

UNIVERSITY OF KERALA**Syllabus of B.Voc (Cyber Security)****Semester I**

General Education				Skill Component			
No.	Title	credit	Hrs/Week	No.	Title	Credit	Hrs/Week
EN1111.4	Speaking and Listening Skills	4	4	CY12	Introduction to Cryptography	4	4
CY11	Introduction to IT	4	4	CY13	Introduction to Programing	4	3
MM1131.10	Mathematics I	4	4	CY14	Fundamentals of information Security	4	3
				CY15	C Programming Lab	3	4
				CY16	IT Lab	3	4
	Total	12	12		Total	18	18

Semester II

General Education				Skill Component			
No.	Title	credit	Hrs/Week	No.	Title	Credit	Hrs/Week
EN1211.4	Writing and presentation skills	4	4	CY21	Fundamentals of Cyber Forensics	4	4
CS1221	Environmental Studies	4	4	CY22	Operating Systems	4	4
MM1231.10	Mathematics II	4	4	CY23	Data structures	4	4
				CY24	Data structures Lab	3	3
				CY25	Cyber Forensics Lab	3	3
	Total	12	12		Total	18	18

Semester III

General Education				Skill Component			
No.	Title	credit	Hrs/Week	No.	Title	Credit	Hrs/Week
CY31	Data Analytics	4	4	CY34	Forensics Tools & Techniques	4	4
CY32	Legal & Ethical Studies	4	4	CY35	Interactive Programming With Python	4	4
CY33	Mathematics & Statistics for Computing	4	4	CY36	Database management system	4	4
				CY37	Database Lab	3	3
				CY38	Python Lab	3	3
	Total	12	12		Total	18	18

Semester IV

General Education				Skill Component			
No.	Title	credit	Hrs/Week	No.	Title	credit	Hrs/Week
CY41	Free and Open Source Soft wares (FOSS)	4	4	CY44	Software Engineering	4	4
CY42	Data Mining	4	4	CY45	Malware Analysis	4	4
CY43	Data and Cyber Security	4	4	CY46	Network Security	4	4
				CY47	Biometrics Security	3	4
				CY48	Network Security Lab	3	2
				CY49	Industrial Training		
	Total	12	12		Total	18	18

Semester V

General Education				Skill Component			
No.	Title	credit	Hrs/Week	No.	Title	credit	Hrs/Week
CY51	Threats in social media	4	4	CY54	Statistical Analysis with R	4	4
CY52	Principles of secure coding	4	4	CY55	R Programming Lab	4	4
CY53	Ethical Hacking	4	4	CY56	Ethical Hacking Lab	4	4
				CY57	Major Project (I st Phase)	4	6
				CY58	Study Tour	2	
	Total	12	12		Total	18	18

Semester VI

General Education				Skill Component			
No.	Title	credit	Hrs/Week	No.	Title	credit	Hrs/Week
CY61	Software Forensics and Vulnerability Analysis	4	4	CY 64	Windows and Linux Forensic Analysis	4	4
CY62	Internet of Things(IoT)	4	4	CY65	Risk Assessment & Security Audit	4	4
CY63	Mobile and Wireless Security	4	4	CY66	Cloud architecture and security	5	4
				CY67	Major Project (II nd Phase)	5	6
	Total	12	12		Total	18	18

Division of marks (Lab examination)

1. First program should be sufficiently simple – **25 marks**
(Logic – 10 marks, Successful compilation – 10 marks, Result– 5 marks)
2. Second program should be based on advanced concepts - **30 marks**
(Logic – 15 marks, Successful compilation – 10 marks, result – 5 marks)
3. Viva Voce - **15 marks**
4. Lab Record - **10 marks**

Total Marks - 80 marks

No. of credits: 4

No. of instructional hours: 4 per week

AIM

1. To familiarize students with English sounds and phonemic symbols.
2. To enhance their ability in listening and speaking.

OBJECTIVES: On completion of the course, the students should be able to

1. Listen to lectures, public announcements and news on TV and radio.
2. Engage in telephonic conversation.
3. Communicate effectively and accurately in English.
4. Use spoken language for various purposes.

COURSE OUTLINE

Module I: Pronunciation: Phonemic symbols – consonants – vowels – syllables - word stress - strong and weak forms- intonation.

Module II :Listening Skills :Difference between listening and hearing – active listening –barriers to listening – academic listening - listening for details - listening and note-taking - listening for sound contents of videos - listening to talks and descriptions - listening for meaning - listening to announcements - listening to news programmes.

Module III: Speaking Skills: Interactive nature of communication - importance of context - formal and informal - set expressions in different situations –greeting – introducing - making requests - asking for / giving permission - giving instructions and directions – agreeing / disagreeing – seeking and giving advice - inviting and apologizing telephonic skills - conversational manners.

Module IV: Dialogue Practice (Students should be given ample practice in dialogue, using core and supplementary materials.

COURSE MATERIAL

Core reading: English for Effective Communication. Oxford University Press, 2013.

Further reading:

1. Marks, Jonathan. English Pronunciation in Use. New Delhi: CUP, 2007.
 2. Lynch, Tony. Study Listening .New Delhi: CUP, 2008.
 3. Kenneth, Anderson, Tony Lynch, Joan MacLean. Study Speaking. New Delhi: CUP, 2008.
- Reference: Jones, Daniel. English Pronouncing Dictionary 17th Edition. New Delhi: CUP, 2009.

Core reading: Dramatic Moments: A Book of One Act Plays. Orient Black Swan, 2013.

The following One-act plays prescribed:

1. Serafin and Joaquin Alvarez Quinters - A Sunny Morning
2. H.H.Munro - The Death Trap
3. Vincent Godefroy - Fail Not Our Feast

CY11 INTRODUCTION TO IT

AIM:

1. To create overall generic awareness about scope of the field of IT and to impart basic personal Computing skills.
2. To create background knowledge for the various courses in the Programme.

OBJECTIVES:

1. To introduce the basic terminology in the field of IT
2. To impart functional knowledge about PC hardware, operations and concepts
3. To impart functional knowledge in the use of GUI Operating System
4. To impart functional knowledge in a standard office package (word processor, spread sheet and Presentation softwares) and popular utilities
5. To impart functional knowledge about networks and internet.
6. To give an overview of computer application in various fields and an overall generic awareness about the scope of the field of IT

COURSE MATERIAL

Module–I: Computer characteristics: Speed, storage, accuracy, diligence; Digital signals, Binary System, ASCII; Historic Evolution of Computers; Classification of computers: Microcomputer, Minicomputer, Mainframes, Supercomputers; Personal computers: Desktop, Laptops, Palmtop, Tablet PC; Hardware & Software; Von Neumann model.

Module–II: Hardware: CPU, Memory, Input devices, output devices. Memory units :RAM(SDRAM, DDRAM, RDRAM etc. feature wise comparison only); ROM-different types: Flash memory; Auxiliary storage: Magnetic devices, Optical Devices; Floppy, Hard disk, Memory stick, CD, DVD, CD-Writer; Input devices- keyboard, mouse, scanner, speech input devices, digital camera, Touch screen, Joystick, Optical readers, bar code reader; Output devices: Display device, size and resolution; CRT, LCD; Printers: Dot-matrix, Inkjet, Laser; Plotters, Sound cards & speaker.

Module-III: Software- System software, Application software; concepts of files and folders, Introduction to Operating systems, Different types of operating systems: single user, multi-tasking, time-sharing multi-user; Booting, POST; Basic features of two GUI operating systems: Windows & Linux (Basic desk top management); Programming Languages, Compiler, Interpreter, Databases; Applicationsoftwares: Generic Features of Word processors, Spreadsheets and Presentation softwares; Generic Introduction to Latex for scientific typesetting; Utilities and their use; Computer Viruses& Protection, Free software, open source.

Module–IV: Computer Networks- Connecting computers, Requirements for a network: Server, Workstation, switch, router, network operating systems; Internet: brief history, World Wide Web, Websites, URL, browsers search engines, search tips; Internet connections: ISP, Dial-up, cable modem, WLL, DSL, leased line; email, email software features (send receive, filter, attach, forward, copy, blind copy); characteristics of web-based systems, Web pages, introduction to HTML.

COURSE MATERIAL

1. E.Balaguruswamy, *Fundamentals of Computers*, McGraw hill, 2014
2. Dennis P Curtain, *Information Technology: The Breaking wave*, McGraw-Hill, 2014
3. Peter Norton, *Introduction to Computers*, McGraw-Hill, Seventh edition

MM1131.10 MATHEMATICS I

AIM: To introduce mathematical concepts and techniques that have applications in computer science field

OBJECTIVES:

1. To introduce advanced differential calculus
2. To introduce solutions of differential equations
3. To introduce Number theory
4. To introduce Complex Number Theory.

COURSE OUTLINE

Module–I: Review of basic differentiation, Differentiation of hyperbolic functions, derivatives of hyperbolic functions, inverse hyperbolic functions logarithmic differentiation, implicit differentiation, Leibnitz’s theorem, Mean value theorem, Rolle’s theorem, Lagrange’s mean-value theorem, Maxima and minima.

Module–II: Differential equations, General Concepts, Formulation and solution of differential equations, solution of higher order linear Des, partial Des, Laplace and Inverse Laplace transforms

Module–III: Theory of Numbers, prime numbers, unique factorization theorem, Euclidean algorithm, congruences, Fermat’s theorem, Wilson’s theorem

Module–IV: Complex Numbers, Separation into real and imaginary parts, Complex mapping

Assignments and Activities: Markov processes. Harmonic analysis and Fourier series, Linear Programming

COURSE MATERIAL

1. Erwin Kreyzig, *Advanced Engineering Mathematics*, New Age International Pvt Ltd.
2. Shanthi Narayan, *Differential Calculus*, S Chand & Company
3. Zafar Ahsan, *Differential Equations and their applications*.
4. RudraPratap, *Getting Started with MATLAB*, Oxford University Press

CY12 INTRODUCTION TO CRYPTOGRAPHY

AIM: To cover the security of information systems based cryptographic approaches

OBJECTIVE: Awareness of Cryptographic techniques, Algorithms types and Modes and algorithm

COURSE OUTLINE

Module I: Symmetric Cipher Models- Substitution techniques- Transposition techniques-. Simplified DES- Block Cipher principles- The Data Encryption Standard, Strength of DES Differential and linear Cryptanalysis. Block Cipher Design principles- Block Cipher modes of operations- Steganography

Module II: IDEA: Primitive operations- Key expansions- One round, Odd round, Even Round- Inverse keys for decryption. AES: Basic Structure- Primitive operation- Inverse Cipher- Key Expansion, Rounds, Inverse Rounds. Stream Cipher –RC4.

Module III: Public key Cryptography: - Principles of Public key Cryptography Systems, Number theory-Fundamental Theorem of arithmetic, Fermat's Theorem, Euler's Theorem, Euler's Totient Function, Extended Euclid's Algorithm, Modular arithmetic. RSA algorithm-Key Management - Diffie-Hellman Key Exchange, Elliptic curve Cryptography

Module IV: Authentication requirements- Authentication functions- Message authentication codes- Hash functions- SHA - 1, MD5, Security of Hash functions and MACs- Authentication protocols-Digital signatures-Digital signature standards. Cryptographic tools: VeraCrypt, 7-Zip

COURSE MATERIAL

1. William Stallings, "Cryptography and Network Security", Pearson Education, 6th Edition, and SBN 10: 0133354695, 2013.
2. Atul Kahate, "Cryptography and Network Security", McGraw Hill Education India (Pvt Ltd), 2nd edition, ISBN 10: 0070151458, 2009.
3. Charlie Kaufman, Radia Perlman, Mike Speciner, "Network Security: Private Communication in a Public World", Prentice Hall, 2nd edition, ISBN 10: 0130460192, 2002
4. Charles Pfleeger, Shari Lawrence Pfleeger "Security in computing", Prentice Hall, 4th Edition, ISBN 10: 0132390779, 2006.

