PSGR
Krishnammal College for Women

DEPARTMENT OF COMPUTER SCIENCE WITH CYBER SECURITY

CHOICE BASED CREDIT SYSTEM (CBCS)
&
LEARNING OUTCOMES BASED CURRICULAR FRAMEWORK (LOCF)

B.Sc COMPUTER SCIENCE WITH CYBER SECURITY

2022-2025 BATCH

PROGRAMME LEARNING OUTCOMES (PLO's)

After Completion of the programme, the student will be able to

PLO1: Design, implement, and evaluate a computer network and information security needs of an organization.

PLO2: Analyze and evaluate the cyber security needs of an organization and society.

PLO3: Explore Current and emerging techniques and technologies to formulate solutions for systems and organizations.

PLO4: Pursue higher studies in the specialized area and also promote life-long learning for professional development.

PLO5: Recognize as world class professionals in IT and in cybercrime and produce women entrepreneurs to increase more employability.

PROGRAMME SPECIFIC OUTCOMES (PSO's)

The students at the time of graduation will

PSO1: Professionally be equipped in the areas of cyber security tools and cyber/computer forensics software/tools.

PSO2: Apply the knowledge of technology and characterize privacy, legal and ethical issues of information security.

PSO3: Analyze modern cyber security tools and applications for their successful Career, to create platforms to become an entrepreneur and a relish for higher studies.

PSGR Krishnammal College for Women

DEPARTMENT OF COMPUTER SCIENCE WITH CYBER SECURITY

CHOICE BASED CREDIT SYSTEM & LEARNING OUTCOMES BASED CURRICULAR FRAMEWORK (LOCF)

B.Sc. Computer Science with Cyber Security – 2022-2025 BATCH

Semester	Part	Subject Code	Title of paper	Category	Instruction hours /	Contact hours	Tutorial hours	Duration of Examination	Examination Marks			Credits
									CA	ESE	Total	
I	I	TAM2201/ HIN2201/ FRE2201	Language I	Language	6	86	4	3	50	50	100	3
	II	ENG2101	English Paper I	Language	6	86	4	3	50	50	100	3
	III	CY22C01	**Core-1**: Python Programming	CC	4	56	4	3	50	50	100	4
	III	CY22CP1	**Lab1:** Python Programming Lab	CC	3	45	-	3	25	25	50	2
	III	PP22C02	**Core –2** : Computational and Algorithmic Thinking for Problem Solving	CC	3	45	-	-	100 #	-	100	3
	III	TH22A29	**Allied A1 :** Number Theory and Cryptography	GE	6	86	4	3	50	50	100	5
	IV	NME21ES	Introduction to Entrepreneurship	AEC	2	26	4	2	50	50	100	2
		NME22A1/ NME22B1/	Advance Tamil/ Basic Tamil	AEC	2	28	4	2	50	50	100	
	I	TAM2202/ HIN2202/ FRE2202	Language II	Language	6	86	4	3	50	50	100	3
	II	ENG2102	English Paper II	Language	5	71	4	3	50	50	100	3

II	III	CY22CO3	**Core – 3:** IT Fundamentals for Cyber Security and Cryptography	CC	5	71	4	3	50	50	100	5
	III	CY22CP2	**Lab -2:** Cyber Security tools Lab	CC	5	75	-	3	25	25	50	3
	III	TH22A06	**Allied A2:** Discrete Mathematics	GE	6	86	4	3	50	50	100	5
	IV		Open Course:(Self study- Online Course)	AEC	-	-	-	-	-	-	-	Grade
		NME22A2/ NME22B2	**Advance Tamil/Basic Tamil	AEC	-	-	-	-	-	-	-	Grade
	V	21PEPS1	Professional English for Physical Sciences	AEC	3	40	5	2	50	50	100	2
	VI	NM12GAW	General Awareness	AEC	Self Study	-	-	Online Test	100	-	-	Grade
III	I	TAM2203A/ HIN2203A/ FRE2203A	Language III	Language	4	58	2	3	50	50	100	3
	II	ENG2203A	English Paper III	English	4	58	2	3	50	50	100	3
	III	CY22C04	**Core - 4**: Computer Networks	CC	4	58	2	3	50	50	100	3
	III	CY22C05	**Core - 5:** Data Structure and Algorithms	CC	4	58	2	3	50	50	100	3
	III	CY22CP3	**Lab 3:** DBMS Lab	CC	5	75	-	3	25	25	50	4
	III	TH22A13	**Allied A3:** Optimization Techniques	GE	4	58	2	3	50	50	100	3
	III	CY22SBCE	**SBS I :** Coursera: Data Structures Lab	SEC	3	45		-	-	100	100	3
	IV	NM22EVS	**Foundation Course-II:** Environmental Studies	AECC	Self-	-	-	-	100	-	100	Grade

	IV	NM22UHR	**Foundation Course III:** Universal Human Values& Human Rights	AECC	2	30	-	-	100	-	100	2
IV	I	TAM2204A/ HIN2204A/ FRE2204A	Language IV	**Language**	4	58	2	3	50	50	100	3
	II	ENG2204A	English Paper IV	**English**	4	58	2	3	50	50	100	3
	III	CY22C06	**Core – 6** Operating Systems Security	**CC**	4	58	2	3	50	50	100	3
	III	CY22C07	**Core 7:** Vulnerability Assessment and Penetration Testing (VAPT**)**	**CC**	4	58	2	3	50	50	100	3
	III	CY22CP4	**Lab 4:** VAPT LAB	**CC**	5	75	-	3	25	25*	50	3
	III	CY22A01 CY22A02	**Allied A4:** **Paper I** –Data Security **Paper II** –Cyber Law & E-Security	**GE**	4	58	2	3	50	50	100	3
	III	CY22SBP2	**SBS: II-**Mobile App Development Lab	**SEC**	3	41	4	-	100	-	100	3
	IV	NM22DTG	**Foundation Course**: IV Design Thinking	**Finishing School Part A**	2	30	-	-	100	-	100	2
		COM15SER	Community Oriented Service		-	-	-	-	-	-	-	Grade

	V		NSS/NCC/YRC/Sports & Games.		-	-	-	-	-	-	100	1
	IV		Job Oriented Course: Security +	-	-	-	-	-	-	-	-	Grade
V	III	CY22C08	**Core 8**:Software Engineeringand Testing	CC	5	73	2	3	50	50	100	4
	III	CY22C09	**Core 9**:Ethical Hacking	CC	5	73	2	3	50	50	100	5
	III	AI22C10	**Core 10**: Machine Learning	CC	5	73	2	3	50	50	100	4
	III	CY22E01 CY22E02	**Elective 1:** Cloud Security Web Application and Security	DSE	5	73	2	3	50	50	100	5
		CY22CP5	**Lab 5:** Ethical HackingLab	CC	5	75	-	3	25#	25#	50	3
	III	CY22SBP3	**SBS III:**Cyber Security Tools Lab-II	SEC	3	41	4	-	100	-	100	3
		CY22AC1 CY22AC2	**Advanced Level Course 1*** Paper 1: CybernThreats and Modeling Paper II: Artificial Intelligence	ACC	-	-	-	3	25	75	100*	5*
	IV	NM21CS1	Cyber Security I	AEC	2	30	-	-	100	-	100	Grade
	IV	CY22INST1	Field work/Institutional Training	DSE	-	-	-	-	100	-	100	2
	VI	CY22COM	Comprehensive Exam	GC	-	-	-	1	-	100	100	Grade

	VI	COM15SER	Community Service 30 Hours	GC	-	-	-	-	-	-	-	-
I-V	VI	16BONL1 16BONL2	Online Course I Online Course II	Online Course I Online Course II	ACC	-	-	-	-	-	-	-
VI	III	CY22C11	IoT and Security	CC	5	73	2	3	50	50	100	4
	III	CY22C12	Malware Analysis	CC	5	73	2	3	50	50	100	4
	III	CY22C13	Digital Forensics	CC	5	73	2	3	50	50	100	3
	III	CY22CP6	Malware Analysis Lab	CC	5	75	-	3	25#	25#	50#	3
	III	CY22PROJ	Project and Viva-Voce	DSE	7	105	-	1	50	50	100	5
	III	CY22SBP4	Digital Forensics Lab	SEC	3	41	4	-	100	-	100	3
	III	CY22AC3 CY22AC4	**ALC*** Big Data Analytics IPv6	ACC	SS	-	-	3	25	75	100	5
	VI	16BONL1 16BONL2	Online Course I Online Course II	ACC	-	-	-	-	-	-	-	-

#CA conducted for 25 marks

#ESE conducted for 100 and converted to 25

*The credit is applicable to a candidate who takes up the advanced learner l course exam.

CC: Core Courses
CA: Continuous Assessment
DSE: Discipline Specific Elective
ESE: End Semester Examination
AEC: Ability Enhancement Course
SEC: Skill Enhancement CourseACC: Additional Credit Course
AECC: Ability Enhancement Compulsory Course
GC: General Course

COURSE NUMBER	COURSE NAME	CATEGORY	L	T	P	CREDIT
CY22C01	PYTHON PROGRAMMING	Theory	56	4	-	4

Preamble

The course covers basic knowledge of Python Programming. It defines the Conditional Statements & Loops, Functions, Tuples, Python data structures and Exception & its tools.

Course Learning Outcomes

On the successful completion of the course, students will be able to

CLO Number	CLO Statement	Knowledge Level
CLO1	Recall the technical strengths, Python Interpreter and the program execution.	K1
CLO2	Understand the purpose of operations, strings, lists, tuples to solve problems	K2
CLO3	Apply functions to solve problems using procedure-oriented approach	K3
CLO4	Analyze the problems and solve it by applying appropriate logic	K4

Mapping with Programme Learning Outcomes

CLOs	PLO1	PLO2	PLO3	PLO4	PLO5
CLO1	S	S	S	M	S
CLO2	S	S	M	S	M
CLO3	M	S	S	S	S
CLO4	S	M	S	S	S

S- Strong; M-Medium; L-Low

PYTHON PROGRAMMING-CY22C01 **56 Hrs**

Syllabus

UNIT I **(10 Hrs)**

Introduction: Why do people use python- Python a scripting language- Users of Python- Need of Python- Python's Technical Strengths- How Python runs programs: Introducing the Python Interpreter- Program Execution-Execution Model Variation: Python Implementation Alternatives.

UNIT II **(10 Hrs)**

Types & Operations: Numbers Types: Numeric type basics, Numbers in action, Other numeric types- Strings Fundamentals: String Basics, String Literals, Strings in action, String Methods – Lists and Dictionaries-Tuples- Files.

UNIT III **(12 Hrs)**

Control Flow: Statements& Syntax: Assignment-Expressions & Print- if tests-While& for loops. unctions: Function Basics: Why use functions- Coding Functions- Definition & Calls. Scopes:

Python basics-Global Statement-Scopes Nested functions.-Arguments: Arguments passing Basics-Special Arguments Matching Modes.

UNIT IV **(12 Hrs)**

Classes &OOP: OOP: Introduction-Class Coding Basics- Class Coding details: Class statement-Methods-Inheritance. Designing with classes: Python and OOP-OOP Inheritance, Composition, Delegation-Methods and Classes act as Objects-Multiple Inheritance.

UNIT V **(12 Hrs)**

Exception &Tools: Exception Basics-Exception Coding Details- Exception Objects- Designing with Exceptions.

Text Book

S. No	Author	Title of the Book	Publisher	Year of Publication
1	Mark Lutz	Learning python	O'Reilly Publication	5th edition, 2013

Reference Books

S. No	Author	Title of the Book	Publisher	Year of Publication
1	Mark Summerfield	Programming in python 3	Pearson Education	2009.
2	Mark Pilgrim	Dive into python 3	Apress publication	2011
3	**Richard L. Halterman**	Fundamentals of Python Programming	Southern Adventist University	2017

Pedagogy

- Lectures, Group discussions, Demonstrations

Course Designer

Dr.K.Sathyakumari

COURSE NUMBER	COURSE NAME	CATEGORY	L	T	P	CREDIT
PP22C02	COMPUTATIONAL AND ALGORITHMIC THINKING FOR PROBLEM SOLVING	Theory	45	-	-	3

Preamble

- This course aims to kindle the young minds to think like a computer scientist, with the idea that Computing and computers will enable the spread of computational thinking.
- Computational thinking is thinking recursively, reformulating a seemingly difficult problem into one which we know how to solve and taking an approach to solving problems, designing systems,and understanding human behavior that draws on concepts fundamental to computer science.

