE CODING TECHNIQUES 9

Protection against DoS attacks - Application Failure Attacks, CPU Starvation Attacks, Insecure Coding Practices in Java Technology; ARP Spoofing and its countermeasures - Buffer Overrun - Stack overrun, Heap Overrun, Array Indexing Errors, Format String Bugs.

UNIT V TESTING SECURE APPLICATIONS 9

Security code overview - Secure software installation, The Role of the Security Tester, Building the Security Test Plan; Testing HTTP - Based Applications, Testing File-Based Applications, Testing Clients with Rogue Servers.

TOTAL PERIODS 45

COURSE OUTCOMES

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

- implement security as a culture and show mistakes that make applications vulnerable to attacks.
- understand various attacks like DoS, buffer overflow, web specific, database specific, web-spoofing attacks.
- demonstrate skills needed to deal with common programming errors.
- identify the nature of the threats to software and incorporate secure coding practices.
- properly handle application faults, implement secure authentication, authorization and data validation controls used to prevent common vulnerabilities.

TEXTBOOKS

1. Writing Secure Code, Michael Howard and David LeBlanc, Microsoft Press, 2nd Edition, 2004.
2. Buffer Overflow Attacks: "Detect, Exploit, Prevent by Jason Deckar", Syngress,1st Edition, 2005.

REFERENCES

1.Threat Modeling, "Frank Swiderski and Window Snyder", Microsoft Professional, 1st Edition, 2004.

2. Gertz, M., & Jajodia, S. (Eds.). "Handbook of database security: applications and trends". Springer Science & Business Media, 2007.

3. Bishop, M. "Computer Security: Art and Science". Pearson Education, Boston, US, 2003.

4. Randall k. Nichols, Panos C. Lekkas , "Wireless Security Models, Threats and Solutions", 1stEdition, Tata McGraw Hill, 2006.

CO-PO MAPPING

Mapping of Course Outcomes with Programme Outcome (3/2/1 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

COs	Programme Outcomes (POs)												Programme Specific Outcomes (PSOs)	
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO 2
CO1	3	2	1	1	1	1	-	-	-	1	1	2	3	2
CO2	2	2	1	1	1	1	-	-	-	1	1	1	3	2
CO3	3	2	3	1	1	1	1	-	1	1	-	1	2	1
CO4	2	2	3	2	1	1	1	-	1	1	-	1	2	3
CO5	3	2	2	1	1	1	1	-	1	1	-	2	1	1

CY20253 INFORMATION ASSURANCE AND SECURITY 3 0 0 3

COURSE OBJECTIVES

To enable the students to

- explore system security related incidents and gain insight on potential defenses and counter measures against common threat/vulnerabilities
- install, configure and troubleshoot information security devices
- study and practice fundamental techniques in developing secure applications
- understand the concept of Security Analyst
- describe the Security Architecture and database audit.

UNIT I INFORMATION SECURITY FUNDAMENTALS 9

Definitions & challenges of security - Attacks & services, Security policies, Security Controls, Access control structures: Cryptography – Deception - Ethical Hacking – Firewalls - Identify and Access Management.

UNIT II SYSTEM SECURITY AND INFORMATION SECURITY MANAGEMENT 9

System Vulnerabilities - Network Security Systems, System Security, System Security Tools, Web Security, Application Security, Intrusion Detection Systems; Monitor systems and apply controls - security assessment using automated tools, backups of security devices; Performance Analysis – Root cause analysis and Resolution, Information Security Policies, Procedures, Standards and Guidelines.

UNIT III SECURITY PARAMETERS AND ACCESS CONTROL MODELS 9

Confidentiality - integrity, and availability; Security violation and threats - Security policy and procedure - Assumptions and Trust - Security Assurance, Implementation and Operational Issues, Security Life Cycle. Discretionary - mandatory, role-based and task-based models, unified models, access control algebra, temporal and spatio-temporal models.

UNIT IV SECURITY POLICIES AND SYSTEM DESIGN 9

Confidentiality policies - Integrity policies, hybrid policies, non-interference and policy composition, international standards; Design principles - representing identity, control of access and information flow, confinement problem. Assurance; Building systems with assurance - formal methods, evaluating systems.