CY13 INTRODUCTION TO PROGRAMMING

AIM: To Expose students to algorithmic thinking and problem solving and impart moderate skills in Programming in an industry-standard programming language.

OBJECTIVES:

1. To expose students to algorithmic thinking and algorithmic representations.
2. To introduce students to basic data types and control structures in C.
3. To introduce students to structured programming concepts.
4. To introduce students to standard library functions in C language.

COURSE OUTLINE

Module I: Introduction to programming; Algorithm and flow charts: definitions, Symbols used to draw flow charts, Program Writing – Structure of the program, Source code, Object code, Executable File, Variables and constants. Rules for naming variables/identifiers; Basic data types in C- int, char, float, double; storage capacity-range of all data types.

Module-II: Basic Elements: Operators and Expressions: Expression Evaluation (Precedence of Operators); Simple I/O statements, Control structures, if, if else, switch-case, for, while, do-while, break, continue. Arrays, Defining simple arrays, Multi-dimensional arrays, declaration, initialization and processing;

Module-III: Functions & Pointers: concept of modular programming, Library, User defined functions, declaration, definition & scope, recursion, Pointers: The & and * Operators, pointer declaration, assignment and arithmetic, visualizing pointers, call by value; call by reference, dynamic memory allocation, storage classes.

Module-IV: Advanced features: Array & pointer relationship, pointer to arrays, array of pointers. Strings: String handling functions; Structures and unions; File handling: text and binary files, file operations, Library functions for file handling, Modes of files.

COURSE MATERIAL

1. Ashok N. Kamthane, *Programming in C*, Pearson Education, Second edition
2. E. Balaguruswamy, *Programming in ANSI C*, McGrawhill, Sixth Edition

CY14 FUNDAMENTALS OF INFORMATION SECURITY

AIM: To create overall general awareness about security for Information assets.

OBJECTIVE: To introduce the basic terminology of information security.

COURSE OUTLINE

Module–I: Introduction to Information Security, The history of Information security, Why is security needed, security principles, Components of an Information system-Confidentiality, integrity, authentication, security policy, basic network security terminology.

Module–II: - Introduction to security attacks-Compromises to individual property, Deliberate software attacks, Espionage, Sabotage, Theft, Attacks- DOS,DDOS, Information Leakage, Regular File Access, Misinformation, Special File/Database Access, Remote Arbitrary Code Execution, Elevation of privileges, Man-in-the-middle, Spam, Social Engineering (Concepts only)

Module–III: cryptography- cryptography, symmetric encryption, substitution ciphers, transposition ciphers, steganography, Block ciphers, modes of operation, Data Encryption Standard, Public key cryptography, applications, strength and weakness, RSA algorithm, Authentication, authentication methods, message digest, digital signatures, digital signature algorithm, DSS, E-mail security: Pretty Good Privacy, working of PGP, S/MIME, MIME, IP Security, Architecture, IPSec: strengths and benefits, IPv4, IPv6, ESP protocol, Web Security: Secure Socket layer, SSL session and connection

Module–IV: firewall, characteristics of firewall, packet filters, application level gateways, firewall architecture, trusted systems. IDS-infrastructure, classification, host based IDS, network based IDS, anomaly, signature detection, Intrusion detection tools-snort, tripwire

COURSE MATERIAL

CORE:

1. Brijendra Singh, *Cryptography & Network Security*, PHI.
2. Pachghare, V.K., *Cryptography and Information Security*, PHI.

REFERENCE

1. Principles of Information Security- Michael E. Whitman, Herbert J. Mattord, Cengage Learning, Fourth edition, 2011
2. Computer Security basics- Rick Lehtinen, O'Reilly, 2nd edition, 2006
3. Absolute beginner's guide to Security, Spam, Spyware & Viruses- Andy Walker, Que publishers, 2005
4. Information Security Management Principles- Andy Taylor, David Alexander, Amanda Finch, David Sutton, BCS publishers, 2008
5. Guide to Computer forensics and Investigations- B. Nelson, A. Phillips, F. Enfinger, C. Steuart, Cengage Learning, 4th edition, 2010

CY15 C PROGRAMMING LAB

AIM: To provide an opportunity for hands-on practice of basic features of DOS, Windows, software Tools (word processor, spread sheet, presentation s/w) and algorithmic thinking and problem solving in an industry standard programming language.

OBJECTIVES: After the completion of this course, the student should be able to:

1. Create, Save, Copy, Delete, Organize various types of files and manage the desk top in general
2. Programming situations with a focus on writing, debugging and analyzing structured programs: Basic data types in C, basic control structures in C, arrays, structures and files, standard library functions in C language.
3. Solving moderately complex problems involving the above and requiring selection of appropriate data structures and efficient algorithm.

COURSE MATERIAL

1. Familiarization of important DOS/Windows/Linux features
2. Practice on basic features of word processor, spread sheet and presentation software.

Part A

The C laboratory work will consist of 15 Experiments

1. Testing out and interpreting a variety of simple programs to demonstrate the syntax and use of the following features of the language: basic data types, operators and control structures.

Part B

2. 1-D Arrays: A variety of programs to declare, initialize, read, print and process 1-D arrays of various basic data types. Processing to include, selection, sum, counting, selective sum, selective counting, reversing etc.
3. Pointers: A large number of trivial programs involving all possible data types to familiarize the syntax of pointers in a variety of situations and to draw memory diagrams based on the observations.
4. Structures: A variety of programs to declare, initialize, read, print and process structures made up of a variety of data types and structures.
5. 2-D Arrays: A variety of programs to declare, initialize, read, print and process 2-D arrays of various basic data types. Processing to include, selection, sum, counting, selective sum, selective counting, reversing etc.
6. Array of Structures and Structure of Arrays: Programs to demonstrate declaration and processing of structure of arrays and array of structures.
7. Pointers to Arrays: A number of programs to demonstrate handling of 1-D and 2-D arrays using pointers and to draw memory diagrams based on the observations.
8. Pointers to Structures: A number of programs to demonstrate use of pointers to structures and to draw memory diagrams based on the observations.
9. Functions –I: Simple Examples of declaring and using functions of the following categories
(i) no argument, no return, (ii) argument, no return, (iii) no argument, return, (iv) argument, return, all pass by value
10. Functions –II: Declaring and using functions with pass by reference, Passing and Returning structures, Recursive functions.
11. Files: Simple Example involving use of multiple files: declaring, opening, closing, reading from and writing to text files.
12. Files: Example involving use of multiple files: declaring, opening, closing, reading from and writing to binary files.

13. Library functions: A variety of Examples demonstrating (i) string processing functions (ii) a variety of selected library functions

COURSE MATERIAL

1. Deitel & Deital, *C: How to Program*, Pearson Education
2. Alan R Feuer, *The C Puzzle Book*, Pearson Education
3. Yashvant Kanetkar, *Test Your C Skills*, BPB Publications, 3rd Edition.

CY16 IT LAB

AIM: To provide awareness on cryptographic approaches.

OBJECTIVE: To impart functional knowledge in various algorithms used in cryptography.

COURSE OUTLINE

Windows: Starting windows
File Management through Windows explorer.
Alter Taskbar, Start Menu and Toolbar properties
Experience using the Search Tools
Make changes to the Control Panel
Use the features of Interface enhancements
Excel: Opening Worksheets and Workbooks
Headers and Footers, Entering Data
Editing Cell Data, Find and Replace, Go To Cell Data
Merge Cells, Cell Styles
Cropping, Rotating an image
Adding a Hyperlink
Embedding an Object
HTML Familiarize Creating an HTML document
Mark up Tags
HTML Tags.
Working with Text
Lists, Tables and Frames
Hyperlinks, Images and Multimedia
Forms and controls.

EN 1211.4: WRITING AND PRESENTATION SKILLS

AIM

1. To familiarize students with different modes of general and academic writing.
2. To help them master writing techniques to meet academic and professional needs.
3. To introduce them to the basics of academic presentation
4. To sharpen their accuracy in writing.

OBJECTIVES: On completion of the course, the students should be able to

1. Understand the mechanism of general and academic writing.
2. Recognize the different modes of writing.

3. Improve their reference skills, take notes, refer and document data and materials.
4. Prepare and present seminar papers and project reports effectively.

COURSE OUTLINE

Module I Writing as a skill – its importance – mechanism of writing – words and sentences - paragraph as a unit of structuring a whole text – combining different sources – functional use of writing – personal, academic and business writing – creative use of writing.

Module II Writing process - planning a text – finding materials - drafting – revising – editing - finalizing the draft - computer as an aid – key board skills - word processing - desk top publishing.

Module III Writing models – essay - précis - expansion of ideas – dialogue - letter writing – personal letters formal letters - CV – surveys – questionnaire - e-mail – fax - job application - report writing.

Module IV Presentation as a skill - elements of presentation strategies – audience – objectives – medium – key ideas -structuring the material - organizing content - audio-visual aids – handouts - use of power point - clarity of presentation - non-verbal communication - seminar paper presentation and discussion.

COURSE MATERIAL

1. English for Effective Communication. Oxford University Press, 2013.
2. Robert, Barraas. Students Must Write. London: Routledge, 2006.
3. Bailey, Stephen. Academic Writing. Routledge, 2006.
4. Hamp-Lyons, Liz, Ben Heasley. Study Writing. 2nd Edition. Cambridge University Press, 2008.
5. Ilona, Leki. Academic Writing. CUP, 1998.
6. McCarter, Sam, Norman Whitby. Writing Skills. Macmillan India, 2009.
7. Jay. Effective Presentation. New Delhi: Pearson, 2009. Mayor, Michael, et al, Ed.
8. Longman Dictionary of Contemporary English. 5th Edition. London: Pearson Longman Ltd, 2009.

CS1221 ENVIRONMENTAL STUDIES

AIM: To create better understanding about the deteriorating condition of our environment among students

OBJECTIVES: On completion this course, student should:

1. Have better awareness and concern about current environmental issues
2. Develop a healthy respect and sensitivity to environment
3. Develop pride in social and environmental activism.

COURSE OUTLINE

Module I: Environmental Studies: Introduction, Multidisciplinary nature, Scope and importance, Concept of sustainability and sustainable development. Ecosystems- Structure, function, Energy flow, food chains, food webs and ecological succession, Forest ecosystem, Grassland ecosystem, Desert ecosystem, Aquatic ecosystems, Natural Resources -Renewable and Non-renewable Resources, land resources and use, land degradation, soil erosion and desertification, Deforestation -Causes and impacts due to mining, dam building on environment, forests, biodiversity and tribal populations, Water: Use and over-exploitation of surface and ground water, floods, droughts, conflict over water -international & interstate, Energy resources renewable and non-renewable, use of alternate energy sources, growing energy needs.

Module II: Biodiversity and Conservation - Levels of biological diversity: genetic, species and ecosystem diversity; Bio geographic zones of India; Biodiversity patterns and global biodiversity hot spots, endangered and endemic species of India, Threats - habitat loss, poaching of wildlife, man-wildlife conflicts, biological invasions; Conservation of biodiversity: In-situ and Ex-situ conservation of biodiversity, Eco system and bio-diversity services: Ecological, economic, social, ethical, aesthetic and Informational value.

Module III: Environmental Pollution - Environmental pollution: types, causes, effects and controls; Air, water, soil and noise pollution, Nuclear hazards and human health risks, Solid waste management: Control measures of urban and industrial waste, Pollution case studies. Environmental Policies 81 Practices ~ Climate change, global warming, ozone layer depletion, acid rain and impacts on human communities and agriculture, Environment Laws: Environment Protection Act; Air (Prevention & Control of Pollution) Act; Water (Prevention and control of Pollution) Act; Wildlife Protection Act; Forest Conservation Act. Nature reserves, tribal populations and rights, and human wild life conflicts in Indian context.