Course Learning Outcomes

On the successful completion of the course, students will be able to

CLO Number	CLO Statement	Knowledge Level
CLO1	Define the basic principles of logical reasoning, problem solving in computational thinking	K1
CLO2	Understanding the applications of propositional logic, problem representation and techniques	K2
CLO3	Apply algorithmic thinking to problem solving using tools	K3
CLO4	Apply and analyze to solve domain specific problems using computational thinking concepts	K4

Mapping with Programme Learning Outcomes

CLOs	PLO1	PLO2	PLO3	PLO4	PL05
CLO1	M	S	S	S	S
CLO2	S	S	S	M	S
CLO3	S	M	S	S	S
CLO4	S	S	M	S	S

S - Strong; M - Medium; L – Low

COMPUTATIONAL AND ALGORITHMIC THINKING FOR PROBLEM SOLVING - PC22C02

45 Hrs

Syllabus

Unit I **7 Hrs**

Basics: Introduction to Computational Thinking- Data Logic - History of Computational Thinking- Applications of Computational Thinking.

Unit II **8 Hrs**

Data- Information and Data - Data Encoding - Logic - Boolean logic - Applications of simple Propositional Logic. Tool: Flowgorithm and Scratch.

Unit III **10 Hrs**

Problem Solving and Algorithmic Thinking: Problem definition- Logical reasoning- Problem decomposition- Abstraction- Problem representation via Algorithmic thinking: Name binding- Selection- Repetition and Control Abstraction- Simple Algorithms – Comparison of performance of Algorithms.

Unit IV **8 Hrs**

Activities in Class: Sudoku-Towers of Hanoi- Graph Coloring-Geographical Map reading- Poem reading-Novel reading- Data analysis on news.

Unit V **12 Hrs**

Problem Solving Techniques- Factoring and Recursion Techniques- Greedy Techniques-Divide and Conquer- Search and Sort Algorithms- Text Processing and Pattern matching. Tool: iPython

Text Book

S. No	Author	Title of the Book	Publisher	Year of Publication
1	David Riley and Kenny Hunt	Computational Thinking for Modern Solver	Chapman & Hall/CRC	2014
2	Paolo Ferragina, Fabrizio Luccio	Computational Thinking First Algorithms	Springer	2018
3	Karl Beecher	Computational Thinking – A beginner's guide to problem solving	BSC publication	2017

Pedagogy

- Lectures, Group discussions, Demonstrations, Case studies

Course Designer

Mrs. R.Jayasree

Evaluation Pattern:

Assessment	Number	Marks
Quiz (online or offline)	5	50
Class Activity	5	25
Group Project (Domain Specific)	1	25
Total		100

COURSE NUMBER	COURSE NAME	CATEGORY	L	T	P	CREDIT
CY22CP1	PYTHON PROGRAMMING LAB	PRACTICAL	-	-	45	2

Preamble

- The course gives hands-on experience on Python Programming and improves the practical skillset.
- The learner will be able to develop the logic for the given problem, recognize and understandthe syntax and construction of Python code.
- The course involved in compiling, linking and debugging Python code and developing somecomplex programs.

Course Learning Outcomes

On the successful completion of the course, students will be able to

CLO Number	CLO Statement	Knowledge Level
CLO1	Identify the basic terminologies of Python programming such as data types, conditional statement, looping statements and functions.	K1
CLO2	Develop programs with implementation of operators & I/O operations	K2
CLO3	Construct programs with features of Lists, Strings.	K3
CLO4	Develop readable programs with files for Exception handling concepts.	K4

Mapping with Programme Outcomes

CLOs	PLO1	PLO2	PLO3	PLO4	PLO5
CLO1	S	S	M	S	M
CLO2	S	S	S	S	S
CLO3	S	S	S	S	M
CLO4	S	S	M	S	S

S- Strong; M-Medium;

PYTHON PROGRAMMING LAB- **45 Hrs**

Program List

- Exercise programs on basic control structures & loops.
- Exercise programs on operators & I/O operations.
- Exercise programs on Python Script.
- Exercise programs on Lists.
- Exercise programs on Strings.
- Exercise programs on functions.
- Exercise programs on recursion & parameter passing techniques.
- Exercise programs on Tuples.
- Exercise programs on file.
- Exercise programs on Exception handling concepts.
- Exercise program to ping two Network Machine using TCP code.
- Exercise program to Hash Encryption and Decryption giving data.

Pedagogy

- Demonstration of working environment/Tools/Software/Program

Course Designer

Dr.K.Sathyakumari

COURSE NUMBER	COURSE NAME	CATEGORY	L	T	P	CREDIT
CY22C03	IT FUNDAMENTALS FOR CYBER SECURITY AND CRYPTOGRAPHY	THEORY	71	4	-	5

Preamble

This course provides the fundamentals of computers and understanding the key issues associated with protecting information assets. The purpose of the course is to provide an overview of the field of cyber security, cybercrime and information assurance.

Course Learning Outcomes

On the successful completion of the course, students will be able to

CLO Number	CLO Statement	Knowledge Level
CLO1	Recall the concepts of input and output devices, Information Security	K1
CLO2	Understand the concepts of Number systems, importance and challenges in Cyber Security.	K2
CLO3	Develop the applications by cybersecurity tools.	K3
CLO4	Analyze & implement the real- time applications by Cyber Security tools.	K4

Mapping with Programme Learning Outcomes

CLOs	PLO1	PLO2	PLO 3	PLO 4	PLO 5
CLO1	S	M	S	S	M
CLO2	S	S	S	S	M
CLO3	S	M	M	S	S
CLO4	S	M	S	S	S

S- Strong; M-Medium; L-Low

IT FUNDAMENTALS FOR CYBER SECURITY AND CRYPTOGRAPHY 71Hrs

Syllabus

UNIT I (12 Hrs)

Introduction: Generations of Computer, Types of Computer - Functional units of a computer system- Input Devices -Output devices – Memory – Storage Devices. Number Systems: Decimal, Binary, Octal and Hexadecimal – Conversion –Computer Codes- Binary Addition, Subtraction- Complements.

UNIT II **(13 Hrs)**

Information security: History of IS-What is security -characteristic of IS-components of an Information system –Security System Development Life Cycle model. – Information Security for technical Administrators: server security- network security

UNIT III **(14Hrs)**

Introduction to Cyber Security: Importance and challenges in Cyber Security - Cyberspace - Cyber threats - Cyber warfare - CIA Triad - Cyber Terrorism - Cyber Security of Critical Infrastructure - Cyber security -Organizational Implications.

UNIT IV **(15 Hrs)**

Cryptography: Concepts and techniques-Plain text and cipher text- Encryption Principles-Cryptanalysis. Authentication methods-passwords-keys versus passwords-Attacking Systems via passwords-Password verification

UNIT V **(17 Hrs)**

Applications of cryptographic Hash Functions: Message authentication- Digital Signatures-Other Applications-Two simple Hash Functions-Cyber Security tools.

.

Text Books

S.No	Author	Title of the Book	Publishers	Year of Publication
1.	PKSinha &PritiSinha	Computer Fundamentals	8th Edition, BPB Publications	2004
2	Donaldson, S., Siegel, S., Williams, C.K., Aslam, A	"Enterprise Cyber security -How to Build a Successful Cyber defense Program against Advanced Threats	A Press, 1st edition	2015
3	Nina Godbole, Sumit Belapure	Cyber Security	Willey	2011
4	William Stallings	Cryptography and Network Security: Principles and Practices	PHI 7th Edition,	2020

Reference Books

S.No	Author	Title of the Book	Publishers	Year of Publication
1	Devan N. Shah	Information Security Principles and Practice	Wiley India	2009
2	George K.Kostopoulous	Cyber Space and Cyber Security	CRC Press	2013

Pedagogy

- Chalk and talk PPT, Discussion, Assignment, Demo, Quiz, Case study.

Course Designer

Dr.J.Maria Shyla

COURSE NUMBER	COURSE NAME	CATEGORY	L	T	P	CREDIT
CY22CP2	**Cyber Security tools Lab**	PRATICAL	-	-	75	3

Preamble

The course is designed to develop application using Cyber Security tools. It helps to apply the concepts of Cyber Security in different applications. The course also covers basic concepts of networks.

Course Learning Outcomes

On the Successful Completion of the course, students will be able to

CLO Number	CLO Statement	Knowledge Level
CLO1	Recall the concepts of network layers.	K1
CLO2	Develop programs with implementation of cyber security tools.	K2
CLO3	Construct programs	K3
CLO4	Implement the real-time applications by cyber security tools.	K4

Mapping with Programme Learning Outcomes

CLOs	PLO1	PLO2	PLO3	PLO4	PLO5
CLO1	S	S	M	S	M
CLO2	S	S	S	S	M
CLO3	S	S	M	S	S
CLO4	S	S	S	S	S

S- Strong; M-Medium; L-Low

Cyber Security tools Lab **75 Hrs**

Program List

- Set up Kali Linux in a virtual machine and set up a network Adapter.
- Scan the network for Kali Linux and Windows target machines in local network and virtual network.
- Identify the open ports using NMAP.
- Sniffing using Wireshark Tool.
- Use password guessing tools to guess a ZIP file password.

- Extract password hashes from Windows machines.
- Experiments on metasploit framework.
- Website Information Gathering techniques
- Prevention against cross site scripting attacks.
- Experiments on SQL injections.

Pedagogy

Demonstration of working environment/Tools/Software/Program

Course Designer

Dr.R.Divya

COURSE NUMBER	COURSE NAME	CATEGORY	L	T	P	CREDIT
CY22C04	COMPUTER NETWORKS	THEORY	58	2	-	3

Preamble

To provide security of the data over the network and to compare OSI and TCP/IP architectures

Course Learning Outcomes

On the successful completion of the course, students will be able to

CLO Number	CLO Statement	Knowledge Level
CLO1	Recall the concepts and terminologies of OSI model, network security and cryptography.	K1
CLO2	Understand the OSI and TCP/IP models.	K2
CLO3	Apply various cryptographic algorithms	K3
CLO4	Analyze how the protocols and services work.	K4

Mapping with Programme Learning Outcomes

CLOs	PLO1	PLO2	PLO3	PLO4	PLO5
CLO1	S	M	S	M	S
CLO2	S	S	S	M	S
CLO3	S	S	M	S	S
CLO4	S	S	M	M	S

S- Strong; M-Medium; L-Low

COMPUTER NETWORKS-CY22C04 58 Hrs

Syllabus

UNIT I 11 Hrs

Introduction: Network, Uses of Networks, Types of Networks**, Reference Models: TCP/IP Model, The OSI Model, Comparison of the OSI and TCP/IP reference model. Architecture of Internet.**

Physical Layer: Guided transmission media, Wireless transmission media, Switching

UNIT II 13 Hrs

Data Link Layer: Design issues, **Error Detection & Correction**, Elementary Data Link Layer Protocols, Sliding window protocols, Multiple Access Protocols, Data link layer switching. Network Layer: Network Layer Design issues, store and forward packet switching, connection less and connection-oriented networks-routing algorithms, IP addresses, IPv4 and IPv6 Protocol, ARP, RARP.

UNIT III **12 Hrs**

Transport Layer: connection establishment, Connection release, Error Control & Flow Control, Crash Recovery. **The Internet Transport Protocols: UDP, TCP.** Application Layer: providing services, Applications layer paradigms: Client server model, HTTP, E-mail, WWW, TELNET

.

UNIT IV **11 Hrs**

Network security- Examples of security violations - **Computer security concepts**-confidentiality-Integrity-Availability-Accountability, Challenges of computer security Hacking-Vulnerability-threats- attacks- **Active attacks and passive attacks-types**- Denial of service attacks-Model for network security.

UNIT V **11Hrs**

Cryptography-Introduction to cryptography – Terminologies- Conventional Encryption: Conventional encryption model - classical encryption techniques - substitution ciphers and transposition ciphers – **steganography - stream and block ciphers - Symmetric Key Ciphers**: Data Encryption Standard (DES), Advanced Encryption Standard (AES), Asymmetric key Ciphers-**Principles of public key crypto systems - RSA algorithm, Diffle-Hellman key exchange algorithm**- Hash Function: Secure Hash Algorithm (SHA-512).

