Sri SAIRAM INSTITUTE OF TECHNOLOGY

An Autonomous Institution

West Tambaram, Chennai - 44

www.sairamit.edu.in

Approved by AICTE, New Delhi
Affiliated to Anna University

DEPARTMENT OF

COMPUTER SCIENCE & ENGINEERING (CYBER SECURITY)

REGULATIONS
2020

Academic Year 2022-23 onwards

AUTONOMOUS

CURRICULUM AND

SYLLABUS
I - VIII
SEMESTERS

SRI SAIRAM INSTITUTE OF TECHNOLOGY

VISION

To be identified as a "Centre of Excellence" with high standards of knowledge dissemination and research opportunities and to transform the students to imbibe qualities of technical expertise, international standards, and high levels of ethical values, who in turn shall contribute to the advancement of society and humankind.

MISSION

We shall dedicate and commit ourselves to attaining and maintaining excellence in technical education through commitment and continuous improvement of infrastructure and equipment and providing an inspiring environment for learning, research, and innovation for our students so they become complete human beings with ethical and social values.

QUALITY POLICY

We at the Sri Sai Ram Institute of Technology are committed to building a beer nation through quality education with team spirit. Our students are enabled to excel in all areas of life and become good citizens. We continuously improve the system, infrastructure, and services to satisfy the students, parents, industry, and society.

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING (CYBER SECURITY)

VISION

To be a centre of excellence in educating and graduating Computer Engineers by providing unique environment that foster research, technological, and social enrichment with intellectual knowledge to acquire international standards.

MISSION

To deliver qualified computer professionals having innovative research capabilities. To inculcate the spirit of moral values that contributes to societal ethics. To provide training programs that bridges the gap between academia and industry. To enhance research quality and productivity through state of the art facilities.

AUTONOMOUS CURRICULA AND SYLLABI
Regulations 2020

SEMESTER I

S. NO	COURSE CODE	COURSE TITLE	WEEK HOURS			TOTAL CONTACT HOURS	CREDITS
			L	T	P		
THEORY							
1	20BSMA101	Engineering Mathematics-I	3	1	0	4	4
2	20HSEN101	Technical English-I	3	0	0	3	3
3	20BSPH101	Engineering Physics	3	0	0	3	3
4	20BSCY101	Engineering Chemistry	3	0	0	3	3
5	20ESCS101	Problem Solving and Programming in C	3	0	0	3	3
6	20ESGE101	Engineering Graphics	1	2	0	3	3
PRACTICALS							
7	20BSPL101	Physics and Chemistry Laboratory	0	0	3	3	1.5
8	20ESPL101	Programming in C Laboratory	0	0	3	3	1.5
VALUE ADDITIONS - I							
9	20HSTA101	Heritage of Tamils	1	0	0	1	1
10	20TPHS101	Skill Enhancement	0	0	2	2	1
11	20HSMG101	Personal Values	2	0	0	2	0
TOTAL						**30**	**24**

SEMESTER II

S. NO	COURSE CODE	COURSE TITLE	WEEK HOURS			TOTAL CONTACT HOURS	CREDITS
			L	T	P		
THEORY							
1	20BSMA204	Discrete Structures	3	1	0	4	4
2	20HSEN201	Technical English – II	3	0	0	3	3
3	20BSPH203	Physics for Information Science	3	0	0	3	3
4	20BSCY201	Environmental Science and Engineering	3	0	0	3	3
5	20ESIT202	Python Programming	3	0	0	3	3
6	20ESIT203	Digital Principles and System Design	2	1	0	3	3
PRACTICALS							
7	20ESPL201	Python Programming Laboratory	0	0	3	3	1.5
8	20ESPL202	Digital Laboratory	0	0	3	3	1.5
9	20ESGE201	Engineering Practices Laboratory	0	0	3	3	1.5
VALUE ADDITIONS - II							
10	20HSTA201	Tamils And Technology	1	0	0	1	1
11	20TPHS201	Skill Enhancement	0	0	2	2	0
12	20HSMG201	Interpersonal Values	2	0	0	2	0
TOTAL						**33**	**24.5**

SEMESTER III

S. NO	COURSE CODE	COURSE TITLE	WEEK HOURS			TOTAL CONTACT HOURS	CREDITS
			L	T	P		
THEORY							
1	20BSMA309	Number Theory	3	1	0	4	4
2	20ITPC301	Data Structures	3	0	0	3	3
3	20CSPC301	Object Oriented Programming	3	0	0	3	3
4	20SCPC301	Software Architecture And Project Management	3	0	0	3	3
5	20SCPC302	Cyber Security Essentials	3	0	0	3	3
6	20SCPC303	Machine Learning in Cyber Security	3	0	0	3	3
PRACTICALS							
7	20CSPL301	Object Oriented Programming Laboratory	0	0	3	3	1.5
8	20SCPL301	Software Engineering Laboratory	0	0	3	3	1.5
9	20ITPL301	Data Structures Laboratory	0	0	3	3	1.5
10	20SCTE301	Live in Lab – I	0	0	2	2	1
VALUE ADDITIONS - III							
12	20SCTP301	Skill Enhancement	0	0	2	2	0
13	20MGMC301	Constitution of India	2	0	0	2	0
		TOTAL				**34**	**24.5**

SEMESTER IV

S. NO	COURSE CODE	COURSE TITLE	WEEK HOURS			TOTAL CONTACT HOURS	CREDITS
			L	T	P		
THEORY							
1	20BSMA402	Probability and Queuing Theory	3	0	0	5	4
2	20CSPW401	Computer Networks (with lab)	3	0	2	5	4
3	20CSPC401	Operating Systems	3	0	0	3	3
4	20CSPC402	Database Management System	3	0	0	3	3
5	20SCPC401	Cryptography & Cyber Security	3	0	0	3	3
6	20ITPC401	Design and Analysis of Algorithms	2	1	0	3	3
PRACTICALS							
7	20SCPL401	Cryptography & Cyber Security Laboratory	0	0	3	3	1.5
8	20CSPL401	Operating Systems Laboratory	0	0	3	3	1.5
9	20CSPL402	Database Management Systems Laboratory	0	0	3	3	1.5
10	20SCTE401	Live in Lab – II	0	0	2	2	1
VALUE ADDITIONS - III							
11	20SCTP401	Skill Enhancement	0	0	2	2	1
		TOTAL				**35**	**26.5**

SEMESTER V

S. NO	COURSE CODE	COURSE TITLE	WEEK HOURS			TOTAL CONTACT HOURS	CREDITS
			L	T	P		
THEORY							
1	20SCPC501	Secure Coding	3	0	0	3	3
2	20SCPC502	Fundamentals of Quantization	3	0	0	3	3
3	20SCPC503	Cyber Attacks	3	0	0	3	3
4	20XXELXXX	Professional Elective - I	3	0	0	3	3
5	20XXOEXXX	Open Elective - I	2	1	0	3	3
PRACTICALS							
6	20SCPL501	Secure Coding Lab	0	0	3	3	1
7	20SCPL502	Cyber Attack Lab	0	0	3	3	1
8	20HSPL501	Communication And Soft Skills Laboratory	0	0	3	3	1
9	20SCTE501	Live In Lab - III	0	0	2	2	1
VALUE ADDITIONS - V							
10	20SCTP501	Skill Enhancement	0	0	2	2	1
		TOTAL					**20.5**

SEMESTER VI

S. NO	COURSE CODE	COURSE TITLE	WEEK HOURS			TOTAL CONTACT HOURS	CREDITS
			L	T	P		
THEORY							
1	20SCPC601	Distributed And Cloud Security	3	0	0	3	3
2	20SCPC602	Quantum Algorithm	3	0	0	3	3
3	20SCPC603	Cyber Law And Ethics	3	0	0	3	3
4	20SCPC604	Penetration Testing & Ethical Hacking	3	0	0	3	3
5	20XXELXXX	Professional Elective - II	3	0	0	3	3
PRACTICALS							
6	20SCPL601	Cloud Security Lab	0	0	3	3	1.5
7	20SCPL602	Penetration Testing Lab	0	0	3	3	1.5
8	20SCTE601	Innovative Design Project	0	0	3	3	1
VALUE ADDITIONS - VI							
9	20SCTP601	Skill Enhancement	0	0	2	2	1
		TOTAL					**20**

SEMESTER VII

S. NO	COURSE CODE	COURSE TITLE	WEEK HOURS			TOTAL CONTACT HOURS	CREDITS
			L	T	P		
		THEORY					
1	20SCPC701	Quantum Cryptography	3	0	0	3	3
2	20SCPC702	Cyber Forensics	3	0	0	3	3
3	20SCPC703	Block Chain Technology	3	0	0	3	3
4	20XXELXXX	Professional Elective - III	3	0	0	3	3
5	20XXOEXXX	Open Elective - II	3	0	0	3	3
		PRACTICALS					
6	20SCPJ701	Project Phase - I	0	0	3	3	2
7	20SCPL701	Quantum Lab	0	0	3	3	1
8	20SCPL702	Cyber Forensics Lab	0	0	3	3	1
		VALUE ADDITIONS - VII					
9	20SCTP701	Skill Enhancement	0	0	2	2	1
		TOTAL					**20**

SEMESTER VIII

S. NO	COURSE CODE	COURSE TITLE	WEEK HOURS			TOTAL CONTACT HOURS	CREDITS
			L	T	P		
		THEORY					
1.	20XXELXXX	Professional Elective - IV	3	0	0	4	3
		PRACTICAL					
2.	20SCPJ801	Project Phase - II	0	0	3	10	4
		TOTAL					**7**

CREDIT DISTRIBUTION

Category	BS	ES	HS	EL	PC+PL	OE	TE	PJ	TP	IS	MC	TOTAL
Credit	29.5	18	9	12	80	6	2	6	3		Y	**165.5**
Percentage	17.4	9	4.5	6	40	3	1	3	1.8			

*IS-Internship

PROFESSIONAL ELECTIVES - I

S. NO	COURSE CODE	COURSE TITLE	WEEK HOURS			TOTAL CONTACT HOURS	CREDIT	STREAM
			L	T	P			
1	20SCEL501	Foundation of Data Science	3	0	0	3	3	COMPUTING
2	20SCEL502	No SQL Database	3	0	0	3	3	COMPUTING
3	20SCEL503	Internet of Things	3	0	0	3	3	Internet of Things
4	20SCEL504	IoT Architechture, Network and Security	3	0	0	3	3	Internet of Things
5	20SCEL505	Software Testing	3	0	0	3	3	COMPUTING
6	20SCEL506	Information Retrieval Techniques	3	0	0	3	3	COMPUTING
7	20SCEL507	Bio Informatics	3	0	0	3	3	Cyber Security
8	20SCEL508	Software Quality Assurance	3	0	0	3	3	COMPUTING
9	20SCEL509	Fundamentals of Edge and Soft computing	3	0	0	3	3	COMPUTING
10	20SCEL510	Information Storage And Management	3	0	0	3	3	COMPUTING

PROFESSIONAL ELECTIVES - II

S. NO	COURSE CODE	COURSE TITLE	WEEK HOURS			TOTAL CONTACT HOURS	CREDIT	STREAM
			L	T	P			
1	20SCEL601	Intrusion Detection Systems	3	0	0	3	3	Cyber Security (Attack)
2	20SCEL602	Vulnerability Discovery & Exploit Development	3	0	0	3	3	Cyber Security (Attack)
3	20SCEL603	Bio Metric Security	3	0	0	3	3	Cyber Security (Attack)
4	20SCEL604	Cyber Threat Intelligence	3	0	0	3	3	Cyber Security (Attack)
5	20SCEL605	Social Network Analysis	3	0	0	3	3	Cyber Security (Attack)
6	20SCEL606	Malware Analysis & Reverse Engineering	3	0	0	3	3	Cyber Security (Attack)
7	20SCEL607	Quantum-resistant Blockchain	3	0	0	3	3	Quantum Computing
8	20SCEL608	Quantum-resistant Cryptography	3	0	0	3	3	Quantum Computing
9	20SCEL609	Quantum Information Theory	3	0	0	3	3	Quantum Computing
10	20SCEL610	Social Engineering	3	0	0	3	3	Cyber Security (Attack)

PROFESSIONAL ELECTIVES - III

S. NO	COURSE CODE	COURSE TITLE	WEEK HOURS			TOTAL CONTACT HOURS	CREDIT	STREAM
			L	T	P			
1	20SCEL701	Quantum Communication	3	0	0	3	3	Quantum Computing
2	20SCEL702	Post-Quantum Cryptography	3	0	0	3	3	Quantum Computing
3	20SCEL703	Emerging Technologies and Policy Implications	3	0	0	3	3	Cyber Law & Policy
4	20SCEL704	IT Security Compliance and Digital Forensics	3	0	0	3	3	Cyber Law & Policy
5	20SCEL705	Quantum-Safe Network Protocols	3	0	0	3	3	Quantum Computing
6	20SCEL706	Multi-core Architectures and Programming	3	0	0	3	3	Data Science
7	20SCEL707	Web Analytics	3	0	0	3	3	Data Science
8	20SCEL708	Quantum Side-Channel Attacks and Countermeasures	3	0	0	3	3	Quantum Computing
9	20SCEL709	National Security and Cyber Security	3	0	0	3	3	Cyber Law & Policy
10	20SCEL710	Quantum Machine Learning	3	0	0	3	3	Quantum Computing

PROFESSIONAL ELECTIVES - IV

S. NO	COURSE CODE	COURSE TITLE	WEEK HOURS			TOTAL CONTACT HOURS	CREDIT	STREAM
			L	T	P			
1	20SCEL801	Cyber Security Policy and Strategy	3	0	0	3	3	Cyber Law & Policy
2	20SCEL802	Quantum Authentication	3	0	0	3	3	Quantum Computing
3	20SCEL803	Quantum Cyber-Physical Systems Security	3	0	0	3	3	Quantum Computing
4	20SCEL804	Cybercrime Legislation	3	0	0	3	3	Cyber Law & Policy
5	20SCEL805	Regulatory Compliance	3	0	0	3	3	Cyber Law & Policy
6	20SCEL806	Risk Management and Liability	3	0	0	3	3	Cyber Law & Policy
7	20SCEL807	Virtual & Augmented Reality	3	0	0	3	3	Data Science
8	20SCEL808	Cyber Security Awareness and Education	3	0	0	3	3	Cyber Law & Policy
9	20SCEL809	Computer Vision	3	0	0	3	3	Data Science
10	20SCEL810	Ethical Hacking and Offensive Cyber Operations	3	0	0	3	3	Cyber Law & Policy

PROGRAM EDUCATIONAL OBJECTIVES (PEOs)

PEO1: Formulate, analyze and solve Engineering problems with strong foundation in Mathematical, Scientific and Engineering fundamentals

PEO2: Analyze the requirements, realize the technical specification and design the Engineering solutions by applying computer science theory and principles.

PEO3: Promote collaborative learning and team work spirit through multi -disciplinary projects and diverse professional activities.

PEO 4 : Equip the graduates with strong knowledge, competence and soft skills that allow them to contribute ethically to the needs of society.

PEO 5 : Accomplish sustainable progress in the emerging areas of Engineering through life-long learning.

PROGRAM SPECIFIC OUTCOMES (PSOs)

PSO1 Demonstrate basic knowledge of computer applications and apply standard practices in software project development.

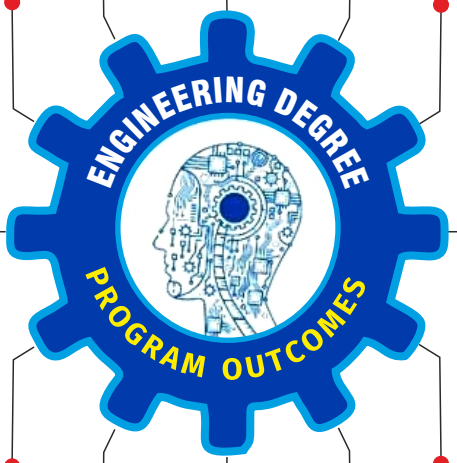
PSO2 Understand, Analyze and Develop computer programs for efficient design of computer-based systems of varying complexity.

COMPONENTS OF THE CURRICULUM (COC)

Course Component	Curriculum Content (% of total number of credits of the program)	Total number of contact hours	Total Number of credits
Basic Sciences(BS)	17.4	31	29.5
Engineering Sciences(ES)	15.0	33	25.5
Humanities and Social Sciences (HS)	5.9	12	10
Professional Electives(EL)	7.1	12	12
Program Core+Program Lab (PC+PL)	36.5	76	62
Program theory with Lab (PW)	2.4	05	04
Open Electives (OE)	3.5	06	06
Talent Enhancement (TE)	2.4	08	04
Project (PJ)	4.1	14	07
Training & Placement (TP)	4.1	14	07
Internships/Seminars (IS)	1.8	-	03
Mandatory Courses (MC)	NA	06	NA
Total number of Credits		**217**	**170**

PROGRAMME OUTCOMES(POs)

PROGRAM OUTCOME REPRESENTS THE KNOWLEDGE, SKILLS AND ATTITUDES THAT THE STUDENTS WOULD BE EXPECTED TO HAVE AT THE END OF THE 4 YEAR ENGINEERING DEGREE PROGRAM



01 Engineering knowledge

Apply the basic principle and knowledge of mathematics, science and engineering principles to solve technical problems.

02 Problem Analysis

Identify and analyze complex engineering problems reaching logical conclusions using the basic principles of mathematics, science and engineering.

03 Development of solutions

Design solutions for well-defined technical problems and assist with the design of systems, components or processes to meet specified needs.

04 Investigate complex problems

Perform investigations, use research based knowledge and conduct experiments, analyze and interpret the results to provide valid conclusions.

05 Modern tool usage

Create, select and apply the latest techniques, resources and modern engineering / IT tools to develop appropriate solutions with an understanding of the limitations.

06 The Engineer and Society

Apply reasoning based on contextual knowledge to assess societal, legal and cultural issues with competency in professional engineering practices.

07 Environment & Sustainability

Demonstrate professional skills, knowledge and contextual reasoning to assess / environmental / societal issues for sustainable development.

08 Apply ethical principles

Apply ethical principles and commit to professional ethics and responsibilities based on the norms of professional engineering pratices.

09 Individual & Teamwork

Function effectively as an individual, and as a member or leader in diverse teams, and in multi-disciplinary professional settings.

10 Communicate effectively

Communicate effectively amongst the engineering community, being able to comprehend & write effective reports, make presentations & give/receive clear instructions.

11 Project management

Demonstrate knowledge and apply the principles of engineering & management in their own / team projects in multidisciplinary environments.

12 Life-long learning

Recognize the need for, and have the preparation, ability to engage in independent and life-long learning in the context of technological change.

SEMESTER - I

20BSMA101 SDG NO. 4	ENGINEERING MATHEMATICS-I	L	T	P	C
		3	1	0	4

OBJECTIVES:

The intent of the course is

- To understand and gain the knowledge of matrix algebra.
- To introduce the concepts of limits, continuity, derivatives and maxima and Minima
- To acquaint the concept of improper integrals and the properties of definite integrals.
- To provide understanding of double integration, triple integration and their application.
- To introduce the concept of sequence and series and impart the knowledge of Fourier series.

UNIT I MATRICES **12**

Symmetric, skew symmetric and orthogonal matrices; Eigenvalues and Eigenvectors of a real matrix – Characteristic equation – Properties of Eigenvalues and Eigenvectors – Cayley-Hamilton theorem (excluding proof) – Diagonalization of a Quadratic form using orthogonal transformation - Nature of Quadratic forms.

UNIT II DIFFERENTIAL CALCULUS **12**

Limits, continuity, Differentiation rules - Maxima and Minima of functions of one variable, partial derivatives (first and second order – basic problems), Taylor's series for functions of two variables, Jacobian, Maxima & Minima of functions of several variables, saddle points; Method of Lagrange multipliers.

UNIT III INTEGRAL CALCULUS **12**

Evaluation of definite integrals - Techniques of Integration-Substitution rule - Integration by parts, Integration of rational functions by partial fraction, Integration of irrational functions. Applications of definite integrals to evaluate surface area of revolution and volume of revolution. Evaluation of improper integrals.

UNIT IV MULTIPLE INTEGRALS **12**

Double integrals – Change of order of integration – Double integrals in polar coordinates – Area enclosed by plane curves – Triple integrals – Volume of solids – Change of variables in double and triple integrals.

UNIT V SEQUENCES AND SERIES **12**

Introduction to sequences and series – power series – Taylor's series – series for exponential, trigonometric, logarithmic, hyperbolic functions – Fourier series – Half range Sine and Cosine series – Parseval's theorem.

TOTAL: 60 PERIODS

TEXTBOOKS:

1. James Stewart, "Calculus: Early Transcendentals", Cengage Learning, 7th Edition, New Delhi, 2015.
2. B. V. Ramana, "Higher Engineering Mathematics", Tata McGraw-Hill, New Delhi, 11th Reprint, 2010.

REFERENCES:

1. G.B. Thomas and R.L. Finney, "Calculus and Analytic Geometry", 9th Edition, Pearson, Reprint, 2002.
2. Erwin Kreyszig, "Advanced Engineering Mathematics", 9th Edition, John Wiley & Sons, 2006.
3. T. Veerarajan, "Engineering Mathematics for first year", Tata McGraw-Hill, New Delhi, 2008.
4. N.P. Bali and Manish Goyal, "A text-book of Engineering Mathematics", Laxmi Publications, Reprint, 2008.
5. B. S. Grewal, "Higher Engineering Mathematics", Khanna Publishers, New Delhi, 40th Edition, 2014.

