

Scheme of Third Year

B. Tech Computer Science and Engineering (Cyber Security)

Scheme of Studies/Examination (w.e.f. Session 2022-23)

Semester V

Bile mobi No.	Course S No.	Subject	L: T:P	Hrs/ Week	Credits	Examination Schedule				Duration of Exam (Hours)
						Major Test	Minor Test	Practical	Total	
1	PC- CS- CYS- 301A	Design and Analysis of Algorithms	3:0:0	3	3	75	25	0	100	3
2	PC- CS- CYS- 303A	Security Threats and Trends	3:0:0	3	3	75	25	0	100	3
3	ES- CS- CYS- 305A	Information Security and Data Hiding	3:0:0	3	3	75	25	0	100	3
4	ES- CS- CYS- 307A	Microprocessor and Interfacing	3:0:0	3	3	75	25	0	100	3
5	HM-902	Business Intelligence and Entrepreneurship	3:0:0	3	3	75	25	0	100	3
6	PC- CS- CYS- 311A	Computer Networks	3:0:0	3	3	75	25	0	100	3
7	PC- CS- CYS- 313L A	Computer Networks Lab	0:0:2	2	1	0	40	60	100	3
8	PC- CS- CYS- 315L A	Design and Analysis of Algorithms Lab	0:0:2	2	1	0	40	60	100	3

9	ES- CS- CYS- 317L A	Microprocessor & Interfacing Lab	0:0: 2	2	1	0	40	60	100	3
		Total		24	21	450	270	180	900	
10	MC- 904A	Energy Resources & Management	3:0: 0	3	3	0	100	0	100	3
11	SIM- 301A*	Seminar on Summer Internship	2:0: 0	2	2	0	50	0	50	-

B. Tech Computer Science and Engineering (Cyber Security)
Scheme of Studies/Examination (w.e.f. Session 2022-23)
Semester VI

S. No.	Course No.	Subject	L: T:P	Hours/ Week	Credits	Examination Schedule				Duration of Exam (Hrs.)
						Major Test	Minor Test	Practical	Total	
1	PC-CS-CYS-302A	Mobile Security	3:0:0	3	3	75	25	0	100	3
2	OEC	OEC-Elective-I	3:0:0	3	3	75	25	0	100	3
3	ES-CS-CYS-304A	Digital Forensics	3:0:0	3	3	75	25	0	100	3
4	PC-CS-CYS-306A	Cryptanalysis	3:0:0	3	3	75	25	0	100	3
5	ES-CS-CYS-308A	Information theory and coding	3:0:0	3	3	75	25	0	100	3
6	PC-CS-CYS-310A	Cloud Security and Management	3:0:0	3	3	75	25	0	100	3
7	PC-CS-CYS-312LA	Information theory and coding Lab	0:0:2	2	1	0	40	60	100	3
8	ES-CS-CYS-314LA	Digital Forensics Lab	0:0:2	2	1	0	40	60	100	3
9	PC-CS-CYS-316LA	Cryptanalysis Lab	0:0:2	2	1	0	40	60	100	3
		Total		24	21	450	270	180	900	

OEC Elective-I
Soft Skills and Interpersonal Communication: OE-CS- CYS -302
Creativity, Innovation and Entrepreneurship: OE-CS- CYS -304
Enterprise Resource Planning: OE-CS- CYS -306
Stochastic Processes and Applications: OE-CS- CYS -308

*The students will choose any One Open Elective course out of the given elective list in VI Semester

Syllabus Third Year

Subject Code PC-CS-CYS-301A	Design and Analysis of Algorithms						
Lecture	Tutorial	Practical	Credit	Major Test	Minor Test	Total	Time
3	0	0	3	75	25	100	3 Hrs.
Purpose	To introduce advanced data structures and algorithms concepts involving their implementation for solving complex applications.						
Course Outcomes (CO)							
CO1	To introduce the basic concepts of Data Structures and their analysis.						
CO2	To study the concept of Dynamic Programming and various advanced Data Structures.						
CO3	To introduce various Graph algorithms and concepts of Computational complexities.						
CO4	To study various Flow and Sorting Networks						

Unit 1: Introduction

Review: - Elementary Data Structures, Algorithms and its complexity (Time and Space), Analysing Algorithms, Asymptotic Notations, Priority Queue, Quick Sort.

Recurrence relation: - Methods for solving recurrence (Substitution, Recursion tree, Master theorem), Strassen multiplication.

Unit 2: Advanced Design and analysis Techniques

Dynamic programming: - Elements, Matrix-chain multiplication, longest common subsequence,

Greedy algorithms: - Elements, Activity- Selection problem, Huffman codes, Task scheduling problem, Travelling Salesman Problem.

Advanced data Structures: - Binomial heaps, Fibonacci heaps, Splay Trees, Red-Black Trees.

Security Threats and Trends							
Subject Code							
PC-CS-CYS-303A							
Lecture	Tutorial	Practical	Credit	Major Test	Minor Test	Total	Time
3	0	0	3	75	25	100	3 Hrs.
Purpose	To provide knowledge of various security threats and current trends						
Course Outcomes (CO)							
CO1	To understand the various security and network threats.						
CO2	To be able to learn about the security threat management and various vulnerabilities.						
CO3	Expose detail of Security monitoring and Auditing tools						
CO4	To understand the various access control mechanisms to protect against threats in the networks						

UNIT-1

Introduction: Security threats, Sources of security threats, Motives, Target Assets and vulnerabilities – Consequences of threats, Email threats, Web, threats, Intruders and Hackers, Insider threats, Cybercrimes. Network Threats: Active/ Passive – Interference – Interception
– Impersonation – Worms – Virus – Spam’s – Ad ware, Spy ware – Trojans and covert channels
– Backdoors – Bots – IP, Spoofing, ARP spoofing, Session Hijacking, Sabotage, Internal threats
Environmental threats, Threats to Server security.

UNIT-2

Security Threat Management: Risk Assessment, Forensic Analysis, Security threat correlation
– Threat awareness, Vulnerability sources and assessment, Vulnerability assessment tools
– Threat identification, Threat Analysis, Threat Modeling, Model for Information Security Planning.