Text Books

S.No.	Authors	Title	Publishers	Year Of Publication
1.	Andrew S. Tanenbaum, David J. Wetherall	Computer Networks	Prentice Hall Press.	2018
2	William Stallings	Network Security Essentials Applications and Standards	Pearson Education(3rd edition)	2017
3	Behrouz A. Ferouzan	Cryptography & Network Security	Tata Mc Graw Hill	2015

Reference Books

S.No.	Authors	Title	Publishers	Year Of Publication
1.	Atul Kahate	Cryptography and Network Security	McGraw Hill	2011
2.	C K Shyamala, N Harini, Dr T R Padmanabhan	Cryptography and Network Security	Wiley India	2010
3.	Kurose, Ross	Computer Networking: A top-down approach	Pearson Education, India,	2010

Pedagogy

- Chalk and talk PPT, Discussion, Assignment, Demo, Quiz, Case study.

Course Designer

Dr.R.Jeevitha

COURSE NUMBER	COURSE NAME	CATEGORY	L	T	P	CREDIT
CY22C05	DATA STRUCTURE AND ALGORITHM	THEORY	58	2	-	3

Preamble

To provide an overview of data structures and algorithm design methods for programming andproblem-solving process.

Course Learning Outcomes

On the successful completion of the course, students will be able to

CLO Number	CLO Statement	Knowledge Level
CLO1	Recall about the concepts of Arrays, Stack, Queue, Link List, Trees and Graph.	K1
CLO2	Understand sorting, searching and hashing algorithm	K2
CLO3	Apply the data structures to solve various computing algorithms and sorting algorithms.	K3
CLO4	Analyze lists, queues, stacks, trees and graph according to the needs of different applications	K4

Mapping with Programme Learning Outcomes

CLOs	PLO1	PLO2	PLO3	PLO4	PLO5
CLO1	S	M	M	S	S
CLO2	S	M	S	M	M
CLO3	M	M	S	M	S
CLO4	S	S	S	M	S

S- Strong; M-Medium; L-Low

DATA STRUCTURE AND ALGORITHM- CY22C05 58 Hrs

Syllabus

UNIT-I 12 Hrs

Introduction to Data Structure: Definition, Basic Terminology, Elementary Data Organization - Types of Data Structures- Linear & Non-Linear Data Structures-Data Structure Operations. Algorithm Specifications: Performance Analysis and Measurement (Time and space analysis). **Abstract Data Types- Advantages of ADT.** Array: Representation of arrays, Types of arrays, Applications of arrays, Sparse matrix and its representation**.**

UNIT-II 12 Hrs

Stacks and Queues: Stack-Stack Representation & Implementation-Stack Operations-**Applications of**

Stack. Queue-Queue Representation & Implementation-Queue Operations-**Types of Queues**.

UNIT-III **11 Hrs**

Linked List: Linked List as Data Structures- Representation of Linked List-Operations on Linked List-Stack as Linked List-Queue as Linked List-**Doubly Linked List-Circular List.**

UNIT-IV **13 Hrs**

Trees: Preliminaries-Binary Trees-**B-Trees**. Graph: Graph Terminologies-**Types of Graphs**-Graph Representation. **Hashing: Hash Functions.** Sorting: Bubble Sort-Selection Sort-QuickSort-Heap Sort-Merge Sort.

UNIT-V **10 Hrs**

Algorithm Design Techniques: Greedy Algorithms - Prim's Algorithm, Kruskal's Algorithm. **Divide and Conquer: Running Time of Divide and conquer algorithms.** Decrease and Conquer-Depth First Search and Breadth First Search. Backtracking Algorithms - n Queens Problem, **Branch and Bound – Traveling Salesman Problem.**

Text Books

S.No.	Authors	Title	Publishers	Year of Publication
1.	Rajesh K. Shukla	Data Structures using C & C++	Wiley India	2009
2.	Seymour Lipschutz, G A Vijayalakshmi Pai	Data Structures	Tata McGraw-Hill	2014

Reference Books

S.No.	Authors	Title	Publishers	Year of Publication
1.	Anany Levitin	Introduction to Design and Analysis of Algorithms	Pearson Education	2009
2.	Wisnu Anggoro	C++ Data Structures and Algorithms	Packt Publishing	2018
3.	YedidyahLangsam, Moshe J.Augentein, aron M.Tenenbaum	Data Structures using C & C++	PHI Learning, 2nd Edition	2009

Pedagogy

- Chalk & talk, PPT, Group Discussion, Assignment, Demo, Quiz, Role play.

Course Designer

Dr. R. Jeevitha

COURSE NUMBER	COURSE NAME	CATEGORY	L	T	P	CREDIT
CY22CP3	DBMS LAB	PRACTICAL	-	-	75	4

Preamble

The lab course provides a way to explore storing and accessing data in database through query languages and PL/SQL programming language. It enables to experience a NoSQL key/value store database MongoDB.

Course Learning Outcomes

On the successful completion of the course, students will be able to

CLO Number	CLO Statement	Knowledge Level
CLO1	Understand basic SQL query statements	K2
CLO2	Gain knowledge on primary and foreign key constraints	K2
CLO3	Apply functions and joins on data	K3
CLO4	Demonstrate PL/SQL programming on databases and differentiate Key/value store database from relational database	K4

Mapping with Programme Learning Outcomes

CLOs	PLO1	PLO2	PLO3	PLO4	PLO5
CLO1	M	M	S	S	M
CO2	S	M	S	S	M
CLO3	S	S	S	S	S
CLO4	S	S	S	S	S

S- Strong; M-Medium; L-Low.

DBMS LAB - CY22CP3 75 Hrs

Program List

- Different data types and operators.
- ER diagram with entities, attribute, keys and relations.
- Integrity constraints
- Built-in functions and views.
- Create, insert, update and alter table.
- Implement PL/SQL Block.
- Control Structures and Embedded SQL

- Splitting and joining the table
- PL/SQL Functions
- PL/SQL Procedure
- A case study and formulate the problem statement on a specify project.

Pedagogy

- Demonstration of working environment/Tools/Software/Program

Course Designers

Mrs. V. Deepa

COURSE NUMBER	COURSE NAME	CATEGORY	L	T	P	CREDIT
CY22SBCE	Coursera: DATA STRUCTURES LAB	Theory	45	-		3

Coursera – DATA STRUCTURES LAB

Course Contents **45 Hrs**

Cryptography: Keeping Information Secret (4 HRS)

Glad Libs: Stories from Templates (4 HRS)

Web Server Logs: From Logs to Visits (2 HRS)

Mini project Vigenere Cipher (3 HRS)

Strings (6 HRS)

Installing and Using Python (3 HRS)

Files and Lists (5 HRS)

Orientation; Writing a C++ Program (6 HRS)

Understanding the C++ Memory Model (4 HRS)

Developing C++ Classes (3 HRS)

C++ Software Solutions (5 HRS)

COURSE NUMBER	COURSE NAME	CATEGORY	L	T	P	CREDIT
CY22CO6	OPERATING SYSTEMS SECURITY	THEORY	58	2	-	3

Preamble

To provide a discussion of the fundamentals of operating system design and to relate these to contemporary design issues and to current directions in the development of operating systems Security.

Course Learning Outcomes

On the successful completion of the course, students will be able to

CLO Number	CLO Statement	Knowledge Level
CLO1	Recall about the basic concepts of operating system and its Security	K1
CLO2	Understand the operating systems objectives and functionality along with system programs and system calls.	K2
CLO3	Applying various concepts and algorithms for scheduling, partitioning, storagemanagement concepts and Security Concepts.	K3
CLO4	Analyze the operating system Storage, Deadlock, File System and Security	K4

Mapping with Programme Learning Outcomes

CLOs	PLO1	PLO2	PLO3	PLO4	PLO5
CLO1	S	M	S	M	S
CLO2	S	S	S	M	S
CLO3	S	S	M	S	S
CLO4	S	S	S	M	S

S- Strong; M-Medium; L-Low

OPERATING SYSTEM SECURITY – CY22CO6 58 Hrs

Syllabus

UNIT I 11hrs

Introduction and process concepts: Definition of OS - **Definition of process - Process States - Process State Transition -** Interrupt Processing - Interrupt classes- Semaphores - **Deadlock and Indefinite postponement**

UNIT II 11hrs

Storage management: Real storage: Real storage management strategies - **Contiguous Vs non-contiguous storage allocation - Single user contiguous storage allocation** - Fixed partition multiprogramming - Variable partition multiprogramming - -**Virtual storage: Virtual storage**

management strategies: Page replacement strategies - working sets - Demand paging-Page Size.

UNIT III 12 hrs

Processor management: Introduction - Job and processor scheduling: **Preemptive Vs Non-preemptive scheduling** – priorities - Deadline scheduling - **FIFO-RR** – Quantum Size - SJF-SRT-HRN - Distributed computing–Pipelining – Vector processing - Array Processing - Dataflow computers – Multiprocessing - **Fault Tolerance**

UNIT IV 12 hrs

Device and information management: Disk performance optimization: Operation of moving head disk storage - **Need for disk scheduling** – **FCFS - SSTF – SCAN** - RAM Disks - Optical Disks - **file and database systems: File system – functions – Organization** - **Access control by user Classes** Allocating and freeing space - file descriptor -Backup and Recovery.

UNIT V 12 hrs

Operating System Security: Introduction – Security Requirements – **Password Protection** – Auditing – Access Controls – Security Kernels – **Fault – Tolerant System** – Cryptography – Operating System -Penetration – Unix Operating System Security – **Worms and Viruses.**

Text Book

S.No.	Authors	Title	Publishers	Year Of Publication
1.	Deitel H.M	An Introduction to Operating System	Addison Wesley Publishing Company, Second edition	2005

Reference Books

S.No.	Authors	Title	Publishers	Year Of Publication
1.	Andrew S.Tanenbaum, Albert S.Woodhull,	Operating Systems-Design and Implementation	Pearson Education, 3rd Edition	2011
2.	Abraham Silberschatz, Peter Baer Galvin, Greg Gagne	Operating System Concepts	John Wiley & Sons,8th edition	2010
3.	Archer J Harries	Operating Systems	Tata McGraw Hill, First Edition	2008

Pedagogy

- Chalk and talk PPT, Discussion, Assignment, Demo, Quiz, Case study.

Course Designer

Dr. G.SANGEETHA

COURSE NUMBER	COURSE NAME	CATEGORY	L	T	P	CREDIT
CY22CO7	Vulnerability Assessment and Penetration Testing (VAPT)	THEORY	58	2	-	3

Preamble

To create an overview about the security assessment risks, vulnerability and Penetration Testing

Course Learning Outcomes

On the successful completion of the course, students will be able to

CLO Number	CLO Statement	Knowledge Level
CLO1	Recall the concepts of Networking Security, Vulnerability and Penetration testing .	K1
CLO2	Understand vulnerability and its implications	K2
CLO3	Applying the various techniques of Security, testing methods	K3
CLO4	Analyze the concept of Threats and Hacking methods	K4

Mapping with Programme Learning Outcomes

CLOs	PLO1	PLO2	PLO3	PLO4	PLO5
CLO1	S	S	M	M	S
CLO2	M	M	S	S	M
CLO3	S	S	S	M	S
CLO4	M	S	S	M	M

S- Strong; M-Medium; L-Low

Vulnerability Assessment and Penetration Testing-CY22C07 58 HRS

UNIT 1 **(12 Hrs)**

Vulnerability Management Governance- Security basics- Understanding the need for security assessments- Types of security tests- Security testing- Vulnerability assessment versus penetration testing- Security assessment- Security audit- Penetration testing standards- Penetration testing lifecycle- OWASP- Benefits of the framework-Setting up a Kali virtual machine - List of tools to be used during assessment.

