VIVEKANANDHA

COLLEGE OF ARTS AND SCIENCES FOR WOMEN

ELAYAMPALAYAM, TIRUCHENGODE (Tk.), NAMAKKAL (Dt.).

[AN ISO 9001 : 2015 CERTIFIED INSTITUTIONS]

Affiliated to Periyar University, Approved by AICTE &
Re-Accredited with 'A+' Grade by NAAC,
Recognized under section 2(f) & 12(B) of UGC Act, 1956)
ELAYAMPALAYAM, TIRUCHENGODE (Tk.), NAMAKKAL (Dt.)

A U T O N O M O U S

PG & RESEARCH DEPARTMENT OF COMPUTER SCIENCE & APPLICATIONS

B.Sc. CS (CYBER SECURITY)

SYLLABUS & REGULATIONS

FOR CANDIDATES ADMITTED FROM 2024-25 ONWARDS
UNDER AUTONOMOUS & OBE PATTERN

VIVEKANANDHA EDUCATIONAL INSTITUTIONS
Angammal Educational Trust
Elayampalayam, Tiruchengode (Tk.), Namakkal (DT)

VIVEKANANDHA COLLEGE OF ARTS AND SCIENCES FOR WOMEN
(AUTONOMOUS)

B.Sc (INFORMATION TECHNOLOGY)

(Candidates admitted from 2024-2025 onwards)

REGULATIONS

I. SCOPE OF THE PROGRAMME

Bachelor of Information Technology can be considered to be one of the most prominent UG level programs in our country. This program mainly deals with the development of computer applications for the purpose of updating computer programming languages. B.Sc.CS [Cyber Security] also aims at creating strong knowledge of theoretical Information Technology subjects who can be employed in software development and testing units of industries. The course has a time period of 3 years with 6 semesters.

II. SALIENT FEATURES

- Regular conduct of guest lectures and seminars
- Campus recruitment
- Provides facilities such as Internet Access and In-House Library
- Provides Career Guidance for Post Graduate Courses like M.Sc, and the Certifications in programming languages
- Conduct of Personality Development Program
- Visiting Faculties from Industries

III. OBJECTIVES OF THE PROGRAMME

The Course Objective of the B.Sc. Information Technology program is to provide advanced and in-depth knowledge of Information Technology and its applications to enable students pursue a professional career in Information and Communication Technology in related industry, business and research. The course designed to impact professional knowledge and practical skills to the students.

IV. ELIGIBILITY FOR ADMISSION

A Candidates seeking admission to the first year Degree course (B.Sc. Information Technology) shall be required to have passed Higher Secondary Examination with Mathematics or Business

Mathematics or Computer Science or Computer Applications or Computer Technology or Statistics (Academic Stream or Vocational Stream) as one of the subject under Higher Secondary Board of Examination, conducted by the Government of Tamilnadu or an examination accepted as equivalent thereto by the syndicate, subject to such conditions as may be prescribed thereto are permitted to appear and qualify for the B.Sc. Information Technology Degree Examination of Periyar University after a course of study of three academic years.

V. DURATION OF THE PROGRAMME

- The course shall extend over a period of three academic years consisting of six semesters. Each academic year will be divided into two semesters. The First semester will consist of the period from July to November and the Second semester from December to April.
- The subjects of the study shall be in accordance with the syllabus prescribed from time to time by the Board of Studies of Vivekanandha College of Arts and Sciences for Women with the approval of Periyar University.

VI. CONTINUOUS INTERNAL ASSESSMENT (CIA)

The performance of the students will be assessed continuously and the Internal

ASSESSMENT MARKS **FOR THEORY PAPERS** WILL BE AS UNDER:

1	Average of Two Tests		-	05
2	Model Exam		-	10
3	Assignment		-	05
4	Attendance		-	05
		To	-	25

ASSESSMENT MARKS **FOR PRACTICAL PAPERS** WILL BE AS UNDER:

1	Model Exam		-	20
2	Observation Note		-	10
3	Attendance		-	10
		To	-	40

PASSING MINIMUM - EXTERNAL

THEORY	In the End Semester Examinations, the passing minimum shall be 40% out of 75 Marks. (30 Marks)
PRACTICAL / MINI PROJECT	In the End Semester Examinations, the passing minimum shall be 40% out of 60 Marks. (24 Marks)

VII. ELIGIBILITY FOR EXAMINATION

A candidate will be permitted to appear for the University Examination only on learning 75 % of attendance and only when her conduct has been satisfactory. It shall be open to grant exemption to a candidate for valid reasons subject to conditions prescribed.

DISTRIBUTION OF MARKS FOR ATTENDANCE:

ATTENDANCE PERCENTAGE	MARKS	
	THEORY	PRACTICAL
75-80	1	2
81-85	2	4
86-90	3	6
91-95	4	8
96-100	5	10

VIII. CLASSIFICATION OF SUCCESSFUL CANDIDATES

Successful candidates passing the Examination of Core Courses (Main & Allied Subjects) & Securing Marks.

a) 75 % and above shall be declared to have passed the examination in First Class with Distinction provided they pass all the examinations prescribed for the course at first appearance itself.
b) 60% and above but below 75 % shall be declared to have passed the Examinations in First Class..
c) 50% & above but below 60% shall be declared to have passed the examinations in Second Class.
d) All the remaining successful candidates shall be declared to have passed the examinations in Third Class.
e) Candidates who pass all the examinations prescribed for the course at the First appearance itself and within a period of three Consecutive Academic years from the year of admission only will be eligible for University Rank.

IX. ELIGIBILITY FOR AWARD OF THE DEGREE

A candidate shall be eligible for the award of the Degree only if she has undergone the above Degree for a period of not less than Three Academic years comprising of six semesters and passed the Examinations prescribed and fulfilled such conditions has have been prescribed therefore.

X. PROCEDURE IN THE EVENT OF FAILURE

If a candidate fails in a particular subject, she may reappear for the university examination in the concerned subject in subsequent semesters and shall pass the examination.

XI. COMMENCEMENT OF THESE REGULATIONS

These regulations shall take effect from the academic year 2023-2024 (i.e.,) for the students who are to be admitted to the First year of the course during the Academic year 2023-24 and thereafter.

XII. TRANSITORY PROVISIONS

Candidates who were admitted to the UG course of study before 2021-2022 shall be permitted to appear for the examinations under those regulations for the period of Three years ie., upto and inclusive of the Examinations of 2023-2024. Thereafter, they will be permitted to appear for the examinations only under the regulations then in force.

EVALUATION OF EXTERNAL EXAMINATIONS (EE)

QUESTION PAPER PATTERN – Theory	
Time duration: 3 Hours	**Max. Marks: 75**
PART- A: **(10 x 1= 10)**	Answer all the Questions Two Questions from each Unit
PART- B: **(5x 7 = 35)**	Answer all the questions One Question from each Unit (Either or Type)
PART- C: **(3 x 10 = 30)**	Answer any **THREE** of the questions One Question from each Unit (3 Out of 5)
IN THE END SEMESTER EXAMINATIONS, THE PASSING MINIMUM SHALL BE 40% OUT OF 75 MARKS. (30 MARKS)	

QUESTION PAPER PATTERN – Practical	
Time duration: 3 Hours	**Max. Marks: 60**
1. One compulsory question from the given list of objectives	**30 Marks**
2. One either/or type question from the given list of objectives	**30 Marks**
IN THE END SEMESTER EXAMINATIONS, THE PASSING MINIMUM SHALL BE 40% OUT OF 60 MARKS. (24 MARKS)	

B.Sc CS (CYBER SECURITY) CURRICULUM FOR ACADEMIC YEAR 2024 – 2025

COURSE PATTERN AND SCHEME OF EXAMINATIONS UNDER AUTONOMOUS, CBCS & OBE PATTERN

FOR THE CANDIDATES ADMITTED FROM THE YEAR 2024 – 2025
SEMESTER: I & II

SEM	PART	COURSE CODE	COURSE TITLE	HRS	CREDIT	MARKS		
						CIA	EE	TOT
I	I	23U1LT01	Tamil-I	6	3	25	75	100
	II	23U1LE01	English–I	4	2	25	75	100
	III	24U1CYC01	Introduction to Python	5	4	25	75	100
	III	24U1CYCP01	Python Programming Lab	5	4	40	60	100
	III	23U1MAGE01	Generic Elective : Numerical Methods	4	3	25	75	100
	III	23U1ENAC01	Soft Skills for Effective Communication – I	2	2	25	75	100
	III	24U1CSAC01	Introduction to HTML	2	2	25	75	100
	IV	23U1VE01	Value Education	2	2	25	75	100
	Total			**30**	**22**	**215**	**585**	**800**
II	I	23U2LT02	Tamil– II	5	3	25	75	100
	II	23U2LE02	English–II	5	3	25	75	100
	III	24U2CYC02	Operating System	5	5	25	75	100
	III	24U2CYCP02	Operating System and Security Lab	5	4	40	60	100
	III	23U2MAGE07	Generic Elective : Basic Statistical methods	4	3	25	75	100
	III	23U2CYAC02	Office Automation	2	2	25	75	100
	IV	24U2CYS01	Human Computer Interaction	2	2	25	75	100
	IV	23U2EVS01	Environmental Studies	2	2	25	75	100
	Total			**30**	**22**	**190**	**510**	**700**

SEMESTER: III & IV

SEM	Part	Course Code	COURSE TITLE	HRS	CREDIT	MARKS		
						CIA	EE	TOT
III	I	23U3LT03	Tamil – III	5	3	25	75	100
	II	23U3LE03	English–III	5	3	25	75	100
	II	24U3CYC04	Artificial Intelligence with Machine Learning	5	4	25	75	100
	III	24U3CYDE01	Elective-1	4	4	25	75	100
	III	24U3CYCP03	Artificial Intelligence with Machine Learning Lab	5	3	40	60	100
	IV	23U3MAGE13	Generic Elective : Operations research	4	3	25	75	100
	IV	NMEC-I	NMEC Course–1	2	2	25	75	100
			Total	**30**	**22**	**190**	**510**	**700**
IV	I	23U4LT04	Tamil- IV	5	3	25	75	100
	II	23U4LE04	English–IV	5	3	25	75	100
	III	24U4CYC05	Forensic audio-video analysis and speaker identification	5	4	25	75	100
	III	24U4CYDE02	Elective-2	4	4	25	75	100
	III	24U4CYCP04	Audio-video analysis Lab	5	3	40	60	100
	III	23U4MAGE15	Generic Elective : Discrete Mathematics	4	3	25	75	100
	IV	NMEC-II	NMEC Course–2	2	2	25	75	100
			Total	**30**	**22**	**190**	**510**	**700**

SEMESTER: V & VI

SEM	Part	COURSE CODE	COURSE TITLE	HRS	CREDIT	MARKS		
						CIA	EE	TOT
V	III	24U5CYC06	Vulnerability Assessment and Penetration Testing	5	4	25	75	100
	III	24U5CYCP05	Vulnerability Assessment and Penetration Testing Lab	4	4	40	60	100
	III	24U5CYC07	Ethical Hacking	5	4	25	75	100
	III	24U5CYCP06	Ethical Hacking Lab	4	4	40	60	100
	III	24U5CYDE03	Core Elective –3	5	4	25	75	100
	III	24U5CYDE04	Core Elective-4:	5	4	25	75	100
	IV	24U5CYS03	SBEC-1 –Basics of Cyber Crime	2	2	25	75	100
	Total			**30**	**26**	**205**	**495**	**700**
VI	III	24U6CYC08	Preserving and Recovering of Digital Evidence	5	4	25	75	100
	III	24U6CYC09	Malware Analysis	5	3	25	75	100
	III	24U6CYCP07	Mobile Devices Forensic Lab	4	3	40	60	100
	III	24U6CYDE05	Core Elective–5	5	4	25	75	100
	III	24U6CYDE06	Core Elective–6	4	4	25	75	100
	III	24U6CYPR01	Project Work	5	5	40	60	100
	IV	24U6CYS03	Files System Forensic	2	2	25	75	100
	V		Extension Activities	0	1	-	-	-
			Total	**30**	**26**	**205**	**495**	**700**
Grand Total				**180**	**140**	**1195**	**3105**	**4300**

DECIPLINE SPECIFIC ELECTIVES

Course Code	DSE	Course Name	Semester
24U3CYDE01	DSE – I	Trends in Digital Forensic	Semester: III
24U3CYDE02	DSE – I	Open Source Technology	Semester: III
24U4CYDE03	DSE – II	Cyber Forensic	Semester: IV
24U4CYDE04	DSE – II	E-Commerce & Digital Payment	Semester: IV
24U5CYDE05	DSE – III	Network Security	Semester: V
24U5CYDE06	DSE – III	Mobile Computing	Semester: V
24U5CYDE07	DSE – IV	Artificial Intelligence & Knowledge Representation	Semester: V
24U5CYDE08	DSE – IV	Cyber Crime & Law	Semester: V
24U6CYDE09	DSE – V	Block Chain Technology	Semester: VI
24U6CYDE10	DSE – V	Cryptography	Semester: VI
24U6CYDE11	DSE – VI	Cloud Security	Semester: VI
24U6CYDE12	DSE – VI	Information Security	Semester: VI

Skill Based Elective Courses (SBEC) (Offer to Same Students)

Course Code	Course Name	Semester
24U2CYS01	Human Computer Interaction	Semester: II
24U2CYS02	Social Media & Security	Semester: II
24U5CYS03	Advanced Excel	Semester: V
24U5CYS04	Sentiment Analysis	Semester: V
24U6CYS05	Analytical Skills	Semester: VI

Programme outcomes (PO) for B.Sc CS (Cyber Security)

- Scientific aptitude will be developed in Students
- Students will acquire basic Practical skills & Technical knowledge along with domain knowledge of different subjects in the science & humanities stream.
- Students will become employable; Students will be eligible for career opportunities in education field, Industry, or will be able to opt for entrepreneurship
- Students will possess basic subject knowledge required for higher studies, professional and applied courses
- Students will be aware of and able to develop solution oriented approach towards various Social and Environmental issues.
- Ability to acquire in-depth knowledge of several branches of Mathematics and aligned areas . This Programme helps learners in building a solid foundation for higher studies in Mathematics
- The skills and knowledge gained leads to proficiency in analytical reasoning, which can be utilized in modeling and solving real life problems.
- Utilize mathematics to solve theoretical and applied problems by critical understanding, analysis and synthesis.
- To recognize patterns and to identify essential and relevant aspects of problems.
- Ability to share ideas and insights while seeking and benefitting from knowledge and insight of others.
- Mould the students into responsible citizens in a rapidly changing interdependent society.