WEB REFERENCES:

1. https://math.mit.edu/~gs/linearalgebra/ila0601.pdf
2. http://ocw.mit.edu/ans7870/18/18.013a/textbook/HTML/chapter30/
3. https://ocw.mit.edu/courses/mathematics/18-02sc-multivariable-calculus-fall-2010/2.-partial-derivatives/
4. http://ocw.mit.edu/ans7870/18/18.013a/textbook/HTML/chapter31/

ONLINE RESOURCES:

1. https://www.khanacademy.org/math/linear-algebra/alternate-bases/eigen-everything/v/linear-algebra-introduction-to-eigenvalues-and-eigenvectors
2. https://www.khanacademy.org/math/differential-calculus

OUTCOMES:

Upon completion of the course, the student should be able to

1. Diagonalize the matrix using orthogonal transformation and apply Cayley Hamilton Theorem to find the inverse and integral powers of a square matrix. (K3)
2. Evaluate the limit, examine the continuity and use derivatives to find extreme values of a function. (K3)
3. Evaluate definite and improper integrals using techniques of integration. (K3)
4. Apply double and triple integrals to find the area of a region and the volume of a surface. (K3)
5. Compute infinite series expansion of a function. (K3)

CO - PO MAPPING :

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

SEMESTER - I

20HSEN101 SDG NO. 4	TECHNICAL ENGLISH - I	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To develop the basic LSRW skills of the students
- To encourage the learners to adapt to listening techniques
- To help learners develop their communication skills and converse fluently in real contexts
- To help learners develop general and technical vocabulary through reading and writing tasks
- To improve the language proficiency for better understanding of core subjects

UNIT I INTRODUCTION 9

Listening – short texts – formal and informal conversations - **Speaking** – basics in speaking – speaking on given topics & situations – recording speeches and strategies to improve - **Reading –** critical reading – finding key information in a given text – shifting facts from opinions - **Writing –** free writing on any given topic – autobiographical writing - **Language Development** – tenses – voices- word formation: prefixes and suffixes – parts of speech – developing hints

UNIT II READING AND LANGUAGE DEVELOPMENT 9

Listening - long texts - TED talks - extensive speech on current affairs and discussions -Speaking – describing a simple process – asking and answering questions - **Reading** comprehension – skimming / scanning / predicting & analytical reading – question & answers – objective and descriptive answers –identifying synonyms and antonyms - process description - **Writing** instructions – **Language Development** – writing definitions – compound words.

UNIT III SPEAKING AND INTERPRETATION SKILLS 9

Listening - dialogues & conversations - **Speaking** – role plays – asking about routine actions and expressing opinions - **Reading** longer texts & making a critical analysis of the given text - **Writing** – types of paragraph and writing essays – rearrangement of jumbled sentences - writing recommendations - **Language Development** – use of sequence words - cause & effect expressions - sentences expressing purpose - picture based and newspaper based activities – single word substitutes

UNIT IV VOCABULARY BUILDING AND WRITING SKILLS 9

Listening - debates and discussions – practicing multiple tasks – self introduction – **Speaking** about friends/places/hobbies - **Reading** -Making inference from the reading passage – Predicting the content of the reading passage - **Writing** – informal letters/e-mails - **Language Development** - synonyms & antonyms - conditionals – if, unless, in case, when and others – framing questions.

UNIT V LANGUAGE DEVELOPMENT AND TECHNICAL WRITING 9

Listening - popular speeches and presentations - **Speaking** - impromptu speeches & debates - **Reading** - articles – magazines/newspapers **Writing** – essay writing on technical topics - channel conversion – bar diagram/ graph – picture interpretation - process description - **Language Development** – modal verbs - fixed / semi-fixed expressions – collocations

TOTAL: 45 PERIODS

TEXT BOOKS:

1. Board of Editors. Using English: A Coursebook for Undergraduate Engineers and Technologists. Orient Blackswan Limited, Hyderabad: 2015.
2. Dhanavel, S.P. English and Communication Skills for Students of Science and Engineering. Orient Blackswan, Chennai, 2011.

REFERENCES:

1. Anderson, Paul V. Technical Communication: A Reader – Centered Approach. Cengage, New Delhi, 2008.
2. Smith-Worthington, Darlene & Sue Jefferson. Technical Writing for Success. Cengage, Mason, USA, 2007.
3. Grussendorf, Marion, English for Presentations, Oxford University Press, Oxford, 2007.
4. Chauhan, Gajendra Singh and et.al.Technical Communication (Latest Revised Edition). Cengage Learning India Pvt. Limited, 2018.

WEB REFERENCES:

1. https://swayam.gov.in/nd1_noc19_hs31/preview
2. http://engineeringvideolectures.com/course/696

ONLINE RESOURCES:

1. https://www.pearson.com/english/catalogue/business-english/technical-english.html
2. https://www.cambridgeenglish.org/learning-english/free-resources/

OUTCOMES:

Upon completion of the course, the student should be able to

1. Express and explain short texts on different topics with key information applying suitable vocabulary (K2)
2 Interpret and dramatize fluently in informal and formal contexts(K2)
3 Choose and apply the right syntax in comprehending diversified general and technical articles (K3)
4 Analyze and write technical concepts in simple and lucid style (K3)
5 Construct informal letters and e-mails thoughtfully (K2)
6 Demonstrate technical concepts and summaries in correct grammar and vocabulary (K2)

CO - PO MAPPING :

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	-	-	-	-	-	-	1	-	2	3	1	1
CO2	-	-	-	-	-	-	-	1	2	3	2	1
CO3	-	-	-	-	-	-	-	-	1	3	3	2
CO4	-	2	-	-	-	-	-	1	2	3	1	1
CO5	-	-	-	-	-	-	-	2	-	3	2	1
CO6	-	-	-	-	-	-	3	-	-	3	2	1

SEMESTER - I

20BSPH101 SDG NO. 4	ENGINEERING PHYSICS	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To educate and enhance the fundamental knowledge in Physics and its applications relevant to various streams of Engineering and Technology

UNIT I CRYSTAL PHYSICS 9

Single crystalline, Polycrystalline and Amorphous materials - single crystals: unit cell, crystal systems, Bravais lattices, directions and planes in a crystal - Miller indices - Interplanar distance - Powder diffraction method - Debye Scherer formula - Calculation of number of atoms per unit cell - Atomic radius - Coordination number - packing factor for SC, BCC, FCC and HCP structures - Polymorphism and allotropy - Diamond and Graphite structure (qualitative) - Growth of single crystals: Solution and Melt growth Techniques.

UNIT II PROPERTIES OF MATTER 9

Elasticity - Stress - strain diagram and its uses - Poisson's ratio - Relationship between three moduli of elasticity (qualitative) - Factors affecting elastic modulus and tensile strength - Twisting couple - shaft - Torsion pendulum: theory and experiment - bending of beams - bending moment - cantilever: theory and experiment - uniform and non-uniform bending: theory and experiment - I-shaped girders - stress due to bending in beams.

UNIT III QUANTUM PHYSICS 9

Black body radiation - Planck's theory (derivation) - Compton effect: theory -

wave particle duality - electron diffraction - progressive waves - wave equation - concept of wave function and its physical significance - Schrödinger's wave equation - Time independent and Time dependent equations - particle in a box (one dimensional motion) - Tunneling (qualitative) - scanning tunneling microscope.

UNIT IV LASERS AND FIBER OPTICS 9

Lasers: population of energy levels, Einstein's A and B coefficients derivation - pumping methods - resonant cavity, optical amplification (qualitative) - three level and four level laser - CO_2 laser - Semiconductor lasers: Homojunction and Heterojunction.

Fiber optics: Principle, Numerical aperture and Acceptance angle - Types of optical fibers (material, refractive index, mode) - Losses associated with optical fibers - Fiber Optical Communication system (Block diagram) - Fiber optic sensors: pressure and displacement.

UNIT V THERMAL PHYSICS 9

Transfer of heat energy - thermal expansion of solids and liquids - bimetallic strips - thermal conduction, convection and radiation - heat conduction in solids (qualitative) - thermal conductivity - Forbe's and Lee's disc method: theory and experiment - conduction through compound media (series and parallel) - thermal insulation - applications: heat exchangers, refrigerators and solar water heaters.

TOTAL : 45 PERIODS

TEXT BOOKS:

1. D.K. Bhattachary & T.Poonam, "Engineering Physics". Oxford University Press, 2015.
2. R.K. Gaur& S.L. Gupta, "Engineering Physics". Dhanpat Rai Publishers, 2012.
3. B.K. Pandey & S.Chaturvedi, "Engineering Physics", Cengage Learning India, 2017.
4. V. Rajendran, "Engineering Physics", Mc Graw Hill Publications Ltd. New Delhi, 2014.
5. M.N. Avadhanulu& P.G. Kshirshagar, "A textbook of Engineering Physics", S. Chand & Co Ltd. 2016.

REFERENCES:

1. D. Halliday, . Resnick & J. Walker, "Principles of Physics", Wiley, 2015.
2. R.A. Serway, & J.W. Jewett, "Physics for Scientists and Engineers", Cengage Learning, 2010.
3. N.K. Verma," Physics for Engineers", PHI Learning Private Limited, 2014.

4. P.A. Tipler & G. Mosca "Physics for Scientists and Engineers", W.H.Freeman, 2020.
5. Brijlal and Subramanyam, "Properties of Matter", S. Chand Publishing, 2018.
6. Shatendra Sharma & Jyotsna Sharma, "Engineering Physics", Pearson, 2018.

OUTCOMES :

Upon completion of the course, the student should be able to

1. To understand the crystal systems and elastic properties of Materials (K2)
2. To distinguish different crystal structures and heat conduction in conductor and insulators (K4)
3. To explain powder diffractionmethod-deformation of materials in response to action load,quantum mechanics to understand wave particle dualism (K2)
4. To apply quantum theory to set up one dimensional Schrodinger's wave equation and applications to a matter wave system and principle of laser action (K3)
5. To analyze bending of beams,types of optical fiber and modes of heat transfer (K4)
6. To discuss light propagation in optical fibers and transfer of heat energy in different measures and its applications (K2)

CO - PO MAPPING :

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	3	3	-	-	-	-	-	-	-	1
CO2	3	2	3	3	-	-	2	-	-	-	-	3
CO3	3	3	3	2	-	-	3	-	-	-	-	2
CO4	3	3	3	3	-	-	-	-	-	-	-	3
CO5	3	3	3	3	-	-	3	-	-	-	-	3
CO6	3	3	3	3	-	-	3	-	-	-	-	3

SEMESTER - I

20BSCY101 SDG NO. 4,6&7	ENGINEERING CHEMISTRY	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To make the students conversant with boiler feed water requirements, related problems and water treatment techniques
- To illustrate the principles of electrochemical reactions, redox reactions in corrosion of materials and methods for corrosion prevention and protection of materials
- To categorize types of fuels, calorific value calculations, manufacture of solid, liquid and gaseous fuels
- To demonstrate the principles and generation of energy in batteries, nuclear reactors, solar cells, windmills and fuel cells
- To recognize the applications of polymers, composites and nano-materials in various fields

UNIT I WATER TECHNOLOGY AND SURFACE CHEMISTRY 9

Water Technology : Introduction – Hard water and Soft water. Hardness of water – types – expression of hardness (numerical problems). Boiler troubles – scale and sludge, priming and foaming, caustic embrittlement and boiler corrosion. Treatment of boiler feed water – Internal treatment (carbonate, phosphate, calgon, colloidal and sodium aluminate conditioning). External treatment – Ion exchange process, Zeolite process –Domestic water treatment (break point chlorination) –Desalination of brackish water – Reverse Osmosis.

Surface Chemistry: Adsorption – types – adsorption of gases on solids – adsorption of solutes from solution – applications of adsorption –role of adsorbents in catalysis and pollution abatement.

UNIT II ELECTROCHEMISTRY AND CORROSION 9

Electrochemistry: Cells – types (electrochemical and electrolytic cell) Redox reaction – single electrode potential (oxidation potential and reduction potential) – measurement and applications –Nernst equation (derivation and problems) – electrochemical series and its significance.

Corrosion: Causes, factors and types – chemical and electrochemical corrosion (galvanic, differential aeration). Corrosion control – material selection and design aspects, cathodic protection methods (sacrificial anodic and impressed current cathodic method) and corrosion inhibitors. Paints: Constituents and its functions. Electroplating of Copper and electroless plating of Nickel.

UNIT III FUELS AND COMBUSTION 9

Fuels: Introduction – classification of fuels – Coal – analysis of coal (proximate and ultimate). Carbonization – manufacture of metallurgical coke (Otto Hoffmann method) – Petroleum – manufacture of synthetic petrol (Bergius process). Knocking – octane number and cetane number – Gaseous fuels – Compressed natural gas (CNG), Liquefied petroleum gases (LPG). Biofuels – Gobar gas and Biodiesel.

Combustion of Fuels: Introduction – calorific value – higher and lower calorific values- theoretical calculation of calorific value – flue gas analysis (ORSAT Method).

UNIT IV ENERGY SOURCES AND STORAGE DEVICES 9

Energy sources: Nuclear fission – nuclear fusion – differences between nuclear fission and fusion – nuclear chain reactions – nuclear energy – light water nuclear power plant – breeder reactor – solar energy conversion – solar cells – wind energy.

Storage devices: Batteries – types of batteries – primary battery (dry cell) secondary battery (lead acid battery, lithium–ion–battery), fuel cells – H_2 -O_2 fuel cell and super capacitors.

UNIT V POLYMERS AND NANOMATERIALS 9

Polymers: Classification – types of polymerization – mechanism (Free radical polymerization) –Engineering polymers: Nylon–6, Nylon–6,6, Teflon, Kevlar and PEEK – preparation, properties and uses – Plastic and its types – Conducting polymers – types and applications. Composites – definition, types, polymer matrix composites – FRP.

Nanomaterials: Introduction – Nanoparticles, Nanoclusters, Nanorods, Nanotubes (CNT: SWNT and MWNT) and Nanowires – Properties (surface to volume ratio, melting point, optical and electrical), Synthesis (precipitation, thermolysis, hydrothermal, electrodeposition, chemical vapour deposition, laser ablation, sol-gel process) and Applications.

TOTAL: 45 PERIODS

TEXT BOOKS:

1. S. S. Dara and S. S. Umare, "A Textbook of Engineering Chemistry", S. Chand & Company LTD, New Delhi, 2015.
2. P. C. Jain and Monika Jain, "Engineering Chemistry" DhanpatRai Publishing Company (P) LTD, New Delhi, 2015.
3. S. Vairam, P. Kalyani and Suba Ramesh, "Engineering Chemistry", Wiley India PVT, LTD, New Delhi, 2013.
4. Ravikrishnan A, 'Engineering Chemistry', Sri Krishna Hitech Publishing Company Pvt. Ltd, New Edition 2021.

REFERENCES:

1. Friedrich Emich, "Engineering Chemistry", Scientific International PVT, LTD, New Delhi, 2014.
2. Prasanta Rath, "Engineering Chemistry", Cengage Learning India PVT, LTD, Delhi, 2015.
3. Shikha Agarwal, "Engineering Chemistry-Fundamentals and Applications", Cambridge University Press, Delhi, 2015.

OUTCOMES

Upon completion of the course, the student should be able to

1. Identify the origin of water resources and develop innovative methods to produce soft water for industrial use and potable water at cheaper cost and recognize the basic design of adsorption systems and its industrial applications. (K2)
2. Recognize the basic concepts of electrochemistry and apply the principles of electrochemistry to corrosion process and the applications of protective coatings to overcome the corrosion. (K2)
3. Disseminating the importance of chemistry of fuels and combustion to enhance the fuel efficiency. (K2)
4. Acquire the basics of non-conventional sources of energy and illustrate the principles and the reaction mechanism of batteries and fuel cells. (K2)
5. Explain the synthesis and applications of polymers, composites and nano-materials. (K2)

CO – PO MAPPING:

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

SEMESTER - I

20ESCS101 SDG NO. 4&9	PROBLEM SOLVING AND PROGRAMMING IN C	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To understand about the programming language
- To develop C Programs using basic Programming Constructs, Loops Arrays and Strings
- To develop applications in C using Functions , Pointers and Structures
- To perform I/O operations and File Handling in C

UNIT I INTRODUCTION TO PROGRAMMING AND ALGORITHMS FOR PROBLEM SOLVING 10

The Basic Model of Computation, Programming Paradigms- Program Development Life Cycle - Algorithm –Pseudo Code – Flow Chart - Programming Languages - Compilation - Linking and Loading - Testing and Debugging - Documentation - Control Structures – Algorithmic Problem Solving- Problems Based on Sequential, Decision Making - Branching and Iteration.

UNIT II BASICS OF C PROGRAMMING 8

Structure of C program - C programming: Data Types – Storage Classes - Constants – Enumeration Constants - Keywords – Operators: Precedence and Associativity - Expressions – Input / Output Statements - Assignment Statements – Decision making Statements - Switch Statement - Looping Statements – Pre-Processor Directives - Compilation Process

UNIT III ARRAYS AND STRINGS 9

Introduction to Arrays: Declaration, Initialization – One Dimensional Array – Example Program: Computing Mean, Median and Mode - Two Dimensional Arrays – Example Program: Matrix Operations (Addition, Scaling, Determinant and Transpose) - String Operations: Length, Compare, Concatenate - Copy – Selection Sort - Linear and Binary Search.

UNIT IV FUNCTIONS AND POINTERS 9

Introduction to Functions: Function Prototype, Function Definition, Function Call, Built-in Functions (String Functions, Math Functions) – Recursion – Example Program: Computation of Sine Series - Scientific Calculator using Built-in Functions - Binary Search using Recursive Functions – Pointers – Pointer Operators – Pointer Arithmetic – Arrays and Pointers –

Array of Pointers – Example Program: Sorting of Names – Parameter Passing: Pass by Value - Pass by Reference – Example Program: Swapping of Two Numbers using Pass by Reference.

UNIT V STRUCTURES and FILE PROCESSING 9

Structure - Nested Structures – Pointer and Structures – Array of Structures – Example Program using Structures and Pointers – Self Referential Structures – Dynamic Memory Allocation - Singly Linked List – Typedef.

Files – Types of File Processing: Sequential Access, Random Access – Sequential Access File - Example Program: Finding Average of Numbers stored in Sequential Access File - Random Access File - Example Program: Transaction Processing Using Random Access Files – Command Line Arguments.

TOTAL: 45 PERIODS

TEXT BOOKS:

1. Reema Thareja, "Programming in C", Oxford University Press, Second Edition, 2016.
2. Kernighan, B.W and Ritchie,D.M, "The C Programming language", Second Edition, Pearson Education, 2012.

REFERENCES:

1. Paul Deitel and Harvey Deitel, "C How to Program", Seventh edition, Pearson Publication, 2015.
2. Jeri R. Hanly & Elliot B. Koffman, "Problem Solving and Program Design in C", Pearson Education, 2013.
3. Pradip Dey, Manas Ghosh, "Fundamentals of Computing and Programming in C", First Edition, Oxford University Press, 2009.
4. Anita Goel and Ajay Mittal, "Computer Fundamentals and Programming in C", Dorling Kindersley (India) Pvt. Ltd., Pearson Education in South Asia, 2011.
5. Byron S. Gottfried, "Schaum's Outline of Theory and Problems of Programming with C", McGraw-Hill Education, 1996.
6. Kanetkar Y, "Let us C", BPB Publications, 2007.
7. Hanly J R & Koffman E.B, "Problem Solving and Programme design in C", Pearson Education, 2009.

WEB REFERENCES:

1. https://www.learn-c.org/
2. https://codeforwin.org/
3. https://www.cprogramming.com/

ONLINE RESOURCES:

1. https://www.linuxtopia.org/online_books/programming_books/gnu_c_programming_tutorial
2. https://nptel.ac.in/courses/106105171
3. https://swayam.gov.in/nd1_noc19_cs42/preview

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the concepts of algorithms for solving a problem. (K2)
2. Illustrate the various constructs in C to develop simple applications. (K3)
3. Understand the concepts of Array & Strings. (K2)
4. Demonstrate the usage of Functions and Pointers. (K3)
5. Explain the Structure and union concepts. (K2)
6. Describe the file manipulation and its organisation.(K2)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	3	3	2	1	1	-	2	2	-	3	2	3
CO2	3	3	3	3	2	-	1	1	2	2	3	3	2	3
CO3	3	3	3	3	2	1	1	1	2	-	3	-	3	2
CO4	3	3	3	3	2	1	-	1	2	2	3	3	1	2
CO5	3	3	3	3	2	1	1	1	2	2	3	3	2	1
CO6	3	3	3	3	2	1	1	1	2	2	3	3	3	2

SEMESTER - I

20ESGE101 SDG NO. 4,6,7, 9, 12,14 &15	ENGINEERING GRAPHICS	L	T	P	C
		1	2	0	3

OBJECTIVES:

- To develop in students, graphic skills for communication of concepts, ideas and design of engineering products
- To visualize the job in three dimensions
- To have a clear conception and appreciation of the shape, size, proportion and design
- To expose the student community to existing national standards related to technical drawings

CONCEPTS AND CONVENTIONS (Not for Examination) 3

Importance of graphics in engineering applications – Use of drafting instruments – BIS conventions and specifications – Size, layout and folding of drawing sheets – Lettering and dimensioning- Projection of Points

UNIT I PLANE CURVES AND FREEHAND SKETCHING 6+9

Basic Geometrical constructions, Curves used in engineering practices: Conics – Construction of ellipse, parabola and hyperbola by eccentricity method – Construction of cycloid on Horizontal Surfaces – construction of involutes of circle for one complete revolution – Drawing of tangents and normal to the above curves.

Visualization concepts and Free Hand sketching: Visualization principles –Representation of Three Dimensional objects – Layout of views- Freehand sketching of multiple views from pictorial views of objects.

UNIT II PROJECTION OF LINES AND PLANE SURFACE 6+9

Orthographic projection- principles-Principal planes- Projection of straight lines (only First angle projections) inclined to both the principal planes - Determination of true lengths and true inclinations by rotating line method- Projection of planes (polygonal and circular surfaces) inclined to both the principal planes by rotating object method.

UNIT III PROJECTION OF SOLIDS 6+9

Projection of simple solids like prisms, pyramids, cylinder and cone when the axis is inclined to one of the principal planes by rotating object method.

UNIT IV PROJECTION OF SECTIONED SOLIDS AND DEVELOPMENT OF SURFACES 6+9

Sectioning of prisms, pyramids, cylinder and cone in simple vertical position when the cutting plane is inclined to one of the principal planes and perpendicular to the other – obtaining true shape of section. Development of lateral surfaces of simple and truncated solids in vertical position – Prisms, pyramids cylinder and cone.

UNIT V ISOMETRIC AND PERSPECTIVE PROJECTIONS 6+9

Principles of isometric projection – isometric scale –Isometric projections of simple solids and truncated solids - Prisms, pyramids, cylinder, cone- Perspective projection of simple solids-Prisms, pyramids and cylinder by visual ray method.