UNIT II **(12 Hrs)**

Security Assessment Prerequisites-Gathering Requirements-Types of vulnerability assessment-Information Gathering-Passive information gathering-Active information gathering-Enumeration and Vulnerability Assessment-Enumerating Services-Using Nmap scripts-Gaining Network Access-Cracking passwords-Identifying hashes-Cracking Windows passwords-Password profiling-Password cracking with Hydra

UNIT III **(12 Hrs)**

Vulnerability Scoring-Requirements for vulnerability scoring-Vulnerability scoring using CVSS-Threat Modeling-**Threat modeling techniques**-Threat modeling tools-Patching and Security Hardening-Patch Enumeration-**Security hardening and secure configuration reviews**- Vulnerability Reporting and Metrics-**Type of reports-Reporting tools**

UNIT IV **(11 Hrs)**

Penetration Testing - **Using Kali Linux** - Using the Metasploit Framework - Finding Vulnerabilities - **Capturing Traffic** - Attacks: exploitation – **Password attacks**.

UNIT V **(11 Hrs)**

Client-side exploitation – **Social engineering** – Bypassing Antivirus Applications - **Web application Testing** – Wireless Attacks.

TEXT BOOKS

S.No.	Authors	Title	Publishers	Year of Publication
1	Sagar Rahalkar	NetworkVulnerability Assessment	Packt Publishing Ltd, 1 edition,	August 2018 (UNIT 1,2,3)
2	Georgia Weidman	"Penetration testing a Hands-on introduction to Hacking",	No starch press	2014(UNIT 4,5)

REFERENCE BOOK

S.No.	Authors	Title	Publishers	Year of Publication
1	Steve Manzuik, Ken Pfeil, Andrew Gold	Network Vulnerability Assessment from Vulnerability	Syngress Media,U.S,	November 2020

Pedagogy

Chalk and talk, PPT, Discussion, Assignment, Demo, Quiz, Case Study

Course Designer

Dr. R. Divya

COURSE NUMBER	COURSE NAME	CATEGORY	L	T	P	CREDIT
CY22CP4	VAPT Lab	PRACTICAL	-	-	75	3

Preamble

The subject is intended to provide the student with the in-depth knowledge of security and testing concepts

Course Learning Outcomes

On the successful completion of the course, students will be able to

CLO Number	CLO Statement	Knowledge Level
CLO1	Design the Fundamental concepts of Security methods	K1
CLO2	Understand by designing various types of network security techniques	K2
CLO3	Apply the networking concepts and Penetration testing methods	K3
CLO4	Implement and configure different types of vulnerability scanning methods	K4

Mapping with Programme Outcomes

CLOs	PLO1	PLO2	PLO3	PLO4	PLO5
CLO1	M	M	S	S	S
CLO2	M	M	S	S	S
CLO3	S	S	S	S	S
CLO4	S	S	S	S	S

S- Strong; M-Medium; L-Low

VAPT LAB -CY22CP4 75 HRS

- Network Discovery with Nmap
- Vulnerability Scanning with OpenVAS
- Packet Analysis with Wireshark
- OSINT and Target Profiling
- Exploitation Using Metasploit Framework
- Web Application Scanning with OWASP ZAP
- Wireless Network Security Assessment
- Social Engineering Awareness Exercise

- Threat Modeling and Risk Assessment
- Report Writing and Presentation

Pedagogy

Demonstration of working environment/Tools/Software/Program

Course Designer

Dr. R. Divya

Course Number	Course Name	Category	L	T	P	Credit
CY22A01	**Data Security**	Theory	58	2	-	3

Preamble

This course provides an overall understanding of the various security techniques and terminologies for data protection.

Course Learning Outcomes

On the successful completion of the course, students will be able to

CLO Number	CLO Statement	Knowledge Level
CLO1	Recall the concepts of data security, data privacy and IoT Security.	K1
CLO2	Understand the privacy terminologies and data privacy management	K2
CLO3	Apply the concepts of Data protection principles, Safeguards and Privacy Program Governance and Compliance and Legal Framework	K3
CLO4	Analyze the techniques of Data Security Threats, Mitigation and Cloud Security.	K4

Mapping with Programme Learning Outcomes

CLOs	PLO1	PLO2	PLO3	PLO4	PLO5
CLO1	S	M	S	S	S
CLO2	S	S	M	S	M
CLO3	S	S	S	M	M
CLO4	S	S	S	M	S

S- Strong; M-Medium; L-Low.

Syllabus

Unit 1 12 Hrs

Introduction to Privacy-Data Protection & Privacy Terminologies - **Data Protection Principles and Approaches to Privacy** - Code for protection of Personal Information - **Information Life Cycle** –Data Security Threats and Mitigation - **Data Storage Security Issues in Cloud Computing**

Unit 2 11 Hrs

Data protection principles and Safeguards-Data protection principles - **Subject access request Damage or distress** - Preventing direct marketing Automated decision taking - **Correcting inaccurate personal data** - Compensation, Exemptions & Complaints - **Big data - CCTV & Data sharing** - Online & apps Privacy by design - Guidance Note on Protecting the confidentiality of Personal Data Safeguarding-Personal Information - **Using Personal Information on Websites and with Other**

Internet related Technologies

Unit 3 11 Hrs

Data Privacy Management-Data Privacy Management controls & Plan - **Data Privacy Management Reference Model** - Data Protection in the context of Police and Criminal Justice - **Cross Border data transf**er - Do not Track Privacy Policy - Developing Privacy Management Tools -Information security practices for data privacy - **Developing a privacy management plan.**

Unit 4 12 Hrs

Privacy Program Governance and Compliance and Legal Framework-**Privacy Organization and Relationship (POR)** - Privacy Policy and Processes (PPP) -Regulatory Compliance Intelligence (RCI) - Privacy legislations - **applicability and interpretation** - Privacy Awareness and Training (PAT) – **Legal Framework for Data protection, Security and Privacy Norms**

Unit 5 12 Hrs

Privacy in cloud computing and IOT-**Privacy in Cloud** -Introduction to Privacy in cloud computing - **Cloud computing paradigm and privacy** - Challenges to privacy in cloud computing - Privacy in IoT - **IoT Governance**

Text Books

S.No.	Authors	Title	Publishers	Year of Publication
1	Thomas H. Lenhard	Data Security, Technical and Organizational Protection Measures against Data Loss and Computer Crime	Springer Wiesbaden	2019
2	Krishan Kumar Goyal , Amit Garg , Saurabh Singhal	Cyber Security and Data Privacy	PHI	2021
3	Dr.A.S Kalyana Kumar	Cloud Computing and Cyber Security: A Secure Crypto- Based Data Outsourcing and Sensitive Data Monitoring in Cloud Paperback	Adhayan book	March 2023

Reference book

S.No.	Authors	Title	Publishers	Year of Publication
1	Heather C. Hudak	Digital Data Security (Get Informed - Stay Informed) Hardcover – Import	Crabtree Forest	2019

Pedagogy

Demonstration of working environment/Tools/Software/Program

Course Designer

Mrs.V.Deepa

Course Number	Course Name	Category	L	T	P	Credit
CY22A02	**Cyber Law & E-Security**	Theory	58	2	-	3

Preamble

This course provides an overall understanding of the concepts of Cyber Law and Security techniques

Course Learning Outcomes

On the successful completion of the course, students will be able to

CLO Number	CLO Statement	Knowledge Level
CLO1	Recall the concepts of Security ,Cyber Space and Cyber Law	K1
CLO2	Understand the cyber law acts, cyber-crimes and e-security methods.	K2
CLO3	Apply the concepts of Cyber Threats, attacks and E- Commerce Security issues.	K3
CLO4	Analyze the techniques of Cyber Acts, Cyber Laws, and Security Problems.	K4

Mapping with Programme Learning Outcomes

CLOs	PLO1	PLO2	PLO3	PLO4	PLO5
CLO1	S	M	S	S	S
CLO2	S	S	M	S	M
CLO3	S	S	S	M	M
CLO4	S	S	S	M	S

S- Strong; M-Medium; L-Low.

Cyber Law & E-Security **58 Hrs**

Unit I 11 Hrs

Fundamentals of Cyber Law - Introduction on cyber space - Jurisprudence of Cyber Law - Scope of Cyber Law- **Introduction to Cyber Laws**—Meaning & scope of Cyber Laws, online contracts, **Requirements & legal aspects of e-contracts (offer and acceptance in e-form),** Cyber Laws & legal issues (cyber jurisprudence, & sovereignty, net neutrality, freedom of speech in cyber space, governance)

Unit II 11 Hrs

Cyber Laws (Information Technology Act, 2000) Part-I -**Digital Signature-definition, meaning, functions,**

procedure, E- Governance (Ss. 4 to 9), E- Records (Ss 11 to 16), Controller of Certifying Authority (powers, functions u/s 17 to 20), Digital Signature Certificates, License to issue Digital Signature Certificates, (suspension, revocation etc.--Ss.21 to 26), Duties of Certifying Authority (Ss.30 to 34), **Provisions relating to Digital Signature Certificates (Ss. 35 to 39)**, Duties of subscriber

Unit III **12 Hrs**

Introduction to Computer crimes- Computer Crimes- **Types of Computer crimes**, **Specific Threats**, Attacks on Computer Systems, Major types of Security Problems / Common threats, Computer Frauds and abuse techniques-**Characteristics and types of computer frauds**-Preventing Computer Frauds and Ethical Considerations--Protecting Information systems from potential threats- **E-Commerce security issues.**

Unit IV **12 Hrs**

Introduction to E-Commerce- Meaning and Definition of E-commerce, **Benefits of E-Commerce to Businesses**, Consumers and Society, **Limitations of E-Commerce, Drivers of E-Commerce**- Categories of e-Commerce- B2B, B2C, C2C, B2G and G2B- B2B applications, B2C applications and C2C applications.

Unit V **12 Hrs**

E-Security- Introduction to E-Security and Security Requirements-Types of Intruders, attacking methods, **Hackers and Crackers- Computer Viruses, Spam, Denial of services- Security Policy, Secure E-Transactions- Types of Information Systems Controls- General Controls** – Physical Controls, Access Controls, Biometric Controls, data Security Controls and Application Controls. Security Tools and Methods- Password, Authentication, Access Control, Encryption, Firewall, Antivirus Software, Digital Identity and digital Signature, Digital Signature Certificate- **Secure Socket Layer and Secure Electronic Transaction Protocols.**

Text Books

S.No.		Authors	Title	Publishers
1		D. P. Mittal	Law of Information Technology (Cyber Law	TAXMANN'S.
2		P.Joseph	E-commerce	PHI
3		V. Taneja , S.Parash**a**	E-Security	Alfa Publications

Reference Book

S.No.	Authors	Title	Publishers	Year of Publication
1	Yatindra Singh	Cyber Laws, Justice	Universal Law Publishing Co.	2018

Pedagogy

Demonstration of working environment/Tools/Software/Program

Course Designer

Dr. R. Jeevitha

COURSE NUMBER	COURSE NAME	CATEGORY	L	T	P	CREDIT
CY22SBP2	SBS:2 MOBILE APP DEVELOPMENT LAB	III	-	-	45	3

Preamble

This course is designed to equip with the knowledge and skills needed to create and deploy mobile apps for a variety of platforms, including iOS and Android.

Course Learning Outcomes

On the Successful Completion of the course, students will be able to

CLO Number	CLO Statement	Knowledge Level
CLO1	Understand basic concepts of Java	K2
CLO2	Demonstrate the Mobile app using Android	K2
CLO3	Apply the techniques to solve real-time problems	K3
CLO4	Analyze the tools and framework for development of mobile app	K4

Mapping with Programme Learning Outcomes

CLOs	PLO1	PLO2	PLO3	PLO4	PLO5
CLO1	M	M	S	S	M
CLO2	M	S	S	S	M
CLO3	S	S	S	S	S
CLO4	S	S	S	S	S

S- Strong; M-Medium; L-Low

List of Programs - 45 Hrs.

- Designing a Simple Toast application.
- Develop an application that uses GUI components, Font and Colours
- Develop an application that uses Layout Managers and event listeners
- Develop a simple calculator application.
- Develop a simple android application using the Image View and Spinner
- Exercises to send SMS and receive SMS
- Create an android application to connect to a website using web view
- Create an android application with progress circle

- Create an android application to demonstrate countdown timer
- Create an android application to find location using location-based services

Pedagogy

Demonstration of working environment/Tools/Software/Program

Course Designer

Dr.S. Nithya

JOB ORIENTED COURSE

Course Name: **Security**

+ Duration: 60 Hrs

Introduction – Explore Microsoft Entra Features – Self managed ADDS, Microsoft Entra ID, managed Microsoft Entra Domain Services – Investigate role in Microsoft Entra ID – Entra Build in roles – Deployment of Entra Domain Services – Create and manage Entra users – Managing Users with Entra groups – Configure Microsoft Entra Units – Implement Passwordless Authentication

Deployment of Microsoft Entra Connect – Exploring Authentication – Configuring PHS – Implementing PTA – Deploy Federation with Microsoft Entra ID – Authentication Decision Tree – Configure Password Writeback .