The above expectations generally can be pooled into 6 broad categories and can be modified according to institutional requirements:

PO1: Knowledge

PO2: Problem Analysis

PO3: Design / Development of Solutions

PO4: Conduct investigations of complex problems

PO5: Modern tool usage

PO6: Applying to society

Programme Specific Outcomes of B.Sc Degree programme in Cyber Security

PSO1 Demonstrate and apply basic knowledge of information technology to the scientific issues and problems being faced in society and the industry.

PSO2 Analyze critical problems and provide computer-based solutions by applying appropriate

tools and technology.

PSO3 Design and develop solutions to problems in the areas related to web page design, Mobile App development, cloud computing, IOT and data analytics of varying complexity.

2. Highlights of the Revamped Curriculum:

- Student-centric, meeting the demands of industry & society, incorporating industrial components, hands-on training, skill enhancement modules, industrial project, project with viva-voce, exposure to entrepreneurial skills, training for competitive examinations, sustaining the quality of the core components and incorporating application oriented content wherever required.
- The Core subjects include latest developments in the education and scientific front, advanced programming packages allied with the discipline topics, practical training, for providing solutions to industry / real life situations. The curriculum also facilitates peer learning with advanced mathematical topics in the final semester, catering to the needs of stakeholders with research aptitude.
- The curriculum is designed so as to strengthen the Industry-Academia interface and provide more job opportunities for the students.
- The Internship during the second year vacation will help the students gain valuable work experience, that connects classroom knowledge to real world experience and to narrow down and focus on the career path.
- Project with viva-voce component in the fifth semester enables the student, application of conceptual knowledge to practical situations.

FIRST YEAR –SEMESTER- I

Subject Title	INTRODUCTION TO PYTHON	Semester	I
Subject Code	24U1CYC01	Specialization	NA
Type	Core: Theory	L:T:P:C	5:0:0:5

Course objective:

- Build basic programs using fundamental programming constructs like variables, conditional logic, looping, and functions
- Work with user input to create fun and interactive programs
- Create simple games with images, animations, and audio using our custom beginner-friendly programming
- Describe the core syntax and semantics of Python programming language.

CO No.	CO Statement	Knowledge Level
CO1	Develop and execute simple Python programs	K1
CO2	Decompose a Python program into functions	K2,K4
CO3	Write simple Python programs using conditionals and looping for solving problems	K3
CO4	Represent compound data using Python lists, tuples, dictionaries etc.	K4
CO5	Read and write data from/to files in Python programs	K4

Unit	Contents	No. of Sessions
I	Introduction: The essence of computational problem solving – Limits of computational problem solving-Computer algorithms-Computer Hardware-Computer Software-The process of computational problem solving-Python programming language - Literals - Variables and Identifiers - Operators - Expressions and Data types, Input / output	12
II	Control Structures: Boolean Expressions - Selection Control - If Statement-Indentation in Python- Multi-Way Selection -Iterative Control- While Statement-Infinite loops- Definite vs. Indefinite Loops- Boolean Flag. String, List and Dictionary, Manipulations Building blocks of python programs, Understanding and using ranges.	12
III	Functions: Program Routines- Defining Functions- More on Functions: Calling Value-Returning Functions- Calling Non-Value-Returning Functions- Parameter Passing - Keyword Arguments in Python - Default Arguments in Python-Variable Scope.	12

IV	Objects and their use: Software Objects - Turtle Graphics – Turtle attributes- Modular Design: Modules - Top-Down Design - Python Modules - Text Files: Opening, reading and writing text files – String Processing- Exception Handling.	**12**
V	Dictionaries and Sets: Dictionary type in Python - Set Data type. Object Oriented Programming using Python: Encapsulation - Inheritance – Polymorphism. Recursion: Recursive Functions.	**12**

Learning Resources	
Text Books	1. Charles Dierbach, "Introduction to Computer Science using Python - A computational Problem solving Focus", Wiley India Edition, 2015.
Reference Books	• Mark Lutz, "Learning Python Powerful Object Oriented Programming", O'reilly Media 2018, 5th Edition. • Timothy A. Budd, "Exploring Python", Tata MCGraw Hill Education Private Limited 2011, 1 st Edition. • John Zelle, "Python Programming: An Introduction to Computer Science", Second edition, Course Technology Cengage Learning Publications, 2013, ISBN 978-1590282410 • Michel Dawson, "Python Programming for Absolute Beginers" , Third Edition, Course Technology Cengage Learning Publications, 2013, ISBN 978-1435455009
Website/Link	http://bedford-computing.co.uk/learning/wp-content/uploads/2015/10/Introduction-to-Computer-Science-Using-Python.pdf

Mapping with Programme Outcomes

S-Strong , M- Medium , L – Low

	PO01	**PO02**	**PO03**	**PO04**
CO1	S	S	S	-
CO2	S	M	M	S
CO3	S	L	L	M
CO4	M	S	M	S
CO5	S	L	S	S

Subject Title	PYTHON PROGRAMMING LAB	Semester	I
Subject Code	24U1CYCP01	Specialization	NA
Type	Practical	L:T:P:C	0:0:5:4

Learning Objectives:

- Acquire programming skills in core Python.
- Acquire Object-oriented programming skills in Python.
- Develop the skill of designing graphical-user interfaces (GUI) in Python.
- Develop the ability to write database applications in Python.
- Acquire Python programming skills to move into specific branches

Course Outcomes:

CO1: To understand the problem solving approaches

CO2: To learn the basic programming constructs in Python

CO3: To practice various computing strategies for Python-based solutions to real world problems

CO4: To use Python data structures - lists, tuples, dictionaries.

CO5: To do input/output with files in Python.

1. Write a program to demonstrate different number data types in Python
2. Write a program to perform different Arithmetic Operations on numbers in Python.
3. Write a Python program using List, Tuples and List comprehensions
4. Write a Python program using Control statements
5. Write a Python program using Functions and String Operations
6. Write a Python program using Text Files
7. Write a Python program using Exceptional Handling
8. Write a Python program using Inheritance
9. Write a program to demonstrate working with dictionaries in python.
10. Write a python program to find factorial of a number using Recursion

Subject Code	Subject Name	Category	L	T	P	S	Credits	Marks		
								CIA	External	Total
24U1CSAC01	INTRODUCTION TO HTML	Skill Enha. Course (SEC)	2	-	-		2	25	75	100

Learning Objectives	
LO1	Insert a graphic within a web page.
LO2	Create a link within a web page.
LO3	Create a table within a web page.
LO4	Insert heading levels within a web page.
LO5	Insert ordered and unordered lists within a web page. Create a web page.

UNIT	Contents	No. Of. Hours
I	Introduction :Web Basics: What is Internet–Web browsers–What is Webpage –HTML Basics: Understanding tags.	6
II	Tags for Document structure (HTML, Head, Body Tag). Block level text elements: Headings paragraph (<p> tag)–Font style elements:(bold, italic, font, small, strong, strike, big tags)	6
III	Lists: Types of lists: Ordered, Unordered– Nesting Lists–Other tags: Marquee, HR, BR-Using Images –Creating Hyperlinks.	6
IV	Tables: Creating basic Table, Table elements, Caption–Table and cell alignment–Rowspan, Colspan–Cell padding.	6
V	Frames: Frameset–Targeted Links–No frame–Forms: Input, Text area, Select, Option.	6
TOTAL HOURS		**30**

Course Outcomes		Programme Outcomes
CO	On completion of this course, students will	
CO1	Knows the basic concept in HTML Concept of resources in HTML	PO1, PO2, PO3, PO4, PO5, PO6
CO2	Knows Design concept. Concept of Meta Data Understand the concept of save the files.	PO1, PO2, PO3, PO4, PO5, PO6
CO3	Understand the page formatting. Concept of list	PO1, PO2, PO3, PO4, PO5, PO6
CO4	Creating Links. Know the concept of creating link to email address	PO1, PO2, PO3, PO4, PO5, PO6
CO5	Concept of adding images Understand the table creation.	PO1, PO2, PO3, PO4, PO5, PO6

Textbooks	
1	"Mastering HTML5 and CSS3 Made Easy", Teach U Comp Inc., 2014.
2	Thomas Michaud, "Foundations of Web Design: Introduction to HTML & CSS"
Web Resources	
1.	https://www.teachucomp.com/samples/html/5/manuals/Mastering-HTML5-CSS3.pdf
2.	https://www.w3schools.com/html/default.asp

Mapping with Programme Outcomes:

CO/PSO	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6
CO 1	3	3	3	3	3	3
CO 2	3	3	2	3	3	3
CO 3	2	3	3	3	3	3
CO 4	3	3	3	3	3	3
CO 5	3	3	3	2	3	3
Weightage of course contributed to each PSO	14	15	14	14	15	15

S-Strong-3 M-Medium-2 L-Low-1

Subject Title	HUMAN COMPUTER INTERACTION	Semester	II
Subject Code	24U2CYS01	Specialization	NA
Type	CORE: THEORY	L:T:P:C	2:0:0:2

COURSE OBJECTIVE:

1. Understand Fundamental HCI Concepts
2. Develop Skills in Designing User Interfaces
3. Apply User-Centered Design (UCD) Methodology

CO No.	CO Statement	Knowledge Level
CO1	Students will understand human cognitive processes, memory, emotions, and individual differences to enhance interaction design and usability.	K1
CO2	Students will understand computer hardware, including input devices, displays, memory, and paper, to improve system design and user interfaces.	K2, K4
CO3	Students will learn interaction models, ergonomic design, and interface styles to create effective user interfaces, including 2D/3D navigation and WIMP elements.	K3
CO4	Students will apply design principles, user focus, and iterative prototyping to create effective screen layouts and incorporate HCI in the software life cycle to improve usability and design rationale.	K1, K2
CO5	Students will analyze and apply design rules, principles, standards, and heuristics to enhance usability and interface effectiveness	K4

Unit	Contents	No. of Hrs
I	**The human:** Introduction - Input–Output channels - Human memory - Thinking: Reasoning and Problem Solving - Emotion - Individual differences. (1.1 to 1.5)	6
II	**The Computer:** Introduction - Text entry devices - Positioning, pointing and drawing - Display devices - Paper: printing and scanning – Memory. (2.1 to 2.8)	6
III	**The interaction:** Introduction - Models of interaction - Frameworks and HCI – Ergonomics: Design Focus: Industrial interfaces - Interaction styles: Design Focus: Navigation in 3D and 2D - Elements of the WIMP interface - Design	6

	Focus: Learning toolbars - Interactivity (3.1 to 3.7)	
IV	**Interaction design basics:** What is design - The process of design - User focus – Screen design and layout - Iteration and prototyping. **HCI in the software process:** The software life cycle - Usability engineering - Iterative design and prototyping - Design rationale. (5.2 to 5.4, 5.7 to 5.8, 6.2 to 6.5)	**6**
V	**Design rules:** Introduction - Principles to support usability – Standards – Guidelines - Golden rules and heuristics - HCI patterns. (7.1 to 7.7)	**6**

Learning Resources	
Text book	Alan Dix, Janet Finlay, Gregory Abowd, Russell Beale, "Human -Computer Interaction", 3rd Edition, Pearson Education, 2004.
Reference book	Serengul Smith-Atakan, "Human-Computer Interaction: Basics and Practice", Bentham books.
Website / Link	https://www.tutorialspoint.com/human_computer_interface/index.htm

Subject title	Social Media & Security	Semester	V
Subject code	24U2CYS02	Specialization	CA
Type	SBEC : Theory	L:T:P:C	2:0:0:2

COURSE OBJECTIVE:

To equip students with the knowledge and skills to analyze, manage, and mitigate security risks associated with social media platforms, ensuring safe and ethical use in both personal and professional contexts.