UNIT-3

Security Elements: Authorization and Authentication, types, policies and techniques – Security certification, Security monitoring and Auditing, Security Requirements Specifications – Security Policies and Procedures, Firewalls, IDS, Log Files, Honey Pots

UNIT-4

Access Control Mechanism: Trusted Computing and multilevel security, Security models, Trusted Systems, Software security issues, Physical and infrastructure security, Human factors – Security awareness, training, Email and Internet use policies.

Suggested Books:

1. Swiderski, Frank and Syndex, “Threat Modeling”, Microsoft Press, 2004.
2. William Stallings and Lawrie Brown, “Computer Security: Principles and Practice”, Prentice Hall, 2008
3. Joseph M Kizza, “Computer Network Security”, Springer Verlag, 2005
Thomas Calabrese and Tom Calabrese, “Information Security Intelligence: Cryptographic Principles & Application”, Thomson Delmar Learning, 2004

Subject Code ES-CS-CYS- 305A	Information Security and Data Hiding						
Lecture	Tutorial	Practical	Credit	Major Test	Minor Test	Total	Time
3	0	0	3	75	25	100	3 Hours
Purpose	1. To understand the fundamentals of Cryptography 2. To understand various key distribution and management schemes						
Course Outcomes							
CO1	Demonstrate the knowledge of cryptography, security concepts and applications.						
CO2	Explore the emerging security for information and IPSec.						
CO3	Identify techniques for data hiding and different types of attacks.						

UNIT-I

Security Attacks (Interruption, Interception, Modification and Fabrication), Security Services (Confidentiality, Authentication, Integrity, Non-repudiation, access Control and Availability) and Mechanisms, A model for Internetwork security. Classical Encryption Techniques, DES, Strength of DES, Differential and Linear Cryptanalysis, Block Cipher Design Principles and Modes of operation, Blowfish, Placement of Encryption Function, Traffic Confidentiality, key Distribution, Random Number Generation.

UNIT-II

Public key Cryptography Principles, RSA algorithm, Key Management, Diffie-Hellman Key Exchange, Elliptic Curve Cryptography. Message authentication and Hash Functions, Authentication Requirements and Functions, Message Authentication, Hash Functions and MACs Hash and MAC Algorithms SHA-512, HMAC. IP Security: Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations and Key Management

UNIT -III

Introduction: Data hiding models, security and privacy aspects, techniques for hiding data Digital audio, video, images and text. Steganography: Introduction, how it is different from cryptography, Classification of steganography algorithms: Transform-based, spatial domain, statistical, other, Applications of steganography: Covert channels, audio data, military, ecommerce. Watermarking: Introduction, how it is different from steganography and cryptography, watermarking algorithms, watermarking applications, limitations in watermarking.

UNIT-IV

Digital rights management issues: e-commerce, copyright protection, intellectual property. Issues, digital signatures, authentication, case studies, business models. Multimedia security and information assurance, visual cryptography, key management; Attacks and benchmarks for data hiding systems; Applications of data hiding technology in medicine, law enforcement, remote sensing, and e-commerce, Software for digital data hiding

Suggested Books:

1. Cryptography and Network Security (principles and approaches) by William Stallings Pearson Education, 4th Edition.
2. Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, Ton Kalker, Digital Watermarking and Steganography, 2nd Edition, Morgan Kaufmann, 2007.
3. Michael T. Rago and Chet Hosmer, Data Hiding: Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices and Network Protocols, 1st Edition, Syngress, 2012
4. Network Security Essentials (Applications and Standards) by William Stallings Pearson Education.
5. Principles of Information Security, Whitman, Thomson.

Subject Code ES-CS-CYS-307A	Microprocessor and Interfacing						
Lecture	Tutorial	Practical	Credit	Major Test	Minor Test	Total	Time
3	0	0	3	75	25	100	3 Hour
Purpose	To learn the architecture and programming of Intel family microprocessors and its interfacing.						
Course Outcomes							
CO 1	To study the Architecture of 8086 microprocessors						
CO 2	To implement the interfacing of memories to 8086 Microprocessor						
CO 3	To learn and analyze the instruction set of 8086 Microprocessor and implementation of assembly language programming of 8086 Microprocessor.						
CO 4	To design and implement the interfacing of interrupts, basic I/O and DMA with 8086 Microprocessor						

Unit I

8086 CPU ARCHITECTURE: 8086 Block diagram; description of data registers, address registers; pointer and index registers, PSW, Queue, BIU and EU. 8086 Pin diagram descriptions. Generating 8086 CLK and reset signals using 8284. WAIT state generation. Microprocessor BUS types and buffering techniques, 8086 minimum mode and maximum mode CPU module.

UNIT-II

Main Memory System Design: Memory devices, 8086 CPU Read/Write timing diagrams in minimum mode and maximum mode. Address decoding techniques. Interfacing SRAMS; ROMS/PROMS. Interfacing and refreshing DRAMS.

UNIT-III

8086 Instruction Set: Instruction formats, addressing modes, Data transfer instructions, string instructions, logical instructions, arithmetic instructions, transfer of control instructions; process control instructions; Assembler directives. 8086 Programming Techniques: Writing assembly Language programs for logical processing, arithmetic processing, timing delays; loops, data conversions.

UNIT-IV

Basic I/O Interface: Parallel and Serial I/O Port design and address decoding. Memory mapped I/O Violated I/O Intel's 8255 and 8251- description and interfacing with 8086. ADCs and DACs, - types, operation and interfacing with 8086. Interfacing Keyboards, alphanumeric displays, multiplexed displays, and stepper motor, optical encoder with 8086. Interrupts and DMA: 8086 Interrupt mechanism; interrupt types and interrupt vector table. Applications of interrupts, Intel's 8259. DMA operation. Intel's 8237.

Suggested Books:

1. Barry B. Brey, "The Intel Microprocessor 8086/8088, 80186", Pearson Education, Eighth Edition, 2009
2. D.V. Hall, Microprocessors and Interfacing, McGraw Hill 2nd ed.
3. Liu, Gibson, "Microcomputer Systems: The 8086/88 Family", 2nd Edition, PHI, 2005
4. Kenneth Ayala, "The 8086 Microprocessor: Programming & Interfacing the PC", Cengage Learning, Indian Edition, 2008
5. Kip Irvine, "Assembly language for IBM PC", PHI, 2nd Edition, 1993
6. Peter Abel, "Assembly language programming", Pearson Edu, 5th Edition, 2002

8086 Programming Techniques: Writing assembly Language programs for logical processing, arithmetic processing, timing delays; loops, data conversions.