Microsoft Entra ID Protection – Configure Risk event Detections – Implementing user risk policy – Sign-in policy – Multifactor Authentication in Azure – Multifactor Authentication Settings – Explore Entra Conditional access – Configure Conditional Access Conditions

Configure Privileged Identity Management – Exploring Zero Trust model – Evolution of IM – Configure privilege management Scope – privileged management on boarding – Implementing privilege management Workflow

Design an enterprise governance Strategy – Analyse the shared responsibility model – Exploring cloud security advantages – Review Azure hierarchy of systems – Configuring Azure policies – Enabling RBAC – Compare RBAC with Azure policies – Configure build in roles – Azure Blueprints – Design an Subscription management plan.

COURSE NUMBER	COURSE NAME	CATEGORY	L	T	P	CREDIT
CY22C08	SOFTWARE ENGINEERING AND TESTING	THEORY	73	2	-	4

Preamble

The course is designed to impact the knowledge on building reliable software products. It also emphasizes various testing's undergone to enhance the quality of the software.

Course Learning Outcomes

On the successful completion of the course, students will be able to

CLO Number	CLO Statement	Knowledge Level
CLO1	Recall about the software evolution, software engineering practice, life cycle models and testing concepts.	K1
CLO2	Understand on Agile models, various Phases of software Project and its life cycle models.	K2
CLO3	Apply the various building models, software testing tactics and its Methodologies.	K3
CLO4	Analyze the System, Acceptance and Performance Testing's criteria and its best practice.	K4

Mapping with Programme Outcomes

CLOs	PLO1	PLO2	PLO3	PLO4	PLO5
CLO1	S	M	S	M	S
CLO2	S	M	S	M	M
CLO3	S	S	M	S	S
CLO4	S	S	M	M	S

S- Strong; M-Medium

SOFTWARE ENGINEERING AND TESTING- CY22C08 73Hrs

Syllabus

UNIT I (14 Hrs)

Introduction to Software Engineering: The Evolving role of Software - **Software - Changing nature of Software - Legacy Software** - Software myths. Software Engineering Practice: Software engineering practice - Communication practices - Planning practices - Modeling practices - Construction practice- Deployment.

UNIT II (15 Hrs)

Software Development Life Cycle models: **Phases of Software project-Quality, Quality Assurance, Quality control** - Testing, Verification and Validation - Process Model to represent Different Phases - Life Cycle models.

UNIT III (15 Hrs)

Agile Development: Agile Process –Agile Process Model-Building the Analysis Model: Requirement Analysis - **Data Modeling concepts - Object Oriented Analysis -Flow Oriented Modeling**-Design Engineering: Design **concepts.**

UNIT IV (14 Hrs)

Testing Tactics: Software Testing Fundamentals -Types of Testing: White Box Testing - Static Testing-Structural Testing-Black box Testing**-Integration Testing: Integration testing-Integration Testing as Type of Testing.**

UNIT V (15 Hrs)

System and Acceptance Testing: System Testing Overview-**Functional testing versus Non-functional Testing-Functional testing - Non-functional Testing** – Acceptance Testing and its criteria –Performance Testing: Factors governing Performance testing**.**

Text Books

S.No	Authors	Title	Publishers	Year and Edition
1.	Roger S. Pressman	Software Engineering: A Practitioner's Approach	McGraw-Hill Education	2014,8th Edition
2.	Srinivasan Desikan , Gopalaswamy Ramesh	Software Testing Principles and Practices	Pearson Education	2012,1st Edition

Reference Books

S.No	Authors	Title	Publishers	Year and Edition
1.	Rajib Mall	Fundamentals of Software Engineering	Prentice Hall of India Pvt Ltd	2010,3rd Edition
2.	Sandeep Desai, Abhishek Srivastava	Software Testing: A Practical Approach	PHI Learning Pvt. Ltd	2016,2nd Edition
3.	David Burns	Selenium 2 Testing Tools: Beginner's Guide	Tata MCGraw Hill Edition	2012,1st Edition

Pedagogy

- Chalk and Talk PPT, Discussion, Assignment, Demo, Quiz, Case study.

Course Designer

Mrs. M Selvanayaki

COURSE NUMBER	COURSE NAME	CATEGORY	L	T	P	CREDIT
CY22C09	Ethical Hacking	THEORY	73	2	-	5

PREAMBLE

The course is designed to introduce the fundamentals of ethical hacking. It provides the fundamental information associated in the art of attacking computer infrastructure for the purposes of testing, auditing, and pre-emptively securing these infrastructures

Course Learning Outcomes

CLO Number	CLO Statement	Knowledge Level
CLO1	Recall about the Ethical Hacking Concepts, Hacking Tools, OS Concepts, Networks Tools.	K1
CLO2	Understand Intrusion Detection, Social Engineering, Buffer Overflows and different types of Attacks and their protection mechanisms.	K2
CLO3	Apply the various tools to identifying the vulnerabilities.	K3
CLO4	Analyze the Intruders attacks on Networks, OS Vulnerabilities, Wireless Networks	K4

Mapping with Programme Outcomes

CLOs	PLO1	PLO2	PLO3	PLO4	PLO5
CLO1	S	M	S	M	S
CLO2	S	M	S	M	M
CLO3	S	S	M	S	S
CLO4	S	S	M	M	S

S- Strong; M-Medium

Ethical Hacking- CY22C09 73Hrs

Syllabus

Unit 1 (15 Hrs)

Introduction to Ethical Hacking-**TCP/IP Concepts-IP Addressing**-CIDR Notation-Planning IP Address assignments-IPv6 Addressing-**Network and Computer Attacks-Malicious Software-Protecting against Malware attacks**-Intruder attacks on Networks and Computers-Addressing Physical Security.

Unit II (14 Hrs)

Footprinting and Social Engineering-Web **Tools for Foot Printing**-Conducting Competitive Intelligence-Introduction to Social Engineering- **Art of Shoulder Surfing-Art of DumpsterDiving**-Art of piggybacking-Phishing.

Unit III (15 Hrs)

Port Scanning-**Port Scanning Tools**-Conducting Ping Sweeps- Understanding Scripting-Enumeration-Enumerating Windows Operating Systems-Programming for Security Professionals-**Desktop and Server OS Vulnerabilities-Windows OS Vulnerabilities**-Tools for Identifying Vulnerabilities—Practices for Hardening Windows Systems-**Linux OS vulnerabilities**.

Unit IV (14 Hrs)

Embedded Operating Systems: The Hidden Threat-Windows and other **Embedded Operating System-Vulnerabilities of Embedded Oss- Hacking Web Servers**-Understanding Web Applications-Understanding Web Application Vulnerabilities- Tools for Web attackers and Security.

Unit V (15 Hrs)

Hacking Wireless Networks-**Understanding wireless Technology-Understanding Wireless Network Standards-Understanding Authentication**-Understanding Warddriving-Understanding Wireless Hacking-Network Protection Systems-Protecting with Firewalls-Protecting with Intrusion Detection and Prevention Systems.

Text Book

S.No	Authors	Title of the Book	Publishers	Year and Edition
1.	Michael T.Simpson,Nocholas D.Anti,Robert S.Wilson	Hands –On Ethical Hacking and Network Defense	Cengage Learning	2023,4th edition

Reference Books

S.No	Authors	Title	Publishers	Year and Edition
1.	Steven DeFino, Barry Kaufman, Nick Valenteen	Official Certified Ethical Hacker Review Guide	Cengage Learning	2020,1st Edition
2	Patrick Engebretson	The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy”	Syngress Basics Series – Elsevier	2013,2nd Edition

Pedagogy

- Chalk and Talk, PPT, Discussion, Assignment, Demo, Quiz, Case study.

Course Designer

Dr.R.Divya

COURSE NUMBER	COURSE NAME	CATEGORY	L	T	P	CREDIT
AI22C10	Machine Learning	THEORY	73	2	-	4

Preamble

This course has been designed to introduce the concepts and techniques of machine learning. *It also emphasizes various* principles, algorithms, and applications of machine learning.

Course Learning Outcomes

CO Number	CLO Statement	Knowledge Level
CLO1	Recall the fundamentals of Machine Learning Concepts.	K1
CLO2	Understand the features of machine learning to apply on real world problems	K2
CLO3	Apply various algorithms of supervised and unsupervised learning	K3
CLO4	Analyze the concepts of linear and non-linear activation functions	K4

Mapping with Programme Outcomes

CLOs	PLO1	PLO2	PLO3	PLO4	PLO5
CLO1	S	M	S	M	S
CLO2	S	S	S	M	S
CLO3	S	S	M	S	S
CLO4	S	S	M	M	S

S- Strong; M-Medium

Machine Learning- AI22C10 73 Hrs

Unit I: (14 Hrs)

The Machine Learning Landscape: Introduction to Machine Learning - Why Use Machine Learning? - Examples of Applications - Types of Machine Learning systems – Main Challenges of Machine Learning – Testing and Validating - Classification and Prediction **- The Role of Python in Machine Learning - Anaconda in Python - Python Libraries.**

Unit 2 (15 Hrs)

Classification: MNIST - Training a Binary Classifier - Performance Measures: Measuring Accuracy Using Cross-Validation - Confusion Matrix - Precision and Recall - Precision/Recall Trade-off - The ROC Curve. Multiclass Classification - Multilabel Classification - Multi Output Classification – Classification Tree. **Advanced Machine Learning: Scikit-Learn Library for Machine Learning** - Cross-Validation. **Support Vector Machine: Linear SVM Classification – Nonlinear SVM Classification.**

Unit 3: (15 Hrs)

Linear Regression: Simple Linear Regression – Steps in Building a Regression Model – Building Simple Linear Regression Model – Multiple Linear Regression: Developing Multiple Linear

Regression Model Using Python – **Categorical Encoding Features - Splitting the Dataset into Train and Validation Sets - Building the Model on a Training Dataset** – Logistic Regression.

Unit 4: (14 Hrs)

Unsupervised Learning Techniques: Clustering – K-Means Clustering – Limits of K-Means – Clustering for Image Segmentation - Clustering for Preprocessing - Clustering for Semi-Supervised Learning – DBSCAN – **Other Clustering Algorithm. Creating Product Segments Using Clustering - Hierarchical Clustering.**

Unit 5: (15 Hrs)

Forecasting: Forecasting Overview - Components of Time-Series Data. Recommender Systems: Overview – Association Rules – Applying Association Rules. Text Analytics: Overview – Sentiment Classification - **Naïve-Bayes Model for Sentiment Classification. Introduction to Artificial Neural Networks with Keras: From Biological to Artificial Neurons**. Deep Computer Vision Using Convolutional Neural Networks: Convolutional Layers

Text Books

S.No	Author	Title of the Book	Publishers	Year and Edition
1	Tom M Mitchell	Machine Learning	Tata McGraw-Hill, New Delhi	2017,1st Edition
2	Anuradha Srinivasa Raghavan, Vincy Joseph	Machine Learning	Wiley India,	2019,1st Edition
3	Zsolt Nagy	Artificial Intelligence and Machine Learning Fundamentals	Packt publisher	2018,1st Edition
4	Dr. S Sridhar Dr. M Vijayalakshmi	Machine Learning	Oxford University Press	2021,1st Edition

Reference Books

S.No.	Authors	Title	Publishers	Year and Edition
1	Manaranjan Pradhan, U Dinesh Kumar	Machine Learning using Python	Wiley India	2019,1st Edition
2	Aurelien Geron	Hands-On Machine Learning with Scikit Learn, Keras and Tensorflow Concepts Tools and Techniques to Build Intelligent Systems	OReilly Media	2019,2nd Edition

Pedagogy

- Chalk and talk PPT, Discussion, Assignment, Demo, Quiz, Case study.

Course Designer

Dr.Sabitha Banu

COURSE NUMBER	COURSE NAME	CATEGORY	L	T	P	CREDIT
CY22E01	CLOUD SECURITY	THEORY	73	2	-	5

Preamble

This course provides a strong knowledge in cloud security and data storage concepts, a well covering of security design patterns, gives a well background view for security issues and management.