CO NO.	CO STATEMENT	KNOWLEDGE LEVEL
CO1	**Understanding Risks**: Identify and assess the security threats and vulnerabilities associated with social media platforms.	K1
CO2	**Privacy Protection**: Learn techniques to safeguard personal and organizational information on social media.	K2
CO3	**Incident Response**: Develop skills to detect and respond to social media-based cyberattacks	K3
CO4	**Policy Development**: Create and implement security policies for safe social media use.	K4
CO5	**Tool Utilization**: Use specialized tools to monitor and secure social media activities effectively.	K4

UNIT	CONTENTS	NO. OF SESSIONS
I	Introduction to Social Media, Understanding Social Media, Different Types and Classifications, The Value of Social Media, Cutting Edge Versus Bleeding Edge, The Problems That Come With Social Media, Is Security Really an Issue? Taking the Good With the Bad.	6
II	Dark side Cybercrime, Social Engineering, Hacked accounts, cyberstalking, cyberbullying, predators, phishing, hackers.	6
III	Being bold versus being overlooked Good social media campaigns, Bad social media campaigns, sometimes it's better to be overlooked, Social media hoaxes, The human factor, Content management, Promotion of social media.	8
IV	Risks of Social media Introduction Public embarrassment, Once it's out there, it's out there False information, Information leakage, Retention and archiving, Loss of data and equipment.	4
V	Policies and Privacy Blocking users controlling app privacy, Location awareness, Security Fake accounts passwords, privacy and information sharing..	6

LEARNING RESOURCES	
Text books	1. Interdisciplinary Impact Analysis of Privacy in Social Networks, Recognizing Your DigitalFriends, Encryption for Peer-to-Peer Social Networks Crowd sourcing and Ethics, Authors:Altshuler Y, EloviciY, Cremers A.B, Aharony N, Pentland A. (Eds.). 2.SocialMediasecurity Https://www.sciencedirect.com/science/article/pii/B97815974998660000
Reference books	1. Michael Cross, Social Media Security Leveraging Social Networking While Mitigating Risk. 2. Online Social Networks Security, Brij B. Gupta, Somya Ranjan Sahoo, Principles, Algorithm, Applications, and Perspectives, CRC press.
Website/link	Website/ Link https://www.trendmicro.com/en_in/research/21/f/best-practices-for-social-media security.html

MAPPING WITH PROGRAMME OUTCOMES

	PO01	PO02	PO03	PO04
CO1	S	S	S	-
CO2	S	M	M	S
CO3	S	L	L	M
CO4	M	S	M	S
CO5	S	L	S	S

S-Strong , M- Medium , L – Low

SEMESTER-II

Subject Title	OPERATING SYSTEM	Semester	II
Subject Code	24U2CYC02	Specialization	NA
Type	Core: Theory	L:T:P:C	5:0:0:5

Course objective:

- To understand the services provided by and the design of an operating system.
- To understand the structure and organization of the file system.
- To understand what a process is and how processes are synchronized and scheduled.
- To understand different approaches to memory management.
- Students should be able to use system calls for managing processes, memory and the file system.

CO No.	CO Statement	Knowledge Level
CO1	Define the Overview of Operating Systems	K1
CO2	Outline the concepts of Process Management	K2
CO3	Define the Storage management policies.	K2
CO4	Apply the methods in Operating Systems	K3
CO5	To do Email analysis	K3

Unit	Contents	No. of Sessions
I	**OPERATING SYSTEMS OVERVIEW**: What OS Do–Computer system Organization–Architecture- Structure–Operations- Process Management–Memory management–Storage management–Protection and Security–Kernel Data structures Computing Environments–Open source OS	**10**
II	**PROCESS MANAGEMENT**: Processes-Process Concept, Process Scheduling, Operations on Processes, Inter process Communication; Threads- Overview, Multi core Programming, Multithreading Models; Windows and Linux model. Deadlocks–Detection–Handling-Prevention–Avoidance.	**10**
III	**STORAGE MANAGEMENT** :Main Memory-Contiguous Memory Allocation, Segmentation, Paging, 32 and 64 bit architecture Examples; Virtual Memory-Demand Paging, Page Replacement, Allocation, Thrashing; Allocating Kernel Memory, OS Examples.	**10**
IV	**I/O SYSTEMS**: Mass Storage Structure-Overview, Disk Scheduling and Management; File System Storage-File Concepts, Directory and Disk Structure, Sharing and Protection; File System Implementation- File System Structure, Directory Structure, Allocation Methods, Free Space Management, I/O Systems	**10**

V	**CASE STUDY**: Linux System- Basic Concepts; System Administration- Requirements for Linux System Administrator, Setting up a LINUX Multi function Server, Domain Name System, Setting Up Local Network Services; Virtualization- Basic Concepts, Setting Up Xen, VMware on Linux Host and Adding Guest OS.	**10**

Learning Resources	
Text Books	1. Abraham Silber schatz, Peter Baer Galvin and Greg Gagne, "Operating System Concepts",9th Edition, John Wiley and Sons Inc., 2012.
Reference Books	1. William Stallings, "Operating Systems–Internals and Design Principles", 7 th Edition, Prentice Hall, 2011. 2. Andrew S. Tanenbaum, "Modern Operating Systems", Second Edition, Addison Wesley, 2001. 3. Charles Crowley, "Operating Systems: A Design-Oriented Approach", Tata McGraw Hill Education", 1996. 4. DM Dhamdhere, "Operating Systems: A Concept-Based Approach", Second Edition, Tata McGraw-Hill Education, 2007.
Website/Link	1. https://en.wikipedia.org/wiki/Operating_system 2. https://www.geeksforgeeks.org/storage-management/

Mapping with Programme Outcomes

COs/POs/ PSOs	PO1	PO2	PO3	PO4	PO5	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	L	M	L	L	L	L	L	L	M	L
CO2	L	L	L	L	L	M	M	M	M	S
CO3	M	M	M	M	M	S	L	M	M	L
CO4	L	L	M	M	S	S	L	M	M	S

S-Strong , M- Medium , L – Low

Subject Title	OPERATING SYSTEM AND SECURITY LAB	Semester	II
Subject Code	24U2CYCP02	Specialization	NA
Type	Core: Theory	L:T:P:C	0:0:5:4

Learning Objectives:

- Acquire programming skills in OS.
- To introduce the concepts of operating systems, designing principles of operating systems and implementation of operating systems.

CO No.	CO Statement	Knowledge Level
CO1	Understanding the concept of OS Installation	K1
CO2	Implement various Operating System on a single machine	K2
CO3	Analyze the problem and Solve	K2
CO4	Solve security problems using tools	K3
CO5	To do Email analysis	K3

1. Installation of Windows Operating system
2. Installation of Linux Operating system
3. Installation of Multiple OS on a single machine
4. Installation of VM Virtual Box Implementation of Security Tools
5. Hex analysis using Hex Editors
6. Registry Editing and Viewing using native tools of OS
7. Hash code generation, comparison of files using tools like Hash Cal
8. File analysis using Sleuth kit
9. Graphical File analysis and Image Analysis
10. Email Analysis involving Header check, tracing route, performing a check on Spam mail and Non-Spam mail.

Recommended Tools to be used: Windows and Linux Operating Systems and Open source Tools

SEMESTER-III

Subject Title	Artificial Intelligence with Machine Learning	Semester	III
Subject Code	24U3CYC04	Specialization	NA
Type	Core Theory	L:T:P:C	5:0:0:4

Course objective:

CO No.	CO Statement	Knowledge Level
CO1	To introduce students to the basic concepts and techniques of Machine Learning.	K1
CO2	To learn Decision trees, KNN and Ensemble Techniques.	K2,K4
CO3	To implement and apply machine learning algorithms to real-world applications.	K3
CO4	To understand the problems using various machine learning techniques.	K4
CO5	To study the recent machine learning software for solving practical problems.	K4

Unit	Contents	No. of Sessions
I	**THE FUNDAMENTALS OF MACHINE LEARNING:** What Is Machine Learning?-Why Use Machine Learning?-Examples of Applications- Supervised / Unsupervised Learning - Batch and Online Learning - Instance-Based Versus Model-Based Learning- Main Challenges of Machine Learning.	12
II	**SUPERVISED LEARNING :** Classification and Regression - Generalization, Overfitting, and Underfitting - Supervised Machine Learning Algorithms : k-Nearest Neighbors - Naive Bayes Classifiers - Decision Trees - Ensembles of Decision Trees - **UNSUPERVISED LEARNING :** Types of Unsupervised learning - Challenges in Unsupervised Learning- Clustering - k-Means Clustering - Agglomerative Clustering	12
III	**GRAPHICAL MODELS** : Bayesian Networks .-. Conditional Independence - Markov Random Fields - Inference in Graphical Models - Mixture Models and EM: K-means Clustering.- K-means Clustering.	12
IV	**LINEAR MODELS FOR REGRESSION:** Linear Basis Function Models - Bayesian Linear Regression - Limitations of Fixed Basis Functions - k – means Algorithm - Naïve Bayes Classification Algorithm: Bayes Rule – types of events – Algorithm – Pros & Cons – Applications.	12

V	**IMPLEMENTING MACHINE LEARNING ALGORITHMS**: Naive Bayes Classification Algorithm: Understanding conditional probability The Bayes Rule – types of events – Algorithm – Laplace correction – Pros & Cons – Applications - Neural Networks: Working of Neural Networks – Pros and Cons - Applications – Support Vector Machine: How does SVM work?- Advantages and Disadvantages of SVM.	**12**

Learning Resources	
Text Books	1. "Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow", Aurélien Géron, O'Reilly Media, 2019. 2. "Introduction to Machine Learning with Python ",Andreas C. Müller and Sarah Guido, O'Reilly Media,2017. 3. "Data Science and Machine Learning in R",Reema Thareja McGraw-Hill India, 2021.
Reference Books	**1.** Pattern Recognition and Machine Learning, Christopher M. Bishop F.R.Eng, 2006 , Springer Publisher. **2.** Tom M. Mitchell- Machine Learning - McGraw Hill Education, International Edition.
Website/Link	1. https://www.techtarget.com/searchenterpriseai/definition/supervised-learning 2. https://keremkargin.medium.com/nlp-tokenization-stemming-lemmatization-and-part-of-speech-tagging-9088ac068768 3. https://pianalytix.com/how-machine-learning-works-in-social-media-2/

Mapping with Programme Outcomes

	PO01	**PO02**	**PO03**	**PO04**
CO1	S	S	S	S
CO2	S	S	S	M
CO3	S	S	S	S
CO4	S	S	M	S
CO5	S	S	S	S

S-Strong, M- Medium, L – Low

Subject Title	Artificial Intelligence with Machine Learning Lab	Semester	III
Subject Code	24U3CYCP03	Specialization	NA
Type	Practical	L:T:P:C	0:0:5:3

Course objective:

CO No.	CO Statement	Knowledge Level
CO1	To introduce students to the basic concepts and techniques of Machine Learning.	K1
CO2	To learn Decision trees, KNN and Ensemble Techniques.	K2,K4
CO3	To implement and apply machine learning algorithms to real-world applications.	K3
CO4	To understand the problems using various machine learning techniques.	K4
CO5	To study the recent machine learning software for solving practical problems.	K4

1. Familiarizing with Anaconda and Jupyter for importing modules and dependencies for ML.

2. Given the following data, which specify classifications for nine combinations of VAR1 and VAR2 predict a classification for a case where VAR1=0.906 and VAR2=0.606, using the result of kmeans clustering with 3 means (i.e., 3 centroids) periments

VAR1	VAR2	CLASS
1.713	1.586	0
0.180	1.786	1
0.353	1.240	1
0.940	1.566	0
1.486	0.759	1
1.266	1.106	0
1.540	0.419	1
0.459	1.799	1
0.773	0.186	1

3. Write a program to demonstrate the working of the decision tree based ID3 algorithm. Use an appropriate data set for building the decision tree and apply this knowledge to classify a new sample.

4. Write a program to implement k-Nearest Neighbour algorithm to classify the iris data set. Print both correct and wrong predictions. Java/Python ML library classes can be used for this problem.

5. Apply EM algorithm to cluster a set of data stored in a .CSV file. Use the same data set for clustering using k-Means algorithm. Compare the results of these two algorithms and comment on the quality of clustering. You can add Java/Python ML library classes/API in the program.

6. Write a program to construct a Bayesian network considering medical data. Use this model to demonstrate the diagnosis of heart patients using standard Heart Disease Data Set. You can use Java/Python ML library classes/API.

7. Assuming a set of documents that need to be classified, use the naïve Bayesian Classifier model to perform this task. Built-in Java classes/API can be used to write the program. Calculate the accuracy, precision, and recall for your data set.

8. Write a Python program to implement Simple Linear Regression and plot the graph.

9. Build an Artificial Neural Network by implementing the Back propagation algorithm and test the same using appropriate data sets.

10. Using Weka tool for SVM classification for chosen domain application.

SEMESTER-IV

ubject Title	Forensic audio-video analysis and speaker identification	Semester	IV
Subject Code	24U4CYC05	Specialization	NA
Type	Core: Theory	L:T:P:C	5:0:0:4

LEARNING OBJECTIVES

- To understand the basics of digital records
- To know the basics of video and audio technology
- To identify and apply speaker identification process.
- To Analyse forensic audio and video.
- To Analyze the Approaches For Speaker Recognition System

COURSE OBJECTIVES

CO No.	CO Statement	Knowledge Level
CO1	To understand the basics of digital records	K1
CO2	To know the basics of video and audio technology	K1
CO3	To identify and apply speaker identification process.	K2
CO4	To analyse forensic audio and video.	K3
CO5	To Analyze the Approaches For Speaker Recognition System	K4

Unit	Contents	No. of Sessions
I	Basic Circuits: Basic Electric Circuits-LR, CR, LCR circuits, Conventional Filters and Digital Filters (high pass filters, low pass filters).Noise Characteristics: Properties of Noise, Acoustic Characteristics of Environments-Diffraction, Reverberation and Diffusion. Recording Formats-Analog and Digital, Audio and Video file formats. Linear and Non –linear Editing.	**12**
II	Introduction to video technology: Concept of Video film production-Introduction to video technology component of Digital Image Processing. Concept of Digital Water Marking. Visual examination technique on video frame image- Facial Image Recognition from video frame image .	**12**
III	Forensic audio and video analysis: Introduction to Forensic Audio & Video Analysis: A basic understanding of forensic audio and video technology-Audio and Video Evidence handling procedures. Authentication of recorded audio and video. Scientific methodology of forensic audio-video analysis. Recovery of digital audio-video / Deleted Video & Audio Files recovery- Exporting evidence as video or still image files-Software used for audio and video analysis.-Admissibility of audio and video evidence in court.	**12**
IV	. Basics of speaker identification: Introduction: Forensic Speaker Identification, Forensic Phonetics-Forensic challenges in Voicerecognition.Forensic Phonetic Parameters: Acoustic vs. Auditory Parameters, Linguistic vs. NonLinguistic Parameters. Forensic Significance: Linguistic Analysis- Requirements on forensic phonetic parameters. The human vocal tract and the production and description of	**12**

	speech parameters: Vocal tract structures. Forensic Significance – Vocal cord activity, Nasals and Nasalization-Phonetic Aspects of Speech: Articulators – Active/Passive, Phonemes –Segmental and Supra segmental, Prosodic featuresStress, Intonation, Duration, Syllables, Nasalization, and Accent features.	
V	Forensic speaker identification: Characterizing Forensic Speaker Identification: Speaker Recognition – Speaker Identification and Verification, Forensic Significance. Components of Speaker Recognition.-Approaches to Speaker Recognition System of Auditory Analysis, Spectrographic approach or Voice Print Identification. Automatic Approach: Gaussian Mixture Models, Long Term Averaging, Vector Quantization, Hidden Markov Models, Neural Networks. Expressing Results in Forensic Speaker Recognition–Likelihood Ratio, Objective/Subjective Methods. Concept of Test and Error in Speaker Identification.- Admissibility of Voice evidence in Court.	**12**