TOTAL: 78 PERIODS

TEXT BOOKS:

1. Venugopal K. and Prabhu Raja V., "Engineering Graphics", New Age International (P) Limited, 2008.
2. T. Jeyapoovan, "Engineering Graphics using AUTOCAD", Vikas Publishing House Pvt Ltd, 7th Edition.

REFERENCES:

1. Bhatt N.D. and Panchal V.M., "Engineering Drawing", Charotar Publishing House, 50th Edition, 2010.
2. Natrajan K.V., "A text book of Engineering Graphics", Dhanalakshmi Publishers, Chennai, 2009.
3. Basant Agarwal and Agarwal C.M., "Engineering Drawing", Tata McGraw Hill Publishing Company Limited, New Delhi, 2008.
4. Gopalakrishna K.R., "Engineering Drawing" (Vol. I&II combined), Subhas Stores, Bangalore, 2007.
5. Luzzader, Warren.J. and Duff,John M., "Fundamentals of Engineering Drawing with an introduction to Interactive Computer Graphics for Design and Production, Eastern Economy Edition, Prentice Hall of India Pvt. Ltd, New Delhi, 2005.
6. N S Parthasarathy and Vela Murali, "Engineering Graphics", Oxford University, Press, New Delhi, 2015.
7. Shah M.B., and Rana B.C., "Engineering Drawing", Pearson, 2nd Edition, 2009.

WEB REFERENCES:

1. https://nptel.ac.in/courses/112/103/112103019/

ONLINE RESOURCES:

1. https://nptel.ac.in/courses/105/104/105104148/

PUBLICATION OF BUREAU OF INDIAN STANDARDS:

1. IS10711 – 2001: Technical products Documentation – Size and lay out of drawing sheets.
2. IS9609 (Parts 0 & 1) – 2001: Technical products Documentation – Lettering.
3. IS10714 (Part 20) – 2001 & SP 46 – 2003: Lines for technical drawings.
4. IS11669 – 1986 & SP 46 – 2003: Dimensioning of Technical Drawings.
5. IS15021 (Parts 1 to 4) – 2001: Technical drawings – Projection Methods

OUTCOMES:

Upon completion of the course, the student should be able to

1. Relate thoughts and ideas graphically in a neat fashion and ability to perform sketching of engineering curves used in engineering practices, multiple views of objects. (K1)
2. Understand the concepts of orthographic projections for basic geometrical constructions. (K2)
3. Acquire the knowledge of orthographic projection in three dimensional object. (K2)
4. Develop knowledge about Sectioning and apply interior shapes of solids. (K3)
5. Analyze the concepts of design in developing various 3 dimensional projections. (K4)
6. Build a strong foundation to analyze the design in various dimensions. (K4)

CO - PO , PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	2	-	-	-	-	-	2	2	-	2	2	2
CO2	3	2	2	-	-	-	-	-	2	2	-	2	2	2
CO3	3	2	2	-	-	-	-	-	2	2	-	2	2	2
CO4	3	2	2	-	-	-	-	-	2	2	-	2	2	2
CO5	3	2	2	-	-	-	-	-	2	2	-	2	2	2
CO6	3	2	2	-	-	-	-	-	2	2	-	2	2	2

SEMESTER - I

20BSPL101 SDG NO. 4	PHYSICS AND CHEMISTRY LABORATORY	L	T	P	C
		0	0	3	1.5

PHYSICS LABORATORY

OBJECTIVES:

- To acquaint the students with practical knowledge of physics principles in various fields such as optics, thermal physics and properties of matter for developing basic experimental skills
- To make the student to acquire practical skills in the determination of water quality parameters through volumetric and instrumental analysis

LIST OF EXPERIMENTS (Any 5 Experiments)

1. Determination of Young's modulus by non-uniform bending method.
2. Determination of rigidity modulus –Torsion pendulum.
3. Determination of velocity of sound and compressibility of liquid – Ultrasonic Interferometer.
4. (a) Determination of wavelength and particle size using Laser.
   (b) Determination of acceptance angle in an optical fiber.
5. Determination of thermal conductivity of a bad conductor – Lee's Disc method.
6. Determination of specific resistance of a given coil of wire – Carey Foster's bridge.
7. Determination of wavelength of mercury spectrum – spectrometer grating.
8. Determination of band gap of a semiconductor.
9. Determination of Hall coefficient by Hall Effect experiment.
10. Determination of solar cell characteristics.

LAB REQUIREMENTS FOR A BATCH OF 30 STUDENTS / 6 (max.) STUDENTS PER EXPERIMENT

1. Young's modulus by non-uniform bending method-experimental set-up – 12 sets
2. Rigidity modulus - Torsion pendulum experimental set-up – 12 sets
3. Ultrasonic Interferometer to determine velocity of sound and compressibility of liquid – 6 sets
4. (a) Experimental set-up to find the wavelength of light, and to find particle size using Laser – 6 sets
   (b) Experimental set-up to find acceptance angle in an optical fiber – 6 sets
5. Lee's disc method- experimental set up to find thermal conductivity of a bad conductor – 6 sets
6. Experimental set-up to find specific resistance of a coil of wire-Carey Foster's Bridge – 6 sets
7. Experimental set-up to find the wavelength of mercury spectrum-spectrometer grating – 6 sets
8. Experimental set-up to find the band gap of a semiconductor – 12 sets
9. Experimental set-up to find the Hall coefficient by Hall Effect Experiment – 6 sets

10. Experimental set-up to study characteristics of solar cells – 6 sets

TEXTBOOKS:

1. J.D. Wilson& C.A. Hernandez Hall "Physics Laboratory Experiments" Houghton Mifflin Company, New York, 2010.
2. M.N. Srinivasan, S. Balasubramanian &R. Ranganathan, "Practical Physics", S. Chand & Sons educational publications, New Delhi, 2011.
3. R. Sasikumar, "Practical Physics", PHI Learning Pvt. Ltd., New Delhi, 2011.

CHEMISTRY LABORATORY

(Any five experiments to be conducted)

OBJECTIVES:

- To acquaint the students with practical knowledge of the basic concepts of chemistry, the student faces during the course of their study in the industry and engineering field
- To make the student to acquire practical skills in the determination of water quality parameters through volumetric and instrumental analysis
- To understand and develop experimental skills for building technical competence

LIST OF EXPERIMENTS (Any five experiments to be conducted)

1. Estimation of HCl using Na_2CO_3 as primary standard and Determination of alkalinity in water samples.
2. Determination of total, temporary & permanent hardness of water by EDTA method.
3. Determination of DO content of water sample by Winkler's method.
4. Determination of chloride content of water sample by argentometric method.
5. Determination of strength of given hydrochloric acid using pH meter.
6. Conductometric titration of strong acid vs strong base.
7. Estimation of iron content of the given solution using potentiometer.
8. Estimation of iron content of the water sample using spectrophotometer (1, 10- Phenanthroline / thiocyanate method).
9. Estimation of sodium and potassium present in water using flame photometers.
10. Determination of molecular weights of polymers using Ostwald's Viscometer.

LAB REQUIREMENTS FOR A BATCH OF 30 STUDENTS / 6 (MAX.) STUDENTS PER EXPERIMENT.

1. Estimation of HCl using Na_2CO_3 as primary standard and Determination of alkalinity in water sample - 6 sets
2. Determination of total, temporary & permanent hardness of water by EDTA method - 6 sets
3. Determination of DO content of water sample by Winkler's method - 6sets
4. Determination of chloride content of water sample by argentometric method – 6 sets
5. Determination of strength of given hydrochloric acid using pH meter - 6 sets
6. Conductometric titration of strong acid vs strong base - 6 sets
7. Estimation of iron content of the given solution using potentiometer - 6 sets
8. Estimation of iron content of the water sample using spectrophotometer (1,10- Phenanthroline / thiocyanate method) - 2 sets
9. Estimation of sodium and potassium present in water using flame photometer - 2 sets
10. Determination of molecular weights of polymer using Ostwald's Viscometer. - 6 sets

TOTAL: 30 PERIODS

TEXT BOOKS:

1. Vogel's Textbook of Quantitative Chemical Analysis (8th edition, 2014).

OUTCOMES:

Upon completion of the course, the student should be able to

1. Apply the principles of thermal physics and properties of matter to evaluate the properties of materials and to determine the physical properties of liquid using ultrasonic interferometer. (K1)
2. Understand measurement technique and usage of new instruments in optics for real time application in engineering. (K2)
3. Apply the knowledge of semiconductor materials to evaluate the band gap and Hall coefficient of materials and to study the characteristics of solar cell for engineering solutions. (K3)
4. Interpret quantitative chemical analysis to generate experimental skills in building technical competence. (K3)

5. Analyze the quality of water for domestic and industrial purpose. (K3)
6. Standardize the solutions using volumetric titrations, conductivity, pH, redox potential and optical density measurements. (K3)

CO- PO MAPPING :

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	3	3	2	1	3	3	2	2	1	1	3
CO2	3	3	3	3	3	3	3	2	2	2	2	3
CO3	3	3	3	3	3	3	3	2	1	1	2	3
CO4	3	2	3	3	1	1	2	2	2	2	3	2
CO5	3	2	3	3	1	1	2	2	2	2	3	2
CO6	3	2	3	3	1	1	2	2	2	2	3	2

SEMESTER - I

20ESPL101 SDG NO. 4&9	PROGRAMMING IN C LABORATORY	L	T	P	C
		0	0	3	1.5

OBJECTIVES:

- To develop programs in C using basic Programming Constructs
- To develop applications in C using Arrays and Strings
- To design and implement applications in C using Functions, Structures
- To develop applications in C using Files

LIST OF EXPERIMENTS

1. Write a program using I/O statements and expressions.
2. Write programs using decision-making constructs.
3. Write a program to find whether the given year is leap year or not? (Hint: not every centurion year is a leap. For example 1700, 1800 and 1900 is not a leap year)
4. Write a program to perform the Calculator operations, namely, addition, subtraction, multiplication, division and square of a number.
5. Write a program to check whether a given number is Armstrong number or not?

6. Write a program tocheck whether a given number is odd or even?
7. Write a program to find the factorial of a given number.
8. Write a program to find out the average of 4 integers.
9. Write a program to display array elements using two dimensional arrays.
10. Write a program to perform swapping using function.
11. Write a program to display all prime numbers between two intervals using functions.
12. Write a program to reverse a sentence using recursion.
13. Write a program to get the largest element of an array using the function.
14. Write a program to concatenate two string.
15. Write a program to find the length of String.
16. Write a program to find the frequency of a character in a string.
17. Write a program to store Student Information in Structure and Display it.
18. The annual examination is conducted for 10 students for five subjects. Write a program to read the data and determine the following:
    (a) Total marks obtained by each student.
    (b) The highest marks in each subject and the marks of the student who secured it.
    (c) The student who obtained the highest total marks.
19. Insert, update, delete and append telephone details of an individual or a company into a telephone directory using random access file.
20. Count the number of account holders whose balance is less than the minimum balance using sequential access file.

TOTAL: 45 PERIODS

LIST OF EQUIPMENT FOR A BATCH OF 30 STUDENTS:

Standalone desktops with C compiler 30 Nos.

(or)

Server with C compiler supporting 30 terminals or more.

OUTCOMES:

Upon completion of the course, the student should be able to

1. Solve some simple problems leading to specific applications. (K3)
2. Demonstrate C programming development environment, compiling, debugging, linking and executing a program. (K3)
3. Illustrate C programs for simple applications making use of basic constructs, arrays and strings. (K3)
4. Construct C programs involving functions and recursion. (K3)

5. Demonstrate C programs involving pointers, and structures. (K3)
6. Interpret applications using sequential and random access file. (K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	3	3	2	1	1	-	2	2	-	3	2	3
CO2	3	3	3	3	2	-	1	1	2	2	3	3	2	3
CO3	3	3	3	3	2	1	1	1	2	-	3	-	3	2
CO4	3	3	3	3	2	1	-	1	2	2	3	3	1	2
CO5	3	3	3	3	2	1	1	1	2	2	3	3	2	1
CO6	3	3	3	3	2	1	1	1	2	2	3	3	3	2

SEMESTER - II

20HSTA101 SDG NO. 4	HERITAGE OF TAMILS	L	T	P	C
		1	0	0	1

UNIT I LANGUAGE AND LITERATURE 3

Language Families in India - Dravidian Languages – Tamil as a Classical Language - Classical Literature in Tamil – Secular Nature of Sangam Literature – Distributive Justice in Sangam Literature - Management Principles in Thirukural - Tamil Epics and Impact of Buddhism & Jainism in Tamil Land - Bakthi Literature Azhwars and Nayanmars - Forms of minor Poetry - Development of Modern literature in Tamil - Contribution of Bharathiyar and Bharathidhasan.

UNIT II HERITAGE - ROCK ART PAINTINGS TO MODERN ART – SCULPTURE 3

Hero stone to modern sculpture - Bronze icons - Tribes and their handicrafts - Art of temple car making - - Massive Terracotta sculptures, Village deities, Thiruvalluvar Statue at Kanyakumari, Making of musical instruments - Mridhangam, Parai, Veenai, Yazh and Nadhaswaram - Role of Temples in Social and Economic Life of Tamils.

UNIT III FOLK AND MARTIAL ARTS 3

Therukoothu, Karagattam, Villu Pattu, Kaniyan Koothu, Oyillattam, Leather puppetry, Silambattam, Valari, Tiger dance - Sports and Games of Tamils.

UNIT IV THINAI CONCEPT OF TAMILS 3

Flora and Fauna of Tamils & Aham and Puram Concept from Tholkappiyam and Sangam Literature - Aram Concept of Tamils - Education and Literacy during Sangam Age - Ancient Cities and Ports of Sangam Age - Export and Import during Sangam Age - Overseas Conquest of Cholas.

UNIT V CONTRIBUTION OF TAMILS TO INDIAN NATIONAL MOVEMENT AND INDIAN CULTURE 3

Contribution of Tamils to Indian Freedom Struggle - The Cultural Influence of Tamils over the other parts of India – Self-Respect Movement - Role of Siddha Medicine in Indigenous Systems of Medicine – Inscriptions & Manuscripts – Print History of Tamil Books.

TOTAL : 15 PERIODS

TEXT-CUM-REFERENCE BOOKS

1. தமிழக வரலாறு - மக்களும் பண்பாடும் - கே.கே. பிள்ளை (வெளியீடு: தமிழ்நாடு பாடநூல் மற்றும் கல்வியியல் பணிகள் கழகம்).
2 கணினித் தமிழ் - முனைவர் இல. சுந்தரம். (விகடன் பிரசுரம்).
3 கீழடி - வைகை நதிக்கரையில் சங்ககால நகர நாகரிகம் (தொல்லியல் துறை வெளியீடு)
4. பொருநை - ஆற்றங்கரை நாகரிகம். (தொல்லியல் துறை வெளியீடு)
5. Social Life of Tamils (Dr.K.K.Pillay) A joint publication of TNTB & ESC and RMRL – (in print)
6. Social Life of the Tamils - The Classical Period (Dr.S.Singaravelu) (Published by: International Institute of Tamil Studies.
7. Historical Heritage of the Tamils (Dr.S.V.Subatamanian, Dr.K.D. Thirunavukkarasu) (Published by: International Institute of Tamil Studies).
8. The Contributions of the Tamils to Indian Culture (Dr.M.Valarmathi) (Published by: International Institute of Tamil Studies.)
9. Keeladi - 'Sangam City Civilization on the banks of river Vaigai' (Jointly Published by: Department of Archaeology & Tamil Nadu Text Book and Educational Services Corporation, Tamil Nadu)
10. Studies in the History of India with Special Reference to Tamil Nadu (Dr.K.K.Pillay) (Published by: The Author)
11. Porunai Civilization (Jointly Published by: Department of Archaeology & Tamil Nadu Text Book and Educational Services Corporation, Tamil Nadu)
12. Journey of Civilization Indus to Vaigai (R.Balakrishnan) (Published by: RMRL) – Reference Book.

தமிழர் மரபு

அலகு I மொழி மற்றும் இலக்கியம்: 3

இந்திய மொழிக் குடும்பங்கள் - திராவிட மொழிகள் - தமிழ் ஒரு செம்மொழி - தமிழ் செவ்விலக்கியங்கள் - சங்க இலக்கியத்தின் சமயச் சார்பற்ற தன்மை - சங்க இலக்கியத்தில் பகிர்தல் அறம் - திருக்குறளில் மேலாண்மைக் கருத்துக்கள் - தமிழ்க் காப்பியங்கள், தமிழகத்தில் சமண பௌத்த சமயங்களின் தாக்கம் - பக்தி இலக்கியம், ஆழ்வார்கள் மற்றும் நாயன்மார்கள் - சிற்றிலக்கியங்கள் - தமிழில் நவீன இலக்கியத்தின் வளர்ச்சி - தமிழ் இலக்கிய வளர்ச்சியில் பாரதியொர் மற்றும் பாரதிதாசன் ஆகியோரின் பங்களிப்பு.

அலகு II மரபு - பாறை ஓவியங்கள் முதல் நவீன ஓவியங்கள் வரை - சிற்பக் கலை: 3

நடுகல் முதல் நவீன சிற்பங்கள் வளர - ஐம்பொன் சிலைகள் - பழங்குடியினர்

மற்றும் அவர்கள் தயாரிக்கும் கைவினைப் பொருட்கள், பொம்மைகள் - கதர் செய்யும் கலை - சுடுமண் சிற்பங்கள் - நாட்டுப்புறத் தெய்வங்கள் - குமரிமுனையில் திருவள்ளுவர் சிலை - இசைக் கருவிகள் - மிருதங்கம், பறை, வீணை, யாழ், நாதஸ்வரம் - தமிழர்களின் சமூக பொருளாதார வாழ்வில் கோவில்களின் பங்கு.

அலகு III நாட்டுப்புறக் கலைகள் மற்றும் வீர விளையாட்டுகள்: 3

தெருக்கூத்து, கரகாட்டம், வில்லுப்பாட்டு, கணியான் கூத்து, ஒயிலொட்டம், தொல்பாவைக் கூத்து, சிலம்பாட்டம், வளரி, புலியாட்டம், தமிழர்களின் விளையாட்டுகள்.

அலகு IV தமிழர்களின் திறைக் கோட்பாடுகள்: 3

தமிழகத்தின் தாவரங்களும், விலங்குகளும் - தொல்கொப்பியம் மற்றும் சங்க இலக்கியத்தில் அகம் மற்றும் புறக் கோட்பாடுகள் - தமிழர்கள் போற்றிய அறக்கோட்பாடு - சங்ககாலத்தில் தமிழகத்தில் எழுத்தறிவும், கல்வியும் - சங்ககால நகரங்களும் துறை முகங்களும் - சங்ககாலத்தில் ஏற்றுமதி மற்றும் இறக்குமதி - கடல்கடந்த நாடுகளில் சோழர்களின் வெற்றி.

அலகு V இந்திய தேசிய இயக்கம் மற்றும் இந்திய பண்ப்பாட்டிற்குத் தமிழர்களின் பங்களிப்பு: 3

இந்திய விடுதலைப்போரில் தமிழர்களின் பங்கு - இந்தியாவின் பிறப்பகுதிகளில் தமிழ்ப் பண்பாட்டின் தாக்கம் - சுயமரியாதை இயக்கம் - இந்திய மருத்துவத்தில், சித்த மருத்துவத்தின் பங்கு - கல்வெட்டுகள், கையெழுத்துப்படிகள் - தமிழ்ப் புத்தகங்களின் அச்சு வரலாறு.

TOTAL : 15 PERIODS

TEXT-CUM-REFERENCE BOOKS

1. தமிழக வரலாறு — மக்களும் பண்பாடும் — கே.கே. பிள்ளை (வெளியீடு: தமிழ்நாடு பாடநூல் மற்றும் கல்வியியல் பணிகள் கழகம்).
2. கணினித் தமிழ் - முனைவர் இல. சுந்தரம். (விகடன் பிரசுரம்).
3. கீழடி - வைகை நதிக்கரையில் சங்ககால நகர நாகரிகம் (தொல்லியல் துறை வெளியீடு)
4. பொருநை - ஆற்றங்கரை நாகரிகம். (தொல்லியல் துறை வெளியீடு)
5. Social Life of Tamils (Dr.K.K.Pillay) A joint publication of TNTB & ESC and RMRL – (in print)
6. Social Life of the Tamils - The Classical Period (Dr.S.Singaravelu) (Published by: International Institute of Tamil Studies.
7. Historical Heritage of the Tamils (Dr.S.V.Subatamanian, Dr.K.D. Thirunavukkarasu) (Published by: International Institute of Tamil Studies).
8. The Contributions of the Tamils to Indian Culture (Dr.M.Valarmathi) (Published by: International Institute of Tamil Studies.)

9. Keeladi - 'Sangam City Civilization on the banks of river Vaigai' (Jointly Published by: Department of Archaeology & Tamil Nadu Text Book and Educational Services Corporation, Tamil Nadu)
10. Studies in the History of India with Special Reference to Tamil Nadu (Dr.K.K.Pillay) (Published by: The Author)
11. Porunai Civilization (Jointly Published by: Department of Archaeology & Tamil Nadu Text Book and Educational Services Corporation, Tamil Nadu)
12. Journey of Civilization Indus to Vaigai (R.Balakrishnan) (Published by: RMRL) – Reference Book.

SEMESTER - I

20TPHS101 SDG NO. 4&5	SKILL ENHANCEMENT	L	T	P	C
		0	0	2	1

OBJECTIVES:

- To enrich social network ethics
- To develop and enhance browsing culture
- To understand the concepts of networking
- To promote self professionalism
- To acquire knowledge about various digital identification procedures

UNIT I SOCIAL NETWORK ETIQUETTES 6

Introduction to social network – Social Networking Etiquettes - Pros and Cons - Usage of Facebook, Instagram, WhatsApp , Telegram, Youtube, Evolution of Android and IOS, Introduction to Linkedin & Benefits. (Practicals – Official Mail id- Linkedin Id Creation, Linkedin Profile Bulilding , Facebook Id and Creation and Modifying the existing FB ID)

UNIT II BROWSING CULTURE 6

Introduction to browsing – Search Engines-Google - Bing -Yahoo!-AOL -MSN –DuckDuckGo ,browsers, phishing – Cookies - URL – https:// extensions , browsing history, Incognito mode- VPN – Pros and Cons – Book mark.