Module IV: Human Communities and the Environment –Human population growth: Impacts on environment, human health and welfare; Resettlement and rehabilitation of project affected persons; case studies; Disaster management: floods, earthquake, cyclones and landslides, Environmental movements: Chipko Silent valley, Bishno is of Rajasthan, Environmental ethics: Role of Indian and other religions and cultures in environmental conservation., Environmental communication and public awareness, Fire & safety: Fire Detection Systems, Fire Control Systems, Care, maintenance, and Inspection

COURSE MATERIAL

1. "Text book for Environmental Studies for undergraduate courses of all branches of Higher Education", Erach Bharucha for University Grants Commission.
2. Fire Safety Management Handbook, Third Edition, Daniel E. Della-Giustina
3. N Arumugan and V Kumaresan, "Environmental Studies", Saras Publication, 2014

MM1231.10 MATHEMATICS II

AIM: To introduce mathematical concepts and techniques that have applications in computer science field

OBJECTIVES:

1. To introduce proof methods in mathematics and mathematical logic
2. To review concepts and techniques of set theory, relations and functions
3. To introduce various algebraic structures
4. To introduce graph theory
5. To develop an excitement in mathematics by highlighting its hidden beauty and significance

COURSE OUTLINE

Module–I: Proof Methods, Logic: Formal proofs, Propositional reasoning, Proofs by contradiction, False Proofs, Proofs by Induction, Symbolic Logic: Boolean expressions, Logical Equivalence, DeMorgan's Law, Tautologies, Implications, Arguments, Fallacies, Normal forms in propositional logic, Resolution

Module–II: Set Theory, Relations, Functions: Review of Set theory concepts, set operations, characteristic functions, fuzzy set theory basics, Relations: operations on relations, equivalence relations & partitions, partial orders, ordered sets, Warshal’s algorithm, Functions, Recursion,

Module–III: Algebraic Structures: Algebra, DeMorgan’s Law, Group, Ring, Polish expressions, Communication Model and error corrections, Hamming Codes

Module–IV: Graph Theory: Introduction, Graph Notation, Topological sort, Graph Propagation algorithm, Depth First, Breadth–first searches, Shortest Path algorithms, directed acyclic graphs

COURSE MATERIAL

1. Ramaswamy, *Discrete Mathematical Structures with Applications to Combinatorics*, Universities Press
2. RajendraAkerkar, RupaliAkerkar, *Discrete Mathematics*, Pearson Education
3. R MSomasundaram, *Discrete Mathematical structures*
4. Calvin C. Clawson, *Mathematical Mysteries, The beauty and magic of Numbers*, Viva Books Pvt Ltd
5. RudraPratap, *Getting Started with MATLAB*, Oxford University Press.

CY21 FUNDAMENTALS OF CYBER FORENSICS

AIM: Introduce basis of cyber forensic

OBJECTIVE: Understanding of cyber forensics concept such as acquisition and analysis

COURSE OUTLINE

Module I INTRODUCTION TO COMPUTER FORENSICS: Introduction to Traditional Computer Crime, Traditional problems associated with Computer Crime. Introduction to Identity Theft & Identity Fraud. Types of CF techniques – Incident and incident response methodology – Forensic duplication and investigation. Preparation for IR: Creating response tool kit and IR team. – Forensics Technology and Systems – Understanding Computer Investigation – Data Acquisition.

Module II EVIDENCE COLLECTION AND FORENSICS TOOLS: Processing Crime and Incident Scenes – Working with Windows and DOS Systems. Current Computer Forensics Tools: Software/ Hardware Tools.

Module III ANALYSIS AND VALIDATION: Validating Forensics Data – Data Hiding Techniques – Performing Remote Acquisition – Network Forensics – Email Investigations – Cell Phone and Mobile Devices Forensics

Module IV ETHICAL HACKING: Introduction to Ethical Hacking – Footprinting and Reconnaissance – Scanning Networks – Enumeration – System Hacking – Malware Threats – Sniffing: ETHICAL HACKING IN WEB - Social Engineering – Denial of Service – Session Hijacking – Hacking Web servers – Hacking Web Applications – SQL Injection – Hacking Wireless Networks – Hacking Mobile Platforms.

COURSE MATERIAL

1. Computer Forensics and Investigations- Bill Nelson, Amelia Phillips, Frank Enfinger, Christofer Steuart, Second Indian Reprint 2009, Cengage Learning India Private Limited.
2. Digital Evidence and Computer Crime – Eoghan Casey, Edition 3, Academic Press, 2011
3. Computer Forensics and Cyber Crime: An Introduction – MarjieBritz, Edition 2, Prentice Hall, 2008
4. Practical guide to Computer Forensics- David Benton and Frank Grindstaff, 2006, Book Surge Publishing, 2006
5. Computer Evidence: Collection & Preservation- Christopher L.T Brown Charles River Media publishing, Edition 1, 2005
6. Computer Investigation (Forensics, the Science of crime-solving) – Elizabeth Bauchner, Mason Crest Publishers, 2005

CY22 OPERATING SYSTEMS

AIM: To introduce students to basic functions and the theoretical underpinnings of modern operating systems.

OBJECTIVES: To introduce students to:

1. Fundamental concepts of systems software
2. Functions of operating systems as a resource manager
3. Strategies for constrained resource allocation
4. Memory and I/O Management techniques

COURSE OUTLINE

Module I: Introduction to Operating System: Introduction, Operating system structures- operating system operations, operating system services, user operating system interface, system programs, system calls, Types of System Calls, operating system structure.

Process Management: Process concept, Process Scheduling, Operations on processes, Inter-process communication, Threads-Overview, Multithreading model, Thread Libraries, Threading issues; CPU Scheduling: Basic concepts, scheduling criteria, scheduling algorithms.

Module II: Process synchronization: Background, Critical section problem, Peterson's solution, Semaphore, Classical synchronization problem- bounded buffer problem, reader/writer problem, The Dining Philosopher's problem.

Deadlocks: deadlock characterization, methods for handling deadlock- deadlock prevention, deadlock avoidance, deadlock detection, deadlock recovery.

Module III: Memory Management & Protection: Basic Hardware, Address binding, logical versus physical address space, Swapping, Contiguous memory allocation memory mapping and protection, memory allocation, fragmentation,

Non-contiguous allocation- paging, segmentation. Virtual memory-Demand Paging, page replacement, Allocation of frames, Thrashing, Allocating Kernel Memory.

Protection and Security: Protection -principles of protection, domain of protection, access matrix, access control; Security- threats, user authentication.

Module IV: Storage management: File system Interface — file concept, access methods, directory structure, File Sharing. File system implementation- file system structure & implementation, directory implementation, allocation methods, free space management; Mass storage management - disk structure, disk scheduling, RAID; I/O Systems- I/O hardware, Application I/O interface, kernel I/O subsystem.

COURSE MATERIAL

1. Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, Operating System Principles
2. Achyut S Godbole, Operating systems, Mc-GRawhill, Third Edition

Assignments and Activities: case study of popular Operating Systems like Android, Windows, Sim Solaris, IOS etc

CY23: DATA STRUCTURES

AIM: To introduce students to various data structures and their features and applicability.

OBJECTIVES: By the end of the course, students should:

1. Be able to write well-structured programs in C
2. Be familiar with data structures like array, structures, lists, stacks, queues, trees and graphs
3. Able to appreciate various searching and sorting strategies

COURSE OUTLINE

Module I: Sequential searching, binary searching, Hashing-linear hashing, hash functions, hash table searching, sorting: bubble sort, selection sort. Stacks and Queues: FIFO and LIFO data structures-stacks using (i) pointers and (ii) arrays. Queues using (i) pointers and (ii) arrays, Operations on stack and queues, applications, polish notation.

Module II: Linked Lists: Concept of static versus dynamic data structures, implementation of linked lists using pointers, operations on linked lists: insertion, deletion and traversing. Doubly linked lists and circular linked lists, applications of linked lists.

Module III: Trees: Concept of linear versus non-linear data structures, various types of trees -binary, binary search trees. Creating a binary search tree, traversing a binary tree (in-order, pre-order and post-order), operations on a tree -insertion, deletion and processing, expression trees, implementation using pointers, applications.

Module IV: Graphs, graph traversal— Depth first and Breadth first traversal of graphs, applications.

COURSE MATERIAL

1. A.K.Sharma, Data Structures Using C, Pearson, Second edition, 2011
2. Nair A.S., Makhalekshmi, Data Structures in C, PHI, Third edition 2011.

Assignments and Activities: Multi-way search trees, B-trees, Hauffman trees, case studies.

CY24: DATA STRUCTURES LAB

The laboratory work will consist of experiments like

Part A

- Linked list: traversal, node deletion, node insertion in singly, doubly and circular lists.
- Implementation of different searching techniques.
- Implementation of different sorting techniques.

Part B

- Stacks: matrix representation and linked list representation: Push, Pop

- Queues; matrix representation and linked list representation: Add, delete
- Circular queue implementation
- Evaluation of expression using stacks
- Tree traversal
- Evaluation of expression using binary trees.
- Infix to postfix and prefix conversion
- Creating and processing binary search tree

CY25 CYBERFORENSICS LAB

AIM: Understand the cyber forensic concepts

OBJECTIVE: Understand the practical and recent tools used in cyber forensics for analysis.

COURSE OUTLINE

The CYBER FORENSICS laboratory work will consist of 8Experiments, these can extended writ to topics related to cyber forensic

1. Survey of Latest developments in Cyber Forensics
2. Registry Editing and Viewing using native tools of OS
3. Hex analysis using Hex Editors
4. Bit level Forensic Analysis of evidential image using FTK, Encase and ProDiscover Tools
5. Hash code generation, comparison of files using tools like HashCalcetc
6. File analysis using Sleuthkitetc
7. Graphical File analysis and Image Analysis
8. Email Analysis involving Header check, tracing route, performing a check on Spam mail and Non-Spam mail.

CY31 DATA ANALYTICS

AIM: To understand the concept of big data

OBJECTIVES: The Student Should Be familiarized

1. Be Exposed To Big Data.
2. Learn Different Ways of Data Analysis.
3. Be Familiar with Data Streams.
4. Learn Mining and Clustering techniques.
5. Be Familiar with Visualization techniques.

COURSE OUTLINE

Module I: INTRODUCTION TO BIG DATA : Introduction To Big Data Platform – Challenges Of Conventional Systems – Web Data – Evolution Of Analytic Scalability, Analytic Processes And Tools, Analysis Vs Reporting – Modern Data Analytic Tools, Stastical Concepts: Sampling Distributions, Resampling, Statistical Inference, Prediction Error.

Module II: DATA ANALYSIS: Regression Modeling, Multivariate Analysis, Bayesian Modeling, Inference And Bayesian Networks, Support Vector And Kernel Methods, Analysis Of Time Series: Linear Systems Analysis, Nonlinear Dynamics – Rule Induction – Neural Networks: Learning and

Generalization, Competitive Learning, Principal Component Analysis and Neural Networks; Fuzzy Logic: Extracting Fuzzy Models from Data, Fuzzy Decision Trees, and Stochastic Search Methods.

Module III: MINING DATA STREAMS : Introduction To Streams Concepts – Stream Data Model And Architecture – Stream Computing, Sampling Data In A Stream – Filtering Streams – Counting Distinct Elements In A Stream – Estimating Moments – Counting Oneness In A Window – Decaying Window

Module IV: Real time Analytics Platform (RTAP) Applications – Case Studies – Real Time Sentiment Analysis, Stock Market Predictions.

COURSE MATERIAL

1. Michael Berthold, David J. Hand, Intelligent Data Analysis, Springer, 2007.
2. Anand Rajaraman and Jeffrey David Ullman, Mining Of Massive Datasets, Cambridge University Press, 2012.
3. Bill Franks, Taming the Big Data Tidal Wave: Finding Opportunities in Huge Data Streams with Advanced Analytics, John Wiley & Sons, 2012.
4. Glenn J. Myatt, Making Sense Of Data, John Wiley & Sons, 2007 Pete Warden, Big Data Glossary, O'Reilly, 2011.
5. Jiawei Han, MichelineKamber “Data Mining Concepts and Techniques”, Second Edition, Elsevier, Reprinted 2008.