UNIT V OPERATING SYSTEMS SECURITY AND DATABASE SECURITY 9

Security Architecture - Analysis of Security in Linux/Windows; Enterprise security - Database auditing, Applications; Network security - operating system security - user security - program security; Special Topics - Data privacy, introduction to digital forensics, enterprise security specification.

TOTAL PERIODS 45

COURSE OUTCOMES

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

- implement security as a culture and show mistakes that make applications vulnerable to attacks.
- understand various attacks like DoS, buffer overflow, web specific, database specific, web-spoofing attacks.
- demonstrate skills needed to deal with common programming errors.
- identify the nature of the threats to software and incorporate secure coding practices.
- properly handle application faults, implement secure authentication, authorization and datavalidation controls used to prevent common vulnerabilities.

REFERENCES

1. Pfleeger, C. P., Pfleeger, S. L., and Margulies, J. Security in Computing, ProQuest Safari TechBooks Online, 2017
2. Wheeler, D. A. Secure programming HOWTO, 2017.
3. Bishop, M. Computer Security: Art and Science. Pearson Education, Boston, US, 2003.
4. Nina Godbole, Information Systems Security: Security Management, Metrics, Frameworks and Best Practices, Wiley, 2017

CO/PO MAPPING

Mapping of Course Outcomes with Programme Outcome
(3/2/1 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

COs	Programme Outcomes (POs)												Programme Specific Outcomes (PSOs)	
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	1	1	1	1	-	1	-	1	1	2	3	2
CO2	2	2	1	1	1	1	-	1	-	1	1	1	3	2
CO3	3	2	3	1	1	1	1	1	1	1	1	1	2	1
CO4	2	2	3	2	1	1	1	-	1	1	1	1	2	3
CO5	3	2	2	1	1	1	1	-	1	1	1	2	1	1

CY20254 **OPERATING SYSTEM SECURITY** **3 0 0 3**

COURSE OBJECTIVES

To enable the students to

- understand the principles of securing a computer system
- have knowledge of security policies and mechanisms in operating systems
- understand vulnerabilities in operating system and software
- have insight into methods for development and test of security in software
- develop familiarity with and understanding of hot issues in computer and network security

UNIT I INTRODUCTION **9**

Secure Operating Systems definition, Security Goals, Trust Model, Threat Model, Access Control Fundamentals - Protection System, Reference Monitor, Assessment Criteria, Multics - Multics Fundamentals, Multics Security Fundamentals, Multics Protection System Models.

UNIT II SECURITY IN ORDINARY OPERATING SYSTEMS **9**

UNIX Security - UNIX Protection System, UNIX Authorization, UNIX Security Analysis, UNIX Vulnerabilities, Windows Security - Windows Protection System, Windows Authorization, Windows Security Analysis, Windows Vulnerabilities.

UNIT III VERIFIABLE SECURITY GOALS **9**

Information Flow, Information Flow Secrecy Models - Denning's Lattice Model, Bell-LaPadula Model, Information Flow Integrity Models, Biba Integrity Model, Low-Water Mark Integrity, Clark-Wilson Integrity.

UNIT IV SECURITY KERNELS **9**

The Security Kernel, Secure Communications Processor, Scomp Architecture, Scomp Hardware, Scomp Trusted Operating Program, Scomp Kernel Interface Package, Scomp Applications, Scomp Evaluation, Gemini Secure Operating System.

UNIT V SECURING COMMERCIAL OPERATING SYSTEMS **9**

Retrofitting Security into a Commercial OS, Commercial Era, Microkernel Era, UNIX Era, IX, Domain and Type Enforcement, Recent UNIX Systems, Case Study: Solaris Trusted Extensions- Building a secure operating system for Linux.

TOTAL PERIODS 45

COURSE OUTCOMES

Upon the completion of the course, the students will be able to

- understand the various security concepts such as confidentiality, privacy etc
- understand various security models
- understand the notion of security policy enforcement and classes of policies
- identify and assess current and anticipated security risks and vulnerabilities
- conceptualize design issues, principles, and good practices in securing systems

TEXTBOOKS

1. Trent Jaeger, "Operating System Security", First Edition, Morgan & Claypool Publishers, 2008.
2. Michael J. Palmer, "Guide to Operating Systems Security", First Edition, Thomson/Course Technology, 2004.