UNIT III NETWORKING 6

Basics of networking - LAN, MAN, WAN, Introduction to network topologies, Protocols , IP Commands (Command line prompt), Define online complier and editor (Practicals – Find Your System IP,Ping Command, Firewall Fortinet, Basic DOS Commands)

UNIT IV PROFESSIONALISM **6**

Dress Code, Body Language, Appropriate Attire ,Communication Skills, Interview preparation – Introducing yourself - How to greet Superiors, Importance of Eye Contact During conversation.

UNIT V DIGITAL IDENTIFICATION **6**

Introduction to NAD - Importance of Aadhar, PAN Card, Passport, Bank Account, Bar Code, QR scan, Payment Gateway (Gpay, Phone Pe, UPI, BHIM, Paytm), Mobile Banking (Practicals - NAD registration Step by Step, Linking bank account with netbanking , Register for payment gateway).

TOTAL : 30 PERIODS

WEB REFERENCES :

Unit I: Social Network Etiquettes:

1. https://sproutsocial.com/glossary/social-media-etiquette/
2. https://www.shrm.org/resourcesandtools/tools-and-samples/hr-qa/pages/socialnetworkingsitespolicy.aspx
3. https://www.frontiersin.org/articles/10.3389/fpsyg.2019.02711/full
4. https://medium.com/@sirajea/11-reasons-why-you-should-use-telegram-instead-of-whatsapp-ab0f80fbfa79
5. https://buffer.com/library/how-to-use-instagram/
6. https://www.webwise.ie/parents/what-is-youtube/
7. https://www.androidauthority.com/history-android-os-name-789433/
8. https://www.mindtools.com/pages/article/linkedin.htm

Unit II: Browsing Culture:

1. https://sites.google.com/site/bethanycollegeofteacheredn/unit--ict-connecting-with-world/national-policy-on-information-and-communication-technology-ict/accessing-the-web-introduction-to-the-browser-browsing-web
2. https://www.wordstream.com/articles/internet-search-engines-history
3. https://www.malwarebytes.com/phishing/
4. https://www.adpushup.com/blog/types-of-cookies/
5. https://www.eff.org/https-everywhere
6. https://www.sciencedirect.com/topics/computer-science/browsing-history\
7. https://www.vpnmentor.com/blog/pros-cons-vpn/
8. https://www.tech-wonders.com/2016/10/use-hush-private-bookmarking-extension-chrome.html

Unit III:Networking

1. https://www.guru99.com/types-of-computer-network.html
2. https://www.studytonight.com/computer-networks/network-topology-types
3. https://www.cloudflare.com/learning/network-layer/what-is-a-protocol/
4. https://www.howtogeek.com/168896/10-useful-windows-commands-you-should-know/
5. https://paiza.io/en

Unit IV : Professionalism

1. https://career.vt.edu/develop/professionalism.html
2. https://englishlabs.in/importance-dress-code/
3. https://www.proschoolonline.com/blog/importance-of-body-language-in-day-to-day-life
4. https://www.thespruce.com/etiquette-of-proper-attire-1216800
5. https://shirleytaylor.com/why-are-communication-skills-important/
6. https://www.triad-eng.com/interview-tips-for-engineers/
7. https://www.indeed.co.in/career-advice/interviewing/interview-question-tell-me-about-yourself
8. https://toggl.com/track/business-etiquette-rules/

Unit V: Digital Identification

1. https://nad.ndml.in/nad-presentation.html
2. https://www.turtlemint.com/aadhaar-card-benefits/
3. https://www.bankbazaar.com/pan-card/uses-of-pan-card.html
4. https://www.passportindex.org/passport.php
5. https://consumer.westchestergov.com/financial-education/money-management/benefits-of-a-bank-account
6. https://en.wikipedia.org/wiki/QR_code
7. https://www.investopedia.com/terms/p/payment-gateway.asp
8. https://www.paisabazaar.com/banking/mobile-banking/

OUTCOMES:

Upon completion of the course, the student should be able to

1. Learn and apply social network ethics. (K3)
2. Understand the browsing culture. (K2)
3. Analyze the networking concepts . (K4)
4. Develop self professionalism. (K3)
5. Gain hands-on experience in various digital identification procedures. (K2)
6. Analyse and apply the different digital payment gateway methods. (K4)

CO- PO MAPPING :

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	-	-	-	-	3	2	-	3	2	3	-	2
CO2	-	-	-	-	3	2	-	3	2	3	-	2
CO3	-	-	-	-	3	2	-	-	1	3	-	2
CO4	-	-	-	-	3	2	-	3	3	3	-	2
CO5	-	-	-	-	3	2	-	-	2	3	-	2
CO6	-	-	-	-	3	2	-	-	2	3	-	2

SEMESTER - I

20HSMG101 SDG NO. 4&5	PERSONAL VALUES	L	T	P	C
		2	0	0	0

OBJECTIVES:

- Values through Practical activities

UNIT I SELF CONCEPT **6**

Understanding self Concept – Identify Yourself – Who am I – an individual, engineer, citizen – Attitude – Measuring Behaviour – Change of Behaviour – Personality – Characteristics in personal, professional life.

UNIT II INDIVIDUAL VALUES **6**

Personal Values – Attributes –Courage – Creativity, Honesty, Perfection, Simplicity, Responsibility – Measuring personal values

UNIT III MORAL VALUES **6**

Moral – Understanding right and wrong – Positive thoughts – Respect to others – Doing good to society.

UNIT IV PHYSICAL AND MENTAL WELL-BEING **6**

Health – Physical fitness –Mental vigour – Diet management – Yoga – Meditation – Peaceful life – Happiness in life

UNIT V DECISION MAKING **6**

Goal Setting – Decision making skill – Overcome of Barriers – Success – Mental strength and weakness

TOTAL: 30 PERIODS

Note:

Each topic in all the above units will be supplemented by practice exercises and classroom activities and projects.

REFERENCE BOOKS:

1. Barun K. Mitra, "Personality Development and Soft Skills", Oxford University Press, 2016.
2. B.N.Ghosh, "Managing Soft Skills for Personality Development" McGraw Hill India, 2012.

OUTCOMES:

Upon completion of the course, the student should be able to

1. Become an individual in knowing the self. (K4)
2. Acquire and express Personal Values, Spiritual values and fitness. (K4)
3. Practice simple physical exercise and breathing techniques. (K2)
4. Practice Yoga asana which will enhance the quality of life. (K1)
5. Practice Meditation and get benefitted. (K1)
6. Understanding moral values and need of physical fitness. (K2)

CO – PO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	-	-	-	-	-	2	2	3	3	1	1	1
CO2	-	-	-	-	-	2	2	3	3	1	1	1
CO3	-	-	-	-	-	2	2	3	3	1	1	1
CO4	-	-	-	-	-	2	2	3	3	1	1	1
CO5	-	-	-	-	-	2	2	3	3	1	1	1
CO6	-	-	-	-	-	2	2	3	3	1	1	1

SEMESTER - II

20BSMA204 SDG NO. 4	DISCRETE STRUCTURES	L	T	P	C
		3	1	0	4

OBJECTIVES:

- To learn the basic concepts of Relations and Functions
- To learn the concepts of Mathematical induction, Permutation and Combination
- To understand the concepts of Logic, Rules of inference and Quantifiers
- To impart the knowledge on Groups, Normal subgroups, Rings and Fields
- To develop Graph Algorithms by using the concepts of Graphs and Trees

UNIT I RELATION AND FUNCTION 12

Binary Relation, Partial Ordering Relation, Equivalence Relation – Sum and Product of functions – Bijective functions – Inverse and composite functions.

UNIT II COMBINATORICS 12

The Principles of Mathematical Induction-The Well-Ordering Principle – Recursive definition – Basic counting techniques – Inclusion and exclusion , Pigeonhole principle – Permutation – Combination.

UNIT III LOGICS AND PROOFS 12

Basic Connectives – Truth Tables – Logical Equivalence: The Laws of Logic, Logical Implication – Rules of Inference – The use of Quantifiers – Proof Techniques: Some Terminology – Proof Methods and Strategies – Forward Proof – Proof by Contradiction – Proof by Contraposition.

UNIT IV ALGEBRAIC STRUCTURES 12

Algebraic Structures with One Binary Operation – Semi Groups, Monoids, Groups, Permutation Groups – Subgroups – Normal subgroups – Algebraic Structures with two Binary Operations - Definition and Examples of Rings and Fields – Boolean Algebra – Identities of Boolean Algebra.

UNIT V GRAPHS AND TREES 12

Graphs and their properties – Degree, Connectivity, Path, Cycle – Sub Graph – Isomorphism – Eulerian and Hamiltonian Walks –Rooted Trees, Trees and Sorting.

TOTAL: 60 PERIODS

TEXT BOOKS:

1. Kenneth H. Rosen, "Discrete Mathematics and its Applications: with Combinatorics and Graph Theory", 7th Edition, Tata McGraw –Hill Education Pvt. Ltd., 2015.
2. J.P. Tremblay and R. Manohar, "Discrete Mathematical Structure with Applications to Computer Science", Tata Mc Graw Hill Education (India) Edition 1997.
3. Narsingh Deo, "Graph theory with applications to Engineering and Computer Science", Prentice Hall Inc., Englewood Cliffs,N.J., 1974.

REFERENCES:

1. Susanna S. Epp, "Discrete Mathematics with Applications", 4th edition, Brooks/Cole, Cengage Learning, 2010.
2. Norman L. Biggs, "Discrete Mathematics", 2nd Edition, Oxford University Press, 2002.
3. Seymour Lipschutz, MarcLipson, "Discrete Mathematics, Schaum's Outlines Series", 3rd edition, McGraw-Hill Education, 2009.
4. C. L. Liu and D. P. Mohapatra, "Elements of Discrete Mathematics: A Computer Oriented Approach", 4th Edition, Tata McGraw–Hill Education Pvt. Ltd, 2012.

WEB REFERENCES :

1. https://web.stanford.edu/class/cs103x/cs103x-notes.pdf
2. https://www.cs.cornell.edu/~rafael/discmath.pdf
3. http://home.iitk.ac.in/~arlal/book/mth202.pdf

ONLINE RESOURCES:

1 https://www.youtube.com/watch?v=h_9WjWENWV8&list=PL3o9D 4Dl2FJ9q0_gtFXPh_H4POI5dK0yG
2 https://www.youtube.com/watch?v=xlUFkMKSB3Y&list=PL0862 D1A947252D203.
3 https://www.youtube.com/watch?v=4LlTmsfDS4Y&list=PLEAYk Sg4uSQ2Wfc_l4QEZUSRdx2ZcFziO&index=13
4 https://www.youtube.com/watch?v=jBsEKyx6Rj0&list=PLwdnzl V3ogoVxVxCTlI45pDVM1aoYoMHf
5. https://www.youtube.com/watch?v=rdXw7Ps9vxc&list=PLHXZ9O QGMqxersk8fUxiUMSIx0DBqsKZS

OUTCOMES:

Upon completion of the course, the student should be able to

1. Classify the relations and functions defined on a set. (K2)
2. Apply counting principle and mathematical induction to solve combinatorial problems. (K3)
3. Construct mathematical arguments using logical connectives, quantifiers and verify the correctness of an argument using symbolic logic, truth tables and proof strategies. (K3)
4. Explain the fundamental concepts of algebraic structures such as groups, rings, fields and Boolean algebra. (K3)
5. Illustrate the concepts of graphs and sorting in trees. (K3)

CO- PO MAPPING

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

SEMESTER - II

20HSEN201 SDG NO. 4	TECHNICAL ENGLISH - II	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To strengthen the listening skills for comprehending and critically analyzing passages
- To enhance students' ability with multiple strategies and skills for making technical presentations
- To participate in group discussions for developing group attitude
- To develop skills for preparing effective job application
- To write effective technical reports

UNIT I LANGUAGE DEVELOPMENT 9

Listening – Listening conversations involving two participants – multiple participants – **Speaking** – conversation methods in real life occurrences using expressions of different emotions and imperative usages – **Reading** passages and short stories - **Writing** – preparation of checklist – extended definition – **Language Development** – tenses - subject - verb agreement

UNIT II VOCABULARY BUILDING 9

Listening – listening formal and informal conversation and participative exercises – **Speaking** - creating greetings/wishes/excuses and thanks – **Reading** – articles/novels-**Writing** summary of articles and concise writing identifying new words – homonyms, homophones, homographs – one-word substitutions – easily confused words - creating SMS and using emoticons - sharing information in social media. **Language Development** - reported speeches – regular and irregular verbs - idioms & phrases

UNIT III WRITING TECHNICAL REPORTS 9

Listening – listening conversation – effective use of words and their sound aspects, stress, intonation & pronunciation – **Speaking** - practicing telephonic conversations – observing and responding. **Reading** – regular columns of newspapers/magazines - **Writing** – reports – feasibility, accident, survey and progress - preparation of agenda and minutes – **Language Development** - using connectives – discourse markers

UNIT IV TECHNICAL WRITING 9

Listening – Model debates & documentaries - **Speaking** – expressing agreement/disagreement, assertiveness in expressing opinions – **Reading** biographies/autobiographies – **Writing** – note-making – formal letters – inviting guests – acceptance/declining letters - **Language Development** – degrees of comparison - numerical adjectives – embedded sentences

UNIT V GROUP DISCUSSION AND JOB APPLICATION 9

Listening – Listening - classroom lectures – recommending suggestions & solutions – **Speaking** – participating in group discussion – learning GD strategies – **Reading** – journal articles - Writing – Job application – cover letter - résumé preparation – **Language Development** – purpose statement – editing – verbal analogies.

TOTAL: 45 PERIODS

TEXT BOOKS :

1. Board of editors. Fluency in English: A Course book for Engineering and Technology. Orient Blackswan, Hyderabad 2016.

2. Ashraf Rizvi. M, Effective Technical Communication. 2nd ed. McGraw Hill, New Delhi, 2018.

REFERENCES

1. Bailey, Stephen. Academic Writing: A Practical Guide for Students. Routledge, New York,2011.
2. Raman, Meenakshi and Sharma, Sangeetha. Technical Communication Principles and Practice. Oxford University Press, New Delhi, 2014.
3. Muralikrishnan& Mishra Sunitha, Communication skills for Engineers 2nd ed. Pearson, Tamilnadu, India 2011. P. Kiranmai and Rajeevan, Geetha. Basic Communication Skills, Foundation Books, New Delhi, 2013.
4. Suresh Kumar, E. Engineering English. Orient Blackswan, Hyderabad, 2015
5. Richards, Jack C. Interchange Students' Book – 2. Cambridge University Press, New Delhi, 2015.

WEB REFERENCES :

1. https://swayam.gov.in/nd1_noc20_hs21/preview
2. https://nptel.ac.in/content/storage2/nptel_data3/html/mhrd/ict/text/109106122/lec1.pdf
3. https://freevideolectures.com/course/3250/introduction-to-film-studies/10

ONLINE RESOURCES

1. https://www.ef.com/wwen/english-resources/
2. https://www.smilesforlearning.org/gclid=EAIaIQobChMI49DF9bnd6AIVSY6PCh1d_gV9EAAYASAAEgIBPvD_BwE.

OUTCOMES:

Upon completion of the course, the student should be able to

1. Define technical terms with the correct use of grammar (K1)
2 Identify new words, phrases, idioms and summarize articles/ write ups effectively (K2)
3 Pronounce words correctly, speak fluently and share opinions and suggestions effectively in conversations, debates and discussions (K3)
4 Construct reports convincingly and write official letters emphatically (K3)
5 Communicate confidently while speaking and writing by employing language strategies (K2)

6 Adapt group behavior, execute their role as a contributing team member and prepare winning job applications (K3)

CO - PO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	-	-	-	-	-	-	-	-	2	3	1	2
CO2	-	2	-	-	-	-	-	-	2	3	1	1
CO3	-	-	-	1	-	-	-	2	2	3	1	1
CO4	-	-	-	-	-	2	-	3	2	3	2	2
CO5	-	-	-	-	-	-	-	-	2	3	2	2
CO6	-	-	-	-	-	-	-	2	2	3	1	2

SEMESTER - II

20BSPH203 SDG NO. 4	PHYSICS FOR INFORMATION SCIENCE	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To understand the essential principles of physics of conducting materials, superconducting and optical properties of materials
- To educate the basic principles of semiconductor device and electron transport properties
- To become proficient in magnetic materials
- To acquire the basic working of nanoelectronic devices

UNIT I CONDUCTING MATERIALS **9**

Classical free electron theory - Expression for electrical conductivity - Thermal conductivity expression - Wiedemann-Franz law - Success and failures - Electrons in metals - Motion of a particle in a three dimensional box (Quantum Mechanical Approach) - degenerate states - Fermi- Dirac statistics - Density of energy states - Electron in periodic potential - Energy bands in solids - Tight binding approximation - Electron effective mass - Concept of hole.

UNIT II SEMICONDUCTOR MATERIALS **9**

Intrinsic Semiconductors - Direct and indirect band gap semiconductors - Carrier concentration in intrinsic semiconductors - extrinsic semiconductors -

Carrier concentration in N-type & P-type semiconductors - Variation of carrier concentration with temperature - Variation of Fermi level with temperature and impurity concentration - Carrier transport in Semiconductor: random motion, drift, mobility and diffusion - Hall effect and devices - Ohmic contacts - Schottky diode.

UNIT III MAGNETIC PROPERTIES OF MATERIALS 9

Magnetic dipole moment - atomic magnetic moments - magnetic permeability and susceptibility - Magnetic material classification: diamagnetism - paramagnetism - ferromagnetism - antiferromagnetism - ferrimagnetism - Ferromagnetism: origin and exchange interaction - Domain Theory - M versus H behaviour - Hard and soft magnetic materials - applications - Magnetic principle in computer data storage - Magnetic hard disc - GMR sensor.

UNIT IV SUPERCONDUCTING & OPTICAL PROPERTIES OF MATERIALS 9

Super conductivity - Type-I and Type-II superconductors - Properties and applications - Classification of optical materials - Carrier generation and recombination processes - Photo current in a P-N diode - Solar cell - LED - Organic LED - Optical data storage techniques and devices.

UNIT V NANO DEVICES 9

Introduction - Size dependence of Fermi energy - Quantum confinement - Quantum structures - Density of states in quantum well, quantum wire and quantum dot structure - Band gap of nanomaterials - Tunneling: single electron phenomena and single electron transistor - Quantum dot laser - Carbon nanotubes: Properties and applications.

TOTAL: 45 PERIODS

TEXT BOOKS:

1. Jasprit Singh, "Semiconductor Devices: Basic Principles", Wiley 2012.
2. Kasap, S.O., "Principles of Electronic Materials and Devices", McGraw-HillEducation, 2017.
3. Kittel, C., "Introduction to Solid State Physics", Wiley, 2018.
4. S.O.Pillai, "Solid State Physics, New Academic Science", 2017.
5. D.K.Bhattacharya & PoonamTandon., "Physics for Information Science and Electronics Engineering", Oxford Higher Education",2017.

REFERENCES:

1. Garcia, N. & Damask, A., "Physics for Computer Science Students", Springer-Verlag, 2012.
2. Hanson, G.W., "Fundamentals of Nanoelectronics", Pearson Education, 2009.

3. Rogers, B., Adams, J. &Pennathur, S., "Nanotechnology: Understanding Small Systems", CRC Press, 2014.

OUTCOMES:

At the end of the course, the students should able to

1. Understand the basic concepts of free electron theory of solids and apply it to determine the conducting properties, carrier concentration and effective mass of an electron in conductors (K2)
2. Illustrate the various types of semiconductors based on band gap energy and doping, expression for carrier concentration, Fermi energy and their variations (K2)
3. Apply the suitable semiconducting materials for Hall device, Schottky and tunnel diode fabrication and acquire the basic knowledge of magnetic materials and its classification (K3)
4. Gain the knowledge on the types of superconducting and optical materials, properties of superconductors, mechanism of carrier generation and recombination in optical data storage devices (K2)
5. Apply the semiconducting, ferrimagnetic and superconducting materials in optical devices, data storage devices and magnetic levitation (K3)
6. Understand the basics of 1D, 2D, 3D quantum structures, single electron transport, carbon nanotubes and its applications (K3)

CO - PO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	3	-	-	3	-	-	-	-	-	-	1
CO2	3	3	-	-	3	-	2	-	-	-	-	3
CO3	3	3	-	2	3	-	3	-	-	-	-	2
CO4	3	3	3	2	3	-	3	-	-	-	-	3
CO5	3	3	3	3	3	-	3	-	-	-	-	3
CO6	3	3	3	2	3	-	-	-	-	-	-	1

SEMESTER - II

20BSCY201 SDG NO. 4,17	ENVIRONMENTAL SCIENCE AND ENGINEERING	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To study the nature and facts about environment
- To find and implement scientific, technological, economic and political solutions to environmental problems
- To study the interrelationship between living organism and environment
- To provide the importance of environment by assessing its impact on the human world; envision the surrounding environment, its functions and its value
- To study the integrated themes and biodiversity, natural resources, pollution control and waste management.

UNIT I ENVIRONMENT, ECOSYSTEMS AND BIODIVERSITY 9

Definition, scope and importance of environment – need for public awareness – Ecosystem: concept of an ecosystem – structure and functions of an ecosystem – Biotic and abiotic components – Biogeochemical cycle (C, N & P) – energy flow in the ecosystem – food chains, food webs and ecological pyramids – ecological succession - keystone species. Introduction to biodiversity definition: genetic, species and ecosystem diversity – values of biodiversity – IUCN Red list species classification - endemic, endangered, rare, vulnerable, extinct and exotic species – Biodiversity at global, national and local levels – India as a mega-diversity nation – hot-spots of biodiversity – threats to biodiversity – man-wildlife conflicts. Conservation of biodiversity: In-situ and ex-situ conservation of biodiversity. Field study of Terrestrial (Forest, Grassland, Desert) and Aquatic ecosystem (Pond, Lake, River, Estuary and Marine)

UNIT II ENVIRONMENTAL POLLUTION 9

Definition – causes, effects and control measures of: Air pollution, Water pollution, Soil pollution Marine pollution, Noise pollution, Thermal pollution and Nuclear pollution – solid waste management: causes, effects and control measures of municipal solid wastes (MSW) – role of an individual in prevention of pollution – Case studies related to environmental pollution.