Subject Code	Business Intelligence and Entrepreneurship						
HM-902A							
Lecture	Tutorial	Practical	Credit	Major Test	Minor Test	Total	Time
3	0	0	3	75	25	100	3
Purpose	To make the students conversant with the basics concepts in management thereby leading to nurturing their managerial skills.						
Course Outcomes (CO)							
CO1	Students will be able understand who the entrepreneurs are and what competences needed to become an Entrepreneur.						
CO2	Students will be able understand insights into the management, opportunity search, identification of a Product; market feasibility studies; project finalization etc. required for small business enterprises.						
CO3	Students can be able to write a report and do oral presentation on the topics such as product identification, business idea, export marketing etc.						
CO4	Students will be able to know the different financial and other assistance available for the small industrial units.						

Unit –I

Entrepreneurship: Concept and Definitions; Entrepreneurship and Economic Development; Classification and Types of Entrepreneurs; Entrepreneurial Competencies; Factor Affecting Entrepreneurial Growth – Economic, Non-Economic Factors; EDP Programs; Entrepreneurial Training; Traits/Qualities of an Entrepreneurs; Manager Vs. Entrepreneur, Entrepreneurial challenges.

Unit-II

Opportunity / Identification and Product Selection: Entrepreneurial Opportunity Search and Identification; Criteria to Select a Product; Conducting Feasibility Studies; Sources of business ideas, Marketing Plan : Conducting of Marketing Research, Industry Analysis, Competitor analysis, market segmentation and positioning, building a marketing plan, marketing mix, launching a new product; export marketing, Methods of Project Appraisal, Project Report Preparation; Specimen of Project Report; Project Planning and Scheduling using Networking Techniques of PERT / CPM.

Unit –III

Small Enterprises and Enterprise Launching Formalities: Definition of Small Scale; Rationale; Objective; Scope; SSI; Registration; NOC from Pollution Board; Machinery and Equipment Selection, Role of SSI in Economic Development of India; major problem faced by SSI, MSMEs – Definition and Significance in Indian Economy; MSME Schemes, Challenges and Difficulties in availing MSME Schemes.

Unit –IV

Role of Support Institutions and Management of Small Business: DIC; SIDO; SIDBI; Small Industries Development Corporation (SIDC); SISI; NSIC; NISBUD; State Financial Corporation SIC; Venture Capital : Concept, venture capital financing schemes offered by various financial institutions in India.

Special Issues for Entrepreneurs: Legal issues – Forming business entity, requirements for formation of a Private/Public Limited Company, Entrepreneurship and Intellectual Property Rights: IPR and their importance. (Patent, Copy Right, Trademarks) , Case Studies-At least one in whole course.

Suggested Books:

1. “Entrepreneurship development small business enterprises”, Pearson, Poornima M Charantimath,2013.
2. Roy Rajiv, “Entrepreneurship”, Oxford University Press, 2011.
3. “Innovation and Entrepreneurship”, Harper business- Drucker’s, Peter, 2006.
4. “Entrepreneurship”, Tata Mc-Graw Hill Publishing Colt new Delhi- Robert D. Hisrich, Mathew J. Manimala, Michael P Peters and Dean A. Shepherd, 8th Edition, 2012
5. Entrepreneurship Development- Shand and Co., Delhi- S.S.Khanka 1999
6. Small-Scale Industries and Entrepreneurship. Himalaya Publishing House, Delhi –Vasant Desai 2003.
7. Entrepreneurship Management -Cynthia, Kaulgud, Aruna, Vikas Publishing House, Delhi, 2003.

Subject Code	Computer Networks						
PC-CS-CYS-311A							
Lecture	Tutorial	Practical	Credit	Major Test	Minor Test	Total	Time
3	0	0	3	75	25	100	3 Hrs.
Purpose	To introduce the architecture and layers of computer network, protocols used at different Layers.						
Course Outcomes (CO)							
CO1	To understand the basic concept of networking, types, networking topologies and layered architecture.						
CO2	To understand data link layer and MAC sub-layer`						
CO3	To understand the network Layer functioning						
CO4	To understand the transport layer and application layer operation						

Unit -I

Introduction to Computer Networks: Data Communication System and its components, Data Flow, Computer network and its goals, Types of computer networks: LAN, MAN, WAN, Wireless and Wired networks, broadcast and point-to-point networks, Network topologies, protocols, interfaces and services, ISO- OSI reference model, TCP/IP architecture.

Physical Layer: Concept of Analog & Digital Signal, Bandwidth, Transmission Impairments: Attenuation, Distortion, Noise, Multiplexing: Frequency Division, Time Division, Wavelength Division, Transmission Media: Twisted pair, Coaxial cable, Fiber optics, Wireless transmission (radio, microwave, infrared), Switching: Circuit Switching, Message Switching, Packet Switching & comparisons, narrowband ISDN, broadband ISDN.

Unit -II

Data link layer: Error Control, Types of errors, framing (character and bit stuffing), error detection & correction methods; Flow control; Protocols: Stop & wait ARQ, Go-Back- N ARQ, sliding window protocols, Selective repeat ARQ, HDLC;

Medium access sub layer: Point to point protocol, FDDI, token bus, token ring; Reservation, polling, Multiple access protocols: Pure ALOHA, Slotted ALOHA, CSMA, CSMA/CD, FDMA, TDMA, CDMA, LLC, Traditional Ethernet, fast Ethernet, Network devices-repeaters, hubs, switches, Bridges, Router, Gateway.

Unit-III

Network layer: Addressing: Internet address, sub-netting; Routing techniques, static vs. dynamic routing , routing table, DHCP, IEEE standards 802.x, Routing algorithms: shortest path algorithm, flooding, distance vector routing, link state routing; Protocols: ARP, RARP, IP, ICMP, IGMP, IPV6; Unicast and multicast routing protocols, ATM.