Course Learning Outcomes

On the successful completion of the course, students will be able to

CLO Number	CLO Statement	Knowledge Level
CLO1	Recall about the concepts of Cloud Computing	K1
CLO2	Understand the infrastructure security level of cloud computing	K2
CLO3	Apply the storage and security management	K3
CLO4	Analyze the security and privacy of cloud environment	K4

Mapping with Programme Outcomes

CLOs	PLO1	PLO2	PLO3	PLO4	PLO5
CLO1	S	M	S	M	S
CLO2	S	M	S	M	M
CLO3	S	S	M	S	S
CLO4	S	S	M	M	S

S- Strong; M-Medium

CLOUD SECURITY- CY22EO1 73 Hrs

Unit-I (14 hrs)

Cloud Computing -Introduction -Cloud Computing Defined-**Evolution of Cloud Computing - The SPI Framework for Cloud Computing-The Traditional Software Model**-The Cloud Services Delivery Model-Cloud Deployment Models- Key Drivers to Adopting the Cloud-The Impact of Cloud Computing on Users-**Governance in the Cloud**-Barriers to Cloud Computing Adoption in the Enterprise

Unit-II (15 hrs)

INFRASTRUCTURE SECURITY: The Network Level: Ensuring Data Confidentiality and Integrity-**Ensuring Proper Access Control-Ensuring the Availability of Internet-Facing Resources Network**-Level Mitigation.**The Host Level :** SaaS and PaaS Host Security-IaaS Host Security-Virtualization Software Security-Virtual Server Security.**The Application Level:**Application-Level Security Threats-DoS and EDoS-End User Security-SaaS Application Security-PaaS Application Security-IaaS Application Security.

Unit-III (15 hrs)

DATA SECURITY AND STORAGE: Aspects of Data Security-Data Security Mitigation-**Provider Data and Its Security:** Storage- Confidentiality -Integrity- Availability-Security in Cloud Computing **IDENTITY AND ACCESS MANAGEMENT:** Trust Boundaries and IAM- Why IAM?- IAM Challenges-IAM Definitions- IAM Architecture and Practice-Getting ready for the cloud-IAM standards and protocols for cloud services.

Unit-IV (15 hrs)

SECURITY MANAGEMENT IN THE CLOUD: Security Management Standards- Security Management in the Cloud-Availability Management-SaaS Availability Management- PaaS Availability Management-IaaS Availability Management-Access Control-Security Vulnerability, Patch, and Configuration Management.**EXAMPLES OF CLOUD SERVICE PROVIDERS-**Amazon Web Services (IaaS)-Google (SaaS, PaaS)-Microsoft Azure Services Platform (PaaS).

Unit- V (14 hrs)

PRIVACY: What Is Privacy-What Is the Data Life Cycle-What Are the Key Privacy Concerns in the Cloud-**Who Is Responsible for Protecting Privacy-Changes to Privacy Risk Management and Compliance in Relation to Cloud Computing**.

Text Books

S.No.	Authors	Title of the Book	Publishers	Year and Edition
1	Tim Mather,Subra Kumaraswamy,Shahed Latif	Cloud Security and Privacy:An Enterprise Perspective on Risks and Compliance	O'Reilly Media, Inc.	2009,1st Edition

Reference Books

S.No.	Authors	Title	Publishers	Year and Edition
1.	Raghu Yeluri and Enrique Castro Leon	Building the Infrastructure for Cloud Security- A Solution View	Apress open	2014, 1st Edition
2	Barrie Sosinsky	Cloud Computing Bible	Wiley-India	2010, 1st Edition

Pedagogy

Chalk & talk PPT, Group Discussion, Assignment, Demo, Quiz, Role play

Course Designer

Dr. Sabitha Banu

COURSE NUMBER	COURSE NAME	CATEGORY	L	T	P	CREDIT
CY22E02	Web Application and Security	THEORY	73	2	-	5

PREAMBLE

This course covers the various techniques for securing ASP.NET Web API, including basic authentication using authentication filters, forms, Windows Authentication, external authentication services, and integrating ASP.NET's Identity system.

Course Learning Outcomes

On the successful completion of the course, students will be able to

CLO Number	CLO Statement	Knowledge Level
CLO1	Recall about the concepts of Cloud Computing	K1
CLO2	Understand the infrastructure security level of cloud computing	K2
CLO3	Apply the storage and security management	K3
CLO4	Analyze the security and privacy of cloud environment	K4

Mapping with Programme Outcomes

CLOs	PLO1	PLO2	PLO3	PLO4	PLO5
CLO1	S	M	S	M	S
CLO2	S	M	S	M	M
CLO3	S	S	M	S	S
CLO4	S	S	M	M	S

S- Strong; M-Medium

WEB APPLICATION AND SECURITY- CY22EO2 73 Hrs

UNIT I (14Hrs)

Setting up a browser client: ASP.NET Web API security architecture **– Setting up your browser client** – Consuming the Web API using JavaScript and jQuery – Authentication and authorization – **Implementing authentication in HTTP message handlers** – Setting the principal – using the [Authorize] attribute – Custom authorization filters

UNIT II (15Hrs)

Enabling SSL for ASP.NET Web API: Enforcing SSL in a Web API controller – Using client certificates in Web API – **Integrating ASP.NET Identity system with Web API** – Creating an empty Web API Application – **Installing the ASP.NET Identity NuGet packages** – Setting up ASP.NET Identity 2.1 – Defining Web API Controllers and methods.

UNIT III (14Hrs)

Securing Web API using OAuth2: Hosting OWIN in IIS and adding Web API to the OWIN pipeline – **Individual user account authentication flow – sending an unauthorized request** – Get an access token – Send an authenticated request. Enabling Basic Authentication using Authentication Filter in

Web API: Basic authentication with IIS – Basic authentication with custom membership - Basic authentication using an authentication filter.

UNIT IV (15Hrs)

Setting an authentication filter – Implementing a Web API authentication filter – Setting an error result – **Combining authentication filters with host-level authentication. Securing a Web API using Forms and Windows Authentication:** Working of forms authentication – Implementing forms authentication in Web API.

UNIT V (15Hrs)

What is integrated windows authentication? - **Advantages and disadvantages of using the integrated windows authentication mechanism - Configuring windows authentication** – Difference between basic authentication and windows authentication. Avoiding Cross-Site Request Forgery Attacks in Web API: - What is CSRF attack? – Anti-forgery tokens using HTML form or Razor View – **Anti-forgery tokens using AJAX**.

Text Book

S.No	Authors	Title of the Book	Publishers	Year and Publication
1.	Rajesh Gunasundaram	ASP.NET Web API Security Essentials	Packt Publications	2019,1st Edition

Reference Books

S.No	Authors	Title of the Book	Publishers	Year and Publication
1.	Jamie Kurtz, Brain Wortman	ASP.NET Web API 2: Building a REST Service from Start to Finish"	Apress Publications	2015,2nd Edition
2.	Neil Madden	API Security in Action	Managing Publications	2020,1st Edition

Peadogogy

- Chalk and Talk PPT, Discussion, Assignment, Demo, Quiz, Case study.

Course Designer

Mrs P.Yashodha

COURSE NUMBER	COURSE NAME	CATEGORY	L	T	P	CREDIT
CY22CP5	Ethical Hacking Lab	PRACTICAL		-	75	3

PREAMBLE

The course is intended to provide the student with the in-depth knowledge of security, importance of data gathering, foot printing and system hacking

Course Learning Outcomes

On the successful completion of the course, students will be able to

CLO Number	CLO Statement	Knowledge Level
CLO1	Design the Fundamental concepts of Security methods	K1
CLO2	Understand by designing various types of network security techniques	K2
CLO3	Apply the networking concepts and Penetration testing methods	K3
CLO4	Implement and configure different types of vulnerability scanning methods	K4

Mapping with Programme Outcomes

CLOs	PLO1	PLO2	PLO3	PLO4	PLO5
CLO1	S	S	M	S	M
CLO2	S	S	S	S	S
CLO3	S	S	M	M	M
CLO4	S	S	S	S	S

S- Strong; M-Medium

Ethical Hacking Lab –CY22CP5 75 Hrs

List of Programs

1. Configure IP addressing using CIDR notation and implement firewall rules using open-source tools on Linux.
2. Utilize open-source footprinting and email spoofing tools to gather information and simulate a social engineering attack.
3. Perform port scanning and enumeration using Nmap and Enum4linux on target systems.
4. Identify and exploit web server vulnerabilities using Nikto and Metasploit.
5. Conduct wireless network penetration tests and set up intrusion detection systems using Aircrack-ng and Snort.
6. Configure IPv6 addressing and conduct malware analysis using OSSEC and Cuckoo Sandbox.
7. Use OSINT tools for competitive intelligence and simulate dumpster diving with Maltego.

8. Write Python scripts for network reconnaissance and exploit Windows desktop vulnerabilities with Exploit-DB.
9. Analyze vulnerabilities in embedded operating systems with Binwalk and conduct web server penetration tests using OWASP ZAP.
10. Analyze wireless network traffic with tcpdump and configure firewall rules with pfSense for wireless network protection.
11. Simulate intruder attacks with Kali Linux and perform physical security assessments with OpenFAIR.
12. Test physical security with piggybacking techniques and execute phishing campaigns using Gophish for employee awareness.

Pedagogy

System, White board, Demonstration through PPT

Course Designer

Dr.R.Divya

COURSE NUMBER	COURSE NAME	CATEGORY	L	T	P	CREDIT
CY22SBP3	Cyber Security Tools Lab-II	PRACTICAL	-	4	41	3

Preamble

This course is designed to equip with the knowledge of Cyber Security Tools to find out the threats and attacks.

Course Learning Outcomes

On the Successful Completion of the course, students will be able to

CLO Number	CLO Statement	Knowledge Level
CLO1	Define the Fundamental concepts of Cyber Security tools.	K1
CLO2	Discuss the various tools to identify the threats.	K2
CLO3	Apply the tools to identify the vulnerabilities and attacks.	K3
CLO4	Analyze different types of scanning methods.	K4

Mapping with Programme Outcomes

CLOs	PLO1	PLO2	PLO3	PLO4	PLO5
CLO1	S	S	M	S	M
CLO2	S	S	S	S	S
CLO3	S	S	M	M	M
CLO4	S	S	S	S	S

S- Strong; M-Medium

Cyber Security tools Lab-II **45Hrs**

- Packet Sniffing with Tcpdump
- Network Intrusion Detection with Snort
- Firewall Configuration with iptables
- Web Application Security Testing with OWASP ZAP
- SSH Hardening with Fail2ban
- VPN Setup with OpenVPN
- Network Traffic Analysis with Bro IDS
- Wireless Security Assessment with Aircrack-ng
- Port Scanning with Masscan
- SSL/TLS Analysis with SSLyze

Pedagogy

System, White board, Demonstration through PPT

Course Designer

Dr.R.Divya

COURSE NUMBER	COURSE NAME	CATEGORY	L	T	P	CREDIT
NM21CS1	CYBER SECURITY 1	Theory	30	-	-	Grade

Preamble

This course introduces fundamental concepts of Cyber Security in the digital era. It provides the knowledge of cybercrimes, cyber laws and also the security of digital devices. It helps to do secure digtal transactions and safe usage of social media.

CYBER SECURITY I 30 Hrs

Syllabus

Unit I (6 Hrs)

Principles of Cyber security: Introduction to Cyber security - Defining cyberspace - Architecture of cyberspace - Communication and web technology - Internet infrastructure for data transfer and governance - Regulation of cyber space - Concept of Cyber security - Issue andchallenges of cyber security.

Unit II (6 Hrs)

Cyber Crime: Introduction to Cyber crime - Classification of Cyber-crimes – Cyber-crime against women and children – Financial frauds - Social engineering attacks – Malware - Zero day and zero click attacks.

Unit III (6 Hrs)

Cyber Law: Cyber Criminals modus-operandi – Reporting of cybercrimes – remedial and mitigation measures – Legal perspective of cybercrime– IT Act 2000 and its amendments – Organization dealing with cyber crimes and cyber security in India.