Disaster management: floods, earthquake, cyclone and landslides – nuclear holocaust – Case studies.

UNIT III NATURAL RESOURCES 9

Forest resources: Use and over – exploitation, deforestation – Land resources: land degradation, man induced landslides, soil erosion and desertification – Water resources: Use and over- utilization of surface and groundwater – dams-benefits and problems, conflicts over water – Mineral resources: Environmental effects of extracting and using mineral resources – Food resources: World food problems, changes caused by agriculture and overgrazing, effects of modern agriculture – fertilizer – pesticide problems, water logging and salinity. Energy resources: Renewable energy (Solar energy, Wind energy, Tidal energy, Geothermal energy, OTE, Biomass energy) and non renewable energy (Coal, Petroleum, Nuclear energy) sources. – role of an individual in conservation of natural resources. Case studies – timber extraction, mining, dams and their effects on forests and tribal people.

UNIT IV SOCIAL ISSUES AND THE ENVIRONMENT 10

Atmospheric Chemistry - Composition and structure of atmosphere. Climate change - greenhouse effect- role of greenhouse gases on global warming. Chemical and photochemical reactions in the atmosphere - Formation of smog, PAN, acid rain (causes, effect and control measures). Oxygen and ozone chemistry - Ozone layer depletion (causes, effect and control measures). environmental ethics: Issues and possible solutions – Green chemistry - 12 principles of green chemistry.

Urbanisation - Urban problems related to energy - Water conservation: rain water harvesting, watershed management – resettlement and rehabilitation of people; its problems and concerns - case studies. Environment Legislations and Laws : Environment (protection) act – 1986. Air (Prevention and Control of Pollution) act – Water (Prevention and control of Pollution) act – Wildlife protection act – Forest conservation act. Biomedical Waste(Management and Handling rules):1998 and amendments- scheme of labelling of environmentally friendly products (Ecomark) - Issues involved in enforcement of environmental legislation - central and state pollution control boards, role of non-governmental organization – Public awareness - Environmental Impact Assessment (EIA).

UNIT V HUMAN POPULATION AND THE ENVIRONMENT 8

Population growth, variation among nations – population explosion – family welfare programme – women and child welfare environment and human health – HIV / AIDS – Role of Information Technology in environment and Human health – Case studies – human rights – value education – Sustainable Development – Need for sustainable development – concept – 17 SDG goals – 8 Millennium Development Goals(MDG).

TOTAL: 45 PERIODS

TEXTBOOKS:

1. Benny Joseph, 'Environmental Science and Engineering', Tata McGraw-Hill, New Delhi, 2006.
2. Gilbert M.Masters, 'Introduction to Environmental Engineering and Science', 2nd edition, Pearson Education, 2004.
3. Ravikrishnan A, 'Environmental Science and Engineering', Sri Krishna Hitech Publishing Company Pvt. Ltd, Revised Edition 2020.

REFERENCES :

1. Dharmendra S. Sengar, "Environmental law", Prentice hall of India Pvt Ltd, New Delhi, 2007.
2. Erach Bharucha, "Textbook of Environmental Studies", Universities Press(I) Pvt Ltd., Hydrabad, 2015.
3. G. Tyler Miller and Scott E. Spoolman, "Environmental Science", Cengage Learning India Pvt. Ltd., Delhi, 2014.
4. Rajagopalan. R, "Environmental Studies-From Crisis to Cure", Oxford University Press, 2005.

OUTCOMES:

Upon successful completion of this course, student should be able to

1. Explain the different components of environment, structure and function of an ecosystem, importance of biodiversity and its conservation. (K1)
2. Aware about problems of environmental pollution, its impact on human and ecosystem, control measures and basic concepts in Disaster Management. (K2)
3. Disseminate the need for the natural resources and its application to meet the modern requirements and the necessity of its conservation. (K2)
4. Illustrate the various aspects of atmospheric chemistry with a focus on climate change and recognize the principles of green chemistry. Describe suitable scientific, technological solutions and Protection Acts to eradicate social and environmental issues. (K2)
5. Recognize the need for population control measures and the environmental based value education concepts to achieve the Sustainable Development Goals. (K2)

CO - PO MAPPING :

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

SEMESTER - II

20ESIT202 SDG NO. 4&9	PYTHON PROGRAMMING	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To develop simple Python programs with conditionals and loops
- To define Python functions and to implement lists, tuples, dictionaries and sets
- To perform file operations and understand OO concepts in Python
- To understand NumPy, Pandas and Matplotlib

UNIT I BASICS OF PYTHON PROGRAMMING **9**

Introduction to Python – Literals – Variables and Identifiers – Data Types – Input Operation – Comments – Reserved words – Indentation – Operators and Expressions - Conditionals: Boolean values and operators - conditional if - alternative if - chained conditional - Iteration - Illustrative programs: Evaluation of expressions - String Operations - Circulate the values of n variables - Square root (Newton's method) - GCD - Sum an Array of Numbers.

UNIT II STRING, LISTS, TUPLES, DICTIONARIES, SETS **9**

Strings: String slices - Immutability - String functions and methods - String module - Lists: List operations - List slices - List methods - List loop - Mutability - Aliasing - Cloning lists - List parameters - Tuples: Tuple assignment - Tuple as return value.

Dictionaries: Operations and Methods - Advanced list processing - List comprehension - Sets: Creating Sets – Operations and methods – Set comprehension - Illustrative programs: Linear search - Binary search - Selection sort - Insertion sort - Merge sort.

UNIT III FUNCTIONS, MODULES, PACKAGES 9

Functions - definition and use - Flow of execution - Parameters and arguments - Fruitful functions: Return values - Parameters - Local and global scope - Function composition - Recursion - Modules – from import statement – Name of Module – Making your own modules - Packages - Packages in Python – Standard Library Modules – Globals(), Locals() and Reload(); Illustrative programs: Fibonacci series using functions - Arithmetic operations using module - Area of different shapes using packages.

UNIT IV FILES, EXCEPTIONS, CLASSES AND OBJECTS 9

Files and exception: Text files - Reading and writing files - Format operator - Command line arguments - Errors and exceptions - Handling exceptions - Classes and Objects: Defining classes - Creating Objects – Data abstraction – Class constructor – Class variables and Object variables – Public and Private data members – Private Methods; Illustrative programs: Word count - Copy file - Creating user defined exception - Creating student class and object.

UNIT V NUMPY, PANDAS, MATPLOTLIB 9

Introduction - Basics of NumPy - N-dimensional Array in NumPy - Methods and Properties - Basics of SciPy - Broadcasting in NumPy Array Operations - Array Indexing in NumPy, Pandas - Introduction - Series - DataFrame - Matplotlib - Basics - Figures and Axes - Method subplot() - Axis container Illustrative Programs: Multiplying a Matrix by a Vector, Solving Linear System of Equations - Using Pandas to Open CSV files - Creating a Single plot.

TOTAL: 45 PERIODS

TEXT BOOKS:

1. Reema Thareja, "Python Programming Using Problem Solving Approach", Oxford University Press 2018.
2. Anurag Gupta, G.P. Biswas, "Python Programming: Problem Solving, Packages and Libraries", McGrawHill, 2020.

REFERENCES:

1. Allen B. Downey, "Think Python: How to Think Like a Computer Scientist", Second edition, Updated for Python 3, Shroff/O'Reilly Publishers, 2016
2. Guido van Rossum and Fred L. Drake Jr, "An Introduction to Python – Revised and updated for Python 3.2", Network Theory Ltd., 2011.
3. John V Guttag, "Introduction to Computation and Programming Using Python'', Revised and expanded Edition, MIT Press , 2013
4. Robert Sedgewick, Kevin Wayne, Robert Dondero, "Introduction to Programming in Python: An Inter-disciplinary Approach", Pearson India Education Services Pvt. Ltd., 2016.

5. Timothy A. Budd, "Exploring Python", Mc-Graw Hill Education (India) Private Ltd., 2015.
6. Kenneth A. Lambert, "Fundamentals of Python: First Programs", CENGAGE Learning, 2012.
7. Charles Dierbach, "Introduction to Computer Science using Python: A Computational Problem-Solving Focus", Wiley India Edition, 2013.
8. Paul Gries, Jennifer Campbell and Jason Montojo, "Practical Programming: An Introduction to Computer Science using Python 3", Second edition, Pragmatic Programmers, LLC, 2013.

WEB REFERENCES:

1. http://greenteapress.com/wp/think-python/
2. www.docs.python.org
3. https://nptel.ac.in/courses/106/106/106106182/

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the syntax and semantics, string operations of python programming language (K2)
2. Develop python programs using control flow statements.(K3)
3. Construct various Data structures to develop python programs. (K3)
4. Illustrate the concepts of Functions, Modules and Packages in Python.(K3)
5. Understand the concepts of Object Oriented Programming, files and Exception handling.(K2)
6. Examine various problem solving concepts in python to develop real time applications.(K4)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	3	3	3	1	1	0	0	1	0	1	2	2
CO2	3	3	3	3	3	1	0	0	0	0	0	1	2	2
CO3	3	3	3	3	3	2	1	0	0	0	0	1	2	2
CO4	3	3	3	3	3	2	1	0	0	0	0	1	2	2
CO5	3	3	3	3	3	2	2	1	0	2	0	2	3	3
CO6	3	3	3	3	3	3	3	2	3	2	3	2	3	3

SEMESTER - II

20ESIT203 SDG NO. 4 & 9	DIGITAL PRINCIPLES AND SYSTEM DESIGN	L	T	P	C
		2	1	0	3

OBJECTIVES:

- To analyze and design combinational circuits
- To analyze and design synchronous and asynchronous sequential circuits
- To understand Programmable Logic Devices
- To write HDL code for combinational and sequential circuits

UNIT I BOOLEAN ALGEBRA AND LOGIC GATES 9

Number Systems – Arithmetic Operations – Binary Codes- Boolean Algebra and Logic Gates – Theorems and Properties of Boolean Algebra – Boolean Functions – Canonical and Standard Forms – Simplification of Boolean Functions using Karnaugh Map – Logic Gates – NAND and NOR Implementations.

UNIT II COMBINATIONAL LOGIC 9

Combinational Circuits – Analysis and Design Procedures – Binary Adder-Subtractor – Decimal Adder – Binary Multiplier – Magnitude Comparator – Decoders – Encoders – Multiplexers – Introduction to HDL – HDL Models of Combinational circuits.

UNIT III SYNCHRONOUS SEQUENTIAL LOGIC 9

Sequential Circuits – Storage Elements: Latches , Flip-Flops – Analysis of Clocked Sequential Circuits – State Reduction and Assignment – Design Procedure – Registers and Counters – HDL Models of Sequential Circuits.

UNIT IV ASYNCHRONOUS SEQUENTIAL LOGIC 9

Analysis and Design of Asynchronous Sequential Circuits – Reduction of State and Flow Tables – Race-free State Assignment – Hazards.

UNIT V MEMORY AND PROGRAMMABLE LOGIC 9

RAM – Memory Decoding – Error Detection and Correction – ROM – Programmable Logic Array – Programmable Array Logic – Sequential Programmable Devices.

TOTAL: 45 PERIODS

TEXT BOOKS:

1. M. Morris R. Mano, Michael D. Ciletti, "Digital Design: With an Introduction to the Verilog HDL, VHDL, and SystemVerilog", 6th Edition, Pearson Education, 2017.

REFERENCES:

1. G. K. Kharate, "Digital Electronics", Oxford University Press, 2010
2. John F. Wakerly, "Digital Design Principles and Practices", Fifth Edition, Pearson Education, 2017.
3. Charles H. Roth Jr, Larry L. Kinney, "Fundamentals of Logic Design", Sixth Edition, CENGAGE Learning, 2013
4. Donald D. Givone, "Digital Principles and Design", Tata Mc Graw Hill, 2003.

ONLINE RESOURCES:

1. https://ocw.mit.edu/courses/online-textbooks/
2. https://nptel.ac.in/courses/117105080/

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understanding Boolean algebra, number systems and simplify Boolean functions using Kmap. (K2)
2. Understand the Combinational and sequential Circuits. (K2)
3. Demonstrate the use of Combinational Circuits and Sequential circuits (K3)
4. Interpret the designs using Programmable Logic Devices. (K3)
5. Apply HDL code for combinational and Sequential Circuits. (K3)
6. Interpret and troubleshoot logic circuits. (K3)

CO – PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	-	-	-	-	-	-	-	-	-	-	3	-	-
CO2	-	2	-	-	-	-	-	-	-	-	3	1	-	-
CO3	-	2	3	-	-	-	-	-	-	-	3	1	-	-
CO4	-	-	-	-	-	-	-	-	-	-	3	-	-	-
CO5	-	-	-	-	1	-	-	-	-	-	-	2	-	-
CO6	-	-	-	-	-	-	-	-	-	-	3	-	-	-

SEMESTER - II

20ESPL201 SDG NO. 4	PYTHON PROGRAMMING LABORATORY	L	T	P	C
		0	0	3	1.5

OBJECTIVES:

- Develop Python programs with conditionals, loops and functions
- Represent compound data using Python lists, tuples, dictionaries
- Read and write data from/to files in Python
- Implement NumPy, Pandas, Matplotlib libraries

LIST OF EXPERIMENTS :

1 Compute the GCD of two numbers
2 Find the maximum and minimum of a list of numbers
3 Linear search and Binary search
4 Selection sort, Insertion sort
5 Merge sort, Quick Sort
6 First n prime numbers
7 Multiply matrices
8 Programs that take command line arguments (word count)
9 Find the most frequent words in a text read from a file
10 Exception Handling – License Process
11 Classes and Objects – Student class
12 Solving Linear System of Equations
13 Using Pandas to Open csv files
14 Creating a Single plot
15 Creating Scatter plot, Histogram

TOTAL: 45 PERIODS

LAB REQUIREMENTS

Python 3

OUTCOMES

On completion of the laboratory course, the student should be able to

1. Illustrate simple programs for describing the syntax, semantics and control flow statements. [K3]
2. Describe the core data structures like String, lists, dictionaries, tuples and sets in Python to store, process and sort the data. [K2]
3. Interpret the concepts of functions, modules and packages in Python. [K3]
4. Illustrate the applications of python libraries. [K3]

5. Describe the file manipulation and its operations. [K2]
6. Demonstrate exceptions and classes and objects for any real time applications. [K3]

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	-	1	2	1	2	-	-	-	1	-	3	3	-	1
CO2	1	2	3	3	3	2	1	1	1	1	1	3	1	2
CO3	-	1	3	3	2	1	-	-	-	-	1	3	-	1
CO4	1	2	3	3	2	-	-	-	-	-	1	3	1	2
CO5	-	-	3	3	2	-	-	1	-	-	2	3	-	-
CO6	-	-	3	3	2	-	-	1	-	-	2	3	-	-

SEMESTER - II

20ESPL202 SDG NO. 4 & 9	DIGITAL LABORATORY	L	T	P	C
		0	0	3	1.5

OBJECTIVES:

- To design and implement the various combinational circuits
- To design and implement combinational circuits using MSI devices
- To design and implement sequential circuits
- To understand and code with HDL programming

LIST OF EXPERIMENTS

1. Verification of Boolean Theorems using basic gates
2. Design and implementation of combinational circuits using basic gates for arbitrary functions, code converters
3. Design and implement Half/Full Adder and Subtractor
4. Design and implement combinational circuits using MSI devices:
   a) 4 bit binary adder/subractor
   b) Parity generator/checker
   c) Magnitude comparator
5. Application using multiplexers
6. Design and implement shift-registers

7. Design and implement synchronous counters
8. Design and implement asynchronous counter
9. Coding combinational circuits using HDL
10. Coding sequential circuits using HDL
11. Design and implementation of a simple digital system (Mini Project)

LAB REQUIREMENTS:

HARDWARE:

DIGITAL TRAINER KITS

DIGITAL IC's required for the experiments in sufficient numbers

SOFTWARE:

HDL, Verilog simulator

TOTAL: 45 PERIODS

OUTCOMES

On completion of the laboratory course, the student should be able to

1. Implement simplified combinational circuits using basic logic gates. (K6)
2. Implement combinational circuits using MSI devices. (K6)
3. Implement sequential circuits like registers and counters.(K6)
4. Simulate combinational and sequential circuits using HDL.(K4)
5. Implement designs using Programmable Logic Devices. (K6)
6. Design and implementation of a simple digital system.(K6)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	2	3	3	2	2	1	1	-	2	2	-	2	1	1
CO2	3	3	3	2	3	2	1	1	2	2	2	3	1	1
CO3	2	3	3	3	3	2	2	1	2	2	2	3	1	1
CO4	3	3	3	3	3	2	2	1	3	3	3	3	1	1
CO5	2	3	3	2	2	-	-	2	-	2	2	2	1	1
CO6	2	3	3	2	2	1	-	-	2	2	3	2	1	1

SEMESTER - II

20ESGE201 SDG NO. 4,9,12	ENGINEERING PRACTICES LABORATORY	L	T	P	C
		0	0	3	1.5

OBJECTIVES:

- To provide exposure to the students with hands on experience on various basic engineering practices in Electrical and Electronics Engineering, Civil and Mechanical Engineering

ELECTRICAL ENGINEERING PRACTICE

1. Residential house wiring using switches, fuse, indicator, lamp and energy meter.
2. Fluorescent lamp wiring.
3. Stair case wiring.
4. Measurement of electrical quantities – voltage, current, power & power factor in RLC circuit.
5. Measurement of energy using single phase energy meter.
6. Measurement of resistance to earth of electrical equipment.

ELECTRONICS ENGINEERING PRACTICE

1. Study of Electronic components and equipments – Resistor, colour coding measurement of AC signal parameter (peak-peak, rms period, frequency) using CRO.
2. Study of logic gates AND, OR, EX-OR and NOT.
3. Generation of Clock Signal.
4. Soldering practice – Components, Devices and Circuits – Using general purpose PCB.
5. Measurement of ripple factor of HWR and FWR.

CIVIL ENGINEERING PRACTICE

Buildings:

Study of plumbing and carpentry components of residential and industrial buildings, safety aspects.

Plumbing Works:

1. Study of pipeline joints, its location and functions: valves, taps, couplings, unions, reducers, elbows in household fittings.
2. Study of pipe connections requirements for pumps and turbines.

3. Preparation of plumbing line sketches for water supply and sewage works.
4. Hands-on-exercise: Basic pipe connections – Mixed pipe material connection – Pipe connections with different joining components.
5. Demonstration of plumbing requirements of high-rise buildings.

Carpentry using Power Tools only:

1. Study of the joints in roofs, doors, windows and furniture.
2. Hands-on-exercise: Wood work, joints by sawing, planing and cutting.

MECHANICAL ENGINEERING PRACTICE

Welding:

1. Preparation of butt joints, lap joints and T- joints by Shielded metal arc welding.
2. Gas welding practice.

Basic Machining:

1. Simple Turning and Taper turning.
2. Drilling Practice.

Sheet Metal Work:

1. Forming & Bending.
2. Model making – Trays and funnels.
3. Different type of joints.

Machine assembly practice:

1. Study of centrifugal pump.
2. Study of air conditioner.

Demonstration on:

1. Smithy operations, upsetting, swaging, setting down and bending. Example – Exercise – Production of hexagonal headed bolt.
2. Foundry operations like mould preparation for gear and step cone pulley.
3. Fitting – Exercises – Preparation of square fitting and V – fitting models.

Total : 45 PERIODS

LIST OF EQUIPMENT FOR A BATCH OF 30 STUDENTS

1. Electrical

1	Assorted electrical components for house wiring	15 Sets
2	Electrical measuring instruments	10 Sets

3	Study purpose items: Iron box, fan and regulator, emergency lamp	 1 Each
4	Megger (250V/500V)	1 No
5	Power Tools: Range Finder Digital Live-wire detector	 2 Nos 2 Nos

2. Electronics

1	Soldering guns	10 Nos
2	Assorted electronic components for making circuits	50 Nos
3	Small PCBs	10 Nos
4	Multimeters	10 Nos

3. Civil

1	Assorted components for plumbing consisting of metallic pipes, plastic pipes, flexible pipes, couplings, unions, elbows, plugs and other fittings.	15 Sets
2	Carpentry vice (fitted to work bench)	15 Nos
3	Standard woodworking tools	15 Sets
4	Models of industrial trusses, door joints, furniture joints	5 each
5	Power Tools: Rotary Hammer Demolition Hammer Circular Saw Planer Hand Drilling Machine Jigsaw	 2 Nos 2 Nos 2 Nos 2 Nos 2 Nos 2 Nos

4. Mechanical

1	Arc welding transformer with cables and holders	5 Nos
2	Welding booth with exhaust facility	5 Nos
3	Welding accessories like welding shield, chipping hammer, wire brush, etc	5 Sets
4	Oxygen and acetylene gas cylinders, blow pipe and other welding outfit.	2 Nos
5	Centre lathe	2 Nos
6	Hearth furnace, anvil and smithy tools	2 Sets
7	Moulding table, foundry tools	2 Sets
8	Power Tool: Angle Grinder	2 Nos
9	Study-purpose items: centrifugal pump, air-conditioner	1 each

OUTCOMES:

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

1. Elaborate on the components, gates, soldering practices. Calculate electrical parameters such as voltage, current, resistance and power. (K1)
2. Design and implement Rectifier and Timer circuits (K2)
3. Measure the electrical energy by single phase and three phase energy meters. (K2)
4. Prepare the carpentry and plumbing joints. (K2)
5. Perform different types of welding joints and sheet metal works (K2)
6. Perform different machining operations in lathe and drilling. (K2)

CO - PO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	1	1	2	1	-	-	1	1	1	1
CO2	3	2	1	1	2	1	-	-	1	1	1	1
CO3	2	2	1	1	1	1	-	-	1	1	1	1
CO4	1	1	1	-	-	2	-	-	1	1	1	2
CO5	2	1	1	-	-	1	1	1	1	1	1	2
CO6	2	1	1	-	-	1	-	1	1	1	1	2

SEMESTER - III

20HSTA201 SDG NO. 4	TAMILS AND TECHNOLOGY	L	T	P	C
		1	0	0	1

UNIT I WEAVING AND CERAMIC TECHNOLOGY 3

Weaving Industry during Sangam Age – Ceramic technology – Black and Red Ware Potteries (BRW) – Graffiti on Potteries.