CY32 LEGAL AND ETHICAL STUDIES

AIMS: To impart knowledge required for the student to emerge as computer professional

OBJECTIVES: By the end of this course, the student should be:

1. Having a clear view of what professionalism is
2. Aware of ethical issues in computing profession
3. Aware of managing quality
4. Aware of quality certifications
5. Having an Exposure to Cyber law

COURSE OUTLINE

Module-I: What is a profession – who is a professional – core qualities of a professional – Environments and their impact and complexity – social attitudes, beliefs and values

Module -II: Codes of ethics - solving ethical conflicts, moral reasoning and ethical theories– responsibilities and rights. Computer ethics: ethics and the internet – hacking – netiquette – privacy

Module-III: Quality Management. Concept of quality, total quality management, 7 sigma principles, ISO certifications, Component maturity models, CMM Levels.

Module-IV: Cyber law: Intellectual property rights – basic ideas – copyright concepts – copyrights applied to softwares – software licensing – patents in software – Indian copyright law and provisions for software – Indian patent law and provisions for software – various licencing models - arguments against copyrights and patents in software – free softwares – GPL software freedoms– open source softwares

Assignments and activities: Professional societies in Computing: IEEE, ACM, BCSI, CSI, Awards in the field of Computing, NASSCOM, Digital Divide, History of Computerisation in India and Kerala, Preparing for a career

COURSE MATERIAL

1. M Govindarajan, S Natarajan, V S Senthil Kumar, Engineering Ethics, PHI, 81-203-2578-8, Rs 150/-
2. Poornima M. Charantimath, Total Quality Management, Pearson Education, ISBN 81-297-0082-4, Rs 150/-
3. Richard Stallman, Free Software: A Perspective, Prajasakthi Book House, Hyderabad, Rs 60/--Indian Copyright Act and Indian Patent Acts

CY33 MATHEMATICS & STATISTICS FOR COMPUTING

AIM: To provide a foundation for integrated studies in mathematics and computer sciences

OBJECTIVE

1. To understand concepts of counting
2. To understand concepts of functions
3. To understand basic concepts of cryptography

COURSE OUTLINE

Module I: Counting- Basic counting-, Permutations and Subsets- Binomial coefficients-Pascal's Triangle, A proof using the Sum Principle, The Binomial Theorem, Labeling and trinomial coefficients, equivalence relations and counting-The Symmetry Principle, Equivalence Relations, The Quotient Principle, Equivalence class counting

Module II: Functions, Functions as relations, One -to-One, Onto and Invertible functions, Mathematical Induction, Graphs , Spanning trees, Rooted Trees, Warshall's algorithm: Shortest paths, Linked representation of directed graphs, Pruning algorithm for shortest path, Dijkstra's shortest path algorithm,

Module III: Introduction to Cryptography, Private Key cryptography, Public-key Cryptosystems, Arithmetic modulo n , Cryptography using multiplication mod n , Solutions to Equations and Inverses mod n , Inverses mod n , GCD, Euclid's Division Theorem, The GCD Algorithm, Computing Inverses, Exponentiation mod n , The RSA Cryptosystem, The Chinese Remainder Theorem, Finding large primes.

Module IV: Recursion Trees, Three Different Behaviors, Master Theorem, Solving More General Kinds of Recurrences

COURSE MATERIAL

1. Discrete Mathematics for Computer Science- Kenneth Bogart, Clifford Stein, Key Curriculum Press, 2006
2. Discrete Mathematics with Algorithms- M.O. Albertson, J.P.Hutchinson, John Wiley & Sons, 1988
3. Miquel A. Lerma, Notes on Discrete Mathematics.

CY34 FORENSICS TOOLS & TECHNIQUES

AIM: The goal is to perform crime investigations by using evidence from digital data

OBJECTIVE: To understand basic concepts of tools and techniques related to forensics methodology

COURSE OUTLINE

Module I: Examination on a Live Windows / Linux System-Volatile Data collection methodology-Preservation of volatile data, Collecting Subject System details, Identifying Users logged into the system, Inspect Network Connections and activity, Current and recent network connections, Collecting process information, Non-volatile Data collection from a live Windows system

Module II: Memory Forensics: Analyzing Physical and Process Dumps for Malware Artifacts- Memory Forensics methodology, Old School Memory Analysis, Windows Memory Forensics Tools, Active, and Windows Memory Forensics Tools work, Linux Memory Forensics Tools work,

Module III: Discovering and Extracting Malware and Associated Artifacts from Windows Systems and Linux systems- Forensic Examinations of Compromised Windows / Linux Systems, Functional Analysis Resuscitating a Windows / Linux Computer, Malware Discovery and Extraction from a Windows/ Linux system

Module IV: Legal considerations- Framing the issues, Statutory limits of authority, protected data, Tools for acquiring data, Acquiring data across Borders, Involving Law Enforcement

COURSE MATERIAL

1. Malware Forensics Investigating and Analyzing Malicious code-James M. Aquilina, Eoghan Casey, Cameron H. Malin, Syngress Publishing, 2008
2. Malware Analyst's Cookbook Tools and Techniques for fighting malicious code- Michael Hale Ligh, Steven Adair, Blake Hartstein, Matthew Richard, Wiley Publishing Inc, 2011
3. Unix and Linux Forensic Analysis DVD ToolKit - Chris Pogue, Cory Altheide, Todd Haverkos, Syngress Inc., 2008
4. Windows Forensic Analysis DVD Toolkit- Harlan Carvey, Edition 2, Syngress Inc., 2007

CY35 INTERACTIVE PROGRAMMING WITH PYTHON

AIM: To understand basic programming Python programming concepts

OBJECTIVE

1. Basic Elements of Programming (Such As Expressions, Conditionals, and Functions).
2. Familiarization of writing plugins in Python as well as network secure programming

COURSE OUTLINE

Module-I: Overview of Programming: Structure of a Python Program, Elements of Python, Introduction to Python: Python Interpreter, Using Python as calculator, Python shell, Indentation. Atoms, Identifiers and keywords, Literals, Strings, Operators (Arithmetic operator, Relational operator, Logical or Boolean operator, Assignment, Operator, Ternary operator, Bit wise operator, Increment or Decrement operator).

Module-II: Creating Python Programs: Input and Output Statements, Control statements (Looping- while Loop, for Loop, Loop Control, Conditional Statement- if...else, Difference between break, continue and pass)

Module-III: Structures: Numbers, Strings, Lists, Tuples, Dictionary, Date & Time, Modules, Defining Functions, Exit function, default arguments.

Module-IV: Introduction to Advanced Python: Objects and Classes, Inheritance, Regular Expressions, Event Driven Programming, GUI Programming.

COURSE MATERIAL

CORE: P. K. Sinha & Priti Sinha, “Computer Fundamentals”, BPB Publications, 2007.

REFERENCE

1. Dr. Anita Goel, Computer Fundamentals, Pearson Education, 2010.
2. T. Budd, Exploring Python, TMH, 1st Ed, 2011
3. Python Tutorial/Documentation www.python.org 2010
4. Allen Downey, Jeffrey Elkner, Chris Meyers, How to think like a computer scientist: learning with Python , Freely available online.2012
5. <http://docs.python.org/3/tutorial/index.html>
6. <http://interactivepython.org/courselib/static/pythonds>
7. <http://www.ibiblio.org/g2swap/byteofpython/read/>

CY36 DATABASE MANAGEMENT SYSTEM

AIM: To introduce basic concepts of data bases, and related techniques and tools

OBJECTIVES:

1. Be aware of basic concepts of data bases and data base management systems
2. Be aware of concepts of relational data bases.
3. Know to normalize relational data bases
4. Skilled in using relational algebra and relational calculus
5. Develop skills to write database queries

COURSE OUTLINE

Module I: Introduction: evolution of data base systems, overview of database management systems, Relational data model, mathematical definition, candidate, primary and foreign keys, set operations on relations, insertion, deletion and update operations, attribute domains.

Module II: The E-R Model, Entities and attributes, relationships - one to one and many to one, many-many. Security- Physical and Logical, Design and maintenance issues, integrity.

Module III: Relational algebra and relational calculus, Introduction to SQL, Table creation, selection, projection and join using SQL

Module IV: Functional Dependencies- inference axioms, Normalization, 1NF, 2NF, 3NF and Boyce-Codd Normal forms, Lossless and lossy decompositions.

COURSE MATERIAL

1. Ramon A. Mata-toledo and Pauline K. Cushman, Fundamentals of Relational Data Bases, Schaum Outlines, Tata McGraw Hill
2. Atul Kahate, Introduction to Dara Base Management Systems, Pearson Education

Assignments and activities: Study of features of MS Access, Open Office Base, Oracle, mySQL, emerging areas.

CY37 DATABASE LAB

AIM: This course will provide hands-on practice in the following topics, under a variety of computing situations with a focus on writing and analyzing SQL statements:

1. Installing and configuring a proper SQL tool
2. Database design and implementation 8 Writing and analyzing SQL statements
3. Create user interface (using java AWT) and study the working of a data base in a front end application

COURSE OUTLINE

The laboratory work will consist of 15-20 Experiments.

Tools to be used include: Personal Oracle 8/ MS Access/OpenOffice Base/Java. Experiments will cover creating tables including defining relations between them, practicing SQL, Experiments designed around a case study, miscellaneous topics including security, connecting databases to front-end applications. Some sample topics are given below:

PART A

1. SQL statements for creating, listing, dropping, checking, updating tables
2. Record manipulation using—insert, delete, update
3. Experiments that clarify the importance of keys (Except foreign key)
4. Queries with an Expression and a column alias
5. A simple query that aggregates (groups) over a whole table
6. A query with a literal string in the SELECT list.
7. Query using the "IS NULL" syntax to list (compare '=NULL' instead of IS NULL")
8. Queries with sub string comparison and ordering
9. Finding values within a certain range
10. Using the- "BETWEEN" keyword
11. SQL functions (String, Numeric, Date functions)
12. Aggregate Functions

PART B

13. Join between two tables (Natural Join, Theta Join etc.)
14. Foreign Key
15. Nested queries
16. The EXISTS and UNIQUE function in SQL.
17. Renaming attributes and joined tables
18. Statements related with VIEWS

CY38 PYTHON LAB

AIM: To provide an opportunity for hands-on practice of basic operation of PYTHON

OBJECTIVES:

1. After the completion of this course, the student should be able to:

2. Solving moderately complex problems involving PYTHON programming.

COURSE OUTLINE

Section: A (Simple programs)

1. Write a menu driven program to convert the given temperature from Fahrenheit to Celsius and vice versa depending upon user's choice.
2. WAP to calculate total marks, percentage and grade of a student. Marks obtained in each of the three subjects are to be input by the user
3. Write a menu-driven program, using user-defined functions to find the area of rectangle, square, circle and triangle by accepting suitable input parameters from user.
4. WAP to display the first n terms of Fibonacci series.
5. WAP to find factorial of the given number.
6. WAP to find sum of the following series for n terms: $1 - 2/2! + 3/3! - \dots - n/n!$
7. WAP to calculate the sum and product of two compatible matrices.

Section: B (Visual Python):

All the programs should be written using user defined functions, wherever possible.