Unit IV (6 Hrs)

Social Media Security: Introduction to social network – Types of social media – Social media platform – Hashtag – Viral content – Security issues related to social media. – **Cyber Security tools:** N map – Introduction to Nmap – Nmap scan types- Nmap command list.

Digital Transaction: Introduction to digital payments – Components of digital payments – Modes of digital payments – Banking cards – UPI (Unified Payment Interface) – e-Wallets. (Aligned 90% with UGC)

Unit V (6 Hrs)

Digital Devices Security: End point device and Mobile phone security – Password policy – Security patch management – Data backup – Device security policy – Cyber security best practices. Installation and configurtion of Computer Anti-Virus.

Case studies: Illustrations of Financial frauds – Digital Signature. Prepare a checklist for secure net banking

Reference books:

1. Raef Meeuwisse , Cybersecurity For Beginners, Lulu Publishing Services,2nd Edition,2017
2. Scott Augenbaum, The Secret to Cybersecurity-A Simple Plan to Protect Your Family and Business from Cybercrime , Forefront Books Publisher,2019
3. Sumit Belapure and Nina GodBole, Cyber security understanding cyber crimes computer forensics and Legal perspectives, Wiley India Pvt Ltd, 2011
4. Christopher Hadnagy, Social Engineering: The Science of Human Hacking,Wiley Publisher, 2nd Edition,2018
5. Pavan Duggal, Artificial Intelligence, Cybercrimes & Cyberlaw,2018
6. Joe Gray, Practical Social Engineering: A Primer for the Ethical Hacker, 2022 Security in the digital age: social media security threads and vulgarabilities by Henry A. Oliver, Create Space Independence publishing platform.

.

COURSE NUMBER	COURSE NAME	CATEGORY	L	T	P	CREDIT
CY22AC1	Cyber Threats and Modeling	Theory	-	-	-	5

PREAMBLE

The learner understands the basic concepts of cyber security threats and modeling and also can learn about email threats, web threats and cyber threat management.

Course Learning Outcomes

On the Successful Completion of the course, students will be able to

CLO Number	CLO Statement	Knowledge Level
CLO1	Recall about the Ethical Hacking Concepts, Hacking Tools, OS Concepts, Networks Tools.	K1
CLO2	Understand Intrusion Detection, Social Engineering, Buffer Overflows and different types of Attacks and their protection mechanisms.	K2
CLO3	Apply the various tools to identifying the vulnerabilities.	K3
CLO4	Analyze the Intruders attacks on Networks, OS Vulnerabilities, Wireless Networks	K4

UNIT I

Getting started : Dive In and Threat Model-Learning to Threat Model – Checklists for Diving In and Threat Modeling.Strategies for Threat Modeling:Structured Approaches to Threat Modeling-Models of Software.

UNIT II

Finding Threats: STRIDE: Understanding STRIDE-Spoofing Threats-Pampering Threats-Repudiation Threats-Information Disclosure Threats-denial-of-Service Threats- Elevation of Privilege Threats-STRIDE Variants

.

UNIT III

Attack Trees: Working with Attack trees-Representing a Tree-Real Attack Trees- Perspective on Attack Trees-Attack Libraries: Properties of Attack Libraries CAPEC-OWASP Top Ten.

UNIT IV

Privacy Tools: Solove's Taxonomy of Privacy-Privacy Considerations for Internet Protocols-Privacy Impact Assessments. Processing and Modeling Threats: Starting the Threat Modeling Project-Tracking with Tables and Lists-Scenario-Specific Elements of Threats Modeling.

UNIT V

Threat Modeling Tools: Open Source Tools-Commercial Tools. Web and Cloud Threats: Web threats-Cloud Tenent Threats-Cloud Provider Threats-Mobile Threats. Human Factors and Usability_ Models of Software Scenarios-Tools and Techniques for Addressing Human Factors- User Interface Tools and Techniques.

Text Books

S.NO	Author	Title Of Book	Publisher	Year And Edition
1	Swiderski, Frank and Syndex	Threat Modeling	Microsoft Press,	2016,1st Edition
2.	Jocelyn O. Padallan	Cyber Security	Arcler Press Publisher	2019,2nd Edition

Reference Book

S.No	Authors	Title	Publishers	Year And Edition
1.	Adam shostack	Threat Modeling – Designing for Security	Wiley	2014

COURSE NUMBER	COURSE NAME	CATEGORY	L	T	P	CREDIT
CY22AC2	ARTIFICIAL INTELLIGENCE	THEORY	-	-	-	5

Preamble

*To provide an overview of Artificial Intelligence, Machine learning algorithm and techniques for decision process***.**

Course Learning Outcomes

On the successful completion of the course, students will be able to

CLO Number	CLO Statement	Knowledge Level
CLO1	Recall about the concepts of AI, Fuzzy logic and Knowledge representation, decision process & learning.	K1
CLO2	Understand the applications of AI and Expert Systems, decision process & reinforcement learning.	K2
CLO3	Apply the knowledge representation, fuzzy logic, decision process and machine learning algorithms.	K3
CLO4	Analyze the artificial intelligence search algorithms, logic in Artificial Intelligence.	K4

Unit-I

Foundations of Artificial Intelligence :Artificial Intelligence - Definition of Artificial Intelligence - Through Problems - History of Artificial Intelligence - Artificial Intelligence - Problems and Techniques - Shift in Focus of AI Towards Providing Smarter Solutions - Knowledge Representation: Introduction – Ontologies – Objects - and Events Representations and Mappings -

Unit-II

Basics of Machine Learning: Neural Networks and Applications - Introduction-Learning in Neural Networks - Choosing Cost Function - Types of Learning - Recurrent Neural Network – Back-propagation - Convolutional Neural Networks and Deep Neural Networks -. Applications of Neural Networks

Unit-III

Statistical Machine Learning: Introduction - Probability Axioms - Bayes' Rule - Bayesian Network - Decision Processes and Reinforcement Learning: Learning - Forms of Learning - LearningDecision Trees - Learning by Examples - Explanation - Based Learning - Regression and Classification with Linear Models - Artificial Neural Networks .

Unit-IV

Applications of Artificial Intelligence-Game Playing: Minimax Search Procedure -Imperfect Real-Time Decisions - Text Analysis and Mining: Language Models - Text Classification - Information Retrieval - Information Extraction - Syntactic Processing - Speech Recognition .

Unit- V

Logic in Artificial Intelligence: First Order Logic: First Order Logic – Prolog: Logic Programming: Symbolic Logic, Clausal Form - Converting English to Prolog Facts and Rules - Prolog Terminology - Variables and Arithmetic Operators - Inference Process of Prolog - Trends In Machine Learning : Artificial Intelligence versus Machine Learning-Artificial Immune System.

Text Book

S.No.	Authors	Title	Publishers	Year and Edition
1.	Lavika Goel	Artificial Intelligence Concepts and applications	Wiley India	2021,1st Edition

Reference Books

S.No.	Authors	Title	Publishers	Year and Edition
1.	Lyla B. Das Sudhish N. George Anup Aprem	Artificial Intelligence And Machine Learning Theory and Practice	IK International Pvt. Ltd	2023, 1st Edition
2.	Mariusz Flasinski	Introduction to Artificial Intelligence	Springer International	2018, 2ndEdition
3.	Stuart J. Russell Peter Norvig	Artificial Intelligence A Modern Approach	Pearson	2015,3rd Edition

COURSE CODE	COURSE NAME	CATEGORY	L	T	P	CREDIT
CY22C11	IoT and Security	THEORY	73	2	-	4

Preamble

This course has been designed to introduce the concepts and techniques of IOT and Security. *It also emphasizes various* principles, algorithms, and applications of IOT and its Security.

Course Learning Outcomes

On the successful completion of the course, students will be able to

CLO Number	CLO Statement	Knowledge Level
CLO1	Recall the fundamentals of IoT Concepts.	K1
CLO2	Understand the features of IoT to apply on real world problems	K2
CLO3	Apply various Protocols on application of IoT	K3
CLO4	Analyze the concepts of security functions	K4

Mapping with Programme Learning Outcomes

CLOs	PLO1	PLO2	PLO3	PLO4	PLO5
CLO1	S	M	S	M	S
CLO2	S	S	S	M	S
CLO3	S	S	M	S	S
CLO4	S	S	M	M	S

S- Strong; M-Medium

IoT and SECURITY- CY22C11 73 Hours

UNIT 1 : 15 Hrs

Preliminaries,Motivation,and Related Work: What is the Internet of Things -Wireless Ad-hoc and Sensor Networks- **IoT Enabled Applications -Home and building automation-Smart cities -Smart Grids-Industrial IoT -Smart Farming**.

Standards: Physical/ Link Layer:IEEE 802.3 (Ethernet)- IEEE 802.11.Network Layer: IP*v*6 and IPv4 - Transport Layer:TCP and UDP .Application Layer : HTTP – AMQP -SIP .The Internet of Things: Desigining the Architecture of an IP-based Internet of Things – Physical/Link Layer – IEEE 802.15.4 and ZigBee- Low-Power Wi-fi – Bluetooth and BLE -Powerline Communications -Network Layer – The 6LoWPAN Adaptation Layer -Transport Layer -Application Layer -CoAP -CoSIP Protocol Specification - The Industrial IoT.

UNIT II : 15 Hrs

Applications in the IoT-The Verticals :Cloud Based Solutions- REST Architectures :The Web of Things- Richardson Maturity Model – Level 0 : the Swamp of POX – Level 1: Resources - Level 2 : HTTP Verbs -Level 3 : Hypermedia **– The Meaning of Levels .The Web of Things - Messaging Queues and Publish /Subscribe Communications: - session Initiation for the IoT-Performance Evaluation** – Optimized Communications :the Dual Network Management Protocol -DNMP Motivations – The DNMP Protocol – Implementation with IEEE802.15.4- and IEEE 802.11s- Performance Evaluation .

UNIT III: 15 Hrs

Discoverability: Service and Resource Discovery- Local and Large – scale Service Discovery - Scalable and Self- **Configuring Architecture for Service Discovery in IoT- Lightweight Service Discovery in Low**-Power IoT Networks

UNIT IV 15 Hrs

Security and Privacy in IoT : Security Issues in IoT -Security Mechanisms Overview – **Privacy Issues in IoT.**

Unit V : 13 Hrs

Cloud and Fog Computing for the IoT :Cloud Computing – Big data Processing Pattern - Big Stream -Big Stream Oriented Architecture – Implementation – Performance Evaluation -Big Stream and Security - Graph Based Cloud Security .The IoT in Practice : Hardware for the IoT – Hardware Platforms:Ardunio- Rasberry Pi.Software for the IoT- **OpenWSN- FreeRTOS-TI-RTOS**

Text Book .

S.No.	Authors	Title	Publishers	Year of Publication & Edition
1	Simone Cirani, Gianluigi Ferrari , Marco Picone ,Luca Veltri	Internet of Things Architectures ,Protocols and Standards	Wiley	2019 ,1st Edition

Reference Books

S.No.	Author	Title of the Book	Publishers \Edition	Year of Publication & Edition
1.	Raj Kamal	Internet Of Things :Architecture and Design Principles	Tata McGraw-Hill, New Delhi	2022,1st Edition
2.	Arsheep Bahga , Vijay Madisetti	Internet of Things – A hands on Approach	Orient Blackswan Private Limited , New Delhi	2015,1st Edition

Pedagogy

Chalk and Talk PPT, Discussion, Assignment, Demo, Quiz, Case study

Course Designer

Dr.S.Angel

COURSE CODE	COURSE NAME	CATEGORY	L	T	P	CREDIT
CY22C12	Malware Analysis	THEORY	73	2	-	4

Preamble

The course is designed to provide a foundational understanding of how malware operates, the threats it poses, and the methodologies used to analyse and mitigate its impact in a real-world cyber security context.