UNIT II DESIGN AND CONSTRUCTION TECHNOLOGY 3

Designing and Structural construction House & Designs in household materials during Sangam Age - Building materials and Hero stones of Sangam age – Details of Stage Constructions in Silappathikaram - Sculptures and Temples of Mamallapuram - Great Temples of Cholas and other worship places - Temples of Nayaka Period - Type study (Madurai Meenakshi Temple)- Thirumalai Nayakar Mahal - Chetti Nadu Houses, Indo - Saracenic architecture at Madras during British Period.

UNIT III MANUFACTURING TECHNOLOGY 3

Art of Ship Building - Metallurgical studies - Iron industry - Iron smelting, steel -Copper and gold- Coins as source of history - Minting of Coins – Beads making-industries Stone beads - Glass beads - Terracotta beads -Shell beads/ bone beats - Archeological evidences - Gem stone types described in Silappathikaram.

UNIT IV AGRICULTURE AND IRRIGATION TECHNOLOGY 3

Dam, Tank, ponds, Sluice, Significance of Kumizhi Thoompu of Chola Period, Animal Husbandry - Wells designed for cattle use - Agriculture and Agro Processing - Knowledge of Sea - Fisheries – Pearl - Conche diving - Ancient Knowledge of Ocean - Knowledge Specific Society.

UNIT V SCIENTIFIC TAMIL & TAMIL COMPUTING 3

Development of Scientific Tamil - Tamil computing – Digitalization of Tamil Books – Development of Tamil Software – Tamil Virtual Academy – Tamil Digital Library – Online Tamil Dictionaries – Sorkuvai Project.

TOTAL : 15 PERIODS

TEXT-CUM-REFERENCE BOOKS

1. தமிழக வரலாறு - மக்களும் பண்பாடும் - கே.கே. பிள்ளை (வெளியீடு: தமிழ்நாடு பாடநூல் மற்றும் கல்வியியல் பணிகள் கழகம்).
2 கணினித் தமிழ் - முனைவர் இல. சுந்தரம். (விகடன் பிரசுரம்).
3 கீழடி - வைகை நதிக்கரையில் சங்ககால நகர நாகரிகம் (தொல்லியல் துறை வெளியீடு)
4. பொருநை - ஆற்றங்கரை நாகரிகம். (தொல்லியல் துறை வெளியீடு)
5. Social Life of Tamils (Dr.K.K.Pillay) A joint publication of TNTB & ESC and RMRL – (in print)
6. Social Life of the Tamils - The Classical Period (Dr.S.Singaravelu) (Published by: International Institute of Tamil Studies.
7. Historical Heritage of the Tamils (Dr.S.V.Subatamanian, Dr.K.D. Thirunavukkarasu) (Published by: International Institute of Tamil Studies).
8. The Contributions of the Tamils to Indian Culture (Dr.M.Valarmathi) (Published by: International Institute of Tamil Studies.)
9. Keeladi - 'Sangam City Civilization on the banks of river Vaigai' (Jointly Published by: Department of Archaeology & Tamil Nadu Text Book and Educational Services Corporation, Tamil Nadu)
10. Studies in the History of India with Special Reference to Tamil Nadu (Dr.K.K.Pillay) (Published by: The Author)
11. Porunai Civilization (Jointly Published by: Department of Archaeology & Tamil Nadu Text Book and Educational Services Corporation, Tamil Nadu)
12. Journey of Civilization Indus to Vaigai (R.Balakrishnan) (Published by: RMRL) – Reference Book.

தமிழும் தொழில்நுட்பமும்

அலகு I நெசவு மற்றும் பானைத் தொழில்நுட்பம்: 3

சங்க காலத்தில் நெசவுத் தொழில் - பானைத் தொழில்நுட்பம் - கருப்பு சிவப்பு பாண்டங்கள் - பாண்டங்களில் கீறல் குறியீடுகள்.

அலகு II வடிவமைப்பு மற்றும் கட்டிடத் தொழில்நுட்பம்: 3

சங்க காலத்தில் வடிவமைப்பு மற்றும் கட்டுமானங்கள் & சங்க கொலத்தில் வீட்டுப் பொருட்களில் வடிவமைப்பு- சங்க காலத்தில் கட்டுமான பொருட்களும் நடுகல்லும் ___ சிலப்பதிகாரத்தில் மேடை அமைப்பு பற்றிய விவரங்கள் - மாமல்லபுரச் சிற்பங்களும், கோவில்களும் - சோழர் காலத்துப் பெருங்கோயில்கள் மற்றும் பிற வழிபாட்டுத் தலங்கள் - நாயக்கர் காலக் கோயில்கள் - மாதிரி கட்டமைப்புகள் பற்றி அறிதல், மதுரை மீனாட்சி அம்மன் ஆலயம் மற்றும் திருமலை நாயக்கர் மஹால் - செட்டிநாட்டு வீடுகள் - பிரிட்டிஷ் கொலத்தில் சென்னையில் இந்தோ-சாரோசெனிக் கட்டிடக் கலை.

அலகு III உற்பத்தித் தொழில் நுட்பம்: 3

கப்பல் கட்டும் கலை -உலோகவியல் - இரும்புத் தொழிற்சாலை - இரும்பை உருக்குதல், எஃகு - வரலாற்றுச் சான்றுகளாக செம்பு மற்றும் தங்க நாணயங்கள் - நாணயங்கள் அச்சடித்தல் - மணி உருவாக்கும் தொழிற்சாலைகள் - கல்மணிகள், கண்ணொடி மணிகள் - சுடுமண் மணிகள் - சங்கு மணிகள் - எலும்புத்துண்டுகள் - தொல்லியல் சான்றுகள் - சிலப்பதிகாரத்தில் மணிகளின் வகைகள்.

அலகு IV வேளாண்மை மற்றும் நீர்ப்பாசனத் தொழில் நுட்பம்: 3

அணை, ஏரி, குளங்கள், மதகு -சோழர்காலக் குமுழித் தூம்பின் முக்கியத்துவம் - கால்நடை பராமரிப்பு - கால்நடைகளுக்காக வடிவமைக்கப்பட்ட கிணறுகள் - வேளாண்மை மற்றும் வேளாண்மைச் சார்ந்த செயல்பாடுகள் - கடல்சார் அறிவு - மீன்வளம் - முத்து மற்றும் முத்துக்குளித்தல் ___ பெருங்கடல் குறித்த பண்டைய அறிவு - அறிவுசார் சமூகம்.

அலகு V அறிவியல் தமிழ் மற்றும் கணித்தமிழ்: 3

அறிவியல் தமிழின் வளர்ச்சி - கணித்தமிழ் வளர்ச்சி - தமிழ் நூல்களை மின்பதிப்பு செய்தல் - தமிழ் மென்பொருட்கள் உருவாக்கம் - தமிழ் இணையக் கல்விக்கழகம் - தமிழ் மின் நூ லகம் - இணையத்தில் தமிழ் அகராதிகள் - சொற்குவைத் திட்டம்.

TOTAL : 15 PERIODS

TEXT-CUM-REFERENCE BOOKS

1. தமிழக வரலாறு ___ மக்களும் பண்பாடும் ___ கே.கே. பிள்ளை (வெளியீடு: தமிழ்நாடு பாடநூல் மற்றும் கல்வியியல் பணிகள் கழகம்).
2. கணினித் தமிழ் - முனைவர் இல. சுந்தரம். (விகடன் பிரசுரம்).

3. கீழடி - வைகை நதிக்கரையில் சங்ககால நகர நாகரிகம் (தொல்லியல் துறை வெளியீடு)
4. பொருநை - ஆற்றங்கரை நாகரிகம். (தொல்லியல் துறை வெளியீடு)
5. Social Life of Tamils (Dr.K.K.Pillay) A joint publication of TNTB & ESC and RMRL – (in print)
6. Social Life of the Tamils - The Classical Period (Dr.S.Singaravelu) (Published by: International Institute of Tamil Studies.
7. Historical Heritage of the Tamils (Dr.S.V.Subatamanian, Dr.K.D. Thirunavukkarasu) (Published by: International Institute of Tamil Studies).
8. The Contributions of the Tamils to Indian Culture (Dr.M.Valarmathi) (Published by: International Institute of Tamil Studies.)
9. Keeladi - 'Sangam City Civilization on the banks of river Vaigai' (Jointly Published by: Department of Archaeology & Tamil Nadu Text Book and Educational Services Corporation, Tamil Nadu)
10. Studies in the History of India with Special Reference to Tamil Nadu (Dr.K.K.Pillay) (Published by: The Author)
11. Porunai Civilization (Jointly Published by: Department of Archaeology & Tamil Nadu Text Book and Educational Services Corporation, Tamil Nadu)
12. Journey of Civilization Indus to Vaigai (R.Balakrishnan) (Published by: RMRL) – Reference Book.

SEMESTER - II

20TPHS201 SDG NO. 4&5	SKILL ENHANCEMENT	L	T	P	C
		0	0	2	1

OBJECTIVES:

- To understand the nuances in resume building
- To explore various virtual meeting tools
- To gain knowledge about online certification courses
- To develop knowledge in Google Suite products
- To enhance presentation skills

UNIT I RESUME BUILDING **6**

Your Strength, Projects, Internship, Paper Presentation, uploading your coding in github, Introduction to HackerRank, HackerEarth virtual online assessment (Auto Proctored) (Practicals - Construct a resume, Register for a online Mock Assessment / Contest)

UNIT II VIRTUAL MEETINGS **6**

Basic Etiquette of virtual meeting – Introduction to Skype - Zoom - Webex - Google Meet - Gotowebinar - Jio meet – Screen Share - Jamboard - Feedback polling - Chatbox

(Practicals - Accept and Register for a mock class to attend - How to host a meeting).

UNIT III ONLINE LEARNING **6**

Online Certification - Coursera – Udemy – Edx – Cisco – Online Practice Platforms - SkillRack – Myslate - FACEprep - BYTS - aptimithra - Contest Registrations - TCS Campus Commune - HackwithInfy, InfyTQ - Virtusa NurualHack - Mindtree Osmosis – Online assessment - AMCAT-PGPA.

(Practicals - Campus Commune Registration , Coursera registration - Mock Registration (KAAR Technologies as sample).

UNIT IV GOOGLE SUITE **8**

Define google suite - Benefits of google suite - Google Search - Sheet - Docs - Forms - Calender - Drive - Slide - Translate - Duo - Earch - Maps - Hangouts- Sites - Books - Blogger

(Practicals – Create google sheets and share - Create google Forms and share, Create Google Slide and share , Google drive creation and share (Knowledge of Rights), Create poll and share.

UNIT V PRESENTATION SKILLS **4**

Email Writing – Group Discussion - Power Point Presentation

(Practicals- Create a self SWOT Analysis report. A PowerPoint Slide Preparation)

TOTAL : 30 PERIODS

WEB REFERENCES :

Unit I: Resume Building:

1. https://zety.com/blog/resume-tips
2. https://resumegenius.com/blog/resume-help/how-to-write-a-resume
3. https://www.hackerearth.com/recruit/
4. https://www.hackerrank.com/about-us

Unit – II:Virtual Meetings

1. https://www.claphamschool.org/our-community/blog/online-learning-etiquette-guide-14-principles-to-guide-students
2. https://online.hbs.edu/blog/post/virtual-interview-tips?c1=GAW_SE_NW&source=IN_GEN_DSA&cr2=search__-__nw__-__in__-

__dsa__-__general&kw=dsa__-__general& cr5=459341920955&cr7=c&gclid=Cj0KCQjw8fr7BRDSARIsAK0Qqr4dRRbboL3kltrwDsr7hm8oIHtN5dfjD3NIFZULuzNwEXxhjpNFQ2caApn5EALw_wcB

3. https://hygger.io/blog/top-10-best-group-meeting-apps-business/
4. https://www.zdnet.com/article/best-video-conferencing-software-and-services-for-business/

Unit – III:Online Learning

1. https://www.coursera.org/browse
2. https://support.udemy.com/hc/en-us/articles/229603868-Certificate-of-Completion
3. https://www.edx.org/course/how-to-learn-online
4. https://www.cisco.com/c/en/us/training-events/training-certifications/certifications.html
5. https://campuscommune.tcs.com/en-in/intro
6. https://www.freshersnow.com/tcs-campus-commune-registration/
7. https://www.infosys.com/careers/hackwithinfy.html
8. https://www.mindtree.com/blog/osmosis-2013-my-experiences
9. https://www.myamcat.com/knowing-amcat
10. https://www.admitkard.com/blog/2020/02/06/amcat/

Unit IV: Google Suite

1. https://www.inmotionhosting.com/blog/what-is-g-suite-and-why-should-i-consider-using-it/
2. https://en.wikipedia.org/wiki/G_Suite
3. https://blog.hubspot.com/marketing/google-suite
4. https://kinsta.com/blog/g-suite/

Unit V: Presentation Skills

1. https://www.mindtools.com/CommSkll/EmailCommunication.htm
2. https://www.grammarly.com/blog/email-writing-tips/
3. https://business.tutsplus.com/articles/how-to-write-a-formal-email--cms-29793
4. https://www.softwaretestinghelp.com/how-to-crack-the-gd/
5. https://www.mbauniverse.com/group-discussion/tips
6. https://slidemodel.com/23-powerpoint-presentation-tips-creating-engaging-interactive-presentations/
7. https://business.tutsplus.com/articles/37-effective-powerpoint-presentation-tips--cms-25421

8 https://blog.prezi.com/9-tips-on-how-to-make-a-presentation-a-success/
9. http://www.garrreynolds.com/preso-tips/design/

OUTCOMES:

On completion of this course, the student should be able to

1. Construct a suitable resume and registration procedure for online mock assessments. (K1)
2. Handle various virtual meeting tools. (K3)
3. Acquire exposure about online certification courses. (K4)
4. Get involved and work in a collaborative manner. (K2)
5. Gain knowledge in various presentation methodologies. (K1)
6. Apply knowledge to practice Google suite features and SWOT analysis. (K3)

CO – PO MAPPING

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	-	-	-	-	3	2	-	3	2	3	-	2
CO2	-	-	-	-	3	2	-	3	2	3	-	2
CO3	-	-	-	-	3	2	-	-	1	3	-	2
CO4	-	-	-	-	3	2	-	3	3	3	-	2
CO5	-	-	-	-	3	2	-	-	2	3	-	2
CO6	-	-	-	-	3	2	-	-	2	3	-	2

SEMESTER - II

20HSMG201 SDG NO. 4 & 5	INTERPERSONAL VALUES	L	T	P	C
		2	0	0	0

OBJECTIVES:

- Values through Practical activities

UNIT I INTERPERSONAL VALUES **6**

Interpersonal Relationships and Values – Importance and Barriers – Building and maintain relationships – Mutual understanding – Respect to others.

UNIT II EFFECTIVE COMMUNICATION **6**

Communication skills –Importance and Barriers - Impressive formation and management – Public speaking

UNIT III GROUP DYNAMICS **6**

Group formation –Teamwork – Identify others attitude and behaviour – Formation of relationship – Personal and professional.

UNIT IV MUTUAL RELATIONSHIP **6**

Building mutual understanding and cooperation – Enhancing decision making skills – Problem solving skills – Comparative Appraisal – Interpersonal needs.

UNIT V POSITIVE ATTITUDE **6**

Fostering trust and cooperation – Developing and maintain positive attitude – Improving socialization – Development of security and comfort.

TOTAL: 30 PERIODS

Note: Each topic in all the above units will be supplemented by practice exercises and classroom activities and projects.

REFERENCE BOOKS:

1. Barun K. Mitra, "Personality Development and Soft Skills", Oxford University Press, 2016.
2. B.N.Ghosh, "Managing Soft Skills for Personality Development", McGraw Hill India, 2012.

OUTCOMES:

Upon completion of the course, the student should be able to

1. Develop a healthy relationship & harmony with others. (K1)
2. Practice respecting every human being. (K3)
3. Practice to eradicate negative temperaments. (K3)
4. Acquire Respect, Honesty, Empathy, Forgiveness and Equality. (K4)
5. Manage the cognitive abilities of an Individual. (K5)
6. Understanding the importance of public speaking and teamwork. (K2)

CO – PO MAPPING :

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	-	-	-	-	-	2	2	3	3	1	1	1
CO2	-	-	-	-	-	2	2	3	3	1	1	1
CO3	-	-	-	-	-	2	2	3	3	1	1	1
CO4	-	-	-	-	-	2	2	3	3	1	1	1
CO5	-	-	-	-	-	2	2	3	3	1	1	1
CO6	-	-	-	-	-	2	2	3	3	1	1	1

SEMESTER - III

20BSMA309 SDG NO. 4	NUMBER THEORY	L	T	P	C
		3	0	0	4

OBJECTIVES:

- The aim of this course is to impart knowledge in the concepts of linear algebra as a prerequisite for the recent thrust areas of technological advancement.
- To understand the basic concepts in number theory
- To examine the key questions in the Theory of Numbers.
- To give an integrated approach to number theory and abstract algebra, and provide a firm basis for further reading and study in the subject.

UNIT I DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS 12

Division algorithm — Base — b representations — Number patterns — Prime and composite numbers — GCD — Euclidean algorithm — Fundamental theorem of arithmetic — LCM.

UNIT II CONGRUENCES 12

Congruences, Solutions of congruences, congruences of deg 1, The function 0(n) - Congruences of higher degree, Prime power moduli, Prime modulus, congruences of degree 2, Prime modulus, Power residues.

UNIT III QUADRATIC RESIDUES 12

Quadratic residues, Quadratic reciprocity, The Jacobi symbol, greatest integer function, arithmetic function, The Mobius Inversion formula, The multiplication of arithmetic functions.

UNIT IV DIOPHANTINE EQUATIONS 12

Diophantine equations, The equation ax + by = c, Positive solutions, Other linear Equations, Sums of four and five squares, Waring's problem, sum of fourth powers, sum of two Squares.

UNIT V CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS 12

Wilson's theorem — Fermat's little theorem — Euler's theorem — Euler's Phi functions — Tau and Sigma functions.

TOTAL: 60 PERIODS

REFERENCES:

1. Bressoud D., Wagon S., "A Course in Computational Number Theory", Key College Publishing, New York, 2000.
2. Graham R.L., Knuth D.E. and Patachink O., "Concrete Mathematics", Pearson education, Second Edition, London, 2002.
3. Niven I., Zuckerman H.S., and Montgomery H.L., "An introduction to the theory of numbers", John Wiley & Sons, Fifth Edition, Singapore, 2004.
4. Kenneth Ireland & Michael Rosen, "A Classical Introduction to Modern Number Theory", Springer International Edition, Second Edition, New York, 2010
3. Koblitz, N., "A course in number theory and Cryptography", Springer Verlag , New York, 1994
5. Rose H.E., "A Course in Number Theory", Clarendon Press, Second Edition, Oxford, 1995

OUTCOMES:

Upon completion of the course, the student should be able to

1. The student would have learnt to solve divisibility problems some techniques of numerical calculations using congruences
2. Students would have learnt application of congruences.
3. Students will be able to apply the Gaussian reciprocity law in public-key cryptography
4. The students will be able to solve some diophantine equations .

CO – PO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	3	2	1	1	-	-	-	-	-	-	1
CO2	3	3	2	1	1	-	-	-	-	-	-	1
CO3	3	3	2	1	1	-	-	-	-	-	-	1
CO4	3	3	2	1	1	-	-	-	-	-	-	1
CO5	3	3	2	1	1	-	-	-	-	-	-	1
CO6	3	3	2	1	1	-	-	-	-	-	-	1

SEMESTER - III

20ITPC301 SDG NO. 4	DATA STRUCTURES	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To understand the concepts of ADT's
- To learn Linear Data Structures – Lists, Stacks, and Queues
- To understand Sorting, Searching and Hashing Algorithms
- To learn Dynamic Data Structures - Tree and Graph

UNIT I LINEAR DATA STRUCTURES – I 9

Stacks and Queues : Abstract Data Types (ADTs) – Stack ADT – Operations - Applications - Evaluating arithmetic expressions- Conversion of Infix to Postfix expression - Queue ADT – Operations - Circular Queue – Priority Queue –Dequeue – Applications of Queues.

UNIT II LINEAR DATA STRUCTURES – II 9

Linked List: List ADT – Array-Based Implementation – Linked List Implementation –– Singly Linked Lists- Circularly Linked Lists- Doubly-Linked Lists – Applications of Lists –Polynomial Manipulation – All Operations (Insertion, Deletion, Merge, Traversal).

UNIT III NON LINEAR DATA STRUCTURES – I 9

Trees : Tree ADT – Tree Traversals - Binary Tree ADT – Expression Trees – Applications of Trees – Binary Search Tree ADT –Threaded Binary Trees- AVL Trees – B-Tree - B+ Tree -Heap – Applications of Heap.

UNIT IV NON LINEAR DATA STRUCTURES – II 9

Graphs : Definition – Representation of Graph – Types of Graph – Breadth First Traversal –Depth First Traversal – Topological Sort – Bi-Connectivity – Cut Vertex – Euler Circuits – Dijkstra‟s algorithm – Bellman-Ford algorithm – Floyd's Algorithm - minimum spanning tree – Prim's and Kruskal's algorithms – Applications of Graphs.

UNIT V SEARCHING, SORTING AND HASHING TECHNIQUES 9

Searching- Linear Search - Binary Search - Sorting - Bubble Sort - Selection Sort - Insertion Sort - Shell Sort – Radix Sort – Hashing- Hash Functions – Separate Chaining – Open Addressing – Rehashing – Extendible Hashing.

TOTAL: 45 PERIODS

TEXT BOOKS:

1. M. A. Weiss, "Data Structures and Algorithm Analysis in C", Pearson Education Asia, 2002.
2. Reema Thareja, "Data Structures Using C", Second Edition, Oxford University Press, 2011.