Learning Resources	
Text Books	1.Forensic Speaker Identification, Philip Rose: CRC Press Book, (2002).
Reference Books	• A Simplified Guide to Forensic Audio and Video Analysis (PDF Notes). • The Physics of Speech, D.B. Fry: Cambridge University Press, (1979). • The Complete Book of Video Techniques Subjects Equipment, David Cheshire: Dorling Kindersley Publication London, (1992).
Website/Link	https://www.forensicsciencesimplified.org/av/AudioVideo.pdf

Mapping with Programme Outcomes

	PO01	**PO02**	**PO03**	**PO04**
CO1	S	S	S	-
CO2	S	M	M	S
CO3	S	L	L	M
CO4	M	S	M	S
CO5	S	L	S	S

S-Strong , M- Medium , L – Low

Subject Title	Audio-video analysis Lab	Semester	IV
Subject Code	24U4CYCP04	Specialization	NA
Type	Core: Practical	L:T:P:C	0:0:5:3

Learning Objectives:

- To Apply Video Preprocessing Techniques.
- To Identify Human and Object.
- Audio and Video Enhancement Techniques.
- To apply Image Content Analysis
- Video Stabilization and Sharpening

COURSE OBJECTIVES

CO No.	CO Statement	Knowledge Level
CO1	To Apply Video PreProcessing Techniques	K1
CO2	To Identify Human and Object.	K1
CO3	Audio and Video Enhancement Techniques	K2
CO4	To apply Image Content Analysis	K3
CO5	Video Stabilization and Sharpening	K4

1. Video preprocessing
2. Working Copy Creation
3. Object identification
4. Human Being identification
5. Audio Enhancement
6. Video Enhancement
7. Image Content Analysis
8. Interlacing Techniques
9. Video Stabilization and Sharpening
10. Masking

SEMESTER V

Subject Title	VULNERABILITY ASSESSMENT AND PENETRATION TESTING	Semester	V
Subject Code	24U5CYC06	Specialization	NA
Type	Core: Theory	L:T:P:C	5:0:0:4

Course objective:

- To think and work like an ethical penetration tester, implementing a repeatable and mature methodology that is tailored for each assessment.
- To successfully identify vulnerabilities, score their risk, and explain mitigations with a given target.
- To responsibly disclose findings in a professional report that can be used to recreate the exploit, explain the impact to the target, and prioritize each finding

CO No.	CO Statement	Knowledge Level
CO1	Understand vulnerability and its implications.	K1
CO2	Formulate the techniques of information gathering	K1
CO3	Discover the system hacking methods and its advancement	K2
CO4	Perform vulnerability assessments and pen testing	K3
CO5	Evaluate the societal role of hacking from a social, ethical and economic standpoint	K4

Unit	Contents	No. of Sessions
I	**PENETRATION TESTING METHODOLOGY**: Types of penetration testing, Vulnerability assessment v/s penetration testing, Security testing methodologies: OSSTMM, ISSAF, OWASP, WASC-TC, Back tracking testing methodology, Ethics.	12
II	**FOOT PRINTING & SOCIAL ENGINEERING**: Information gathering methodologies- Competitive Intelligence- DNS Enumerations- Social Engineering attacks.	12
III	**SCANNING & ENUMERATION** :Port Scanning-Network Scanning-Vulnerability Scanning- NMAP scanning tool OS Fingerprinting- Enumeration	12
IV	**SYSTEM HACKING**: Password cracking techniques- Key loggers- Escalating privileges Hiding Files Steganography technologies- Countermeasures.	12
V	**SNIFFERS & SQL INJECTION**: Active and passive sniffing- ARP Poisoning-Session Hijacking- DNS Spoofing Conduct SQL Injection attack - Countermeasures.	12

Learning Resources	
Text Books	1. Shakeel Ali &Tedi Heriyanto, "Backtrack -4: Assuring security by penetration

	testing", PACKT Publishing., 2011. 2. Kimberly Graves, "CEH: Official Certified Ethical Hacker Review Guide", Wiley Publishing Inc.,
Reference Books	• Penetration Testing : Hands on Introduction to Hacking " , GeorgiaWeidman,1stEdition,NoStarchPress. • ThePenTesterBlueprintStartingaCareerasanEthicalHacker",L.Wylie,KimCrawly,1stEdition,WileyPublications
Website/Link	https://www.tutorialspoint.com/penetration_testing/penetration_testing_vulnerability_assessment.htm

Mapping with Program Outcomes:

COs/POs / PSOs	PO1	PO2	PO3	PO4	PO5	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	L	M	L	L	L	L	L	L	M	L
CO2	L	L	L	L	L	M	M	M	M	S
CO3	M	M	M	M	M	S	L	M	M	L
CO4	L	L	M	M	S	S	L	M	M	S

S – Strong; **L** – Low; **M** – Medium

Subject Title	VULNERABILITY ASSESSMENT AND PENETRATION TESTING LAB	Semester	V
Subject Code	24U5CYCP05	Specialization	NA
Type	Core: Practical	L:T:P:C	0:0:4:4

Course objective:

- To think and work like an ethical penetration tester, implementing a repeatable and mature methodology that is tailored for each assessment.
- To successfully identify vulnerabilities, score their risk, and explain mitigations with a given target.
- To responsibly disclose findings in a professional report that can be used to recreate the exploit, explain the impact to the target, and prioritize each finding

CO No.	CO Statement	Knowledge Level
CO1	Understand vulnerability and its implications.	K1
CO2	Formulate the techniques of information gathering	K1
CO3	Discover the system hacking methods and its advancement	K2
CO4	Perform vulnerability assessments and pen testing	K3
CO5	Evaluate the societal role of hacking from a social, ethical and economic standpoint	K4

1. Information gathering through Social Engineering
2. Understanding Data Packet Sniffers
3. Understand the process of phishing attacks and the security levels
4. Implementing Web Data Extractor and Web site watcher.
5. Vulnerability scanning using tool Nessus.
6. Vulnerability assessment using tool Burp Suite.
7. Penetration Testing and its justification
8. Performing sql injection attacks.
9. Denial of Service and Session Hijacking using Tear Drop, DDOS attack.
10. Windows Hacking – NT LAN Manager, Secure 1 password recovery

Subject Title	**ELECTIVE-I** Ethical Hacking	Semester	V
Subject Code	24U5CYC07	Specialization	NA
Type	Elective : Theory	L:T:P:C	5:0:0:4

Course objective:

1. Build basic programs using fundamental programming constructs like variables, conditional logic, looping, and functions
2. Work with user input to create fun and interactive programs
3. Create simple games with images, animations, and audio using our custom beginner-friendly programming
4. Describe the core syntax and semantics of Python programming language.

CO No.	CO Statement	Knowledge Level
CO1	Define the Overview of Computer Networks &Hacking Techniques	K1
CO2	Understand the concepts of Threats & Attack Vectors	K2,K4
CO3	Define the Web based & Social attacks	K3
CO4	Apply Network forensics &Outline industrial policy standards	K4
CO5	Discover the of Vulnerability Assessment, Penetration Testing	K4
Unit	Contents	No. of Sessions
I	Overview of Networking &Ethical Hacking: IntroductiontoNetwork and Communication technologies – Overview of OSI Model and TCP/IP Protocol. IP Addressing and NAT. Routers and Routing Protocols. Important Terminologies - Asset, Vulnerability, Threat, Risk. Introduction to Hacking, Phases involved in Hacking: Foot printing, Scanning, System Hacking, Session Hijacking. Basic Cryptography Concepts- Symmetric Encryption Algorithms, Purpose of Cryptography, Data Encryption Standard (DES), Triple DES, Advanced Encryption Standard (AES).Penetration Testing– Methodologies: OSSTMM, NIST, OWASP.	12
II	Threats, Vulnerabilities and Attacks: Network threats and vulnerabilities, Types of networkattacks-eavesdropping, spoofing, modification, Cross-sitescripting, DNSSpoofing, ARPPoisoning, Web Jacking. Evading anti viruses and firewalls, Tools used; Attacks on Wireless Networks. CIA Triad, Security Concepts-exploit, threat, vulnerability, risk, and attack.MalwareTerminology: Root kits, Trapdoors, Botnets, and Key loggers. Active and Passive Security Attacks. Teardrop, DoS, DDoS, XSS, SQL injection, MITM Attack. Evading IDS, Firewall and Honey pots. Intrusion Detection Systems (IDS),Intrusion Detection Tools.	12

III	Web based Attacks & web Security – Firewalls, IDS, IPS, IDPS – Types and Technologies .Passwords, Cryptographic authentication protocol, Kerberos, X.509 LDAP Directory. Digital Signatures. Web Security, SSL Encryption, TLS, SET. Trusted systems–Electronic payment protocols, Virtualprivatenetworks.WebserverAttacks, DNSServerHijacking, DirectoryTraversal Attacks, MITM /Sniffing Attack, Phishing Attacks, Website Defacement, Web server Misconfiguration, HTTP Response Splitting Attack, SSHBrute-force Attack, WebApplicationAttacks, SessionManagementAttack, SQLInjectionAttacks.	12
IV	Network Forensics, System Hacking & VAPT: Monitoring of computer network and activities,Live Packet Capturing and Analysis. Searching and collection of evidences from the network. Network Intrusion Detection and Analysis: SQL Injection, Event Log Aggregation – role of logsinforensicanalysis,toolsandtechniques.Investigatingnetworkattacks.PasswordCracking, Malware Threats, Trojan Concept, Virus and Worms Concepts, Virus Analysis and DetectionMethods,Malware Analysis.DoS/DDoS Concepts, Identity Theft Overview.	12
V	VAPT, Incident Response and Industrial Policy Standards: Vulnerability Assessment, Types ofVulnerabilityAssessment, PenetrationTesting, TypesofPenetrationTesting, PhasesofPenetrationTesting, Security Testing Methodology. Vulnerability Assessment versus Penetration Testing. Automated Assessment Tools – Incident Response Planning for disaster and recovery - Evidence Handling – Requirements of Regulated Industries – IntrusionDetectionSystems. InformationSecurityLawsandStandards: PaymentCardIndustryDataSecurityStandard (PCI-DSS), ISO/IEC 27001:2013, Health Insurance Portability and Accountability Act (HIPAA), SarbanesOxleyAct(SOX).InformationSecurityPolicies,TypesofSecurityPolicies.	12

Learning Resources

Text Books	1. Hacker Techniques, Tools and Incident Handling, Sean Philip Oriyano and Michael Gregg. 2. William Stallings;"Network Security Essentials", 3rdEdition, Pearson Education, 2006. 3. "Ethical Hacking and Countermeasures (Book1)", EC-Council, Publisher: Course Technology; 2ndedition–2016. 4. 4.AtulKahate;"CryptographyandNetworkSecurity"McGrawHillEducation(India),2008
Reference Books	5. CEHv10:CertifiedEthicalHacker-Version10Study-14May2018. 6. ShonHarris;"Allin OneCISSP,ExamGuideSixthEdition",McGrawHill, 2013. 7. SherriDavidoffandJonathanHam;"NetworkForensics–TrackingHackersthroughCyberspace",PearsonPublications,2012.
Website/Link	http://bedford-computing.co.uk/learning/wp-content/uploads/2015/10/Introduction-to-Computer-Science-Using-Python.pdf

Subject Title	ETHICAL HACKING LAB	Semester	V
Subject Code	24U5CYCP06	Specialization	NA
Type	Practical	L:T:P:C	0:0:4:4

Learning Objectives:

- To explain ethical hacking methodology
- To use techniques, skills and modern tools necessary to gather the information and to identify the vulnerabilities.

Course Outcomes:

CO No.	CO Statement	Knowledge Level
CO1	Define the Overview of Computer Networks	K1
CO2	Outline the concepts of Networking	K1
CO3	Define the Social attacks	K2
CO4	Apply Network forensics	K1
CO5	Outline industrial policy standards	K3

1. Port Scanning using NMap, Super scan
2. Enumeration-SNMP, SMTP, Unix / Linux, LDAP, NTP
3. Monitoring Live Network capturing packets and analyzing over the live network using Wire shark
4. Vulnerability Scanning
5. Firewall, Intrusion detection and Honey pots
6. Password Guessing and Password cracking
7. Buffer over flow attacks
8. Monitoring Network Communication: Working with Trojans, Backdoors and sniffer
9. Clients id script injection to a web application using XSS
10. Wireless Network attacks, Bluetooth attacks
11. Website mirroring using HTTrack and hosting on a Local Network
12. Penetration testing and justification of penetration testing through risk analysis, SQLinjection Attacks
13. Steganographic Tools
14. Cryptanalysis Tools

Subject title	Advanced Excel	Semester	V
Subject code	24U5CYS03	Specialization	CA
Type	SBEC : Theory	L:T:P:C	2:0:0:2

COURSE OBJECTIVE:

The objective of this course is to help the students learn the advanced features of Excel, to summarise, analyse, explore, and present visualisations of data in the form of charts, graphs.