1. Write a menu-driven program to create mathematical 3D objects I. curve II. sphere III. cone IV. arrow V. ring VI. Cylinder.
2. WAP to read n integers and display them as a histogram.
3. WAP to display sine, cosine, polynomial and exponential curves.
4. WAP to plot a graph of people with pulse rate p vs. height h. The values of p and h are to be entered by the user.
5. WAP to calculate the mass m in a chemical reaction. The mass m (in gms) disintegrates according to the formula $m=60/(t+2)$, where t is the time in hours. Sketch a graph for t vs. m, where $t \geq 0$.
6. A population of 1000 bacteria is introduced into a nutrient medium. The population p grows as follows: $P(t) = (15000(1+t))/(15+ e)$ where the time t is measured in hours. WAP to determine the size of the population at given time t and plot a graph for P vs t for the specified time interval.
7. Input initial velocity and acceleration, and plot the following graphs depicting equations of motion: I. velocity wrt time ($v=u+at$) II. distance wrt time ($s=u*t+0.5*a*t*t$) III. distance wrt velocity ($s=(v*v-u*u)/2*a$)

CY41 Free and Open Source Soft wares (FOSS)

AIM: To introduce different free and open source softwares

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

1. Explain the features of free & open source software
2. Work with PHP
3. Demonstrate the working of MySQL

COURSE OUTLINE

Module I: Open source software: Features, advantages over proprietary software, examples, Free software: concepts, features, free software Vs Open Source software, free software movements. Policies, GPL, Free OS, History and Features of Linux, Various flavours of Linux, Linux Kernel and Shell, Graphical Desktops- GNOME, KDE, Linux File System and Directories

Module-II: The building blocks of PHP: variables, globals & superglobals Data types: Set type, type casting, test type, Operators & Expressions, Flow control functions in PHP, Functions: Defining a

function variable scope, calling a function, returning values ,setting default values for arguments, passing variable reference Arrays: creating arrays(associative & multidimensional), Array related functions Working with strings: Formatting strings, indexing, strlen() functions

Module-III: Forms in PHP: Creating a simple input form, combining HTML & PHP code on a single page, redirecting the user ,creating a send mail form, File upload form Cookies: Introduction, setting a cookie with PHP, deleting a cookie, session function overview: starting a session,working with session variables, passing session IDs in the query string, destroying sessions &unseting variables

Module-IV: Database concepts: Open source database software: MySQL features MySQL data types: Numeric ,date & time, string Table creation in MySQL: insert, select, where clause, ordering the result, like operator Selecting Multiple tables :using join, using queries Modifying records :update command, replace command, delete command date & time functions in MySQL Interacting with MySQL using PHP :connecting to MYSQL, Executing queries, Retrieving error messages, inserting data with PHP, retrieving data with PHP

COURSE MATERIAL

1. Julie C.Meloni, PHP, MySQL and Apache, Pearson Education
2. Ivan Byross, HTML, DHTML, Javascript, Perl, BPB Publication

CY42 DATA MINING

AIM: To get an entry-level understanding of the concepts of Data Mining

OBJECTIVES:

1. To get an understanding of the general properties of data in large databases
2. Understand a variety of real-world applications that require mining
3. To get an overview of data warehousing and different data mining techniques
4. How to discover useful patterns and associations in huge quantities of data

COURSE OUTLINE

Module I: Overview: Data, Information, Knowledge; Knowledge Discovery; Types of data for Mining; Application Domains; Data Mining Functionalities; Data Processing – Understanding Data, Pre-processing Data –Forms of Data Pre-processing, Data Cleaning (Definition and Phases only), Need of Data Integration, Steps in Data Transformation, Need of Data Reduction;

Module II: Data Warehouse: Database Systems & Data Warehouses – Difference; Data Warehouse – Definition & Features; Multidimensional Data Model – Data Cubes ; OLAP (Definition and Functions only); Market Basket Analysis; Association Rule – Overview; Criteria for classifying Frequent Pattern Mining ; Mining Single Dimensional Boolean Association Rule – Apriori Algorithm;

Module III: Classification: Classification vs Prediction; Issues; Use of Decision Trees for Classification; Bayesian Classification – Bayes’ Theorem, Naïve Bayesian Classifier; Lazy Learners - k–Nearest Neighbour Method; Rule-Based Classification – Using IF-THEN rules for classification;

Module IV: Cluster Analysis: Introduction & Requirements; Characteristics of Clustering Techniques; Types of Data in Cluster Analysis; Categories of Clustering- Partitioning Methods; Outlier Detection in Clustering; Activities and Assignments: Mining Web, Temporal, Text, Multimedia, Medical data and

other Applied Data Mining areas; OLAP tools; Introduction to RapidMiner and other free and open-source data mining tools

COURSE MATERIAL

1. Sumitha Tiwari & Neha Chaudhary, Data Mining and Warehousing, Dhanpat Rai & Co
2. Jiawei Han and Micheline Kamber, Data Mining Concepts and Techniques, Elsevier
3. Arun K Pujari, Data Mining Techniques, Universities Press
4. G.K Gupta, Introduction to Data Mining With Case Studies, PHI.

CY43 DATA AND CYBER SECURITY

AIM: To make awareness of overall cyber security and data concepts

OBJECTIVE:

1. To understand the need of protecting sensitive and personal information
2. Importance of Data rights and ownership
3. Basic concepts cyber forensic investigation and evidence recovery

COURSE OUTLINE

Module I-DATA AND EVIDENCE RECOVERY- Introduction to Deleted File Recovery, Formatted Partition Recovery, Data Recovery Tools, Data Recovery Procedures and Ethics, Preserve and safely handle original media, Document a "Chain of Custody", Complete time line analysis of computer files based on file creation, file modification and file access, Recover Internet Usage Data, Recover Swap Files/Temporary Files/Cache Files, Introduction to Encase Forensic Edition, Forensic Tool Kit (FTK) etc, Use computer forensics software tools to cross validate findings in computer evidence-related cases.

Module II-CYBER CRIMES AND CYBER LAWS- Introduction to IT laws & Cyber Crimes – Internet, Hacking, Cracking, Viruses, Virus Attacks, Pornography, Software Piracy, Intellectual property, Legal System of Information Technology, Social Engineering, Mail Bombs, Bug Exploits, and Cyber Security etc...

Module III-CYBER FORENSICS INVESTIGATION- Introduction to Cyber Forensic Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Encryption and Decryption methods, Search and Seizure of Computers, Recovering deleted evidences, Password Cracking

Module IV-CYBER SECURITY- Introduction to Cyber Security, Implementing Hardware Based Security, Software Based Firewalls, Security Standards, Assessing Threat Levels, Forming an Incident Response Team, Reporting Cybercrime, Operating System Attacks, Application Attacks, Reverse Engineering & Cracking Techniques and Financial Frauds, Future scope of cyber security.

COURSE MATERIALS

1. Network Security Bible- Eric Cole, Ronald Krutz, James W. Conley, Edition 2, Wiley India Pvt Ltd, 2010
2. Network Security Essentials – William Stallings, Edition 4, Pearson Education, 2011
3. Ulysess Black, “Internet Security Protocols: Protecting IP Traffic”, Prentice
4. Fundamentals of Network Security- E. Maiwald, McGraw- Hill, 2004

5. Managing Information Security- John R. Vacca, Elsevier Inc, 2010
6. Cryptography and Network Security-William Stallings
7. Horowitz E., Sahani S., “Design and Analysis of Algorithms”, 3rd Edition, University Press, 2002.

CY44 SOFTWARE ENGINEERING

1. AIM:

- ❖ To introduce the basic concepts of software engineering

2. OBJECTIVES: At the end of the course, the students should be able to

- ❖ Understand the importance of basic processes in software Development life cycle.
- ❖ Understand the various activities incorporate with different models and know their significance.
- ❖ Create a systematic approach in software development.
- ❖ Familiarize students with requirements in engineering and classical software design techniques.
- ❖ Familiarize with various software testing techniques and tools.

3. SYLLABUS:

Module 1: Introduction: Characteristics of Software, Product and Process, Need for Software Process, Characteristics of a Software Process, Software Development Process models, Software Development Life Cycle Model: Waterfall Model, Prototyping, iterative development, Spiral Model, time-boxing model; Comparison of different Life Cycle Models,

Module 2: Software Project Management, Project Estimation Techniques, Software Requirements Analysis and Definition: Software Requirements, Overview of SA/SD Methodology, Requirements Specification: Need for SRS, Characteristics of an SRS, Components of an SRS, Specification Languages, Structure of a Requirements document. Functional Specification with Use cases, developing use cases, Structured Analysis, Matrices, quality metrics, Planning a project, effort estimation, COCOMO model, quality plan, risk management-assessment, control.

Module 3: Function oriented design: Problem partitioning, abstraction, modularity, Top-down and Bottom-up Strategies, coupling, cohesion, design notations-structure charts, structured design, Data Flow Diagrams, Developing the DFD Model of a system, Entity Relationship Diagram, Developing ERD of a system, Decision Trees, Decision Tables, Structured English, first-level factoring, factoring input, output and transform branches, transaction analysis, verification.

Module 4: Object-oriented design: Object-oriented design concepts, Comparison between Algorithmic Decomposition and Object-Oriented Decomposition Unified Modelling Language, Object Oriented Design using UML, Class Diagram, Sequence Diagram, Collaboration Diagram; detailed design, algorithm design, state modelling of classes, design walkthroughs, critical design review, consistency checkers **Testing** error, fault and failure, test oracles, test cases, Black Box Testing, Equivalence Class Partitioning, Boundary Value Analysis, Cause Effect Graphing, White Box Testing- control flow based and data-flow based testing, test plan, test case specifications

4. REFERENCES:

4.1 Core

- ❖ Rajib Mall, *Fundamentals of Software Engineering*, Second Edition, PHI

4.2 Additional

- ❖ Pankaj Jalote, *An Integrated Approach to Software Engineering*, Narosa

- ❖ Waman S. Jawadekar, *Software Engineering*, McGraw hill, 2013
- ❖ *Software Engineering (Seventh edition)*, Ian Sommerville – Addison Wesley.
- ❖ *Software Engineering: A practitioners approach (Sixth Edition)*, Roger S Pressman-Mc Graw Hill.
- ❖ *Journals and Magazines*: (i) *Software Development*, CMP Media. (ii) *Software Quality Professional*, ASQ.

4.3 Internet Resources:

- ❖ <http://courses.cs.vt.edu/csonline/SE/Lessons/>
- ❖ http://www.omg.org/gettingstarted/what_is_uml.htm
- ❖ <http://www-106.ibm.com/developerworks/java/library/co-design5.html>
- ❖ <http://www-106.ibm.com/developerworks/java/library/j-jmod0508/>
- ❖ www.rspa.com

5. Activities and Assignments: *Preparing various documents, case studies, preparing test plans, UML diagrams, Metrics for various development phases, Agile Programming Methodologies, extreme Programming, Formal Methods, CASE Tools*

CY45 MALWARE ANALYSIS

AIM: To study the process of determining the functionality, origin and potential of malwares and to determine if they are malware and the impact that malware might have on the systems within a system

OBJECTIVE: Study the life cycle of malware, its design using open source and VIRUS analysis

COURSE OUTLINE

Module I - INTRODUCTION Computer Infection Program- Life cycle of malware- Virus nomenclature- Worm nomenclature- Tools used in computer virology.

Module II – IMPLEMENTATION OF COVERT CHANNEL: Non self-reproducing Malware- Working principle of Trojan Horse- Implementation of Remote access and file transfer- Working principle of Logical Bomb- Case Study: Conflicker C worm.

Module III - VIRUS DESIGN AND ITS IMPLICATION: Virus components- Function of replicator, concealer and dispatcher- Trigger Mechanisms- Testing virus codes- Case Study: Brute force logical bomb.

Module IV - MALWARE DESIGN USING OPEN SOURCE: Computer Virus in Interpreted programming language- Designing Shell bash virus under Linux- Fighting over infection- Anti –antiviral fighting – Polymorphism- Case study: Companion virus.