Course Learning Outcomes

On the successful completion of the course, students will be able to

CLO Number	CLO Statement	Knowledge Level
CLO1	Recall about the process of malware analysis, including both static and dynamic techniques.	K1
CLO2	Understand the fundamental concepts of malware and its various types.	K2
CLO3	Apply the various tools for malware prevention, detection, and mitigation.	K3
CLO4	Analyze the functions of malicious windows programs, Malware Behavior and Malware Focused Network Signatures	K4

\

Mapping with Programme Learning Outcomes

CLOs	PLO1	PLO2	PLO3	PLO4	PLO5
CLO1	S	M	S	S	S
CLO2	S	S	M	S	M
CLO3	S	S	S	M	M
CLO4	S	S	S	M	S

S- Strong; M-Medium

Malware Analysis-CY22C12 73 Hrs

Syllabus

UNIT 1 15 Hrs

Basic Static Techniques- Antivirus Scanning- **Hashing: A Fingerprint for Malware- Finding Strings- Packed and Obfuscated Malware-** Portable Executable File Format- Static Analysis in Practice- The PE File Headers and Sections- Malware Analysis In Virtual Machines- Basic Dynamic Analysis.

UNIT-II 14 Hrs

Advanced Static Analysis- X86 Disassembly- **Levels of Abstraction- Reverse Engineering- The x86 Architecture- IDA PRO- Loading an Executable**- The IDA Pro Interface- Using Cross-References - Analyzing Functions- Enhancing Disassembly- Extending IDA with Plug-ins

Unit III **15 Hrs**

Recognizing C Code Constructs In Assembly- Analyzing Malicious Windows Programs- The Windows API - **The Windows Registry- Networking APIs- g Running Malware** - The Native API.

Unit IV **14 Hrs**

Advanced Dynamic Analysis- Debugging- Ollydbg- **Malware Functionality- Malware Behavior**- Covert Malware Launching

UNIT V **15 Hrs**

Malware Focused Network **Signatures- Anti Reverse Engineering: Anti-Disassembly**- Anti Debugging- Anti Virtual Machine Techniques

Text Book

S.No	Authors	Title	Publishers	Year and Edition
1.	Michael Sikorski, Andrew Honig	Practical Malware Analysis-The Hands on Guide to Dissecting Malicious Software	William Pollock No Starch Press	2012,2nd Edition

Reference Books

S.No	Authors	Title	Publishers	Year and Edition
1.	Michael Hale Ligh, Steven Adair, Blake Hartstein, Matthew Richard	Malware Analyst's Cookbook Tools and Techniques for fighting malicious code	Wiley Publishing Inc,	2011,1st Edition
2.	Victor Marak	Windows Malware Analysis Essentials	Packt Publishing	2015,1st Edition

Pedagogy

Chalk and Talk PPT, Discussion, Assignment, Demo, Quiz, Case study

Course Designer

Dr.R.Divya

COURSE CODE	COURSE NAME	CATEGORY	L	T	P	CREDIT
CY22C13	DIGITAL FORENSICS	Theory	73	2	-	3

Preamble

The course covers clear understanding of how digital evidence complements traditional scientific evidence and how it can be used more effectively in a range of criminal investigations.

Course Learning Outcomes

On the successful completion of the course, students will be able to

CLO Number	CLO Statement	Knowledge Level
CLO1	Recall the digital devices and their evaluation, technology	K1
CLO2	Understand the handling of devices	K2
CLO3	Apply the principles for evidence creation and interpretation	K3
CLO4	Analyze the mobile devices, online crime and a case study	K4

Mapping with Programme Learning Outcomes

CLOs	PLO1	PLO2	PLO3	PLO4	PLO5
CLO1	S	S	S	M	S
CLO2	S	S	M	S	M
CLO3	M	S	S	S	S
CLO4	S	M	S	S	S

S- Strong; M-Medium; L-Low

DIGITAL FORENSICS- 73 Hrs

Syllabus

UNIT –I 15 Hrs

Introduction-Key developments-Digital devices in society-Technology and culture-**Evidential Potential of Digital Devices- Closed vs. open systems-Evaluating digital evidence potential.**

UNIT –II 14 Hrs

Device Handling-Seizure issues-Device identification-**Networked devices-Contamination**.

UNIT –III 15 Hrs

Examination Principles-Previewing-Imaging-Continuity and hashing-Evidence locations. **Evidence Creation**-A seven-element security model-A developmental model of digital systems-Knowing-Unknowing-Audit and logs. **Evidence Interpretation**-Data content- Data context.

UNIT-IV **14 Hrs**

Mobile Devices-**Mobile phones and PDAs**-GPS-Other personal technology.

UNIT –V **15 Hrs**

Intelligence-Device usage-**Profiling and cyber profiling-Evaluating online crime: automating the model**-Application of the formula to case studies-From success estimates to profiling-**Case Studies and Examples**-Introduction-Copyright violation-Missing person and murder-The view of a defence witness.

Text Book

S. No	Author	Title of the Book	Publisher	Year of Publication and Edition
1	Angus M. Marshall	**Digital Forensics**-Digital Evidence in Criminal Investigation	Wiley	2008,1st Edition

Reference Books

S. No	Author	Title of the Book	Publisher	Year of Publication and Edition
1	Eamon P. Doherty	Digital Forensics for Handheld Devices	CRC Press Taylor & Francis	2021,1st Edition
2	Nilakshi Jain, Dhananjay R. Kalbande	Digital Forensic: The Fascinating World of Digital Evidences	Wiley	2016,1st Edition

Pedagogy

Chalk and Talk, PPT, Discussion, Assignment, Demo, Quiz, Case study

Course Designer

Dr Sabitha Banu A

COURSE CODE	COURSE NAME	CATEGORY	L	T	P	CREDIT
CY22CP6	**Malware Analysis Lab**	Practical	-	-	75	3

Preamble

The course is designed to provide a foundational understanding of the techniques, tools, and methodologies used to analyze malware samples**.**

Course Learning Outcomes

On the successful completion of the course, students will be able to

CLO Number	CLO Statement	Knowledge Level
CLO1	Recall **static** and **dynamic analysis** approaches for dissecting and understanding malware behavior.	K1
CLO2	Understand the techniques, tools, and methodologies.	K2
CLO3	Apply the various tools for malware prevention, detection, and mitigation.	K3
CLO4	Analyze static analysis using tools like hex editors, disassemblers, and decompilers to extract meaningful information from malware binaries	K4

Mapping with Programme Learning Outcomes

CLOs	PLO1	PLO2	PLO3	PLO4	PLO5
CLO1	S	M	S	S	S
CLO2	S	S	M	S	M
CLO3	S	S	S	M	M
CLO4	S	S	S	M	S

S- Strong; M-Medium

List of Programs

- File Hashing Basics
- Finding Strings in a File
- Basic Disassembly in IDA Freeware
- Basic Function Analysis
- Identifying Windows API Calls
- Registry Interaction Analysis

- Simple Debugging with OllyDbg
- Process Monitoring
- Observing Anti-Debugging Behavior
- Virtual Machine Detection

Pedagogy

- Lectures, Group discussions, Demonstrations

Course Designer

Dr.R.Divya

COURSE CODE	COURSE NAME	CATEGORY	L	T	P	CREDIT
CY22SBP4	Digital Forensics Lab	Practical	-	-	45	3

Preamble:

The course is designed to understand how to recover and analyze digital evidence from various platforms.

Course Learning Outcomes

On the successful completion of the course, students will be able to

CLO Number	CLO Statement	Knowledge Level
CLO1	Recall digital devices and their evaluation ,technology.	K1
CLO2	Understand the principles, processes, and importance of digital forensics in cybersecurity and legal investigations.	K2
CLO3	Apply industry-standard tools to investigate digital evidence effectively..	K3
CLO4	Analyze volatile memory and network traffic to identify malicious activities and potential evidence.	K4

Mapping with Programme Learning Outcomes

CLOs	PLO1	PLO2	PLO3	PLO4	PLO5
CLO1	S	M	S	S	S
CLO2	S	S	M	S	M
CLO3	S	S	S	M	M
CLO4	S	S	S	M	S

S- Strong; M-Medium

List of Programs

- Recognizing Digital Devices as Evidence
- Understanding Closed vs. Open Systems
- Simulating Safe Device Handling
- Identifying Networked Devices in a Home Setup
- Hashing Basics
- Viewing System Logs

- Creating a Simple Security Model for Evidence Handling
- Accessing and Identifying Data on a Mobile Device
- Tracking a Simple GPS Location
- Building a Simple Cyber Profile from Device Usage

Pedagogy

- Lectures, Group discussions, Demonstrations

Course Designer

Dr.Sabitha Banu A

COURSE CODE	COURSE NAME	CATEGORY	L	T	P	CREDIT
CY22AC3	Big Data Analytics	Theory	-	-	-	5

Objectives

This Course deals with the Basics of Big Data and Hadoop architecture. It deals with working of MapReduce and Query Model of NoSQL Databases. It also includes the Advantages of MongoDB

Syllabus

UNIT I

Overview of Big Data: Defining Big Data - Big Data Types – Big Data Analytics – Industry Examples of Big Data - Big Data and Data Risk – Big Data Technologies – Benefits of Big Data.

UNIT II

Basics of Hadoop: Big Data and Hadoop – Hadoop Architecture – Main Components of Hadoop Framework – Analysing Big Data with Hadoop – Benefits of Distributed Applications –Hadoop Distributed File System – Advantages of Hadoop – Ten Big Hadoop Platforms.

UNIT III

MapReduce: Introduction to MapReduce –Working of MapReduce – Map operations MapReduce User Interfaces.

UNIT IV

NoSQL Databases: NoSQL Data Management – Types of NoSQL Databases – Query Model for Big Data – Benefits of NoSQL – MongoDB – Advantages of MongoDB over RDBMS – Replication in MongoDB.

UNIT V

HBase, CASSANDRA and JAQL: Introduction to HBase – Row-oriented and Column-

oriented Data Stores – HDFS Vs HBase – Hbase Architecture – HBase Data Model – Introduction to Cassandra –Features of Cassandra . Introduction to JAQL – JSON – Componentsof JAQL.

Text Book

S. No	Author	Title of the Book	Publisher	Year of Publication and Edition
1	V.K. Jain	Big Data and Hadoop	Khanna Book Publishing	2017,1st Edition

Reference Books

S. No	Author	Title of the Book	Publisher	Year of Publication& Edition
1	Frank J Ohlhorst	Big Data Analytics: Turning Big Data into Big Money	Wiley and SAS Business Series	2012, 1st Edition
2	Anand Rajaraman, Jeffrey David Ullman	Mining of Massive Datasets	Cambridge University Press	2012, 1st Edition

Course Designer

Mrs.P.Yashodha

COURSE CODE	COURSE NAME	CATEGORY	L	T	P	CREDIT
CY22AC4	IPv6	Theory	-	-	-	5

Objectives

Provides a fundamental issue in network protocol design and implementation withthe principles underlying TCP/IP protocol design; historical development of the Internet Protocol Version-6; IPv6 and QoS, IP network migrations and applications

Syllabus

UNIT I

Internet and the Networking Protocols: Historical Development - OSI Model - Internet IP/UDP/TCP – IPv4 Addressing Review

UNIT II

Next Generation Internet Protocol: Internet Protocol Version 6 (IPv6) - History of IPv6 - IPv6 Header Format - Problems with IPv4 - Features of IPv6 - IPv6 Addressing format and Types. ICMPv6 – Features - General Message Format - ICMP Error & Informational Message types - Neighbor Discovery- Path MTU Discovery

UNIT III

Security and Quality of Service in IPv6: Types of Threats - Security Techniques- IPSEC Framework - QoS in IPv6 Protocols

UNIT IV

Routing with IPv6: Routing in the Internet and CIDR – Multicasting - Unidirectional Link Routing - RIPng OSPF for IPv6 - PIM-SM & DVMRP for IPv6.

UNIT V

IPv4/IPv6 Transition Mechanisms: Tunneling - Automatic Tunneling - Configured tunneling - Dual Stack Translation- Migration Strategies for Telcos and ISPs.

Text Books

S. No	Author	Title of the Book	Publisher	Year of Publication and Edition
1	Silvia Hagen	IPv6 Essentials	O'Reilly Media	2014,3rd Edition
2	Joseph Davies	Understanding IPv6	Microsoft Press	2012,1st Edition
3	Stephen A. Thomas	IPng and the TCP/IP protocols	John Wiley & Sons edition	2016,1st Edition

Referencee Books

S. No	Author	Title of the Book	Publisher	Year of Publication and Edition
1	Douglas E Comer	Internetworking with TCP/IP Volume One	Pearson India	2015,6th Edition
2	Rick Graziani	IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6	Cisco Press	2012,1st Edition

Course Designer

Dr.Sabitha Banu A