REFERENCES:

1. Thomas H. Cormen, Charles E. Leiserson, Ronald L.Rivest, Clifford Stein, "Introduction to Algorithms", Second Edition, Mcgraw Hill, 2002.
2. Stephen G. Kochan, "Programming in C", 3rd edition, Pearson Education.
3. Aho, Hopcroft and Ullman, "Data Structures and Algorithms", Pearson Education, 1983.
4. Ellis Horowitz, SartajSahni, Susan Anderson-Freed, "Fundamentals of Data Structures in C", Second Edition, University Press, 2008.

WEB REFERENCES :

1. https://www.programiz.com/dsa
2. http://masterraghu.com/subjects/Datastructures/ebooks/rematharej a.pdf

OUTCOMES:

Upon completion of the course, the student should be able to

1. Implement abstract data types for linear data structures. (K3)
2. Implement abstract data types for non-linear data structure. (K3)
3. Apply the different linear and non-linear data structures to problem solutions. (K3)
4. Implement the various sorting and searching algorithms. (K3)
5. Solve Problem involving Graph, Trees and Heap. (K3)
6. Choose appropriate data structures to solve real world problems efficiently. (K3)

CO- PO, PSO MAPPING :

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	2	2	1	2	1	1	1	0	2	2	3	3	1	1
CO2	2	2	1	2	1	1	1	0	2	2	3	3	1	1
CO3	3	3	2	3	3	1	1	1	2	2	3	3	1	1
CO4	2	2	1	2	3	2	1	0	1	1	2	1	1	2
CO5	2	2	1	2	3	0	0	1	2	1	2	2	1	2
CO6	3	3	3	3	1	0	0	0	1	1	2	1	2	2

SEMESTER - III

20CSPC301 SDG NO. 4 & 9	OBJECT ORIENTED PROGRAMMING	L	T	P	C
		2	1	0	3

OBJECTIVES:

- To understand Object Oriented Programming concepts and principles of Packages, Inheritance and Interfaces
- To define Exceptions and use I/O streams
- To develop a Java application with threads and generic classes
- To design and build simple Graphical User Interfaces

UNIT I INTRODUCTION TO OOP AND JAVA FUNDAMENTALS 10

Object Oriented Programming – Abstraction – Objects and Classes – Encapsulation– Inheritance – Polymorphism– OOP in Java – Characteristics of Java – The Java Environment – Java Source File – Compilation - Fundamental Programming Structures in Java – Defining Classes in Java – Constructors - Methods - Access Specifiers – Static Members - Comments - Data Types- Variables - Operators- Control Flow- Arrays- Packages – Javadoc Comments.

UNIT II INHERITANCE AND INTERFACES 9

Inheritance – Super Classes– Sub Classes –Protected Members – Constructors in Sub Classes– The Object Class – Abstract Classes and Methods – Final Methods and Classes – Interfaces – Defining an Interface - Implementing Interface - Differences between Classes and Interfaces and Extending Interfaces – Object Cloning -Inner Classes -Array Lists -Strings.

UNIT III EXCEPTION HANDLING AND I/O 9

Exceptions – Exception Hierarchy – Throwing and Catching Exceptions – Built-in Exceptions-Creating own Exceptions - Stack Trace Elements - Input / Output Basics – Streams – Byte Streams and Character Streams – Reading and Writing Console – Reading and Writing Files.

UNIT IV MULTI-THREADING AND GENERIC PROGRAMMING 8

Differences between Multi-Threading and Multitasking - Thread Life Cycle - Creating Threads - Synchronizing Threads - Inter-Thread Communication - Daemon Threads - Thread Groups - Java Concurrency Packages - Generic Programming – Generic Classes – Generic Methods – Bounded Types – Restrictions and Limitations.

UNIT V LAMBDAS STREAMS AND REACTIVE PROGRAMMING 9

Lambda Expressions – Library Enhancements to Support Lambdas – No Parameter-Single Parameter - Multiple Parameters – With or Without Return Keyword-Comparator– Filter Collection Data-Streams-Generating Streams-Java Stream Interface Methods – For each-Map-Filter-Limit-Sorted - Parallel Processing - Reactive Programming– ReactiveX– ReactiveX Classes– Creating Operator– Reactive Subjects.

TOTAL: 45 PERIODS

TEXT BOOKS:

1. Herbert Schildt, "Java - The Complete Reference", 8th Edition, McGrawHill Education, 2011.
2. E.Balagursamy- "Programming with Java", 6th Edition, McGrawHill Education, 2019.

REFERENCES:

1. Paul Deitel, Harvey Deitel, "Java SE 8 for Programmers", 3rd Edition, Pearson, 2015.
2. Steven Holzner, "Java 2 Blackbook", Dream Tech Press, 2011.
3. Timothy Budd, "Understanding Object-Oriented Programming with Java", Updated Edition, Pearson Education, 2000.
4. Kathy Sierra, Bert Bates, Trisha Gee, "Head First Java", 3rd Edition, O'Reilly, 2022.
5. Joshua Bloch, " Effective Java", Third Edition, Addison Wesley, 2018.

WEB REFERENCES:

1. https://www.w3schools.com/java/java_oop.asp
2. https://www.edureka.co/blog/object-oriented-programming/
3. https://www.ntu.edu.sg/home/ehchua/programming/java/J3a_OOPBasics.html

ONLINE RESOURCES :

1. https://www.ntu.edu.sg/home/ehchua/programming/java/J3a_OOPBasics.html
2. https://introcs.cs.princeton.edu/java/lectures/

OUTCOMES:

Upon completion of the course, students should be able to

1. Comprehend Object Oriented Programming Concepts in Java. (K2)
2. Illustrate the purpose of packages, Java documents and Analyze the various types of Inheritance. (K4)

3. Apply the Object Oriented Programming Concepts to develop the reusable Applications. (K3)
4. Illustrate the java applications using Java Exceptions and I/O Streams.(K4)
5. Understand the concept of Multithreading and Generic Classes in Java. (K2)
6. Design and implement Lambda expressions, streams and reactive programming. (K6)

CO- PO, PSO MAPPING :

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	2	1	2	2	-	2	-	-	-	-	-	2	3	2
CO2	3	1	3	2	-	2	-	-	2	-	-	2	3	2
CO3	3	1	3	2	-	2	-	-	-	-	-	2	3	3
CO4	3	1	3	2	-	2	-	-	-	-	-	2	3	2
CO5	3	1	3	2	3	2	-	-	-	-	-	2	3	2
CO6	3	1	3	2	3	2	-	-	1	-	-	2	3	2

SEMESTER - III

20SCPC301 SDG NO. 4	SOFTWARE ARCHITECTURE AND PROJECT MANAGEMENT	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To understand the phases in a software project.
- To recognize the Cost estimation, risk and mitigation of Software project
- To understand fundamental concepts of requirements engineering and Analysis Modelling.
- To analyze the various software design methodologies, testing and maintenance measures.
- To Study the quality and Reliability of software products.

UNIT I INTRODUCTION **6**

Programming in the small vs. programming in the large, software project failures and importance of software quality and timely availability, engineering approach to software development, role of software engineering towards successful execution of large software projects, emergence of software engineering as a discipline; Basic concepts of life cycle models – different models - Agile and milestones;

UNIT II SOFTWARE REQUIREMENTS & OBJECT ORIENTED ANALYSIS, DESIGN AND CONSTRUCTION 10

Software Requirements Analysis, Design and Construction: Introduction to SRS and requirement elicitation techniques, requirement modeling techniques – decision tables, event tables, state transition tables, Petri nets OOAD and Construction:Introduction to UML,Use cases, -Concepts - the principles of abstraction, modularity, specification, encapsulation and information hiding, concepts of abstract data type, Class Responsibility Collaborator (CRC) model, quality of design, design measurements, design patterns, Refactoring, object-oriented construction principles, object-oriented metrics. Secure development and build environment.

UNIT III SOFTWARE PROJECT MANAGEMENT AND ESTIMATION TECHNIQUES 11

Software Project Management: Software project planning –identification of activities and resources, concepts of feasibility study, techniques for estimation of schedule and effort,introduction to the concepts of risk and its mitigation, configuration management. Estimation Techniques:Software cost estimation models and concepts of software engineering economics, techniques of software project control and reporting,Introduction to measurement of software size, software metrics and metrics-based control methods, measures of code and design quality.

UNIT IV SOFTWARE TESTING 9

Introduction to faults and failures; basic testing concepts; concepts of verification and validation; black box and white box tests; white box test coverage – code coverage, condition coverage, branch coverage; basic concepts of black-box tests – equivalence classes, boundary value tests, usage of state tables, testing use cases, transaction-based testing, testing for non-functional requirements – volume, performance and efficiency, concepts of inspection. Security testing of software: Unit testing, integration testing, validation and system testing, fuzzing.

UNIT V SOFTWARE QUALITY AND RELIABILITY 9

Internal and external qualities; process and product quality; principles to achieve software quality; introduction to different software quality models like McCall, Boehm, FURPS / FURPS+, Dromey, ISO – 9126; introduction to Capability Maturity Models (CMM and CMMI), introduction to software reliability, reliability models and estimation.

TOTAL : 45 PERIODS

TEXT BOOKS:

1. Roger S. Pressman, "Software Engineering – A Practitioner's Approach", Seventh Edition, Mc Graw-Hill International Edition, 2010.
2. Ian Sommerville, "Software Engineering", 9th Edition, Pearson Education Asia, 2011.

REFERENCES:

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

ONLINE RESOURCES:

1. http://nptel.ac.in/.
2. http://infolab.stanford.edu/~burback/watersluice/watersluice.html.

WEB REFERENCES:

1. https://www.vssut.ac.in/lecture_notes/lecture1428551142.pdf.
2. http://www.darshan.ac.in/Upload/DIET/Documents/CE/2160701_Software%20Engineering%20Study%20Material%20GTU_23042016_032444AM.pdf.
3. https://jnec.org/lab-manuals/cse/te/se.pdf.

OUTCOMES:

Upon completion of the course, the student should be able to

1. Define the key approaches of engineering that yield the importance of software project quality.(K1)
2. Understand the different activities in software project plan , activities , management and cost estimation techniques.(K2)
3. Understand the software requirement specifications and the principles of unified modelling language to model the business requirements.(K2)
4. Select and apply the various testing concepts in software projects to maintain stable software products.(K3)
5. Compare and contrast the reliability and quality metrics of a software product.(K2)

CO- PO, PSO MAPPING:

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

SEMESTER - III

20SCPC302 SDG NO. 4 & 9	CYBER SECURITY ESSENTIALS	L	T	P	C
		3	0	0	3

OBJECTIVES:

- Students should be able to understand.
- The difference between threat, risk, attack and vulnerability.
- How threats materialize into attacks.
- Where to find information about threats, vulnerabilities and attacks.
- Typical threats, attacks and exploits and the motivations behind them.

UNIT I INTRODUCTION TO CYBER SECURITY 9

Introduction -Computer Security - Threats -Harm - Vulnerabilities - Controls - Authentication -Access Control and Cryptography - Web—User Side - Browser Attacks - Web Attacks Targeting Users - Obtaining User or Website Data - Email Attacks

UNIT II SECURITY IN OPERATING SYSTEM & NETWORKS 9

Security in Operating Systems - Security in the Design of Operating Systems - Rootkit - Networking basics (home network and large-scale business networks), Networking protocols, Security of protocols, sample application hosted on-premises.

UNIT III DIGITAL SECURITY 9

Basics of digital security, protecting personal computers and devices, protecting devices from Virus and Malware, Identity, Authentication and

Authorization, need for strong credentials, keeping credentials secure, protecting servers using physical and logical security, World Wide Web (www), the Internet and the HTTP protocol, security of browser to web server interaction,

UNIT IV PRIVACY IN CYBERSPACE 9

Introduction to cyber-attacks, application security (design, development and testing), operations security, monitoring, identifying threats and remediating them, Principles of data security - Confidentiality, Integrity and Availability, Data Privacy, Data breaches, preventing attacks and breaches with security controls, Compliance standards, Computer Ethics.

UNIT V MANAGEMENT AND INCIDENTS 9

Security Planning - Business Continuity Planning - Handling Incidents - Risk Analysis - Dealing with Disaster - Emerging Technologies - The Internet of Things - Economics - Electronic Voting - Cyber Warfare- Cyberspace and the Law - International Laws - Cyber crime - Cyber Warfare and Home Land Security.

TOTAL : 45 PERIODS

TEXT BOOKS:

1. Charles P. Pfleeger Shari Lawrence Pfleeger Jonathan Margulies, Security in Computing, 5th Edition , Pearson Education , 2015

REFERENCES:

1. George K.Kostopoulous, Cyber Space and Cyber Security, CRC Press, 2013.
2. Martti Lehto, Pekka Neittaanmäki, Cyber Security: Analytics, Technology and Automation edited, Springer International Publishing Switzerland 2015
3. Nelson Phillips and Enfinger Steuart, —Computer Forensics and Investigations||, Cengage Learning, New Delhi, 2009.

OUTCOMES:

Upon completion of the course, the student should be able to

CO- PO, PSO MAPPING:

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

SEMESTER - III

20SCPC303 SDG NO. 4	MACHINE LEARNING IN CYBER SECURITY	L	T	P	C
		3	0	0	3

OBJECTIVES:

- Study about uninformed and Heuristic search techniques.
- Learn techniques for reasoning under uncertainty
- Introduce Machine Learning and supervised learning algorithms
- Study about ensembling and unsupervised learning algorithms
- The students will learn to implement, train and validate the machine learning models and understand the recent algorithms in machine learning through case studies

UNIT I PROBLEM SOLVING 9

Problem solving – search algorithms – uninformed search strategies – Heuristic search strategies – Local search and optimization problems – adversarial search – constraint satisfaction problems (CSP).

UNIT II SUPERVISED LEARNING 9

Foundations of supervised learning - Decision trees and inductive bias, Regression Vs Classification, Supervised: Linear Regression, Logistic Regression, Generalisation, Training, Validation and Testing, Problem of Overfitting, Bias vs Variance, Performance metrics, Decision Tree, Random Forest, Perceptron, Beyond binary classification. Case study: Anomaly detection

UNIT III ADVANCED SUPERVISED LEARNING 9

Advanced supervised learning - Naive Bayes, Bayesian Belief Network, K-

Nearest Neighbour, Support vector machines, Markov model, Hidden Markov Model, Parameter Estimation: MLE and Bayesian Estimate, Expectation Maximisation, Neural Networks.

UNIT IV UNSUPERVISED LEARNING 9

Unsupervised Learning: Curse of Dimensionality, Dimensionality Reduction Techniques, Principal component analysis, Linear Discriminant Analysis Clustering: K-means, Hierarchical, Spectral, subspace clustering, association rule mining. Case Study: Spam filtering /machine learning for end point protection/network protection/ Application security

UNIT V PROBABILISTIC REASONING 9

Acting under uncertainty – Bayesian inference – naïve bayes models. Probabilistic reasoning – Bayesian networks – exact inference in BN – approximate inference in BN – causal networks.

TOTAL : 45 PERIODS

TEXT BOOKS:

1. Stuart Russell and Peter Norvig, "Artificial Intelligence – A Modern Approach", Fourth Edition, Pearson Education, 2021.
2. Tom Mitchell. Machine Learning. First Edition McGraw Hill Education; 2017

REFERENCES:

1. Christopher M Bishop. Pattern Recognition and Machine Learning. Springer 2010
2. Richard O. Duda, Peter E. Hart, David G. Stork. Pattern Classification. Wiley, Second Edition;2007
3. Kevin P. Murphey. Machine Learning, a probabilistic perspective. The MIT Press Cambridge, Massachusetts, 2012.

OUTCOMES:

Upon completion of the course, the student should be able to

1. Use appropriate search algorithms for problem solving
2. Apply reasoning under uncertainty
3. Understand issues and challenges of machine learning: data, model selection, model complexity, various machine learning algorithms in a range of real-world applications.
4. Understand strengths and weaknesses of many popular machine learning approaches.

5. Analyse the underlying mathematical relationships within and across Machine Learning algorithms.
6. Apply the paradigms of supervised and un-supervised learning on use cases of security.

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	-	-	1	-	1	-	-	-	2	1	2	2	1	2
CO2	-	-	-	-	1	-	-	-	2	1	2	2	1	2
CO3	-	-	1	-	-	-	2	-	1	-	3	3	2	2
CO4	1	-	-	-	1	-	-	-	2	-	3	2	1	2
CO5	1	-	1	-	1	-	-	-	2	-	2	2	2	2
CO6	3	2	-	2	3	3	2	3	3	3	3	-	-	3

SEMESTER - III

20CSPL301 SDG NO. 4 & 9	OBJECT ORIENTED PROGRAMMING LABORATORY	L	T	P	C
		0	0	3	1.5

OBJECTIVES:

- To understand Object Oriented Programming concepts and basic characteristics of Java
- To know the principles of Packages, Inheritance and Interfaces
- To develop a Java application with Threads and Generic classes
- To make the students understand life cycle of the Applets and its functionality

LIST OF EXPERIMENTS :

1. Basic JAVA Programs
   a. Write a program to find the sum of individual digits of a positive integer.
   b. Write a program to generate the first n terms of the sequence.
   c. Write a program to generate all the prime numbers between 1 and n, where n is a value supplied by the user.
   d. Write a program to find both the largest and smallest number in a list of integers.

e. Write a program to find factorial of list of number reading input as command.

2. Write a program to calculate bonus for different departments using method overriding.
3. Write a program to sort list of elements in ascending and descending order and show the exception handling.
4. Write a program to implement the concept of importing classes from user defined package and creating packages.
5. Write programs that illustrate how the following forms of inheritance are supported:
   a) Single inheritance
   b) Multiple inheritance
   c) Multi level inheritance
   d) Hierarchical inheritance
6. Write a program to demonstrate use of implementing interfaces.
7. Write a program to implement interfaces all string operations.
8. Write a program to create student report using applet, read the input using text boxes and display the output using buttons.
9. Write a program to implement thread priorities.
10. Write a program to implement thread, applets and graphics to animate ball movement.
11. JAVA Applet program
    a) Write a Applet program using paint brush
    b) Write a program to display analog clock using Applet
    c) Write a program to create different shapes and fill colors using Applet
12. JAVA Event Handling program
    a) Write a program that display the x and y position of the cursor movement using Mouse
    b) Write a program that identifies key-up key-down event user entering text in a Applet
13. JAVA programs on Swings
    a) Write a program to build a Calculator in Swings
    b) Write a program to display the digital watch in swing
    c) Write a program that to create a single ball bouncing inside a Jpanel.
    d) Write a program JTree as displaying a real tree upside down

TOTAL : 45 PERIODS

LAB REQUIREMENTS :

Hardware :

Desktop Systems - Pentium IV with 2 GB RAM
160 GB HARD Disk
Monitor 1024 x 768 colour

Software :

Windows operating system
JDK 1.8

OUTCOMES:

On completion of this laboratory course, the student should be able to

1. Write Java programs in accordance with the object oriented programming concepts. (K6)
2. Design user defined java packages. (K6)
3. Create Java programs using Inheritance and Polymorphism. (K6)
4. Implement Error-handling techniques using Exception handling and Multithreading. (K6)
5. Develop Applet program and GUI using Swing components. (K6)
6. Enumerate the event handling techniques in Java Programming. (K5)

CO- PO, PSO MAPPING :

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	2	2	-	2	-	-	-	-	2	2	3	2
CO2	2	2	3	2	-	2	-	-	-	-	2	2	3	2
CO3	2	2	3	2	-	2	-	-	2	2	2	2	3	2
CO4	3	3	2	2	-	2	-	-	-	-	2	2	3	2
CO5	3	3	3	2	-	2	-	-	-	-	2	2	3	2
CO6	2	3	3	2	-	2	-	-	2	2	2	2	3	2

SEMESTER - III

20SCPL301 SDG NO. 4	SOFTWARE ENGINEERING LABORATORY	L	T	P	C
		0	0	3	1.5

OBJECTIVES:

- To understand the concepts of software engineering
- To understand the effectiveness of software project management
- To understand the metrics and models of software quality and reliability
- To implement software requirement analysis, design and construction
- To know the various software testing methods

LIST OF EXPERIMENTS :

1. 1. Preparation of required document for standard Application program in standard format(SRS).
2. DFD of standard application problem.
3. To prepare time line chart/Gantt Chart for selected software project.
4. Implement requirements modeling techniques and methods.
5. To perform the user's view analysis, Structural, behavioral diagram for the suggested system: Use case diagrams.
6. Implement of CRC model
7. Implement metrics of code and design quality
8. Implement verification and validation procedure
9. Implement Test plan /Test script
10. Implement Software Testing - Prepare test plan, perform validation testing, coverage analysis, memory leaks, develop test case hierarchy, Site check and site monitor

TOTAL: 30 PERIODS

LAB REQUIREMENT FOR A BATCH OF 30 STUDENTS / 2 STUDENTS PER EXPERIMENT

EQUIPMENTS:

Argo UML/Star UML/UML Graph/Selenium or Equivalent

OUTCOMES:

On completion of this laboratory course, the student should be able to

1. To utilize engineering approach to software development. (K3)
2. To practice various software life cycle models. (K3)
3. To implement software quality models. (K6)

4. To analyze the techniques of requirements gathering and modeling. (K4)
5. To implement class responsibility collaborator model. (K6)
6. To execute both white box and black box testing. (K6)

CO – PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	2	2	-	-	-	-	1	-	3	2	1	-
CO2	2	3	1	1	-	1	-	-	-	-	-	-	-	-
CO3	2	2	2	1	2	-	-	-	-	-	-	-	1	1
CO4	-	3	2	1	2	-	-	-	2	1	-	1	2	1
CO5	2	3	-	1	-	1	-	-	-	-	-	-	2	-
CO6	-	3	3	-	-	-	-	-	-	1	-	-	2	-

SEMESTER - III

20ITPL301 SDG NO. 4	DATA STRUCTURES LABORATORY	L	T	P	C
		0	0	3	1.5

OBJECTIVES:

- To implement Linear and Non-linear Data Structures
- To understand the different operations of Search Trees
- To implement Graph Traversal algorithms
- To get familiarized to Sorting and Searching algorithm

LIST OF EXPERIMENTS :

1. Array implementation of Stack and Queue ADTs
2. Array implementation of List ADT
3. Linked list implementation of List, Stack and Queue ADTs
4. Applications of List, Stack and Queue ADTs
5. Implementation of Binary Trees and operations of Binary Trees
6. Implementation of Binary Search Trees
7. Implementation of AVL Trees
8. Implementation of Heaps using Priority Queues

9. Graph representation and Traversal algorithms
10. Applications of Graphs- Implementation of searching and sorting algorithms
11. Implementation of any two Collision Techniques in Hashing

TOTAL: 45 PERIODS

LAB REQUIREMENTS :

Turbo C/Dev C++, Borland C

OUTCOMES:

On completion of this laboratory course, the student should be able to

1. Write functions to implement linear and non-linear data structure operations. [K1]
2. Suggest appropriate linear / non-linear data structure operations for solving a given problem. [K2]
3. Design and analyze the time and space efficiency of data structure.[K2]
4. Apply sorting and searching techniques. [K3]
5. Apply appropriate hash functions that result in a collision free scenario for data storage and retrieval. [K3]
6. Choose and implement efficient data structures and apply them to solve problems. [K3]

CO- PO, PSO MAPPING :

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	2	3	1	2	1	1	-	-	-	-	2	2	2	2
CO2	2	3	2	2	2	1	-	-	-	-	2	3	2	2
CO3	3	3	2	2	1	1	-	-	-	-	2	2	2	2
CO4	3	3	2	2	1	1	-	-	-	-	2	3	2	2
CO5	1	2	2	1	2	1	-	-	-	-	1	1	2	2
CO6	1	2	2	1	1	-	-	-	-	-	1	1	2	2

SEMESTER - III

20CSTE301 SDG NO. 4,11&15	LIVE-IN-LAB - I	L	T	P	C
		0	0	2	1

OBJECTIVES:

- To understand the engineering aspects of design with reference to simple products
- To foster innovation in design of products
- To develop design that add value to products and solve technical problems.
- To create awareness among the students of the characteristics of several domain areas where IT can be effectively used

COURSE PLAN :

Study: Take minimum three simple products, processes or techniques in the area of specialization, study, analyze and present them. The analysis shall be focused on functionality, construction, quality, reliability, safety, maintenance, handling, sustainability, cost etc. whichever are applicable. Each student in the group has to present individually; choosing different products, processes or techniques.