COURSE MATERIAL

1. *Malware Forensics Investigating and Analyzing Malicious code*-James M. Aquilina, Eoghan Casey, Cameron H. Malin, Syngress Publishing, 2008
2. *Malware Analyst's Cookbook Tools and Techniques for fighting malicious code*- Michael Hale Ligh, Steven Adair, Blake Hartstein, Matthew Richard, Wiley Publishing Inc, 2011
3. *Unix and Linux Forensic Analysis DVD ToolKit* - Chris Pogue, Cory Altheide, Todd Haverkos, Syngress Inc., 2008
4. *Windows Forensic Analysis DVD Toolkit*- Harlan Carvey, Edition 2, Syngress Inc., 2007

5. Windows Forensic Analysis- Harlan Carvey, Dave Kleiman, Syngress Inc., 2007
6. Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry – Harlan Carvey, SyngressInc, Feb 2011
7. File System Forensic Analysis- Brian Carrier, Addison Wesley, Edition 1, 2005
8. Handbook of Digital Forensics and Investigation- Eoghan Casey, Academic Press, 2009
9. Digital Forensics with Open Source Tools- Cory Altheide, Harlan Carvey, Syngress Inc, Edition1, April 2011
10. ErciFiliol, “Computer Viruses: from theory to applications”, Springer, 1st edition, ISBN 10: 2-287-23939-1, 2005.
11. Mark.A .Ludwig, “The Giant black book of computer viruses, Create Space Independent Publishing Platform, 2nd edition, ISBN 10: 144140712X, 2009.

CY46 NETWORK SECURITY

AIM: Familiarize the concepts about security in network.

OBJECTIVE

To understand security related to windows and wireless systems.

To understand need of integrated security

COURSE OUTLINE

Module I: Introduction of Computer network: Topologies, Classification (LAN, MAN, WAN), OSI model, TCP /IP protocol-SMTP, FTP, telnet State of Network Security, Cyber Security, New approaches to cyber security, interfacing with the organization, Information security principles- Key principles of network security, Formal Processes, Risk Management, Calculating and managing risk, Information System Security Management- Access Control Attacks and threats-Malicious code

Module II: Windows Security- Windows Security at the heart of the defense, Out-of-the-box Operating system hardening, Attacks against the Windows workstation, Linux Security-, Hardening Linux, Web Browser and Client risk, servers, , E-mail security-, Security Issues with DNS, DNS attacks, Server security.

Module III: VoIP, Wireless Security- The Cellular phone network, Wireless transmission systems, Pervasive Wireless Data Network Technologies, IEEE Wireless LAN specification, Bluetooth, WAP, Network segments-Perimeter Defense, NAT, Basic architecture issues, Subnetting, switching and VLANs, Firewalls, Intrusion detection systems,

Module IV : Integrated cyber security- Validating your security- overview, Current state of penetration testing, Formal penetration testing methodology, Steps to explore a system, Data Protection, Endpoint security, Insider threats and data protection, Critical problems facing.

COURSE MATERIAL

1. Network Security Bible- Eric Cole, Ronald Krutz, James W. Conley, Edition 2, Wiley India Pvt Ltd, 2010
2. Network Security Essentials – William Stallings, Edition 4, Pearson Education, 2011
3. Cryptography and Network Security: Principles and Practice-William Stallings, Edition 3, Pearson education, 2003

4. Hacking Exposed- Network Security secrets and solutions, Joel Scambray, McGraw Hill, Edition 5, 2005
5. Wireless Security : Models, Threats and Solutions- Randall K. Nichols, Panos C. Lekkas, McGraw Hill, Edition 1, 2001

CY47 BIOMETRIC SECURITY

AIM: Fundamental knowledge in Biometrics Course Educational

OBJECTIVE: To provide students with understanding of biometrics, biometric equipment and standards applied to security. Course Outcomes:

1. Demonstrate knowledge of the basic physical and biological science and engineering principles underlying biometric systems.
2. Understand and analyze biometric systems at the component level and be able to analyze and design basic biometric system applications

COURSE OUTLINE

Module I Biometrics- Introduction- benefits of biometrics over traditional authentication systems -benefits of biometrics in identification systems-selecting a biometric for a system –Applications - Key biometric terms and processes - biometric matching methods -Accuracy in biometric systems

Module II Physiological Biometric Technologies: Fingerprints - Technical description –characteristics - Competing technologies - strengths – weaknesses – deployment - Facial scan - Technical description - characteristics - weaknesses-deployment - Iris scan - Technical description – characteristics - strengths – weaknesses – deployment - Retina vascular pattern 39 GVPCE(A)

Module III: Technical description – characteristics - strengths – weaknesses – deployment - Hand scan - Technical description-characteristics - strengths – weaknesses deployment – DNA biometrics. Behavioral Biometric Technologies: Handprint Biometrics - DNA Biometrics. Signature and handwriting technology - Technical description – classification – keyboard / keystroke dynamics- Voice – data acquisition - feature extraction - characteristics - strengths – weaknesses-deployment.

Module IV: Multi biometrics and multi factor biometrics - two-factor authentication with passwords - tickets and tokens – executive decision - implementation plan

COURSE MATERIAL

1. Samir Nanavathi, Michel Thieme, and Raj Nanavathi: “Biometrics -Identity verification in a network”, 1st Edition, Wiley Eastern, 2002.
2. John Chirillo and Scott Blaul: “Implementing Biometric Security”, 1st Edition, Wiley Eastern Publication, 2005.
3. John Berger: “Biometrics for Network Security”, 1st Edition, Prentice Hall, 2004.

CY48 NETWORK SECURITY LAB

AIM: To provide an opportunity for hands-on practice for security tools in networks.

OBJECTIVES: After the completion of this course, the student should be able to:

1. Manipulate the port scanning tools.
2. Familiarize with practical concepts about Firewall, IDP

COURSE MATERIAL

1. Port Scanning using NMap, Superscan
2. Enumeration-SNMP, SMTP, Unix/Linux, LDAP, NTP
3. Monitoring Live Network capturing packets and analyzing over the live network using Wireshark
4. Vulnerability Scanning
5. Firewall, Intrusion detection and Honey pots
6. Password Guessing and Password cracking
7. Buffer overflow attacks

CY49 INDUSTRIAL TRAINING

Students should go to a software firm and undergo training on an emerging tool.

CY51 THREATS IN SOCIAL MEDIA

AIM: It helps to understand the cyber threats in social media

OBJECTIVE: On successful completion of the course the student should have understood the cyber threats in Social websites, classify their types, discuss the cyber threats and its impact

COURSE OUTLINE

Module I: Media & Journalism - Overview – History, Types , advantages and disadvantages of various media –Journalism – Types of Journalism, Investigative Journalism – Yellow Journalism – Ethics of a Journalist

Module II: Social Media – Print and Television media – Social Networking Sites, Types, advantages and disadvantages, Social Media ethics – Do's and Don'ts in various social medias

Module III: Victimization in social media – Types of victimization – Profiles of social media victims - causes of victimization – trends in victimization in social media in India and other countries. Impact of Social Media threats - Harm to Brand Reputation - Lost Productivity - Strains on Bandwidth – Data Leaks & Disclosure

Module IV: Threats against Organizations from Social Media - Executive impersonations - Account takeover -Watering hole phishing and malware - Customer scams - Corporate impersonations - Information Leakage – Planning of an attack - Clickbait attacks - Hashtag/ traffic Hijacking .Social media security policies – individuals - Organizational Security Policies

COURSE MATERIAL

1. Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Paperback– Import Edition, Create Space Independent Publishing Platform, 11 August 2015
2. Threats and anti threats Strategies for Social Networking Websites by Amir Rokiifard, volume5, International Journal of Computer networks and Communications, July 2013

3. Securing the Social Media in the Enterprise by Henry Dalziel, 1st Edition, Elsevier Publication, 2015
4. [http://www.amazon.in/Building-Social-Applications-Gavin Bell/dp/8184048327?tag=googinhydr](http://www.amazon.in/Building-Social-Applications-Gavin-Bell/dp/8184048327?tag=googinhydr) 18418-21
5. https://onlinecourses.nptel.ac.in/noc16_cs07

CY52: PRINCIPLES OF SECURE CODING

AIM: To safeguards computer software against the accidental security vulnerabilities.

OBJECTIVE: Introduction to secure coding in different languages.

COURSE OUTLINE

Module I – INTRODUCTION: Need for secure systems- Proactive security development process- Security principles to live by and threat modeling.

Module II - SECURE CODING IN C: Character strings- String manipulation errors – String Vulnerabilities and exploits – Mitigation strategies for strings- Pointers – Mitigation strategies in pointer based vulnerabilities – Buffer Overflow based vulnerabilities.

Module III - SECURE CODING IN C++ AND JAVA: Dynamic memory management- Common errors in dynamic memory management- Memory managers- Double –free vulnerabilities –Integer security- Mitigation strategies.

Module IV- DATABASE AND WEB SPECIFIC INPUT ISSUES: Quoting the Input – Use of stored procedures- Building SQL statements securely-XSS related attacks and remedies.

COURSE MATERIAL

1. Michael Howard, David LeBlanc, “Writing Secure Code”, Microsoft Press, 2nd Edition, 2003.
2. Robert C. Seacord, “Secure Coding in C and C++”, Pearson Education, 2nd edition, 2013.

CY53 ETHICAL HACKING

AIM: Familiarize methods preventive measures for vicious attacks

OBJECTIVE: Introduction to reconnaissance methods, different cyber attacks

COURSE OUTLINE

Module I: Ethical Hacking overview, Network and computer attacks, Foot printing and social Engineering, Port Scanning, Enumeration Exploitation- techniques, buffer overflows, BASH, Format strings. Networking- OSI Model, Sockets, network sniffing, TCP/IP Hijacking. Hacking web servers, Hacking Wireless Networks, Network Protection Systems, Shell code, counter measure.

Module II: Dumpster Diving, Tailgating, Shoulder Surfing- basics, locations, electronic deduction, killer real life surfing sessions. Physical Security-Introduction, Lock bumping. Social Engineering

Module III: End point and server hacking- hacking windows, UNIX, Infrastructure hacking- remote connectivity and VOIP hacking, wireless hacking, hacking hardware.

Module IV: Reconnaissance, Web-based Exploitation, Maintaining Access with Backdoors and Rootkits.

COURSE MATERIAL

1. Hands on ethical hacking and network defense by Michael T Simpson, Kent Backman, James Corley, Cengage Learning, 2 edition, 2010
2. The Basics of Hacking and Penetration Testing by Patrick Engebretson, Syngress Basics Series, edition 01,

CY54 STATISTICAL ANALYSIS WITH R

AIM: Familiarize with concepts of R

OBJECTIVE: Introduction to programming concepts of R, probability Statistics

COURSE OUTLINE

Module I: Probability & Statistics: Introduction to Statistics- Descriptive Statistics, Summary Statistics Basic probability theory, Statistical Concepts (uni-variate and bi-variate sampling, distributions, re-sampling, statistical Inference, prediction error),

Module II: Probability Distribution (Continuous and discrete- Normal, Bernoulli, Binomial, Negative Binomial, Geometric and Poisson distribution) , Bayes' Theorem, Central Limit theorem, Data Exploration & preparation, Concepts of Correlation, Regression, Covariance, Outliers etc.

Module III: R Programming: Introduction & Installation of R, R Basics, Finding Help, Code Editors for R, Command Packages, Manipulating and Processing Data in R, Reading and Getting Data into R, Exporting Data from R, Data Objects-Data Types & Data Structure. Viewing Named Objects, Structure of Data Items, Manipulating and Processing Data in R (Creating, Accessing, Sorting data frames, Extracting, Combining, Merging, reshaping data frames), Control Structures, Functions in R (numeric, character, statistical)

Module IV: working with objects, Viewing Objects within Objects, Constructing Data Objects, Building R Packages, Running and Manipulating Packages, Non parametric Tests- ANOVA, chi-Square, t-Test, U-Test, Introduction to Graphical Analysis, Using Plots(Box Plots, Scatter plot, Pie Charts, Bar charts, Line Chart), Plotting variables, Designing Special Plots, Simple Linear Regression, Multiple Regression

COURSE MATERIAL

1. Statistical Analysis with R for Dummies (For Dummies (Computers))
2. A Handbook of Statistical Analyses Using R Brian S. Everitt and Torsten Hothorn
3. R Programming for Data Science Roger D Peng
4. Data Analysis with R Fischetti, Tony
5. Statistical Analysis of Network Data with R - Gabor Csardi Eric Kolaczyk Csardi Kolaczyk)

CY55 R Programming LAB

AIM: To get an idea of R Programming

OBJECTIVE: Introduce R Programming using nuts and bolts, control structures and clustering.