Unit-IV

Transport layer: Process to process delivery; UDP; TCP, RPC, Congestion control algorithm: Leaky bucket algorithm, Token bucket algorithm, choke packets; Quality of service: techniques to improve QoS.

Application layer: DNS; SMTP, SNMP, FTP, HTTP & WWW; Firewalls, Bluetooth, Email, S/MIME, IMAP,

Network Security: Cryptography, user authentication, security protocols in internet, public key encryption algorithm, digital signatures.

Suggested Books:

1. Behrouz A. Forouzan, "Data communication and Networking", Tata McGraw Hill, Fourth Edition, 2011.
2. Computer Networks, 4th Edition, Pearson Education by Andrew S. Tanenbaum
3. Larry L. Peterson, Peter S. Davie, "Computer Networks", Elsevier, Fifth Edition, 2012.
4. William Stallings, "Data and Computer Communication", Eighth Edition, Pearson Education, 2007
5. James F. Kurose, Keith W. Ross, "Computer Networking: A Top–Down Approach Featuring the Internet", Pearson Education, 2005.

Subject Code	Computer Networks Lab						
PC-CS-CYS-313LA							
Lecture	Tutorial	Practical	Credit	Minor Test	Practical	Total	Time
0	0	2	1	40	60	100	3 Hour
Purpose	To explore networking concepts using Java programming & networking tools.						
Course Outcomes (CO)							
CO1	Do Problem Solving using algorithms.						
CO2	Design and test simple programs to implement networking concepts using Java.						
CO3	Document artifacts using applied addressing & quality standards.						
CO4	Design simple data transmission using networking concepts and implement.						

COMPUTER NETWORKS LAB

1. Create a socket for HTTP for web page upload and download.
2. Write a code simulating ARP /RARP protocols.
3. Study of TCP/UDP performance.
4. Performance comparison of MAC protocols
5. Performance comparison of routing protocols.
6. Write a program:
 - a. To implement echo server and client in java using TCP sockets.
 - b. To implement date server and client in java using TCP sockets.
 - c. To implement a chat server and client in java using TCP sockets.
7. Write a program:
 - a. To implement echo server and client in java using UDP sockets
 - b. To implement a chat server and client in java using UDP sockets.
 - c. To implement a DNS server and client in java using UDP sockets.
8. To flood the server from a spoofed source address leading to a DoS attack.
9. To sniff and parse packets that pass through using raw sockets.
10. To implement simple calculator and invoke arithmetic operations from a remote client.
11. To implement bubble sort and sort data using a remote client.
12. To simulate a sliding window protocol that uses Go Back N ARQ.

Subject Code		Design and Analysis of Algorithms Lab					
PC-CS-CYS-315LA							
Lecture	Tutorial	Practical	Credit	Minor Test	Practical	Total	Time
0	0	2	1	40	60	100	3
Purpose	The student should be made to Learn the algorithm analysis techniques, become familiar with the different algorithm design techniques and understand the limitations of Algorithm power.						
Course Outcomes (CO)							
CO1	The student should be able to Design algorithms for various computing problems.						
CO2	The student should be able to Analyse the time and space complexity of algorithms.						
CO3	The student should be able to Critically analyse the different algorithm design techniques for a given problem.						
CO4	The student should be able to Modify existing algorithms to improve efficiency.						

- Sort a given set of elements using the Quick sort method and determine the time required to sort the elements. Repeat the experiment for different values of n , the number of elements in the list to be sorted and plot a graph of the time taken versus n . The elements can be read from a file or can be generated using the random number generator.
- Using Open, implement a parallelized Merge Sort algorithm to sort a given set of elements and determine the time required to sort the elements. Repeat the experiment for different values of n , the number of elements in the list to be sorted and plot a graph of the time taken versus n . The elements can be read from a file or can be generated using the random number generator.
- Obtain the Topological ordering of vertices in a given digraph.
 - Compute the transitive closure of a given directed graph using Warshall's algorithm.
- Implement 0/1 Knapsack problem using Dynamic Programming.
- From a given vertex in a weighted connected graph, find shortest paths to other vertices using Dijkstra's algorithm.
- Find Minimum Cost Spanning Tree of a given undirected graph using Kruskal's algorithm.
- Print all the nodes reachable from a given starting node in a digraph using BFS method.
 - Check whether a given graph is connected or not using DFS method.

8. Find a subset of a given set $S = \{s_1, s_2, \dots, s_n\}$ of n positive integers whose sum is equal to a given positive integer d . For example, if $S = \{1, 2, 5, 6, 8\}$ and $d = 9$ there are two solutions $\{1, 2, 6\}$ and $\{1, 8\}$. A suitable message is to be displayed if the given problem instance doesn't have a solution.
9. Implement any scheme to find the optimal solution for the Traveling Salesperson problem and then solve the same problem instance using any approximation algorithm and determine the error in the approximation.
10. Find Minimum Cost Spanning Tree of a given undirected graph using Prim's algorithm.
11. Implement All-Pairs Shortest Paths Problem using Floyd's algorithm. Parallelize this algorithm, implement it using Open and determine the speed-up achieved.
12. Implement N Queen's problem using Back Tracking.
13. Use divides and conquers method to recursively implement Binary Search

Subject Code	Microprocessor & Interfacing Lab						
ES-CS-CYS-317LA							
Lecture	Tutorial	Practical	Credit	Minor Test	Practical	Total	Time
0	0	2	1	40	60	100	3 hours
Purpose	To learn programming of Intel family microprocessors and its interfacing.						
Course Outcomes (CO)							
CO1	Understand basic concept of 8085, 8086 Microprocessors and 8051 Microcontrollers.						
CO2	Develop an assembly language program for 8086 Microprocessors as well as C language program for 8051 Microcontroller.						
CO3	Experiment with interfacing the various Peripheral to 8086 Microprocessors and 8051 Microcontrollers.						
CO4	Design the systems based on 8051 Microcontrollers.						