CO NO.	CO STATEMENT	KNOWLEDGE LEVEL
CO1	Handle large amounts of data	K1
CO2	Aggregate numeric data and summarise into categories and subcategories	K2
CO3	Filtering, sorting, and grouping data or subsets of data	K3
CO4	Create pivot tables to consolidate data from multiple files	K4
CO5	Presenting data in the form of charts and graphs	K4

UNIT	CONTENTS	NO. OF SESSIONS
I	Basics of Excel – Customizing common options – Absolute and relative cells – Protecting and un-protecting worksheets and cells – Working with Functions – Writing conditional expressions – logical functions – lookup and reference functions: VlookUP with Exact Match, Approximate Match, – Using VLookUP to consolidate Data from Multiple Sheets.	6
II	Data Validations - Specifying a valid range of values - Specifying a list of valid values – Specifying custom validations based on formula – Working with Templates – Designing the structure of a template - Sorting and Filtering Data - Sorting tables – multiple-level sorting - custom sorting - Filtering data for selected view - advanced filter options.	6
III	Creating Pivot tables Formatting and customizing Pivot tables – advanced options of Pivot tables – Pivot charts – External data sources – data consolidation feature to consolidate data – Show Value As % of Row, % of Column, Running Total, Compare with Specific Field – Viewing Subtotal under Pivot.	8
IV	More Functions: Date and time functions – Text functions – Database functions – Power Functions – Formatting Using auto formatting option for worksheets – Using conditional formatting option for rows,	4

	columns and cells – WhatIf Analysis – Data Tables.	
V	Charts: Formatting Charts – 3D Graphs – Bar and Line Chart together – Secondary Axis in Graphs – Sharing Charts with PowerPoint / MS Word, Dynamically – Inline Charts, data Charts – Overview of all the new features.	**6**

LEARNING RESOURCES	
Text books	1. Excel 2019 All-in-One For Dummies – 2018- Greg Harvey
Reference books	1.Microsoft Excel 2019 Pivot Table Data Crunching-2019,Bill Jelen and Michael Alexander 2. **"Excel 2019 Bible"Author**: Michael Alexander, Richard Kusleika, and John Walkenbach,**Publisher**: Wiley,**Publication Year**: 2018 **3."Excel Power Pivot & Power Query For Dummies" Author**: Michael Alexander **Publisher**: WileyN **Publication Year**: 2016
Website/link	1) https://www.tutorialspoint.com/advanced_excel/advanced_excel_tutorial.pdf 2) https://www.coursera.org/learn/excel-advanced 3) https://www.upgrad.com/blog/advanced-excel-formulas-a-must-know-for-all-professionals/

MAPPING WITH PROGRAMME OUTCOMES

	PO01	**PO02**	**PO03**	**PO04**
CO1	S	S	S	-
CO2	S	M	M	S
CO3	S	L	L	M
CO4	M	S	M	S
CO5	S	L	S	S

S-Strong , M- Medium , L – Low

Subject Title	Sentiment Analysis	Semester	VI
Subject Code	24U5CYS04	Specialization	CA
Type	SBEC : Theory	L:T:P:C	2:0:0:2

Course objective:

To introduce to computational study of people's opinions, sentiments, emotions, moods, and attitudes

CO No.	CO Statement	Knowledge Level
CO1	To understand the underlying structure of the problem commonly used to express opinions, sentiments, and emotions	K1
CO2	To understand the underlying structure of the language constructs commonly used to express opinions, sentiments, and emotions	K2,K4
CO3	To understand core areas of sentiment analysis	K3
CO4	To understand rules and extraction of entity in sentiment analysis	K4
CO5	To understand sentiment lexicon generation	K4

Unit	Contents	No. of Sessions
I	Introduction, Sentiment analysis applications, Sentiment analysis research, Sentiment analysis as mini-NLP,The Problem of Sentiment Analysis, Definition of opinion, Definition of opinionsummary.	6
II	Different types of opinions, Document Sentiment Classification, Supervised sentiment classification, Unsupervised sentiment classification, Sentiment rating prediction, Cross-Domain Sentiment Classification, Cross-Language Sentiment Classification.	6
III	Sentence Subjectivity and Sentiment Classification, Subjectivity, Sentence Subjectivity Classification, Sentence Sentiment Classification, Aspect Sentiment Classification	6
IV	Rules of Sentiment composition, Negation and Sentiment, Aspect and Entity Extraction, Frequency based aspect extraction, Exploring syntactic relations, Using supervised learning	6
V	Sentiment Lexicon Generation, Dictionary based approach, Corpus based approach, Sentimentword embedding, Analysis of Comparative Opinions, Problem definition, Identifying comparative sentences, Identifying the preferred entity set, Special types of comparison	6

Learning Resources	
Text Books	Sentiment Analysis: Mining Opinions, Sentiments, and Emotions, by Bing Liu
Reference Books	1. Sentiment Analysis in Social Networks By Federico Pozzi, Elisabetta Fersini, EnzaMessina, Bing Liu · 2016 2. Sentiment Analysis for Social Media, Antonio Moreno, Carlos A. Iglesias, MDPI 2020 3. New Opportunities for Sentiment Analysis and Information Processing, AakanshaSharaff, G. R. Sinha, Surbhi Bhatia, IGI Global, 2021 4. Sentiment Analysis and Knowledge Discovery in Contemporary Business, Dharmendra Singh Rajput, Ramjeevan Singh Thakur, S. Muzamil Basha, IGI Global, 2018
Website/Link	https://www.analyticsvidhya.com/blog/2021/06/nlp-sentiment-analysis/ https://www.geeksforgeeks.org/what-is-sentiment-analysis/

Mapping with Programme Outcomes

	PO01	PO02	PO03	PO04
CO1	S	S	S	-
CO2	S	M	M	S
CO3	S	L	L	M
CO4	M	S	M	S
CO5	S	L	S	S

S-Strong , M- Medium , L – Low

SEMESTER VI

Subject Title	PRESERVING AND RECOVERING OF DIGITAL EVIDENCE	Semester	VI
Subject Code	24U6CYC08	Specialization	NA
Type	Core: Theory	L:T:P:C	5:0:0:4

Course objective:

- To learn to analyze different laws related to computer crime, how to Secure Digital Evidences, to understand the Investigation.

CO No.	CO Statement	Knowledge Level
CO1	It helps to recover, analyze, and preserve computer and related materials in such a manner that it helps the investigation agency to present them as evidence in a court of law.	K1
CO2	It helps to postulate the motive behind the crime and identity of the main culprit	K1
CO3	Designing procedures at a suspected crime scene which helps you to ensure that the digital evidence obtained is not corrupted	K2
CO4	Data acquisition and duplication: Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.	K3

Unit	Contents	No. of Sessions
I	Digital Investigation : Digital evidence and computer crime, history and terminals of computer crime investigation, technology and law, the investigate process, investigate reconstruction, modus operandi, motive and technology, digital evidence in the court room.	**12**
II	Computer basics for digital investigators : applying forensic science to computers, forensic examination of windows systems, forensic examination of Unix systems, forensic examination of Macintosh systems, forensic examination of handheld devices.	**12**
III	Duplication and Preservation of Digital Evidence : Data Recovery – Evidence Collection and Data Seizure - Preserving the Digital Crime Scene, Computer Evidence Processing Steps, Legal Aspects of Collecting And Preserving Computer Forensic Evidence. Computer Image Verification and Authentication : Special Needs of Evidential Authentication, Practical Considerations, Practical Implementation.	**12**
IV	Investigating Computer Crime : Investigating computer intrusions, investigating cyberstalking, digital evidence as alibi.	**12**

V	Guidelines : Handling the digital crime scene – digital evidence examination guidelines.	**12**

Learning Resources	
Text Books	1. Digital Evidence and Computer Crime Forensic science, Computers and Internet, Eoghan Casey,Second Edition, 2011 ,Elsevier Academic Press. 2. A Electronic Discovery and Digital Evidence in a Nut Shell-Daniel J Capra,Shira A scheindlin,-Third Edition, 2009 The Sedona Conerence-Academic Press. 3. The Best Damn Cybercrime and Digital Forensics Book Perio,Jack Wiles, Anthony Reyes , Jesse Varsalone,2007 Syngress Publishing. 4. Computer Evidence and Computer Crime: Forensic Science, Computers, and the Internet.Casey, Eoghan, 2000 , Cambridge University Press. 5. Computer Forensics Computer Crime Scene Investigation,Vacca, John R. ,2002,Charles River Media.

Mapping with Programme Outcomes

COs/POs/ PSOs	PO1	PO2	PO3	PO4	PO5	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	L	M	L	L	L	L	L	L	M	L
CO2	L	L	L	L	L	M	M	M	M	S
CO3	M	M	M	M	M	S	L	M	M	L
CO4	L	L	M	M	S	S	L	M	M	S

S-Strong , M- Medium , L – Low

Subject Title	MALWARE ANALYSIS	Semester	VI
Subject Code	24U6CYC09	Specialization	NA
Type	Core: Theory	L:T:P:C	5:0:0:3

Course objective:

- To learn the different perspective of malwares, designs, implications and analysis in all respective.

CO No.	CO Statement	Knowledge Level
CO1	Define malware and its life cycle process	K1
CO2	Outline the working principle of malwares	K1
CO3	Summaries the designs and implications of malwares.	K2
CO4	Ability to examine different kinds the malwares.	K3

Unit	Contents	No. of Sessions
I	Fundamentals of Malware Analysis (MA), Reverse Engineering Malware (REM) Methodology, Brief Overview of Malware analysis lab setup and configuration, Introduction to key MA tools and techniques, Behavioral Analysis vs. Code Analysis, Resources for Reverse - Engineering Malware (REM) Understanding Malware Threats, Malware indicators, Malware Classification, Examining Clam AV Signatures, Creating Custom Clam AV Databases, Using YARA to Detect Malware Capabilities, Creating a Controlled and Isolated Laboratory, Introduction to MA Sandboxes, Ubuntu, Zeltser's REMnux, SANS SIFT, Sandbox Setup and Configuration New Course Form, Routing TCP/IP Connections, Capturing and Analyzing Network Traffic, Internet simulation usingINetSim, Using Deep Freeze to Preserve Physical Systems, Using FOG for Cloning and Imaging Disks, Using MySQL Database to Automate FOG Tasks.	12
II	Scanners: Virus Total, Jotti, and NoVirus Thanks, Analyzers: Threat Expert, CWSandbox,Anubis, Joebox, Dynamic Analysis Tools: Process Monitor, Regshot, HandleDiff, Analysis Automation Tools: Virtual Box, VM Ware, Python , Other Analysis Tools Malware Forensics: Using TSK for Network and Host Discoveries, Using MicrosoftOffline API to Registry Discoveries , Identifying Packers using PEiD, Registry Forensicswith Reg Ripper Plu-gins:, Bypassing Poison Ivy's Locked Files, Bypassing Conficker'sFile System ACL Restrictions, Detecting Rogue PKI Certificates.	12
III	Malware and Kernel Debugging: Opening and Attaching to Processes, Configuration of JIT Debugger for Shellcode Analysis, Controlling Program Execution, Setting and Catching Breakpoints, Debugging with Python Scripts and Py Commands, DLL Export Enumeration, Execution, and Debugging, Debugging a VMware Workstation Guest (on Windows), Debugging a Parallels Guest (on Mac OS X). Introduction to WinDbg Commands and Controls, Detecting Rootkits with WinDbgScripts, Kernel	12

	Debugging with IDA Pro	
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.	**12**
V	Memory Forensics and Volatility: Dumping with MoonSols Windows Memory Toolkit, Accessing VM Memory Files Overview of Volatility, Investigating Processes in Memory Dumps, Code Injection and Extraction, Detecting and Capturing Suspicious Loaded DLLs, Finding Artifacts in Process Memory, Identifying Injected Code with Malfind andYARA. Using WHOIS to Research Domains, DNS Hostname Resolution, Querying, Passive DNS, Checking DNS Records, Reverse IP Search New Course Form, Creating Static Maps, Creating Interactive Maps.	**12**

Learning Resources	
Text Books	1. Michael Sikorski, Andrew Honig, Practical Malware Analysis: The Hands-On Guide to DissectingMalicious Software publisher William Pollock, 2012. 2. Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters, The Art of Memory Forensics:Detecting Malware and Threats in Windows, Linux, and Mac Memory, 1st Edition, 2014. 3. Mark.A .Ludwig, "The Giant black book of computer viruses, Create Space Independent PublishingPlatform, 2 nd edition, ISBN 10: 144140712X, 2009.

Mapping with Programme Outcomes

COs/POs/ PSOs	PO1	PO2	PO3	PO4	PO5	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	L	M	L	L	L	L	L	L	M	L
CO2	L	L	L	L	L	M	M	M	M	S
CO3	M	M	M	M	M	S	L	M	M	L
CO4	L	L	M	M	S	S	L	M	M	S

S-Strong , M- Medium , L – Low

Subject Title	MOBILE DEVICES FORENSIC LAB	Semester	VI
Subject Code	24U6CYCP07	Specialization	NA
Type	Core: Practical	L:T:P:C	0:0:4:3

Course objective:

- To enable the students to learn the basic mobile forensic tools and techniques.