COURSE OUTLINE

The 11 number of experiments.

1. Introduction R Nuts and Bolts (I)
2. RNuts and Bolts (II)
3. Getting Data In and Out of R
4. Control Structures and Functions
5. Loop Functions
6. Data Manipulation (dplyr, reshape2 packages)
7. String Operations (stringr package)
8. Packaging, Debugging and Object Oriented Programming
9. Data Visualization (ggplot2 package)
10. Clustering
11. Regression and Classification

CY56 ETHICAL Hacking LAB

AIM: To understand the security attacks and preventive measures to be taken.

OBJECTIVE: After completion of this lab, they will be able to:

1. Monitor networks attacks
2. Penetration testing
3. Familiarize with steganographic tools

COURSE OUTLINE: This course consist of following concepts:

1. Monitoring Network Communication: Working with Trojans, Backdoors and sniffer
2. Client side script injection to a web application using XSS
3. Wireless Network attacks, Bluetooth attacks
4. Website mirroring using HTTrack and hosting on a Local Network
5. Penetration testing and justification of penetration testing through risk analysis, SQL injection Attacks
6. Steganographic Tools

CY57 MAJOR PROJECT (1ST PHASE)

The guide lines given for the course **CS342** has to be followed for this course.

An analysis and design report should be submitted at the end of this course. This report should be valued internally and marks should be awarded.

Up to coding should be finished in 5th semester.

Coding should begin in the 6th semester

CY58 STUDY TOUR

Students should be taken for at least 3-5 day tour any of the software industry and the credits should be awarded based on the study tour report submitted

CY61 SOFTWARE FORENSICS AND VULNERABILITY ANALYSIS

AIM: To familiarize software security, operations and service level security.

OBJECTIVE: To understand the need for software security and awareness of application-Level Threats and Vulnerabilities

COURSE OUTLINE

Module I: Introduction to Software Security - Dealing with Widespread Security Failures, Bugtraq, CERT Advisories, RISKS Digest, Technical Trends Affecting Software Security, Penetrate and Patch, Engineering, Security Goals, Prevention, Traceability. Monitoring, Privacy and Confidentiality, Multilevel Security, Anonymity, Authentication, Integrity, Know Your Enemy – Common Software Security Pitfalls. Software Project Goals.

Module II: Managing Software Security Risk: Software Risk Management For Security, The Role Of Security Personnel, Software Security Personnel in the Life Cycle, Deriving Requirements, Risk Assessment, Design For Security, Implementation and Testing, A Dose People To Think About Security,

Module III: Practice, When Development Goes Astray, Code Review (Tools) - Architectural Risk Analysis - Penetration Testing - Risk-Based Security Testing - Abuse Cases - Security Requirements – Security Operations

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

COURSE MATERIAL

1. John Viega & Gary McGraw: Building Secure Software: How to Avoid Security Problems the Right Way (Addison-Wesley Professional Computing Series)
2. Gary McGraw: Software Security: Building Security in (Addison-Wesley Professional Computing Series)
3. Abhijit Belapurkar, Anirban Chakrabarti and et al., “Distributed Systems Security: Issues, Processes and solutions”, Wiley, Ltd., Publication, 2009.
4. Abhijit Belapurkar, Anirban Chakrabarti, Harigopal Ponnappalli, Niranjana Varadarajan, Srinivas Padmanabhuni and Srikanth Sundarajan, “Distributed Systems Security: Issues, Processes and Solutions”, Wiley publications, 2009.

CY62 INTERNET OF THINGS

AIM: IoT is aimed at enabling the interconnection and integration of the physical world and the cyber space. It represents the trend of future networking and leads the third wave of the IT industry revolution.

OBJECTIVES: Understand IoT Market perspective, Data and Knowledge Management and use of Devices in IoT Technology, Understanding State of the Art – IoT Architecture, Real World IoT Design Constraints, Industrial Automation and Commercial Building Automation in IoT.

COURSE OUTLINE

Module I: Introduction to IoT: - Genesis of IoT, Digitization, Impact, Connected Roadways - Challenges-safety, mobility, environment, Connected Factory -industry – mechanical assistance, mass production, electronics and control, integration, Smart Connected Buildings – heating, ventilation, HVAC systems, BAS System, BACNet, Smart Creatures, Convergence of IT and OT, IoT Challenges – Scale, Security, Privacy, Big data and data analytics. IoT Network Architecture and Design: - Drivers Behind New Network Architectures, Comparing IoT Architectures, A Simplified IoT Architecture, The Core IoT Functional Stack, IoT Data Management and Compute Stack

Module II: Engineering IoT Networks: Smart Objects - Sensors, Actuators, and Smart Objects, Sensor Networks, Connecting Smart Objects: Communications Criteria IoT Access Technologies

Module III: IP as the IoT Network Layer: Business Case for IP, Need for Optimization, Optimizing IP for IoT, Profiles and Compliances, Application Protocols for IoT: Transport Layer, IoT Application Transport Methods

Module IV: Securing IoT: A Brief History of OT Security, Common Challenges in OT Security, How IT and OT Security Practices and Systems Vary, Formal Risk Analysis Structures: OCTAVE and FAIR, The Phased Application of Security in an Operational Environment

COURSE MATERIAL

1. David Hanes Gonzalo Salgueiro, Patrick Grossetete, Robert Barton, Jerome Henry “IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things”, Pearson, 2017
2. Graham Meikle “The Internet of Things”, Polity Press, 2017,
3. Vijay Madiseti and Arshdeep Bahga, “Internet of Things (A Hands-on-Approach)”, 1stEdition, VPT, 2014.

CY63 MOBILE AND WIRELESS SECURITY

AIM: To enhance students learning in *security* architectures

OBJECTIVE: Student will be familiarized with *mobile/wireless* communications security concepts

COURSE OUTLINE

Module I – INTRODUCTION Security and Privacy for Mobile and Wireless Networks: Introduction-State of the Art- Areas for Future Research- General Recommendation for Research. Pervasive Systems: Enhancing Trust Negotiation with Privacy Support: Trust Negotiation- Weakness of Trust Negotiation- Extending Trust Negotiation to Support Privacy

Module II - MOBILE SECURITY Mobile system architectures, Overview of mobile cellular systems, GSM and UMTS Security & Attacks, Vulnerabilities in Cellular Services, Cellular Jamming Attacks & Mitigation, Security in Cellular VoIP Services, Mobile application security.

Module III - SECURING WIRELESS NETWORKS Overview of Wireless security, Scanning and Enumerating 802.11 Networks, Attacking 802.11 Networks, Attacking WPA protected 802.11 Networks, Bluetooth Scanning and Reconnaissance, Bluetooth Eavesdropping, Attacking and Exploiting Bluetooth, Zigbee Security, Zigbee Attacks

Module IV - ADHOC NETWORK SECURITY: Security in Ad Hoc Wireless Networks, Network Security Requirements, Issues and Challenges in Security Provisioning, Network Security Attacks, Key Management in Adhoc Wireless Networks, Secure Routing in Adhoc Wireless Networks

COURSE MATERIAL

1. C. Siva Ram Murthy, B.S. Manoj, “Adhoc Wireless Networks Architectures and Protocols”, Prentice Hall, x ISBN 9788131706885, 2007.
2. Nouredine Boudriga, ”Security of Mobile Communications”, ISBN 9780849379413, 2010.

CY64: WINDOWS AND LINUX FORENSIC ANALYSIS

AIM: To addresses topics in the area of forensic analysis of systems running WINDOWS and LINUX.

OBJECTIVE: To familiarize Windows Forensic Analysis, Registry Analysis, Rootkit Detection, Linux Forensic Analysis

COURSE OUTLINE

Module I: Windows Forensic Analysis- Live Response Response - Locard’s Exchange Principle, Order of Volatility, Nonvolatile Information, Live-Response Methodologies, Data Analysis- Data Analysis, Agile Analysis, Windows Memory Analysis-Collecting Process Memory, Dumping Physical Memory, Alternative Approaches for Dumping Physical Memory, Analyzing a Physical Memory Dump.

Module II: Registry Analysis- Inside the Registry, Registry Analysis- RegRipper, System Information, Autostart Locations, USB Removable Storage Devices, Mounted Devices, Portable Devices, Finding Users, Tracking User Activity, Redirection, Virtualization, Deleted Registry Keys, File Analysis-Log Files, Event Logs, Other Log files, Recycle Bin, XP System Restore Points, Alternative Methods of Analysis, Executable File Analysis- Static Analysis, Dynamic Analysis.

Module III: Rootkits, Rootkit Detection-Live Detection, GMER, Helios, MS Strider GhostBuster, F-Secure BlackLight, Sophos Anti-Rootkit, Postmortem Detection, Prevention.

Module IV: Linux Forensic Analysis- Live Response Data Collection- Prepare the Target Media, Format the Drive, Gather Volatile Information, Acquiring the Image, Initial Triage and Live Response

COURSE MATERIAL

1. Unix and Linux Forensic Analysis DVD ToolKit - Chris Pogue, Cory Altheide, Todd Haverkos, Syngress Inc., 2008
2. Windows Forensic Analysis DVD Toolkit- Harlan Carvey, Edition 2, Syngress Inc., 2009
3. Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry - Harlan Carvey, SyngressInc, Feb 2011
4. File System Forensic Analysis- Brian Carrier, Addison Wesley, and Edition 1, 2005

CY 65 RISK ASSESSMENT & SECURITY AUDIT

AIM: To process, analyse and evaluate the security risks, and determine the mitigation measures to reduce risk and also risk assessment to provide appropriate levels of security for information

OBJECTIVE: To provide an idea on risk assessment, data collection and cybercrime investigation.

COURSE OUTLINE

Module I –Security Management: Security plan, Security analysis, change Management-Capability Maturity Model, Disaster Recovery-Policies and procedures, System Security Management-Configuration Control Board, Management Procedures.

Module II – Protecting Storage Media: Protection of System Documentation-Security in software applications, Operating System and Package Maintenance ,Protection of Development Suite and Test Data, Exchanges of Information and Software, Security Requirements of systems.

Module III – Introduction: What is risk, risk management –overview of risk management, identification, Risk analysis, Incident Management: Incident notification, Incident classification

Module IV –Incident Response: Incident Response team, Incident response process: Incident recording, Incident notification, Incident classification, Incident Tracking, Response

COURSE MATERIAL

1. Brijendra Singh, Cryptography & Network Security, PHI.

CY66 CLOUD ARCHITECTURE AND SECURITY

AIM: Equip students to protect data, applications and the associated infrastructure of cloud computing.

OBJECTIVE: Students will be familiarized with cloud applications, technologies and cloud security concepts.

COURSE OUTLINE

Module I- CLOUD COMPUTING FUNDAMENTALS: Cloud Computing definition, private, public and hybrid cloud. Cloud types; IaaS, PaaS, SaaS. Benefits and challenges of cloud computing, public vs private clouds, role of virtualization in enabling the cloud; Business Agility: Benefits and challenges to Cloud architecture.

Module II- CLOUD APPLICATIONS :Technologies and the processes required when deploying web services-Deploying a web service from inside and outside a cloud architecture, advantages and disadvantages- Development environments for service development; Amazon, Azure, Google App.