List of Experiments

For 8086 Microprocessor write an Assembly Language Program to

- 1 Add / Sub two 16 bit numbers.
- 2 Multiply two 16 bit unsigned/ signed numbers.
- 3 Divide two unsigned/ signed numbers (32/16 , 16/8, 16/16, 8/8)
- 4 Find smallest/ largest number from array of n numbers.
- 5 Arrange numbers in array in ascending/ descending order.
- 6 Convert Hex to Decimal, Decimal to Hex.
- 7 Compare two strings using string instructions / without using string instructions.
- 8 Display string in reverse order, string length, Concatenation of two strings.
- 9 To find 1's and 2's complement of a number.
- 10 To find the Fibonacci Series.
- 11 To find Log of a given number using look up table.
- 12 To find Factorial of a number.
- 13 To write an ALP using 8051 Microcontrollers to perform addition, subtraction, multiplication and division of two eight bit numbers.
- 14 To write an ALP using 8051 Microcontrollers to perform logical operation i.e., AND, OR, XOR and Complement of two eight bit numbers.
- 15 To write an ALP using 8051 Microcontrollers to perform multi byte addition and subtraction of unsigned number.

Suggested Books:

1. Kenneth Ayala," The 8051 Microcontroller" 3rd ed. CENGAGE Learning.
2. M.A. Mazidi, J.G. Mazidi, R. D. McKinlay," The 8051 Microcontroller and Embedded systems using assembly and C" -2nd Ed, Pearson Education.

Subject Code MC-904A	Energy Resources & Management						
Lecture	Tutorial	Practical	Credit	Major Test	Minor Test	Total	Time
3	0	0	3	0	100	100	3
Purpose	To make the students conversant with the basic concepts and conversion of various form of Energy						
COURSE OUTCOMES							
CO1	An overview about Energy Resources, Conventional and Non-conventional sources						
CO2	Understand the Layout and working of Conventional Power Plants						
CO3	Understand the Layout and working of Non-Conventional Power Plants						
CO4	To understand the Energy Management, Audit and tariffs, Role of Energy in Economic development and Energy Scenario in India						

UNIT-I

Introduction: Types of energy, Conversion of various forms of energy, Conventional and Non-conventional sources, Need for Non-Conventional Energy based power generation.

UNIT-II

Conventional Energy sources: Types of Conventional Energy sources, Selection of site, working of Thermal, Hydro, Nuclear and Diesel power plants and their schematic diagrams & their comparative advantages/ disadvantages.

UNIT-III

Non-Conventional Energy sources: Types of Non-Conventional Energy sources, Basic principle, site selection of Solar energy power plant, photovoltaic technologies, PV Systems and their components, Wind energy power plant, Bio energy plants, Geothermal energy plants and Tidal energy plants.

UNIT-IV

Energy Management: General Principles of Energy Management, Energy Management Strategy, Modern trends and developments towards Computerizations of Power System.

Energy Audit: Need, Types, Methodology and Approach.

Subject Code PC-CS- CYS-302A	Mobile Security							
	Lecture	Tutorial	Practical	Credit	Major Test	Minor Test	Total	Time
	3	0	0	3	75	25	100	3 Hours
Purpose	1. To learn about drity 2. Identify and analyze various the security issues in mobile phone device and OS							
Course Outcomes								
CO1	Study the concepts in mobile security							
CO2	Learn various OS, acquisition and analysis of android.							
CO3	Learn various security of Windows and ios.							
CO4	Understand the purpose of malware analysis.							

Energy Scenario: Lay out of power system, Role of Energy in Economic development, energy demand, availability and consumption, Indian energy scenario, long term energy scenario, energy sector reforms in India, energy strategy for the future.

Suggested Books:

1. Energy Studies-Wiley Dream Tech India.
2. Non-conventional energy resources- Shobhnath Singh, Pearson.
3. Electrical Power Systems : Soni, Gupta, Bhatnagar – Dhanpat Rai & Sons
4. NEDCAP: Non Conventional Energy Guide Lines
5. Non conventional energy sources : G.D. Roy
6. Non Conventional energy resources :B H Khan - McGraw Hill
7. Applied Solar Energy : Meinel A B - Addison Wesley Publications
8. Direct Energy ConversionGeorge: Sutton -McGraw

UNIT-I

Introduction to Mobile Security: Mobile Phone Basics, Inside Mobile devices, Cell Phone Crime, SIM Card SIM Security, Mobile Architecture, Building Blocks – Basic security and cryptographic techniques, service discoverprotocol, Mobile P2P system, Mobile Networking.

dr

UNIT-II

Android Device and OS - History and evolution of Android - Android Open-Source Project (AOSP) - Android Market- Overview of Android Devices (Phones, Tablets, Net books, etc.) - Android ROM and Boot loaders - Android updatemechanism

Android Device Acquisition & Analysis - Procedures for acquiring an Android device - Imaging an android Logical vs. physical acquisition - Analysis Techniques - Android File System Forensics

– Android Data and App Security - Data theft from Android devices - Encrypted android devices - Corporate mobile security policies and procedures - Android software development security strategies

UNIT-III

Windows Phones - Introduction and History of Windows Phone OS - Legacy and Current OS - Windows Phone 7 - Analysis techniques - File system forensics - Common application forensic analysis

Windows Phones - Acquisition of Windows Phones - Windows Phone Analysis

iOS – Understanding the Internals of iOS Devices, iPhone models, iPhone hardware, iPad models, iPad hardware, File system, The HFS Plus file system, Disk layout, iPhone operating system, Data Acquisition from iOS Devices, Operating modes of iOS devices, Physical acquisition, Acquisition via a custom ram disk, Acquisition via jailbreaking, Data Acquisition from iOS Backups, iTunes backup, iCloud backup

UNIT-IV

Mobile Malware Analysis – Introduction to Mobile Malware, Mobile Malware, Phishing, Smishing and Vishing, Malware Attack and Defense, Visual Payload, Hoaxes, and Threats, Taxonomy of Mobile Malware

Mobile Malware Analysis – Analyzing Mobile Malware, learning about Dynamic Software Analysis, Using Mobile Sandbox, Analyzing Mobile Malware, Mobile Device Assets & MM Payloads analyzing Mobile, Forensic Investigation of MM on a Mobile Device

Suggested Books:

1. Pallapa Venkataram, Satish Babu: “Wireless and Mobile Network Security”, 1st Edition, Tata McGraw Hill, 2010.
2. Frank Adelstein, K.S.Gupta: “Fundamentals of Mobile and Pervasive Computing”, 1st Edition, Tata McGraw Hill 2005.
3. Randall k. Nichols, Panos C. Lekkas: “Wireless Security Models, Threats and Solutions”, 1st Edition, Tata McGraw Hill, 2006.
4. Bruce Potter and Bob Fleck: “802.11 Security”, 1st Edition, SPD O’REILLY 2005.
5. James Kempf: “Guide to Wireless Network Security, Springer. Wireless Internet Security – Architecture and Protocols”, 1st Edition, Cambridge University Press, 2008.