CO No.	CO Statement	Knowledge Level
CO1	Define the mobile forensics	K1
CO2	Outline the techniques behind retrieval of device information.	K1
CO3	Define the data recovery techniques.	K2
CO4	Apply different Mobile forensics tools.	K3

Unit	Contents	No. of Sessions
I	Screen lock bypassing techniques	5
II	Extracting device information	5
III	Gaining root access in Android	5
IV	Jailbreak iOS devices	5
V	Imaging a memory (SD) card	5
VI	Data Recovery Techniques	5
VII	Extracting details from Android devices using AFLogical tool	5
VIII	Extracting data from a mobile phone such as deleted data, call history, data files, passwords, data from various apps using tool MOBILedit	5
IX	Analyzing an Android in ADB.	5
X	Acquisition of volatile memory from Linux based devices using tool LiMe	5

Learning Resources	
Reference Books	1. Practical Mobile Forensics: Dive Into Mobile Forensics on IOS, Android, Windows, and Blackberry devices with This Action-Packed Practical Guide Paperback – 21 July 2014 by Satish Bommisetty ,Rohit Tamma ,Heather Mahalik 2. Practical Mobile Forensics- Third Edition: A hands-on guide to mastering mobile forensics for the iOS, android, and the Windows Phone platforms, 3rd Edition by Rohit Tamma Oleg Skulkin Heather Mahalik SatishBommisetty.

Mapping with Programme Outcomes

COs/POs/ PSOs	PO1	PO2	PO3	PO4	PO5	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	L	M	L	L	L	L	L	L	M	L
CO2	L	L	L	L	L	M	M	M	M	S
CO3	M	M	M	M	M	S	L	M	M	L
CO4	L	L	M	M	S	S	L	M	M	S

S-Strong , M- Medium , L – Low

Electives

Subject Title	Elective – I Trends in Digital Forensic	Semester	III
Subject Code	24U3CYDE01	Specialization	NA
Type	Elective : Theory	L:T:P:C	4:0:0:4

Course objective:

- The students will understand the recent trends of digital forensics in various domains.
- To emphasize the fundamentals and importance of digital forensics
- To apply open-source forensics tools to perform digital investigation and understand the underlying theory behind these tools.
- Knowledge on digital forensic

CO No.	CO Statement	Knowledge Level
CO1	Understand Digital forensics for IoT-based networks	K1
CO2	To understand Digital forensics for software privacy and security	K1
CO3	It provides conceptual understanding of Digital forensics for artificial intelligence and Big Data	K2
CO4	It provides conceptual understanding of Digital forensics for Big Data	K3
CO5	To understand and analyze on Digital forensics of quantum computing	K4
Unit	**Contents**	**No. of Sessions**
I	Digital forensics for IoT-based networks-Applying Digital Forensics to IoT and WSNs- Challenges in IoT and WSN Forensics- Device Level Investigation-Network Level Investigation-Cloud Level Investigation.	12
II	Digital forensics for software privacy and security- Introduction-Data Collection- current trend of privacy in digital forensics-Privacy prevention in Users perspective-Privacy prevention in forensics investigator perspective- Privacy prevention in technologies perspective.	12
III	Digital forensics for artificial intelligence- introduction- Artificial intelligence- Representation of knowledge-Explaining the reasoning process- Knowledge discovery-Adaption.	12
IV	Big data and digital forensics-How Big Data Is Helping Cybersecurity- The Analysis of Current and Historical Data for Threat Visualization- Security controls in big data tools-Data Authenticity and Integrity	12
V	Digital forensics of quantum computing- Introduction- Quantum Computation- Quantum Forensics- Security and Privacy Aspects Using Quantum Internet-The Role of Quantum Computing in Software Forensics	12

	and Digital Evidence	

Learning Resources	
Text Books	• Digital Forensics for IoT and WSNs"- Research paper by Umit Karabiyik, Kemal Akkaya A Survey on Privacy Issues in Digital Forensics – Research paper by Ali Dehghantanha, Asou Aminnezhad, Mohd Taufik Abdullah • THE USE OF ARTIFICIAL INTELLIGENCE IN DIGITAL FORENSICS: AN INTRODUCTION – Research paper by Dr Faye Mitchell • BIG DATA ANALYTICS FOR CYBER SECURITY - Bharath Krishnappa • Digital Quantum Forensics: Challenges and Responses -Research paper by Richard Overill
Reference Books	• Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd Edition Author: Eoghan Casey Publisher: Academic Press ISBN: 9780123742681
Website/Link	https://codehs.com/tutorial/jennifer/digital-forensics

Subject Title	ELECTIVE-I : OPEN SOURCE TECHNOLOGY	Semester	III
Subject Code	24U3CYDE02	Specialization	NA
Type	Elective : Theory	L:T:P:C	4:0:04

Course objective:

1. Introduces Open Source methodologies.
2. To make the students to gain experience using open source tools, languages and frameworks to prepare forcareers in software development.

CO No.	CO Statement	Knowledge Level
CO1	Understanding the concepts of softwares	**K1,K2**
CO2	Understanding Open source History and Initiatives	**K3**
CO3	Importance of Communities in Open software	**K1,K2**
CO4	Analyze the servers	**K1,K3, K5**
CO5	Understand the concept of ethics in open source	**K1,K4**
Unit	Contents	No. of Sessions
I	Introduction : Open Source, Free Software, Free Software vs. Open Source software, Public Domain Software, FOSS does not mean no cost. History : BSD, The Free Software Foundation and the GNU Project..	12
II	Open Source History, Initiatives, Principle and methodologies. Philosophy : Software Freedom, Open Source Development Model Licences and Patents: What Is A License, Important FOSS Licenses (Apache,BSD,GPL, LGPL), copyrights and copylefts, Patents Economics of FOSS : Zero Marginal Cost, Income-generation opportunities, Problems with traditional commercial software, Internationalization	12
III	Community Building: Importance of Communities in Open Source Movement- JBoss Community- Starting and Maintaining an Open Source Project - Open Source Hardware	12
IV	Apache HTTP Server and its flavors- WAMP server (Windows, Apache, MySQL, PHP)- Apache, MySQL, PHP, JAVA as development platform	12
V	Open source vs. closed source Open source government, Open source ethics. Social and Financial impacts of open source technology, Shared	12

	software, Shared source.	

Learning Resources	
Text Books	1. Sumitabha Das "Unix Concepts and Applications, Tata McGraw Hill Education 006 2.The Official Ubuntu Book, 8th Edition 3.Kailash Vedera, Bhavyesh Gandhi, "Open Source Technology", University Science press
Reference Books	4.Paul Kavanagh, "Open Source Software: Implementation and Management",Elsevier Digital Press
Website/Link	The Linux Documentation Project : http://www.tldp.org Docker Project Home : http://www.docker.com

CO Number	PO1	PO2	PO3	PO4
CO1	**S**	**L**	**M**	**L**
CO2	**S**	**M**	**M**	**L**
CO3	**M**	**S**	**M**	**M**
CO4	**S**	**S**	**M**	**M**
CO5	**L**	**M**	**M**	**S**

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

Subject Title	**ELECTIVE-II :** Cyber Forensic	Semester	IV
Subject Code	24U4CYDE03	**Specialization**	**NA**
Type	**Elective : Theory**	**L:T:P:C**	**4:0:0:4**

Course objective:

- Discuss the security issues over network layer and transport layer
- Apply security principles in the application layer
- Explain computer forensics
- Use forensics tools Analyze and validate forensics data
- Apply Data Hiding Techniques

CO No.	CO Statement	Knowledge Level
CO1	Discuss the security issues over network layer and transport layer	K1
CO2	Apply security principles in the application layer	K1
CO3	Explain computer forensics	K2
CO4	Use forensics tools Analyze and validate forensics data	K3
CO5	Apply Data Hiding Techniques	K4
Unit	**Contents**	**No. of Sessions**
I	NETWORK LAYER SECURITY &TRANSPORT LAYER SECURITY: IPSec Protocol - IP Authentication Header - IP ESP - Key Management Protocol for IPSec .Transport layer Security: SSL protocol, Cryptographic Computations – TLS Protocol.	12
II	PGP - S/MIME - Internet Firewalls for Trusted System: Roles of Firewalls – Firewall related terminology- Types of Firewalls - Firewall designs - SET for E-Commerce Transactions.	12
III	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.	12
IV	EVIDENCE COLLECTION AND FORENSICS TOOLS Processing Crime and Incident Scenes – Working with Windows and DOS Systems. Current Computer Forensics Tools: Software/ Hardware Tools.	12
V	ANALYSIS AND VALIDATION Validating Forensics Data – Data Hiding	12

	Techniques – Performing Remote Acquisition – Network Forensics – Email Investigations – Cell Phone and Mobile Devices Forensics.	

Learning Resources	
Text Books	1.Man Young Rhee, "Internet Security: Cryptographic Principles", "Algorithms and Protocols", Wiley Publications, 2003. 2.Nelson, Phillips, Enfinger, Steuart, "Computer Forensics and Investigations", Cengage Learning, India Edition, 2008.
Reference Books	3.John R.Vacca, "Computer Forensics", Cengage Learning, 2005 4. Richard E.Smith, "Internet Cryptography", 3 rd Edition Pearson Education, 2008. 5. MarjieT.Britz, "Computer Forensics and Cyber Crime": An Introduction", 3 rd Edition, Prentice Hall, 2013.
Website/Link	• https://annamalaiuniversity.ac.in/studport/download/engg/it/resources/Cyber%20Forensics.pdf • https://www.mgu.ac.in/uploads/2019/08/cyber-forensic.pdf?x82015

CO Number	PO1	PO2	PO3	PO4
CO1	S	L	M	L
CO2	S	M	M	L
CO3	M	S	M	M
CO4	S	S	M	M
CO5	L	M	M	S

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

Subject Title	**ELECTIVE-II :** E-Commerce & Digital Payment	Semester	IV
Subject Code	24U4CYDE04	Specialization	NA
Type	Elective : Theory	L:T:P:C	4:0:0:4

Course objective:

1. This course provides an introduction to information systems for business and management. It is designed to familiarize students with organizational and managerial and technical foundations of systems.
2. Digital transactions are to reduce the costs and risks of handling cash. focuses on learning of new technologies.

CO No.	CO Statement	Knowledge Level
CO1	Determine key terminologies and concepts including IT,marketing, management, economics, accounting, finance in the major areas of business.	K1
CO2	Design, develop and implement Information Technology solutions for business problems.	K2,K3
CO3	Analyze the impact of E-commerce on business models and strategy.	K2,K4
CO4	Understand ethical issues that occur in business, evaluatealternative courses of actions and evaluate the implications of those actions .	K4
CO5	Assess electronic payment systems. Describe Internet tradingrelationships including Business to Consumer, Business-to- Business, Intra-organizational.	K4,K5
Unit	**Contents**	**No. of Sessions**
I	E-commerce: The revolution is just beginning, Ecommerce: ABrief History, Understanding Ecommerce: organizing Themes.	12
II	E-commerce Business Models, Major Business to Consumer (B2C) business models, Major Business to Business (B2B) business models, Business models in emerging E-commerce areas, How the Internet and the web change business: strategy, structure and process, The Internet: Technology Background, TheInternet Today, Internet II-The Future Infrastructure, The World Wide Web, The Internet and the web : features.	12

III	A systematic Approach, The e-commerce security environment, Security threats in the e-commerce environment, Technology solution, Management policies, Business procedures, and public law.	12
IV	The Internet Audience and Consumer Behaviour, Basic Marketing Concepts, Internet Marketing Technologies, B2C and B2B E-commerce marketing and business strategies, The Retail sector, Analyzing the viability of online firms, E-commerce in action: E-tailing Business Models, Common Themes in online retailing, The service sector: offline and online, Online financial services, Online Travel Services, Online career services	12
V	Introduction to digital payment - different methods for digital payment - benefits of digital payment - Economic Progress -Payment Gateway.	12

Learning Resources

Text Books	1. Kenneth C. Laudon, "E-Commerce : Business, Technology, Society",5th Edition, Pearson, 2019. 2. S. J Joseph," E-Commerce: an Indian perspective", PHI. 5th Edition, 2010
Reference Books	1.Daniel Minoli & Emma Minoli, "Web Commerce Technology Handbook". TataMcGraw Hill – 2017. 2. Jaspal Singh , " Digital Payments in India -Background, Trends and Opportunities".
Website/Link	https://www.tutorialspoint.com/e_commerce/e_commerce_payment_systems.html

CO Number	PO1	PO2	PO3	PO4
CO1	**L**	**L**	**S**	**M**
CO2	**S**	**S**	**M**	**S**
CO3	**M**	**S**	**S**	**M**
CO4	**L**	**M**	**M**	**S**
CO5	**M**	**S**	**S**	**S**

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

Subject Title	**ELECTIVE -III :** Network Security	Semester	V
Subject code	**24U5CYDE05**	**Specialization**	**NA**
Type	**Core: Theory**	**L:T:P:C**	**5:0:0:4**

Course objective:

- This course facilitate to student to understand the concept of Vulnerability Assessment and Penetration Testing in all respect.
- Basics of Security and networks, information security

CO No.	CO Statement	Knowledge Level
CO1	To understand the basics of network security	K1
CO2	To discuss about the network security attacks and network security assessment	K1
CO3	To understand the concept of encryption mechanisms and its standards.	K2
CO4	To apply the defensive mechanisms for network security.	K3
CO5	To develop improved communication and collaborative skills in meeting security threats as a team member or team leader	K4

Unit	Contents	No. of Sessions
I	**Introduction**: - Types of Computer Networks, Reference Models - ISO-OSI Reference Model, TCP/IP Reference Model. Protocol Hierarchies Network layer: Routing Algorithm , ARP,RARP-Transport Layer: Elements of transport protocols, UDP, Segment Structure, TCP ,Service model, TCP Protocol, Application Layer: HTTP, DNS. Computer Security Concepts, the OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, A Model for Network Security. Access Control Models, Chinese Wall, Clark-Wilson, Bell-LaPadula, Non Interference and Role Base Model.	**12**
II	**Intrusion detection/prevention system**: Overview, Approached Used for IDS/IPS, Network Based IDS/IPS, Host based IDS/IPS, Honeypots, Detection of Polymorphic/Metamorphic worms, Distributed Intrusion Detection Systems and Standards, SNORT, Tipping Point IPS, McAfee Approach to IPS, Security Community's Collective Approach to IDS/IPS Hash and Authentication: Authentication, Hash functions, HMAC, Password Based Authentication, Password Based Encryption Standard, Automated Password	**12**