Module III– SECURING THE CLOUD Security Concepts: Confidentiality, privacy, integrity, authentication, non-repudiation, availability, access control, defence in depth, least privilege- how these concepts apply in the cloud and their importance in PaaS, IaaS and SaaS. E.g. User authentication in the cloud.

Module IV– VIRTUALIZATION SECURITY :Multi-tenancy Issues: Isolation of users/VMs from each other- How the cloud provider can provide this- Virtualization System Security Issues: e.g. ESX and ESXi Security, CLOUD SECURITY MANAGEMENT :Security management in the cloud – security management standards- SaaS, PaaS, IaaS

COURSE MATERIAL

1. GautamShroff, “Enterprise Cloud Computing Technology Architecture Applications”, Cambridge University Press; 1 edition [ISBN: 978-0521137355], 2010.
2. Toby Velte, Anthony Velte, Robert Elsenpeter, “Cloud Computing, A Practical Approach”, Tata McGraw-Hill Osborne Media; 1 edition 22, [ISBN: 0071626948], 2009.
3. Tim Mather, SubraKumaraswamy, ShahedLatif, “Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance”, O'Reilly Media; 1 edition, [ISBN: 0596802765], 2009.

CY67 MAJOR PROJECT (IIND PHASE)

1. AIM: To expose student to industry-standard project practices based on cyber forensics and security practices, applying the knowledge acquired through various courses.

2. OBJECTIVES: To provide an opportunity to apply the knowledge gained through various courses in solving a real life problem

1. To provide an opportunity to apply security and forensics practices for software development, network monitoring, malware analysis etc.
2. To introduce the student to a professional environment and/or style typical of a global IT industry
3. To provide an opportunity for practical as well real life scenarios in midst of an threat or attack
4. To provide an opportunity for effective, real-life protection and detection of threats
5. To provide an opportunity to practice cryptographic algorithms.

3. PROJECT GUIDELINES

Group Size – Maximum 3

No. of records – No. of group members + 1 (Department copy)

Certificate should include the names of all members

The minimal phases for the project are: Project search, finalization and allocation, Investigation of system requirements, Data and Process Modelling, System Design, Program design, Program coding and unit testing, System integration, System implementation and acceptance testing.

3.1 Planning the Project: The Major Project is an involved Exercise which has to be planned well in advance. The topic should be chosen in Semester 4 itself and the case study of Course should as far as possible, be based on the project topic, though on Exceptional cases, for valid reasons, the project guide may waive this condition. Related reading, training and discussions should start from semester 5 itself.

3.2 Selection of project work: Project work could be of 3 types:

a) Developing solution for a real-life problem: In this case, a requirement for developing cyber security based solution already Exists and the different updated versions of system or application is to be implemented successfully. Examples are modified cryptography algorithms & tools, application which can produce security, detection or prevention etc. The scope for creativity and Exploration in such projects is limited, but if done meticulously, valuable Experience in the industrial context can be gained.

(b) Innovative Product development: These are projects where a clear-cut requirement for developing a computer based solution may not be existing, but a possible utility for the same is conceived by the proposer.

(c) Research level project: These are projects which involve research and development and may not be as structured and clear cut as in the above case... These projects provide more challenging opportunities to students, but at EX level is a difficult choice. If any student identifies proper support in terms of guidance, technology and references from External organizations and also the supervisors are convinced of the ability of the student(s) to take up the project, it shall be permitted. The methodology and reporting of such projects could be markedly different from type (a) and is left to the proposer/external supervisor of the projects.

3.3 Selection of Team: To meet the stated objectives, it is imperative that Major Project is done through a team effort. Though it would be ideal to select the team members at random(drawing lots) and this should be strongly recommended, due to practical considerations, students may also be given the choice of forming themselves into teams with 3 to 5 members (teams less than 3 members may be permitted in Exceptional cases, for valid reasons). A gender mix should also be strongly suggested. A team leader shall be elected through drawing lots. Teams shall maintain team meeting minutes and ensure that every team member has tasks assigned in writing. Team meeting minutes shall form a part of the Project Report. Even if students are doing projects as groups, each one must independently take up different modules of the work and must submit the reports also independently (though, in such cases, some common materials is permissible). Evaluation will also be done independently.

3.4 Selection of Tools: No restrictions shall be placed on the students in the choice of platforms/tools/languages to be utilized for their project work, though open source is strongly recommended, wherever possible. No value shall be placed on the use of tools in the evaluation of the project.

3.5 Selection of Organization& Guide: No restrictions shall be placed on the students in the choice of organization where project work may be done, in terms of locality, type (public/private) etc. It is the duty of the Head of Institute/Principal of College to ensure that the Aim, Objectives and full project guidelines

are communicated to the external organization. The guide should ideally be a post-graduate with minimum 2 years of work experience.

Students may also choose to do project in the college/institute (or partially in the college/institute and partially in an external organization), especially product-based work, but in such cases the supervisors must ensure that (i) industry practices are followed (ii) the students undertake a planned visit to an IT industry with international operations to make up for the loss of experience and (iii) the services of an external guide with industry experience is obtained.

3.6 Project Management: Head of Institute/Principal of College should publish a list of students, projects topics, internal guide and external organization (if any) and teams agreed, before the end of semester 5. Changes in this list may be permitted for valid reasons and shall be considered favorably by Head of Institute/Principal of College any time before commencement of the project. Any request for change after commencement should be considered by a committee of 3 teachers and their recommendation shall be accepted by Head of Institute/Principal of College.

Gantt-chart of proposed activities and a draft statement of project deliverables (which may subsequently be altered if justified) should be prepared before the commencement of the project. The actual completion of each phase should be noted on the chart in the course of the project work. Students should submit a fortnightly report of progress which could be indication of percentage of completion marked on the original Gantt-chart, with any notes attached. Students should ideally keep a daily activity log sheet. Team meetings should be documented in the format given at the end. Changes in the submitted documents are possible, as project development is essentially an evolutionary process. The project guide must ensure that changes are necessary due to the knowledge gained in succeeding phases of the project. The date of completion of a phase should be brought forward if the changes made are deemed to be errors and not due to additional knowledge gained from a succeeding phase.

3.7 Documentation:

The following are the major guidelines:

The final outer dimensions of the report shall be 21cm X 30 cm. The color of the flap cover shall be light green.

Only hard binding should be done, with title of the thesis and the words “<BRIEF TITLE> BSc (CS) Project Report 200...” displayed on the spine in 20 point, Bold, Times New Roman, as in example below.

In case the title is too long, a shorter version of it may be used (Like “Image Pro” instead of “Image Pro – An Interactive Image Processing package”). It is highly recommended that Latex be used for documentation.

- The text of the report should be set in 12 pt, Times New Roman, Single Spaced.
- Headings should be set as follows: CHAPTER HEADINGS 20 pt., Times New Roman, Bold, All Caps, and Centered.

MATRIX BASED SHOULDER SURFING SECURITY SYSTEM: BVoc (CY) PROJECT 2018

1. SECTION HEADINGS 12 pt, Times New Roman, Bold, All Caps, Left Adjusted.

1.1 Section Sub-headings 12 pt, Times New Roman, Bold, Left Adjusted.

Titles of Figures, Tables etc are done in 12 point, times New Roman, Italics, and Centered.

<PROJECT TITLE>
<STUDENT'S NAME>
<COLLEGE NAME>
PROJECT REPORT

Submitted in partial fulfilment of the
Requirements for the award of
BVoc (Cyber Security) degree of
University of Kerala
2018

Some general guidelines on documentation stylistics are:

- Double quotes and single quotes (“”, “”) should be used only when essential. In most cases words put in quotes are better highlighted by setting them in italics. Eg: This process is known as “morphing”. This process is known as morphing.
- Page numbers shall be set at right hand top corner, paragraph indent shall be set as 3.
- Only single space need be left above a section or sub-section heading and no space may be left after them.
- Certificate should be in the format: “Certified that this report titled..... is a bonafide record of the project work done by Sri/Kum..... under our supervision and guidance, towards partial fulfillment of the requirements for the award of the Degree of BVoc(Cyber Security) of the University of Kerala” with dated signatures of Internal; Guide, external guide and also Head of Institute/College.
- If the project is done in an external organization, another certificates on the letterhead of the organization is required: “Certified that his report titled..... is a bonafide record of the project work done by Sri/Kum..... under any supervision and guidance, at theDepartment of..... (Organization) towards partial fulfilment of the requirements for the award of the Degree of BVoc (Cyber Security) of the University of Kerala”.
- References shall be IEEE format (see any IEEE magazine or transaction). Take care in use of italics and punctuation. While doing the project, keep note of all books you refer, in the correct format, and include them in alphabetical order in your reference list. Eg: A book is cited as: Kartalopoulos, S V Understanding Neural Networks and Fuzzy Logic, BPB Publishers, 1996, pp. 21-27. (Pp.21-27 indicates that pages 21-27 have been referred. If the whole book is being referred, this may be omitted. If a single page is referred, say 7, it may be cited as p.7 Report writing is NOT a hasty activity done after finishing the project. Students must try to develop the report along with the work, so as to give it flesh and blood. Drafts should be read, modified, spell checked and grammar checked at least thrice during the course of the project and before a final printout is taken, the same may be got approved from the internal guide. The students should send two interim reports to internal guides. This will also help the students in their report writing.

The Gantt chart, fortnightly progress reports, and team meeting minutes mentioned in section 3.5 should appear as appendix to the project report. Regarding the body of the report, as an indicative Example, the following is given (though students should not attempt to fit every kind of project report into this format):

- Overview (background objectives purpose, scope, and applicability)

- survey of technologies
- Requirements and analysis (problem definition, requirements specification, software and hardware requirements, conceptual models)
- System design (basic modules, procedural design, logic diagrams, algorithms design)
- user interface design
- Implementation and testing (implementation approaches, coding details and code efficiency
Testing approach (e.g. unit testing, integrated testing etc.))
- Results and discussion
- future scope

3.8 Methodology:

The project report should generally contain details of the following steps (though students should not attempt to fit every kind of project into this format):

(a) Analysis

- Study of existing systems and its drawbacks (general)
- Understanding the functionalities of the system (detailed)
- Preparation of requirement
- Conduct of Feasibility study
- Identification of relevant modules
- Relationship between modules

(b) Design

- Design of each subsystems
- Design of each modules
- Design of communications between modules
- Design of Algorithms for problem solving
- User interface Design
- Any other steps if necessary

(c) Coding and Implementation

(d) Testing

(e) Security, Backup and Recovery Mechanisms

(f) Online help and User Manuals

(g) Upgradability Possibilities

3.9 Project IPR &Utilisation: The intellectual property rights in all project work done by the students shall vest with the University of Kerala, except in cases where some external organizations seek undertaking from students to concede IPR in all work done in their organization or under their guidance. Where possible, students should attempt to obtain at least a joint IPR for the University. In cases where project works are of public utility, students shall be asked to publish their work including source code and documentation, in so far as their rights are clear.

COURSE MATERIAL

1. Network Security Bible- Eric Cole, Ronald Krutz, James W. Conley, Edition 2, Wiley India Pvt Ltd, 2010
2. Network Security Essentials – William Stallings, Edition 4, Pearson Education, 2011
3. Cryptography and Network Security: Principles and Practice-William Stallings, Edition 3, Pearson education, 2003

4. Hacking Exposed- Network Security secrets and solutions, Joel Scambray, McGraw Hill, Edition 5, 2005
5. Frederic P B, Mythical Man-month, Essays on Software Engineering, Addison Wesley
David Lamport,
6. Latex: A document Preparation System, 2/e, Pearson Education

Evaluation criteria

a. System analysis and design	20 marks
b. Output	10 marks
c. Candidate role and contribution in the project	10 marks
d. Demo	15 marks
e. Overall quality	10 marks
f. Viva	15 marks
Total	80 marks