REFERENCE

1. Gerardus Blokdyk, "Mobile Operating System Security A Complete Guide", First Edition, 5 STAR Cooks, 2021.
2. David A. Wheeler, "Secure Programming for Linux and Unix HOWTO"Free Software Foundation, 2003.
3. Ronald L. Krutz, Russell Dean Vines, "Cloud Security" [ISBN: 0470589876],2010.
4. Randall k. Nichols, Panos C. Lekkas , "Wireless Security Models, Threats and Solutions", 1st Edition, Tata McGraw Hill, 2006.

CO-PO MAPPING

Mapping of Course Outcomes with Programme Outcome (3/2/1 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak														
COs	**Programme Outcomes (POs)**												**Programme Specific Outcomes (PSOs)**	
	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO1**	**PSO2**
CO1	3	2	1	1	1	1	-	-	-	1	1	2	3	2
CO2	2	2	1	1	1	1	-	-	-	1	1	1	3	2
CO3	3	2	3	1	1	1	1	-	1	1	-	1	2	1
CO4	2	2	3	2	1	1	1	-	1	1	-	1	2	3
CO5	3	2	2	1	1	1	1	-	1	1	-	2	1	1

OPEN ELECTIVE COURSES OE-I

CY20901 INFORMATION SECURITY RISK MANAGEMENT 3 0 0 3

COURSE OBJECTIVES

To enable the students to

- introduce the terminology, technology, and its applications
- understand the concept of Security Analyst
- introduce the tool, technologies and programming languages which is used in day to day security analyst job role.
- critically understand the strengths and weaknesses of disaster management approaches.
- describe the concept oof risk reduction and risk assessment.

UNIT I INFORMATION SECURITY MANAGEMENT 9

Information Security Overview - Threat and Attack Vectors, Types of Attacks, Common Vulnerabilities and Exposure (CVE), Security Attacks; Fundamentals of Information Security, - Computer Security Concerns, Information Security Measures.

UNIT II FUNDAMENTALS OF INFORMATION SECURITY 9

Key Elements of Networks - Logical Elements of Networks - Critical Information Characteristics - Information States.

UNIT III DATA LEAKAGE, INFORMATION SECURITY POLICIES, PROCEDURES AND AUDITS 9

What is Data Leakage and Statistics - Data Leakage Threats - Reducing the Risk of Data Loss, Key Performance Indicators (KPI), Database Security Information Security Policies; Necessity-Key Elements and Characteristics, Security Policy Implementation, Configuration, Security Standards, Guidelines and Frameworks.

UNIT IV INFORMATION SECURITY MANAGEMENT- ROLES AND RESPONSIBILITIES 9

Security Roles and Responsibilities - Accountability, Roles and Responsibilities of Information Security Management, Team Responding to Emergency Situation; Risk Analysis Process.

UNIT V RISK ASSESSMENT DISASTER RISK 9

Concept and Elements - Disaster Risk Reduction, Global and National Disaster Risk Situation; Techniques of Risk Assessment - Global Co-Operation in Risk Assessment and Warning, People's Participation in Risk Assessment, Strategies for Survival.

TOTAL PERIODS 45

COURSE OUTCOMES

Upon the completion of the course, the students will be able to

- know the various security concepts such as confidentiality, privacy etc
- understand various security models
- realize the notion of security policy enforcement and classes of policies
- identify and assess current and anticipated security risks and vulnerabilities
- conceptualize design issues, principles, and good practices in securing systems

TEXTBOOKS

1. Management of Information Security by Michael E.Whilman and Herbert J.Mattord, Fourth Edition, 2013
2. R. Nishith, Singh AK, "Disaster Management in India: Perspectives, issues and strategies"'New Royal book Company.

REFERENCES

1. Network Security Essentials (Applications and Standards) by William Stallings Pearson Education.
2. Sahni, Pardeep Et. Al. (Eds.)," Disaster Mitigation Experiences and Reflections", Prentice Hall of India, New Delhi.
3. Cryptography and Network Security (principles and approaches) by William Stallings Pearson Education, 4th Edition.
4. Goel S. L., Disaster Administration and Management Text and Case Studies", Deep &Deep Publication Pvt. Ltd., New Delhi.