	Generator Standard, Password based Security protocols, One-time password and token, OPenID and OAuth..	
III	**Symmetric Key Ciphers and Wireless LAN security:** Block ciphers, Stream Ciphers, US Govt's Cryptography Module Standards, Side channel attacks and defensive mechanisms Public Key Cryptography, Infrastructure and Certificates: DH protocol, Digital Signatures, PKC characteristics, ECC, Certificates and Public Infrastructure, PKCS, X.509 certificate and Private Key File Formats, US Govt. Standards, Attacks which target PKI and certificates, Email security.	**12**
IV	**Secure Socket /Transport Layer Security (SSL/TLS) Protocols for Transport Layer Security:** Handshake Protocol and Attacks, Record Protocol, SSL/TLS, DTLS, US Govt. Recommendations, EV-SSL, Establishing a CA, Web server Certificate Setup and Client Computer Configuration, CA's self signed root certificate, Browser security configurations Virtual Private Networks for Network Layer Security: Network security, IPSec, IKE, Data Lin Layer VPN protocols, VPN Configuration Procedure Examples.	**12**
V	**Network Access Control and Wireless Network Security:** Overview of NAC, Kerberos, TPM, Multiple Factor Authentications, 802.1X, Enterprise Wireless Network Security Protocols Cyber Threats and Their Defense: DNS protection, Router security, Spam	**12**

Learning Resources	
Text Books	1. Network Security Essentials – William Stallings, Edition 4, Pearson Education, 2011 2. I Chwan-Hwa (John) Wu , J. David Irwin, Introduction to Computer Networks and Cybersecurity, CRC Press, 2013 3. Network Security Bible- Eric Cole, Ronald Krutz, James W. Conley, Edition 2, Wiley India Pvt Ltd, 2010 4. Cryptography and Network Security: Principles and Practice-William Stallings, Edition 6, Pearson education, 2013 5. "The Internet", Douglas. E. Comer, Prentice hall of India – Third Edition 6.Cyber Law Crimes, Barkhs and U. Rama Mohan, Third Edition ,2017,Asia Law House 7. Cyber Laws Simplified, Viveek Sood, Fourth reprint 2008,McGraw Hill.
Reference Books	• Information Security and cyber laws, Saurabh Sharma, student series, Vikas publication. Encryption, Ankit Fadia and J. Bhattacharjee, Vikas publication
Website/Link	https://nptel.ac.in/courses/106105031/ https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-858-computer-systems-security-fall-2014/index.htm https://www.edx.org/course/network-security-2

Subject Title	ELECTIVE -III :MOBILE COMPUTING	Semester	V
Subject Code	24U5CYSDE06	Specialization	NA
Type	Elective : Theory	L:T:P:C	5:0:0:4

COURSE OBJECTIVE:

1. To make the student to understand the concepts of mobile computing.
2. To familiar with the network protocol stack.
3. To be exposed to Ad-Hoc networks.
4. Gain knowledge about different mobile platforms and application development.

CO Number	CO Statement	Knowledge Level
CO1	Remember the basic concepts of mobile computing.	K1
CO2	Understanding mobile IP.	K1,K2
CO3	Apply Mobile Telecommunication system.	K3
CO4	Evaluate mobile ad hoc system.	K4
CO5	Implement mobile operating system.	K5

Unit	Contents	Levels	Sessions
I	Introduction-Mobile Computing – Mobile Computing Vs wireless Networking – Mobile Computing Applications – Characteristics of Mobile computing – Structure of Mobile Computing Application. MAC Protocols – Wireless MAC Issues. Fixed Assignment Schemes – Random Assignment Schemes – Reservation Based Schemes	K1	14
II	Mobile Internet Protocol and Transport Layer-Overview of Mobile IP – Features of Mobile IP – Key Mechanism in Mobile IP – route Optimization. Overview of TCP/IP – Architecture of TCP/IP- Adaptation of TCP Window – Improvement in TCP Performance.	K1,K2	18
III	Mobile Telecommunication System-Global System for Mobile Communication (GSM) – General Packet Radio Service (GPRS) – Universal Mobile Tele communication System (UMTS).	K3	18

IV	Mobile Ad-Hoc Networks-Ad-Hoc Basic Concepts – Characteristics – Applications – Design Issues – Routing – Essential of Traditional Routing Protocols –Popular Routing Protocols – Vehicular Ad Hoc networks (VANET) – MANET Vs VANET –Security.	**K4**	**18**
V	Mobile Platforms and Applications-Mobile Device Operating Systems – Special Constrains & Requirements – Commercial Mobile Operating Systems – Software Development Kit: iOS, Android, BlackBerry, Windows Phone – M-Commerce – Structure– Pros & Cons – Mobile Payment System – Security Issues.	**K5**	**18**
	Learning Resources		
Text Books	Prasant Kumar Pattnaik, Rajib Mall, ‒Fundamentals of Mobile Computing‖, PHI Learning Pvt. Ltd, New Delhi 2012.		
Reference Books	1. Jochen H. Schller, ‒Mobile Communications‖, Pearson Education, New Delhi, 2007, 2nd Edition. 2. Dharma Prakash Agarval, Qing and An Zeng, "Introduction to Wireless and Mobile systems", Thomson Asia Pvt Ltd. 2005. 3. Uwe Hansmann, LotharMerk, Martin S. Nicklons and Thomas Stober, ‒Principles of Mobile Computing‖, Springer 2003.		
Website / Link	NPTEL & MOOC courses titled Mobile Computing 1. https://nptel.ac.in/courses/106/106/106106147/		

Subject Title	ELECTIVE IV-ARTIFICIAL INTELLIGENCE & KNOWLEDGE REPRESENTATION	Semester	V
Subject Code	24U5CYDE07	Specialization	NA
Type	Elective : Theory	L:T:P:C	5:0:0:4

Course objective:

- This course introduces the basic concepts and techniques of Artificial Intelligence (AI). The course aims to introduce intelligent agents and reasoning, heuristic search techniques, game playing, knowledge representation, reasoning with uncertain knowledge.

CO No.	CO Statement	Knowledge Level
CO1	Identify problems that are amenable to solution by specific AI methods.	K1
CO2	Represent knowledge in Prolog and write code for drawing inferences	K1
CO3	Identify appropriate AI technique for the problem at hand	K2
CO4	Compare strengths and weaknesses of different artificial Intelligence techniques	K3
CO5	Sensitive towards development of responsible Artificial Intelligence	K4

Unit	Contents	No. of Sessions
I	**Introduction**: Introduction to artificial intelligence-problem solving using search-Heuristic Search Techniques-Adversarial search-games-optimal decision in games-alpha beta pruning-stochastic games	12
II	**Knowledge Representation**: Propositional logic, first order predicate logic, resolution principle, unification, semantic nets, conceptual dependencies, frames, scripts, production rules, conceptual graphs.	12
III	**Reasoning with Uncertain Knowledge**: Uncertainty, non-monotonic reasoning, truth maintenance systems, default reasoning and closed world assumption, Introduction to probabilistic reasoning, Bayesian probabilistic inference, introduction to fuzzy sets and fuzzy logic, reasoning using fuzzy logic.	12
IV	**Problem Solving and Searching Techniques**: Problem characteristics, production systems, control strategies, breadth first search, depth first search, hill climbing and its variations, heuristics search techniques: best first search, A* algorithm, constraint satisfaction problem, means-end analysis.	12
V	**Game Playing**: introduction to game playing, min-max and alpha-beta pruning algorithms. Prolog Programming: Introduction to Programming in Logic (PROLOG), Lists, Operators, basic Input and Output.	12
Learning Resources		
Text Books	1. Rich, E. & Knight,K. (2012). Artificial Intelligence. 3rd edition. Tata McGraw Hill. 2. Russell, S.J. & Norvig, P. (2015) Artificial Intelligence - A Modern	

	Approach. 3rd edition. Pearson Education
Reference Books	1. Artificial Intelligence: A Modern Approach by S. Russell and P. Norvig, Prentice Hall.
Website/Link	1. https://onlinecourses.nptel.ac.in/noc23_cs09/preview

Mapping with Program Outcomes:

COs/POs / PSOs	PO1	PO2	PO3	PO4	PO5	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	L	M	L	L	L	L	L	L	M	L
CO2	L	L	L	L	L	M	M	M	M	S
CO3	M	M	M	M	M	S	L	M	M	L
CO4	L	L	M	M	S	S	L	M	M	S

S – Strong; **L** – Low; **M** – Medium

Subject Title	ELECTIVE-IV: CYBER CRIME & LAW	Semester	V
Subject Code	24U5CYDE08	Specialization	NA
Type	Elective : Theory	L:T:P:C	5:0:0:4

Course objective:

- Understanding the nature of cybercrime
- Legal and ethical considerations
- Cyber security
- Investigation and forensics
- Prevention and response
- Emerging trends and technologies

CO No.	CO Statement	Knowledge Level
CO1	Remember the basic concepts of Cyber Crimes	K1
CO2	Analyze the concepts of Digitalization	K1
CO3	Implementation of Digitalization	K2
CO4	Functionalities and Authorization of digital transactions	K3
CO5	Understanding the laws and its acts	K4

Unit	Contents	No. of Sessions
I	**Cyber Crimes** Introduction — Computer Crime and Cyber Crimes: Distinction between Cyber Crime and Conventional Crimes; Cyber Forensic; Kinds of Cyber Crimes — Cyber Stalking, Cyber Terrorism, Forgery and Fraud, Crimes Related to IPRs, Computer Vandalism: Privacy of Online Data; Cyber Jurisdiction; Copyright Issues; Domain Name Dispute, etc.	12
II	Definition and Terminology (Information Technology Act, 2000) Concept of Internet, Internet Governance, E-contract, E-forms, Encryption, Data Security. Access, Addressee, Adjudicating Officer, Affixing Digital Signatures, Appropriate Government, Certifying Authority, Certification Practice Statement, Computer, Computer Network, Computer Resource, Computer System, Cyber Appellate Tribunal, Data, Digital Signature, Electronic Form, Electronic Record.	12
III	Electronic Records Authentication of Electronic Records; Legal Recognition of Electronic Records; Legal Recognition of Digital Signatures; Use of Electronic Records and Digital Signatures in Government and its Agencies; Retention of Electronic Records; Attribution, Acknowledgement and Dispatch of Electronic Records; Secure Electronic Records and Digital Signatures.	12
IV	Regulatory Framework Regulation of Certifying Authorities; Appointment and Functions of Controller; License to Issue Digital Signatures Certificate; Renewal of License; Controller's Powers; Procedure to be	12

	Followed by Certifying Authority; Issue, Suspension and Revocation of Digital Signatures Certificate, Duties of Subscribers; Penalties and Adjudication; Appellate Tribunal; Offences K5 18 V	
V	**Cyber law in India:** Need for cyber law in India, History of cyber law in India, Information Technology Act,2000, Overview of other laws amended by the IT Act 2000, National Policy on Information Technology 2012	**12**

Learning Resources	
Text Books	Cyber Crimes and Laws, Dr.U.S.Pandey, Dr.Verinder Kumar, Dr.Harman Preet Singh, Himalaya Publishing House,2017 edition.
Reference Books	xt book on Cyber Law, Pavan Duggal, second Edition, Universal law 2017
Website/Link	https://www.mygreatlearning.com/academy/learn-for-free/courses/introduction-to- cyber-crime

Mapping with Program Outcomes:

COs/POs / PSOs	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PSO1**	**PSO2**	**PSO3**	**PSO4**	**PSO5**
CO1	L	M	L	L	L	L	L	L	M	L
CO2	L	L	L	L	L	M	M	M	M	S
CO3	M	M	M	M	M	S	L	M	M	L
CO4	L	L	M	M	S	S	L	M	M	S

S – Strong; **L** – Low; **M** – Medium

Subject Title	Elective – V Block Chain Technology	Semester	VI
Subject Code	24U6CYDE09	Specialization	NA
Type	Core: Theory	L:T:P:C	5:0:0:4

Course objective:

- This course aims at facilitating the student to learn the fundamentals of block chain technologyand how it will power the economy of tomorrow.

CO No.	CO Statement	Knowledge Level
CO1	Understand emerging abstract models for Blockchain Technology	K1
CO2	To understand the Cryptocurrency and Bitcoin	K1
CO3	It provides conceptual understanding of the function of storing and using Bitcoin	K2
CO4	To understand and analyze the Community and Regulations of Blockchain	K3

Unit	Contents	No. of Sessions
I	**Introduction to Blockchain&Crypto currencies:** Blockchain-Public Ledgers, Blockchain as Public Ledgers -Bitcoin, Blockchain 2.0, Smart Contracts, Block in a Blockchain, Transactions-Distributed Consensus, The Chain and the Longest Chain - Cryptographic Hash Functions – Hash Pointers and Data Structures – Digital Signatures – Public Keys as Identities – A Simple Crypto currency. (**Chapter 1)**	**12**
II	**How Bitcoin Achieves Decentralization:** Centralization vs. Decentralization- Distributed consensus – Consensus without identity using a block chain-Incentivesand proof of work. **(Chapter 2)**	**12**
III	**Mechanics of Bitcoin:** Bit coin transactions – Bit coin Scripts – Applications of Bit coin scripts – Bit coin blocks –The Bit coin network-Limitations and improvements. **(Chapter 3)**	**12**
IV	**How to Store and Use Bitcoins:** Simple Local Storage – Hot and Cold Storage – Splitting and Sharing Keys – Online Wallets and Exchanges – Payment Services – Transaction Fees – Currency Exchange Markets.(**Chapter 4)**	**12**
V	**Community, Politics, and Regulation:** Consensus in Bit coin – Bitcoin Core Software – Stakeholders: Who's in Charge? – Roots of Bitcoin – Governments Notice Bitcoin – Anti Money-Laundering – Regulation – New York's Bit LicenseProposal**. (Chapter 7)**	**12**

Learning Resources	
Text Books	1. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. "Bitcoin and cryptocurrency technologies: a comprehensive introduction". Princeton University Press, 2016. **(Units I, II, III, IV & V)**

Mapping with Programme Outcomes

COs/POs/ PSOs	PO1	PO2	PO3	PO4	PO5	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	L	M	L	L	L	L	L	L	M	L
CO2	L	L	L	L	L	M	M	M	M	S
CO3	M	M	M	M	M	S	L	M	M	L
CO4	L	L	M	M	S	S	L	M	M	S

S-Strong , M- Medium , L – Low

Subject Title	Elective – V Cryptography	Semester	VI
Subject Code	24U6CYDE10	Specialization	NA
Type	Core: Theory	L:T:P:C	5:0:0:4

Course objective:

- To understand Cryptography Theories, Algorithms and Systems.
- To understand necessary Approaches and Techniques to build protection mechanisms in order to securecomputer networks.