Subject Code ES-CS-CYS-304A	Digital Forensics						
Lecture	Tutorial	Practical	Credits	Major Test	Minor Test	Total	Time
3	0	0	3	75	25	100	3 Hours
Purpose	To aware engineering graduates of every discipline to understand cybercrimes and their Operandi toanalyze the attack.						
Course Objectives							
CO1	To postulate the introduction of digital forensics and motive behind the crime and identity ofthe main culprit with the current tools used.						
CO2	To identify the evidence quickly, and also to estimate the potential impact of the malicious activity on the victim Interpret the cyber pieces of evidence, Digital forensic process model						
CO3	To understand various artifacts related to systems in areas of windows System and Computer operating System						
CO4	To analyze Digital forensic case study which offers a complete report on the investigation process withthe associated legal aspects.						

Unit-1

Introduction: Digital forensic and investigations as a profession, Digital forensics versus other related disciplines, A brief History of Digital Forensics, purpose of Digital Forensics, Digital Forensic Investigation

Process, Legal Considerations of Digital forensics, Branches of Digital Forensic.

Current digital Forensics Tools: Needs & Types of Digital Forensics Tools, Tasks Performed by Digital Forensics Tools, Tool Comparisons, Computer Forensics Software Tools- Command-Line Forensics Tools, UNIX/Linux Forensics Tools, Other GUI Forensics Tools, Computer Forensics Hardware Tools- Forensic Workstations, Using a Write-Blocker.

UNIT – 2

Identification of Data: Timekeeping, Forensic Identification and Analysis of Technical Surveillance Devices, Reconstructing Past Events: How to Become a Digital Detective, Useable File Formats, Unusable File Formats, ConvertingFiles, Investigating Network Intrusions and Cyber Crime, Network Forensics and Investigating logs, investigating network Traffic, Investigating Web attacks, Router Forensics. Cyber forensics tools and case studies.

Digital Forensics Process Model: Introduction to cybercrime scene, Documenting the scene and evidence, maintainingthe chain of custody, forensic cloning of evidence, Live and dead system forensic, hashing concepts to maintain the integrity of evidence, Report drafting.

UNIT – 3

Windows Systems and artifacts: Introduction, Windows File Systems, File Allocation Table, New Technology File System, File System Summary, Registry, Event Logs, Prefetch Files, Shortcut Files, Windows Executables.

Computer Operating system Artifacts: Finding deleted data, hibernating files, examining window registry, recycle bin operation, understanding of metadata, Restore points and shadow copies

UNIT – 4

Legal aspects of digital forensics: Understanding of legal aspects and their impact on digital forensics, Electronics discovery **Case Study:** case studies related to Digital Forensics, Understanding of Internet resources, Web browser, Email header forensic, social networking sites.

Suggested Books:

1. Cory Altheide, Harlan Carvey, Digital Forensics with Open Source Tools, Syngress imprint of Elsevier.
2. Bill Nelson, Amelia Phillips, Christopher Steuart, “Guide to Computer Forensics and Investigations”, Fourth Edition, Course Technology.
3. Angus M. Marshall, “Digital forensics: Digital evidence in criminal investigation”, John – Wiley and Sons, 2008.
4. The Law of Evidence, Dr. Sr. Myneni, New Edition, Asian Law House, 2010

Subject Code PC-CS- CYS-306A	Cryptanalysis						
Lecture	Tutorial	Practical	Credit	Major Test	Minor Test	Total	Time
3	0	0	3	75	25	100	3 Hours
Purpose	To understand the importance of cryptanalysis in our increasingly computer-driven world.						
Course Outcomes (CO)							
CO1	To develop a mathematical foundation for the study of cryptography.						
CO2	To understand Number Theory and Algebra for design of cryptographic algorithms						
CO3	To understand the role of cryptography in communication over an insecure channel.						
CO4	To analyze the different public key encryption schemes and elliptic curves and pairings based on different security models						

UNIT-I

Classical cryptography and overview: Introduction to Cryptographic Techniques, Classical cryptosystems and their cryptanalysis, Model of secure communication, Security services, Overview of attacks, X.800 Security Architecture for Open System Interconnection (OSI), and cryptanalysis. Security Protocols: Authentication: Kerberos, X.509 Authentication Service, Secure Socket Layer (SSL), Secure Electronic Transaction (SET), Email security,,: PGP, S/MIME, IP Security (IPSec)

UNIT II

Mathematical background: Introduction to Number theory, Modular arithmetic, prime number generation, GCD, Euclidean Algorithm, Extended Euclidean Algorithm, Fast Exponentiation, Chinese Remainder Theorem, Fermat's and Euler's Theorem

UNIT III

Private key cryptography: Symmetric Encryption. Definitions. Chosen Plaintext Attack. Chosen Ciphertext Attack, Variations on DES, RC4, RC5 and Blowfish, Hash Functions. Message Authentication Codes. Collision-Resistance. Public key cryptography: RSA, ElGamal, DSA, Elliptic curve cryptosystems, Public Key Cryptography standard (PKCS), PKI, Digital Certificates, and Key management techniques, message digest: SHA-1, MD5

UNIT IV

Public Key Cryptosystems of RSA, Rabin, etc. their security and cryptanalysis.. Finite fields: Construction and examples. Diffie Hellman key exchange. Discrete logarithm problem in general and on finite fields. Cryptosystems based on Discrete logarithm problem such as Massey Omura cryptosystems. Algorithms for finding discrete logarithms, their analysis. Polynomials on finite fields and their factorization/irreducibility and their application to coding theory. Elliptic curves, Public key cryptosystems particularly on Elliptic curves. Problems of key exchange, discrete logarithms and the elliptic curve logarithm problem. Implementation of elliptic curve cryptosystems