CO-PO MAPPING

Mapping of Course Outcomes with Programme Outcome (1,2,3 indicates the strength of correlation) (1-LOW;2-MEDIUM;3-HIGH)														
CO	Programme Outcome (POs)												**Programme Specific Outcomes (PSOs)**	
	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO1**	**PSO2**
CO1	2	1	1	1	1	2	1	1	-	1	1	-	1	2
CO2	2	1	1	1	1	-	-	-	1	-	-	1	1	1
CO3	2	2	2	2	2	-	1	2	-	1	-	-	1	2
CO4	2	2	2	2	2	1	2	2	2	2	2	-	2	3
CO5	2	2	2	3	3	2	2	2	2	2	2	2	2	3

CY20902 **CYBER CRIME AND CYBER LAWS** 3 0 0 3

COURSE OBJECTIVES

To enable students to

- identify the different types of cybercrimes and cybercriminals.
- know about various cyber offenses.
- learn about different tools and methods used in cyber line.
- discuss on security aspects of cyber law.
- gain insights of IT act.

PRE-REQUISITES:Nil

UNIT I INTRODUCTION TO CYBERCRIME 9

Cybercrime definition and origins, Cybercrime and information security, Classifications of cybercrime, Types of Cybercriminals, A global Perspective on cybercrimes.

UNIT II CYBER OFFENSES 9

How criminal plan the attacks, Cyber stalking, Cyber café and Cybercrimes, Bot nets, Proliferation of Mobile and Wireless Devices, Credit Card Frauds , Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication Service Security, Attacks on Mobile/Cell Phones.

UNIT III TOOLS AND METHODS USED IN CYBER LINE 9

Phishing, Password Cracking, Key loggers and Spywares, Virus and Worms, Steganography, DoS and DDoS Attacks, SQL Injection, Buffer Over Flow, Attacks on Wireless Networks, Phishing, Identity Theft (ID Theft).

UNIT IV CYBER LAWS 9

The Security Aspect of Cyber Law ,The Intellectual Property Aspect in Cyber Law, The Evidence Aspect in Cyber Law , The Criminal Aspect in Cyber Law, Global Trends in Cyber Law , Legal Framework for Electronic Data, Interchange Law Relating to Electronic Banking , The Need for an Indian Cyber Law

UNIT V THE INDIAN IT ACT 9

Cyber Crime and Criminal Justice: Penalties, Adjudication and Appeals Under IT Act, 2000, IT and its Amendments, Consequences of not addressing the weaknesses in IT Act.

TOTAL PERIODS: 45

COURSE OUTCOMES

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

- explain the different types of cybercrimes and cybercriminals.
- describe the various cyber offenses.
- elucidate about different tools and methods used in cyber line.
- summarize on security aspects of cyber law.
- know the importance of IT act.

TEXT BOOKS

1. Nina Godbole, Sunit Belapure, Cyber Security, Wiley India, New Delhi.
2. The Indian Cyber Law by Suresh T. Vishwanathan; Bharat Law House New Delhi.

REFERENCES

1. The Information technology Act, 2000; Bare Act- Professional Book Publishers, New Delhi.
2. Cyber Law & Cyber Crimes By Advocate Prashant Mali; Snow White Publications, Mumbai.
3. Nina Godbole, Information Systems Security, Wiley India, New Delhi.
4. Kennetch J. Knapp, Cyber Security &Global Information Assurance, Information SciencePublishing.

CO/PO MAPPING :

CO/PO Mapping (3/2/1 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak														
COs		Programmes Outcomes (POs)												
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	1	3	2	1	-	-	-	1	1	2	3	2
CO2	2	2	1	3	2	2	-	-	-	2	1	1	3	2
CO3	3	2	3	3	2	2	2	-	1	2	-	1	3	1
CO4	2	2	3	2	2	2	2	-	1	2	-	1	3	3
CO5	3	2	2	1	2	1	1	-	1	2	-	2	1	1