CO No.	CO Statement	Knowledge Level
CO1	Understand the fundamentals of networks security, security architecture, threats and vulnerabilities	K1,K2,K3
CO2	Apply the different cryptographic operations of symmetric cryptographic algorithms	K2,K3
CO3	Apply the different cryptographic operations of public key cryptography	K4,K1
CO4	Apply the various Authentication schemes to simulate different applications	K4,K5
CO5	Understand various Security practices and System security standards	K1,K3

Unit	Contents	No. of Sessions
I	Security trends - Legal, Ethical and Professional Aspects of Security, Need for Security at Multiple levels, Security Policies - Model of network security – Security attacks, services and mechanisms – OSI security architecture – Classical encryption techniques: substitution techniques, transposition techniques, steganography	12
II	MATHEMATICS OF SYMMETRIC KEY CRYPTOGRAPHY: Algebraic structures - Modular arithmetic-Euclid‘s algorithm-Congruence and matrices - Groups, Rings, Fields- Finite fields- SYMMETRIC KEY CIPHERS: SDES – Block cipher Principles of DES – Strength of DES	12
III	MATHEMATICS OF ASYMMETRIC KEY CRYPTOGRAPHY: Primes – Primality Testing – Factorization – Euler‘s totient function, Fermat‘s and Euler‘s Theorem - Chinese Remainder Theorem – Exponentiation and logarithm - ASYMMETRIC KEY CIPHERS: RSA cryptosystem – Key	12

	distribution – Key management – Diffie Hellman key	
IV	Authentication requirement – Authentication function – MAC – Hash function – Security of hash function and MAC – SHA – Digital signature and authentication protocols – DSS- Entity Authentication: Biometrics, Passwords,	**12**
V	Electronic Mail security – PGP, S/MIME – IP security – Web Security - SYSTEM SECURITY: Intruders – Malicious software – viruses – Firewalls.	**12**

Learning Resources	
Text Books	1. William Stallings, Cryptography and Network Security: Principles and Practice, PHI3rd Edition, 2006.
Reference Books	1. C K Shyamala, N Harini and Dr. T R Padmanabhan: Cryptography and NetworkSecurity, Wiley India Pvt.Ltd 2. Behrouz A. Forouzan, Cryptography and Network Security, Tata McGraw Hill 2007. 3. Charlie Kaufman, Radia Perlman, and Mike Speciner, Network Security: PRIVATE Communication in a PUBLIC World, Prentice Hall, ISBN 0-13-046019-2
Website Link	https://www.geeksforgeeks.org/cryptography-and-its-types/

Mapping with Programme Outcomes

COs/POs/ PSOs	PO1	PO2	PO3	PO4	PO5	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	L	M	L	L	L	L	L	L	M	L
CO2	L	L	L	L	L	M	M	M	M	S
CO3	M	M	M	M	M	S	L	M	M	L
CO4	L	L	M	M	S	S	L	M	M	S

S-Strong , M- Medium , L – Low

Subject Title	Elective VI: Cloud Security	Semester	VI
Subject Code	24U6CYDE11	Specialization	NA
Type	Core: Theory	L:T:P:C	4:0:0:4

Course objective:

- The course provides knowledge on cloud computing and its security aspects.

CO No.	CO Statement	Knowledge Level
CO1	Understand the fundamentals of Cloud and Web security.	K1
CO2	Explore the knowledge on cloud applications.	K1
CO3	Acquire knowledge on Virtualization Techniques	K2
CO4	Apply the concepts in Cloud security management	K3

Unit	Contents	No. of Sessions
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.	12
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.	12
III	**SECURING THE CLOUD**: Security Concepts - Confidentiality,privacy, integrity, authentication, nonrepudiation, 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. Userauthentication in the cloud.	12
IV	**VIRTUALIZATION SECURITY** : Multi-tenancy Issues: Isolation of users/VMs fromeach other- How the cloud provider can provide this- Virtualization System Security Issues: e.g. ESX and ESXi Security, ESX file system security- storage considerations, backup and recovery- Virtualization System Vulnerabilities.	12
V	**CLOUD SECURITY MANAGEMENT**: Security management in the cloud – security management standards- SaaS, PaaS, IaaS availability management- access control- Data security and storage in cloud.	12

Learning Resources	
Text Books	1. GautamShroff, "Enterprise Cloud Computing Technology Architecture Applications", Cambridge University Press; 1 edition [ISBN: 978-0521137355], 2010. 2. A Comprehensive Guide to Secure Cloud Computing Ronald L. Krutz, Russell DeanVines, India 2010 3. Toby Velte, Anthony Velte, Robert Elsenpeter, "Cloud Computing, A Practical Approach", TataMcGraw-Hill Osborne Media; 1 edition 22, [ISBN:0071626948], 2009.

Mapping with Programme Outcomes

COs/POs/ PSOs	PO1	PO2	PO3	PO4	PO5	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	L	M	L	L	L	L	L	L	M	L
CO2	L	L	L	L	L	M	M	M	M	S
CO3	M	M	M	M	M	S	L	M	M	L
CO4	L	L	M	M	S	S	L	M	M	S

S-Strong , M- Medium, L – Low

Subject Title	Elective VI : INFORMATION SECURITY	Semester	II
Subject Code	24U6CYDE12	Specialization	NA
Type	Core: Theory	L:T:P:C	4:0:0:4

Course objective:

- Protect and defend computer systems and networks from cyber security attacks.
- Diagnose and investigate cyber security events or crimes related to computer systems and digital evidence.
- Effectively communicate in a professional setting to address information security issues.

CO No.	CO Statement	Knowledge Level
CO1	Define the Security and its models	K1
CO2	Outline the concepts of attacks.	K2
CO3	Define the risk management policies.	K2
CO4	Employ the methods Intrusion detection and prevention and security Planning	K3
CO5	To prepare students with the technical knowledge and skills	K3

Unit	Contents	No. of Sessions
I	Introduction to Information Security, The history of Information security, What is security, CNSS security model, Components of an Information system, Balancing Information security and access, Approaches to Information security implementation, The systems development life cycle, The security systems development life cycle, Security professionals and the organization, Communities of Interest. Information Security: is it an Art or a Science	12
II	The need for security: Introduction, Business needs first, Threats-Compromises to individual property, Deliberate software attacks, Deviations in quality of service, Espionage, Sabotage, Theft, Attacks: Malicious Code, Hoaxes, Backdoors, Password crack, Brute force, Dictionary, Denial of service and Distributed denial of service, Spoofing, Man-in-the-middle, Spam, Mail bombing, Sniffers, Social Engineering, Pharming, Timing attack, Secures of software development	12
III	Risk Management: Introduction, An overview of Risk Management, Risk Identification : l an and Organize, Asset Identification and Inventory Classifying and Prioritizing Information assets, Information Asset Valuation, Identifying and Prioritizing Threats, Vulnerability identification Risk Assessment: Introduction, Likelihood, Risk Determination, Identify Possible Controls, Documenting the Results of Risk Assessment Risk Control Strategies: Defend, Transfer, Mitigate, Accept, Terminate	12
IV	Information security planning and governance- Planning levels, Planning and the CISO, Information security governance, Information security policy, standards and practices- Definitions, EISP, ISSP, SysSP, Policy management, The Information security blueprint, Designing of security	12

	architecture, Security education training and awareness program, Continuity strategies, Security technology Firewalls and VPNs, Access control-Identification, Authentication, Authorization, Accountability, Firewall processing modes, Firewalls categorized by generation, Firewalls categorized by structure, Firewall architectures, Selecting the right firewall, Configuring and managing firewalls, Content filters, Protecting remote connections-Remote access, VPNs.	
V	Intrusion detection and prevention systems- Why IDPS?, types, detection models, response behavior, strengths and limitations, deployment and implementation, measuring the effectiveness. Honey pots, Honey nets and padded cell systems- Trap-and-trace systems, Active intrusion prevention	**12**

Learning Resources

Text Books	1. Principles of Information Security- Michael E. Whitman, Herbert J. Mattord, Cengage Learning, Fourth edition,2011
Reference Books	1. Information Security Management Principles- Andy Taylor, David Alexander, Amanda Finch, David Sutton, BCSpublishers,2008 2. GuidetoComputerforensicsandInvestigations- B.Nelson,A.Phillips,F.Enfinger,C.Steuart,CengageLearning,4thedition,2010 3. Applied Information security: A Hands- On guide to Information security- R. Boyle, PrenticeHall,2010 4. Fundamentals of Network Security- E. Maiwald, McGraw- Hill, 2004 5. Managing Information Security- John R. Vacca, Elsevier Inc, 2010 6. Computer Security basics- Rick Lehtinen,O'Reilly,2nd edition, 2006 7. Absolute beginner's guide to Security, Spam, Spyware& Viruses-Andy Walker, Quepublishers,2005
Website/Link	1. Vidya-MitraPortal:http://vidyamitra.inflibnet.ac.in/index.php/search 2. Tutorialspoint:https://www.tutorialspoint.com/information_security_cyber_law/

Mapping with Programme Outcomes

COs/POs/ PSOs	PO1	PO2	PO3	PO4	PO5	PSO1	PSO2	PSO3	PSO4	PSO5
CO1	L	L	L	L	L	L	L	L	M	L
CO2	L	M	L	L	L	M	L	M	M	S
CO3	L	M	M	M	M	S	L	M	M	L
CO4	L	L	M	M	S	S	L	M	M	S

S-Strong , M- Medium , L – Low

Subject title	ANALYTICAL SKILLS	Semester	VI
Subject code	24U6CYS05	Specialization	CA
Type	SBEC : Theory	L:T:P:C	2:0:0:2

COURSE OBJECTIVE:

Intended to inculcate quantitative analytical skills and reasoning as an inherent ability in students.

CO NO.	CO STATEMENT	KNOWLEDGE LEVEL
CO1	Understand the basic concepts of arithmetic ability, quantitative ability, logical reasoning, business computations and data interpretation and obtain the associated skills.	K1
CO2	Apply the skills and competencies acquired in the related areas	K2
CO3	Analyze the problem and use logic to interpret and handle different situations	K3
CO4	Solve problems pertaining to quantitative ability, logical reasoning and verbal ability inside and outsidethe campus.	K4
CO5	Acquire competency in the use of verbal reasoning	K4

UNIT	CONTENTS	NO. OF SESSIONS
I	Number system: Types of numbers, rules of divisibility, multiplicity and squaring of numbers, HCF and LCM of numbers. Average: Average of numbers, Arithmetic Mean, Real-life examples of average, Application1based questions	6
II	Number series: Series Completion, Analogy, Classification. Coding-Decoding: Letter Coding, Direct Letter Coding, Number / Symbol Coding, deciphering message word codes, number and symbol codes for messages	6
III	Percentage: Concept of Percentage, Comparison based questions, Application-based questions. Profit and Loss: Profit or Loss, Cost price, Selling price, Calculation of profit and loss percent, Application-based questions, conceptual formulae.	6
IV	Simple interest: the concept of simple interest, general formulas, application-based questions. Compound interest: basic concepts	6

	and formula-based questions, the difference between simple interest and compound interest	
V	Alphabet Test: Alphabetical order of words, Letter-word problems, Word formation by unscrambling letters. Number Test: Number Test, Position switching of numbers. Blood Relation: Coded Relations, relation-based puzzle.	**6**

LEARNING RESOURCES	
Text books	1. A MODERN APPROACH TO NON-VERBAL REASONING by R S AGGARWAL, S Chand Publishing 2. QUANTITATIVE APTITUDE FOR COMPETITIVE EXAMINATIONS by R S AGGARWAL, S Chand Publishing 3. QUANTITATIVE APTITUDE by ABHIJIT GUHA, Tata McGraw Hill, India
Reference books	1. Analytical skills by Showick Thorpe, published by S Chand And Company Limited, Ramnagar,New Delhi-110055 2. Quantitative Aptitude and Reasoning by R V Praveen, PHI publishers. 3. Quantitative Aptitude for Competitive Examination by Abhijit Guha, Tata Mc Graw HillPublications
Website/link	1) What Are Analytical Skills? Definition and Examples - Forage (theforage.com) 2) What Are Analytical Skills? 9 Examples & Tips to Improve (betterup.com) 3) 7 Steps To Improve Your Analytical Thinking Skills (talentbridge.com)

MAPPING WITH PROGRAMME OUTCOMES

	PO01	PO02	PO03	PO04
CO1	S	S	S	-
CO2	S	M	M	S
CO3	S	L	L	M
CO4	M	S	M	S
CO5	S	L	S	S

S-Strong , M- Medium , L – Low