Suggested Books:

1. Behrouz A. Forouzan and D. Mukhopadhyay, Cryptography & Network Security, McGraw Hill, New Delhi.
2. William Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall

3. Douglas R. Stinson, *Cryptography: Theory and Practice*, Chapman and Hall
4. J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, CRC press

Subject Code-ES-CS-CYS-308A	Information Theory and Coding						
Lecture	Tutorial	Practical	Credit	Major Test	Minor Test	Total	Time
3	0	0	3	75	25	100	3 Hours
Purpose	Information theory provides a means for measuring redundancy or efficiency of symbolic representation within a given language.						
CO 1	Define the amount of information per symbol and information rate of a discrete memory less source						
CO 2	Apply lossless source codes for discrete memoryless source to improve the efficiency of information.						
CO 3	Explain the Galois field and the related properties and operations.						
CO 4	Apply different channel coding techniques for error detection and correction schemes.						
CO 5	Analyze the coded word for error detection and correction due to channel noise						

UNIT-1

Introduction to information theory: Uncertainty, Information and Entropy, Information measures for continuous random variables, source coding theorem. Discrete Memory less channels, Mutual information, Conditional entropy.
Data compaction via Source coding schemes: Shannon-Fane code & Hempel-Ziv coding channel capacity. Prefix code, Shannon limit Huffman code, Channel coding theorem.

UNIT-2

Cyclic Code: Code Algebra, Encoder & decoder for cyclic codes, generating cyclic code by generating polynomial, properties of Galois fields (GF) polynomial operations over Galois fields, parity check polynomial.

UNIT-3

Linear Block Code: Coding & decoding of linear block code, error correcting codes, minimum distance consideration, conversion of non-systematic form of matrices into systematic form.

UNIT-4

Convolutional Code: Trllis and state diagram, Convolutional encoders. Code Tree, Maximumlikelihood decoding of convolutional code: The Viterbi Algorithm fee distance of a convolutional code.

Suggested Books:

1. Ranjan Bose, Information Theory, Coding and Cryptography, Publication, 2005. Cover, Thomas, and Joy Thomas.
2. Elements of Information Theory. 2nd ed. New York, NY: Wiley-Interscience, 2006. ISBN: 9780471241959

SubjectCode PC-CS- CYS-310A	Cloud Security and Management						
Lecture	Tutorial	Practical	Credit	Major Test	Minor Test	Total	Time
3	0	0	3	75	25	100	3 Hours
Purpose	To understand the advantages, challenges, security issues of cloud computing						
Course Outcomes (CO)							
CO1	To provide an in-depth and comprehensive knowledge of the Cloud Computing fundamental issues, technologies and implementations.						
CO2	Identify the infrastructure of cloud computing, including SaaS, PaaS, IaaS, and virtualization etc.						
CO3	Evaluate the security issues related to the development of cloud applications.						
CO4	Learn Identity and Access Management in the cloud						

UNIT -I

Overview of Computing Paradigm: Recent trends in Computing, Grid Computing, Cluster

Computing, Distributed Computing, Utility Computing, Cloud Computing Evolution of cloud computing,

Introduction to Cloud Computing: Cloud Computing (NIST Model), History of Cloud Computing, Cloud service providers, Properties, Characteristics & Disadvantages, Pros and Cons of Cloud Computing, Benefits of Cloud Computing, Cloud computing vs. Cluster computing vs. Grid computing, Cloud Computing Architecture, Cloud computing stack, Comparison with traditional computing architecture (client/server), Services provided at various levels.

UNIT 2

Introduction to virtualization: Different approaches to virtualization, Hypervisors, , Hardware Virtualization, Software Virtualization, Memory Virtualization, Storage Virtualization, Data Virtualization, Network Virtualization.

Service Models (XaaS): Infrastructure as a Service (IaaS), Platform as a service (PaaS), Software as a Service (SaaS), Deployment Models, Public cloud, Private cloud, Hybrid cloud, Community cloud, Infrastructure as a Service (IaaS): Introduction to IaaS, IaaS definition, Platform as a Service (PaaS): Introduction to PaaS, Service Oriented Architecture (SOA), Cloud Platform and Management, Computation, Storage, Examples: Google App Engine, Microsoft Azure, Salesforce.com, Software as a Service (PaaS): Introduction to SaaS, Webservices, Web 2.0, Web OS, Case Study on SaaS.

UNIT-3

Cloud Security: Cloud Computing Software Security Fundamentals, Cloud Information Security Objectives, Cloud Security Services, Relevant Cloud Security Design Principles, SecureCloud Software Requirement, Infrastructure Security, Network level security, Host level security, Application level security, Data security and Storage, Data privacy and security Issues,

Jurisdictional issues raised by Data location

UNIT-4

Service Management in Cloud Computing: Service Level Agreements (SLAs), Billing & Accounting, Comparing Scaling Hardware: Traditional vs. Cloud, Economics of scaling: Benefitting enormously, Managing Data, Looking at Data, Scalability & Cloud Services, Database & Data Stores in Cloud Large Scale Data Processing

Identity and Access Management: Identity and Access Management in the cloud, Identity and Access Management functions, Identity and Access Management (IAM) Model, Identity Federation, Identity Provisioning Recommendations.

Suggested Books:

1. Cloud Computing Bible, Barrie Sosinsky, Wiley, India, 2010
2. Cloud Computing: Principles and Paradigms, Editors: Rajkumar Buyya, James Broberg, Andrzej M. Goscinski, Wiley, 2011.
3. Cloud Computing: Principles, Systems and Applications, Editors: Nikos Antonopoulos, Lee Gillam, Springer, 2012.
4. Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Ronald L. Krutz, Russell Dean Vines, Wiley, India, 2010

Subject Code PC-CS-CYS-312 LA	Information Theory and Coding Lab						
Lecture	Tutorial	Practical	Credit	Minor Test	Practical	Total	Time
0	0	2	1	40	60	100	3 Hours
Purpose	Information theory provides a means for measuring redundancy or efficiency of symbolic representation within a given language.						
Course Outcomes (CO)							
CO 1	Analyze about information and various entropies and demonstrate various entropies and information.						
CO 2	Understand working of various codes like linear block, cyclic, convolution and BCH codes. and Apply source coding techniques						
CO 3	Construct codes using different coding techniques						
CO 4	Apply various coding schemes for text, speech and audio						

List of Practicals

1. Determination of entropy of a given source
2. Determination of various entropies and mutual information of a given channel (Noise free channel)
3. Determination of various entropies and mutual information of a given channel (Binary symmetric channel)
4. Generation and evaluation of variable length source coding using MATLAB (Huffman Coding and decoding)
5. Coding & decoding of Linear block codes
6 Coding & decoding of Cyclic codes
6. Coding and decoding of convolution codes
8 Coding and decoding of BCH codes.

Subject Code ES-CS-CYS-314LA	Digital Forensic Lab						
Lecture	Tutorial	Practical	Credit	Minor Test	Practical	Total	Time
0	0	2	1	40	60	100	3 Hours
Purpose	To familiarize the students with the basics of Digital Forensic tools and technologies.						
Course Outcomes (CO)							
CO1	To familiarize students with the tools and network of Digital Forensics.						
CO 2	To have a clear understanding of Network related commands in windows and Linux						
CO 3	Study of the phases of investigation process using tools of Digital forensic.						
CO 4	To analyze case study of forensic investigation.						

List of Practicals

- 1 Study of Digital Forensics and different tools used for forensic investigation.
- 2 Study of Network Related Commands (Windows)
- 3 Study of Network related Commands (Linux).
- 4 How to Recover Deleted Files using Forensics Tools.
- 5 Study the steps for hiding and extract any text file behind an image file/ Audio file using Command Prompt.
- 6 How to make the forensic image of the hard drive using EnCase Forensics.
- 7 How to Restoring the Evidence Image using EnCase Forensics
- 8 How to Collect Email Evidence in Victim PC.
- 9 Comparison of two Files for forensics investigation by Compare IT software
- 10 Collecting Information about given Domain
- 11 Crawling through Websites and Banner Grabbing
Using Google Search in Information Collection.
- 12 Live Forensics Case Investigation using Autopsy

Subject Code PC-CS- CYS-316LA	Cryptanalysis Lab						
Lecture	Tutorial	Practical	Credit	Minor Test	Practical	Total	Time
0	0	2	1	40	60	100	3 Hours
Purpose	To familiarize the students with the different cryptographic techniques.						
Course Outcomes (CO)							
CO1	To develop cryptography techniques using different cipher algorithms.						
CO2	To understand Number Theory and Algebra for design of cryptographic algorithms						
CO3	To understand the role of cryptography in communication over an insecure channel.						
CO4	To understand the symmetric key encryption schemes based on different security models						

Experiments

1. Write a program to perform encryption and decryption 3 using the following algorithms:
a) Ceaser Cipher b) Substitution Cipher c) Hill Cipher
2. Implementation of various Stream Ciphers, such as, additive cipher, multiplicative cipher, and affine cipher with cryptanalysis.
3. Write a program to implement the DES and AES algorithm logic
4. Implementation of Euclidean's algorithm, Chinese remainder theorem, Primality test, Fermat's algorithms, Euler algorithm.
5. Write a program to implement the Blowfish algorithm
6. Using Cryptography, encrypt the text "Hello world" using Blow Fish.
7. Create your own key using Java key tool.
8. Write a program to implement RSA Algorithm,
9. Implement the Diffie Hellman Key Exchange mechanism using HTML and JavaScript.
10. Configure SSH (Secure Shell) and send/receive a file on this connection to verify the correctness of this system using the configured parameters.
11. Calculate the message digest of a text using the SHA,1 algorithm in JAVA.
12. Calculate the message digest of a text using the MD5 algorithm in JAVA

Subject Code	Enterprise Resource Planning						
OE-CS-CYS-306							
Lecture	Tutorial	Practical	Credit	Major Test	Minor Test	Total	Time
3	0	0	3	75	25	100	3 Hours
Purpose	Empower skills to understand common business modern information systems						
CO 1	Understand the E-commerce architecture						
CO 2	Analyze the management of information in ERP						
CO 3	Demonstrate a working knowledge of how data and transactions are integrated						
CO 4	Evaluate organizational opportunities and challenges in the design system						

UNIT 1

ERP Introduction, Benefits, Origin, Evolution and Structure: Conceptual Model of ERP, the Evolution of ERP, the Structure of ERP.

UNIT 2

Business Process Reengineering, Data ware Housing, Data Mining, Online Analytic Processing (OLAP), Product Life Cycle Man-agement (PLM), LAP, Supply chain Management. ERP Implementation Basics, ERP Implementation Life Cycle, Role of SDLC/SSAD, Object Oriented Architecture, Consultants, Vendors and Employees

UNIT 3

ERP Marketplace and Marketplace Dynamics: Market Overview, Marketplace Dynamics, the Changing ERP Market. ERP- Functional Modules: Introduction, Functional Modules of ERP Software, Integration of ERP, Supply chain and Customer Relationship Applications.

UNIT 4

ERP & E-Commerce, Future Directives- in ERP, ERP and Internet, Critical success and failure factors, Integrating ERP into organizational culture. Using ERP tool: either SAP or ORACLE format to case study.

Suggested Books:

1. Vinod Kumar Garg and Venkitakrishnan N K, "Enterprise Resource Planning Concepts and Practice", PHI.
2. Joseph A Brady, Ellen F Monk, Bret Wagner, "Concepts in Enterprise Resource Planning", Thompson Course Technology.
3. Alexis Leon, "ERP Demystified", Tata McGraw Hill
4. Rahul V. Altekar "Enterprise Resource Planning", Tata McGraw Hill, Vinod Kumar Garg and Venkitakrishnan N K,
5. "Enterprise Resource Planning – A Concepts and Practice", PHI
6. Mary Summer, "Enterprise Resource Planning"- Pearson Education