Design: The project team shall identify an innovative product, process or technology and proceed with detailed design. At the end, the team has to document it properly and present and defend it. The design is expected to concentrate on functionality; design for strength is not expected.

Note: *The one hour/week allotted for tutorial shall be used for discussions and presentations. The project team (not exceeding four) can be students from different branches, if the design problem is multidisciplinary.*

EVALUATION:

1. First evaluation (Immediately after first internal examination) : 20 marks
2. Second evaluation (Immediately after second internal examination): 20 marks
3. Final evaluation (Last week of the semester) : 60 marks

Note: *All the three evaluations are mandatory for course completion and for awarding the final grade.*

OUTCOMES:

Upon completion of the course, the student should be able to

1. List the problems and conduct literature survey to identify the gap and come up with an application oriented research problem in the specific domain.(K1)
2. Understand the project characteristics and explore necessary tools and components needed at various stages of the project(K2)
3. Design and validate the proposed system using simulation.(K3)
4. Develop the Prototype of the proposed system by adapting Industrial safety standards and best financial management practices(K5)
5. Analyze the obtained results and prepare a technical report.(K4)
6. Evaluate the project and go for journals and patents publication.(K5)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	2	2	2	2	2	2	3	2	2	3	3	3
CO2	3	3	3	2	3	3	2	2	3	3	3	3	3	3
CO3	3	3	3	2	3	3	2	2	3	3	3	3	3	3
CO4	2	2	2	1	2	1	1	1	3	2	3	3	3	2
CO5	2	2	2	1	2	1	1	1	3	2	3	3	3	2
CO6	2	2	2	1	2	1	1	1	3	2	3	3	3	2

SEMESTER - III

20CSTP301 SDG NO. 4	SKILL ENHANCEMENT	L	T	P	C
		0	0	2	1

APTITUDE & COGNITIVE SKILLS – PHASE 1

OBJECTIVE:

- To educate and enrich the students on quantitative ability, reasoning ability, and verbal ability.
- Improve their quantitative ability.
- Improve the ability of arithmetic reasoning
- Enhance their verbal ability through vocabulary building and grammar
- Equip with creative thinking and problem solving skills

UNIT I QUANTITATIVE ABILITY – I **10**

Problems on Trains - Time and Distance - Height and Distance - Time and Work

UNIT II QUANTITATIVE ABILITY – II **10**

Problems on Ages - Alligation or Mixture - Chain Rule - Simple Interest - Simple Equation - Theory Of Equation.

UNIT III REASONING ABILITY – I **8**

Analytical Reasoning - Pipes and Cistern - Logical Problems - Logical Games - Logical Deduction - Data Sufficiency - Arithmetic Reasoning

UNIT IV VERBAL ABILITY – I **10**

Idioms & Phrases - Synonyms - Antonyms - Classification

UNIT V CREATIVITY ABILITY – I **7**

Venn Diagrams -Cube and Cuboids - Dice - Cubes and Dice - Figure Matrix.

TOTAL : 45 PERIODS

REFERENCES:

1. Quantitative Aptitude for Competitive Exams by R. S. Agarwal
2. Quantum CAT by Sarvesh Verma
3. A Modern Approach to Logical Reasoning by R. S. Agarwal
4. Verbal Ability and Reading Comprehension by Arun sharma

PROBLEM SOLVING USING C PROGRAMMING - PHASE 2

OBJECTIVES:

- To provide exposure to problem-solving through programming.
- To train the student to the basic concepts of the C-programming language.
- To provide exposure to problem-solving through programming.
- To give the student hands-on experience with the concepts

UNIT I INTRODUCTION TO PRINCIPLES OF PROGRAMMING **9**

Introduction to Programming , Programming Domain : Scientific Application , Business Applications, Artificial Intelligence, Systems Programming , Web Software Categories of Programming Languages: Machine Level Languages, Assembly Level Languages , High Level Languages Programming Design Methodologies : Top Down and Bottom UP Program Development Cycle with case study, Program Execution and Translation Process ,Problem solving using

Algorithms and Flowcharts, Performance Analysis and Measurements: Time and Space complexity.

UNIT II INTRODUCTION TO C PROGRAMMING 9

Features of C and its Basic Structure, Simple C programs, Constants, Integer Constants, Real Constants, Character Constants, String Constants, Backslash Character Constants, Concept of an Integer and Variable, Rules for naming Variables and assigning values to variables, Floating-point Numbers, Converting Integers to Floating-point and vice-versa, Mixed-mode Expressions, The type cast Operator, The type char, Keywords, Character Input and Output, Formatted input and output, The gets() and puts() functions, Interactive Programming.

UNIT III OPERATORS, EXPRESSIONS AND CONTROL STATEMENTS 9

Arithmetic Operators, Unary Operators, Relational and Logical Operators, The Conditional Operator, Library Functions, Bitwise Operators, The Increment and Decrement Operators, The Size of Operator, Precedence of operators, The goto statement, The if statement, The if-else statement, Nesting of if statements, The conditional expression, The switch statement, The while loop, The do…while loop, The for loop, The nesting of for loops, The break statement and continue statement.

UNIT IV ARRAYS, STRINGS AND POINTERS 9

One Dimensional Arrays, Passing Arrays to Functions, Multidimensional Arrays, Strings, Basics of Pointers, Pointers and One-dimensional Arrays, Pointer Arithmetic, Pointer Subtraction and Comparison, Similarities between Pointers and One-dimensional Arrays, Null pointers, Pointers and Strings, Pointers and two-dimensional arrays, Arrays of Pointers.

UNIT V STRUCTURES, UNIONS AND FUNCTIONS 9

Basics of Structures, Arrays of Structures, Pointers to Structures, Self-referential Structures, Unions, Function Philosophy, Function Basics, Function Prototypes, and Passing Parameters: Passing Parameter by value and Passing Parameter by reference, passing string to function, Passing array to function, Structures and Functions Recursion.

TOTAL : 45 PERIODS

REFERENCES:

1. Programming in ANSI C - Balagurusamy - Tata McGraw-Hill Education, 2008
2. Programming in C (3rd Edition), by Stephen G. Kochan, Sams, 2004
3. Programming in C - Stephen G. Kochan, III Edition, Pearson Education.

COURSE OUTCOMES :

Upon completion of this course, the students should be able to:

1. Analyze their quantitative ability. (K4)
2. Understand the ability of arithmetic reasoning along with creative thinking and problem solving skills. (K2)
3. Create their verbal ability through vocabulary building and grammar. (K6)
4. Evaluate the situations to analyze the computational methods in order to identify and abstract the programming task involved. (K5)
5. Analyze tasks in which the numerical techniques are applicable in order to apply them to write, edit, compile, debug, correct, recompile and run programs. (K4)
6. Analyze and Design applications using Arrays, Strings,Pointers,Structures and Unions. (K4)

CO- PO & PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	-	-	-	-	3	2	-	3	2	3	-	2	-	-
CO2	-	-	-	-	3	2	-	3	2	3	-	2	-	-
CO3	-	-	-	-	3	2	-	-	1	3	-	2	-	-
CO4	-	-	-	-	3	2	-	3	3	3	-	2	2	2
CO5	-	-	-	-	3	2	-	-	2	3	-	2	2	2
CO6	-	-	-	-	3	2	-	-	2	3	-	2	2	2

SEMESTER - III

20MGMC301 SDG NO. 4	CONSTITUTION OF INDIA	L	T	P	C
		2	0	0	0

OBJECTIVES:

At the end of the course, the student is expected to

- To know about Indian constitution
- To know about central government functionalities in India
- To know about state government functionalities in India
- To know about Constitution function
- To Know about Constitutional remedies

UNIT I INTRODUCTION 6

Historical Background – Constituent Assembly of India – Philosophical foundations of the Indian Constitution – Preamble – Fundamental Rights – Directive Principles of State Policy – Fundamental Duties

UNIT II STRUCTURE AND FUNCTION OF CENTRAL GOVERNMENT 6

Union Government – Structures of the Union Government and Functions – President – Vice President – Prime Minister – Cabinet – Parliament – Supreme Court of India.

UNIT III STRUCTURE AND FUNCTION OF STATE GOVERNMENT 6

State Government – Structure and Functions – Governor – Chief Minister – Cabinet – State Legislature – Judicial System in States – High Courts and other Subordinate Courts.

UNIT IV CONSTITUTION FUNCTIONS 6

Indian Federal System – Centre – State Relations – President's Rule – Constitutional Amendments – Constitutional Functionaries.

UNIT V CONSTITUTIONAL REMEDIES 6

Enforcement of fundamental rights - Power of parliament to modify the rights the conferred by this part in their application to forces.

TOTAL: 30 PERIODS

TEXT BOOKS:

1. Durga Das Basu, "Introduction to the Constitution of India ", Prentice Hall of India, New Delhi.
2. R.C. Agarwal, (1997) "Indian Political System", S. Chand and Company, New Delhi.
3. M.V. Pyle (2019) , "An Introduction to The Constitution of India, 5/e", Vikas Publishing, New Delhi.
4 P.M. Bakshi, (2018) , "Constitution of India", Universal Law Publishing, New Delhi.

REFERENCES:

1. Sharma, Brij Kishore, "Introduction to the Constitution of India", Prentice Hall of India, New Delhi.
2. U.R.Gahai, "Indian Political System", New Academic Publishing House, Jalandhar.

OUTCOMES:

Upon completion of the course, the student should be able to

1. Explain the Constitution and Fundamental rights of citizens (K2)
2. Discuss the structure, hierarchy and functions of Central Government (K2)
3. Explain the functions of Supreme Court and Judiciary Systems in the state (K2)
4. Discuss the structure, hierarchy and functions of State Government (K2)
5. Recall the Centre-State relationship, constitutional amendments and functionaries (K1)
6. Discuss the remedies and rights available to India Citizens (K2)

CO – PO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	-	-	-	-	-	1	1	-	-	-	-	-
CO2	-	-	-	-	-	1	1	-	-	-	-	-
CO3	-	-	-	-	-	1	1	-	-	-	-	-
CO4	-	-	-	-	-	1	1	-	-	-	-	-
CO5	-	-	-	-	-	2	1	3	-	-	-	-
CO6	-	-	-	-	-	2	1	2	3	-	-	-

SEMESTER - IV

20BSMA402 SDG NO. 4	PROBABILITY AND QUEUEING THEORY	L	T	P	C
		3	1	0	4

OBJECTIVES:

- To impart necessary basic knowledge in Probability theory, Random Processes and Queueing models which are invariably used in Computer science courses

UNIT I PROBABILITY AND RANDOM VARIABLES 12

Probability – Axioms of probability – Conditional probability – Baye's theorem - Discrete and Continuous random variables – Moments – Moment generating functions – Binomial, Poisson, Geometric, Uniform, Exponential, Erlang and Normal distributions.

UNIT II TWO-DIMENSIONAL RANDOM VARIABLES 12

Joint distributions – Marginal and Conditional distributions – Covariance – Correlation and Linear Regression – Transformation of Random Variables – Central Limit Theorem (for independent and identically distributed random variables).

UNIT III RANDOM PROCESSES 12

Classification – Stationary process – Markov process - Poisson process – Discrete parameter Markov chain – Chapman Kolmogorov equations – Limiting distributions.

UNIT IV QUEUEING MODELS 12

Markovian queues – Birth and Death processes – Single and multiple server Queueing models – Little's formula - Queues with finite waiting rooms –Self-service model.

UNIT V ADVANCED QUEUEING MODELS 12

Finite source models - M/G/1 queue – Pollaczek-Khinchin formula - M/D/1 and M/EK/1 as special cases – Series queues – Open Jackson networks.

TOTAL: 60 PERIODS

TEXT BOOKS:

1 Ibe, O.C., "Fundamentals of Applied Probability and Random Processes", Elsevier, 1st Indian Reprint, 2007. (1.1-1.3, 1.6, 1.7 - 1.7.1, 1.8, 1.13 - Exercise problems in the above sections ; 2.1 – 2.8, 3.1 – 3.5, 3.9 , 4.1 - 4.3, 4.4 - 4.4.2, 4.7 – 4.11, 5.1 - 5.7, 6.1 – 6.3, 6.8, 6.10, 8.1 - 8.5, 10.5 (10.5.1 - 10.5.6), 10.6, 10.7 – 10.7.1-10.7. 5) (Units I, II & III).

2. Gross, D., Shortle, J.F, Thompson, J.M and Harris. C.M., "Fundamentals of Queueing Theory", Wiley Student 4th Edition, 2014. (1.1 – 1.5, 1.7, 2.1 - 2.7, 4.1, 4.2, 5.1 – 5.1.1) (Units IV and V)

REFERENCES:

1. Hwei Hsu, "Schaum's Outline Theory and Problems of Probability, Random variables and Random Processes", Tata Mcgraw Hill Edition, New Delhi, 2004.
2. Taha, H.A., " Operations Research", 9th Edition , Pearson India Education Services, Delhi,2016.
3. Trivedi, K.S., "Probability and Statistics with Reliability, Queueing and Computer Science Applications", 2nd Edition, John Wiley and Sons, 2002.
4. Yates, R.D. and Goodman. D.J., "Probability and Stochastic Processes", 2nd Edition, Wiley India Pvt. Ltd., Bangalore, 2012.
5. Veerarajan T., "Probability and Statistics, Random Processes and Queueing Theory", TataMc-Graw Hill Education Pvt. Ltd., New Delhi

WEB REFERENCES:

1. https://nptel.ac.in/courses/117103017/
2. https://nptel.ac.in/courses/111105041/
3. http://home.iitk.ac.in/~skb/ee679/ee679.html

ONLINE RESOURCES:

1. https://freevideolectures.com/course/3066/performance-evaluation-of-computer-systems/5
2. https://freevideolectures.com/course/3066/performance-evaluation-of-computer-systems/6

OUTCOMES:

Upon completion of the course, the student should be able to

1. Apply the knowledge of basic concepts of probability, one dimensional random variables and standard distributions in real life situations. (K3)
2. Study the relationship between two random variables and transformation by applying its basic concepts. (K3)
3. Apply the concepts of random processes in engineering disciplines. (K3)
4. Acquire the skills in analyzing Markovian queuing models. (K3)
5. Analyze the behavior of Non-Markovian queuing models, series queues and open networks. (K3)

CO- PO MAPPING :

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

SEMESTER - IV

20CSPW401 SDG NO. 4 & 9	COMPUTER NETWORKS WITH LABORATORY	L	T	P	C
		3	0	2	4

OBJECTIVES:

- To understand the protocol layering and physical level communication
- To understand the various components required to build different networks and analyze the performance of a network
- To learn the functions of network layer and the various routing protocols
- To familiarize the functions and protocols of the Transport layer

UNIT I INTRODUCTION AND PHYSICAL LAYER 9

Networks – Types – Protocol Layering – TCP/IP Protocol suite – OSI Model – Physical Layer: Performance – Transmission media – Switching – Circuit-switched Networks – Packet Switching.

UNIT II DATA LINK LAYER & MEDIA ACCESS 9

Introduction – Data Link Layer - Addressing – DLC Services – Data-Link Layer Protocols – HDLC – PPP - Media Access Control - Wired LANs: Ethernet - Wireless LANs – Introduction – IEEE 802.11, Bluetooth – Connecting Devices.

UNIT III NETWORK LAYER 9

Network Layer Services – Packet switching – Performance – IPV4 Addresses – Forwarding of IP Packets - Network Layer Protocols: IP, ICMP v4 – Unicast Routing Algorithms – Protocols – Multicasting Basics – IPV6 Addressing – IPV6 Protocol.

UNIT IV TRANSPORT LAYER **9**

Introduction – Transport Layer Protocols – Services – Port Numbers – User Datagram protocol – Transmission Control Protocol – SCTP.

UNIT V APPLICATION LAYER **9**

WWW and HTTP – FTP – Email –Telnet –SSH – DNS – SNMP.

LIST OF EXPERIMENTS : **15**

1. Simple client server program.
2. Socket program for echo/ping commands.
3. Implementing Link state routing algorithm.
4. Implementing distance vector routing algorithm.
5. Study of Network Simulator (NS2 or NS3) and Simulation of Congestion Control Algorithms using NS.
6. Study of TCP/UDP performance using Simulation tool.
7. Simulation of error correction code (like CRC).
8. Traffic Analysis using Wireshark.

TOTAL: 60 PERIODS

LAB REQUIREMENTS:

1. C/C++/JAVA/Equivalent compiler
2. Network Simulator like NS2/OPNET/Wireshark

TEXT BOOKS:

1. Behrouz A. Forouzan, “Data communications and networking with TCP/IP protocol suite", Sixth Edition, McGraw Hill, cop. 2022.
2. Larry L. Peterson, Bruce S. Davie, “Computer Networks: A Systems Approach”, Fifth Edition, Morgan Kaufmann Publishers Inc., 2012.

REFERENCES:

1. William Stallings, “Data and Computer Communications”, Tenth Edition, Pearson Education, 2014.
2. Nader F. Mir, "Computer and Communication Networks", Second Edition Prentice Hall, 2014.
3. Ying-Dar Lin, Ren-Hung Hwang and Fred Baker, “Computer Networks: An Open Source Approach”, McGraw Hill Publisher, 2011.
4. James F. Kurose, Keith W. Ross, Computer Networking, A Top-Down Approach Featuring the Internet, Sixth Edition, Pearson Education, 2013.

5. Andrew S. Tanenbaum, David J. Wetherall,"Computer Networks ", 5th edition, Pearson Education,2011

WEB REFERENCES:

1. https://swayam.gov.in/nd2_cec19_cs07/preview
2. https://nptel.ac.in/courses/106105081/
3. https://www.isi.edu/nsnam/ns/

ONLINE RESOURCES:

1. https://ptgmedia.pearsoncmg.com/images/9780789749048/samplepages/0789749041.pdf
2. https://www.cse.iitb.ac.in/~sri/cs348/cs378-lab00-overview.pdf
3. https://freevideolectures.com/course/2276/computer-networks
4. https://www.youtube.com/watch?v=g8iY36onLeM&list=PLWPirh4EWFpHJrW1D9UB24wsbM3zx7QMx

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the basic layers and its functions in computer networks. (K2)
2. Demonstrate the performance of a network. (K2)
3. Explain the basics of how data lows from one node to another. (K2)
4. Understand IEEE standards, analyze and design routing algorithms. (K2)
5. Describe the working of various transport and application layer protocols.(K2)
6. Apply the protocols for various functions in the network.(K3)

CO-PO, PSO MAPPING :

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	3	1	3	2	2	-	2	1	-	1	3	2
CO2	3	3	2	-	-	-	1	-	-	-	-	-	2	1
CO3	3	3	3	-	1	-	1	-	-	1	-	1	3	1
CO4	3	3	3	-	-	-	1	-	-	1	-	-	2	2
CO5	3	3	3	-	1	-	2	-	-	1	-	1	3	2
CO6	3	3	3	-	1	-	1	-	-	1	-	-	3	2

SEMESTER - IV

20CSPC401 SDG NO. 4&9	OPERATING SYSTEMS	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To understand the basic concepts, functions of Operating Systems, Processes and Threads
- To analyze Scheduling algorithm and understand the concept of Deadlock
- To analyse various Memory Management schemes and understand I/O management and File Systems
- To be familiar with the basics of Linux system and Mobile OS like iOS and Android

UNIT I OPERATING SYSTEM OVERVIEW 7

Computer System Overview-Basic Elements - Instruction Execution - Interrupts - Memory Hierarchy - Cache Memory - Direct Memory Access - Multiprocessor and Multicore Organization - Operating System Overview-Objectives and Functions - Evolution of Operating System - Computer System Organization Operating System Structure and Operations - System Calls - System Programs - OS Generation and System Boot.

UNIT II PROCESS MANAGEMENT 11

Processes - Process Concept - Process Scheduling - Operations on Processes - Inter-process Communication - CPU Scheduling - Scheduling Criteria - Scheduling Algorithms- Multiple - Processor Scheduling - Real Time Scheduling - Threads - Overview - Multithreading Models - Threading Issues - Process Synchronization - The Critical - Section Problem - Synchronization Hardware - Mutex Locks - Semaphores - Classic Problems of Synchronization - Critical Regions - Monitors - Deadlock – System Model - Deadlock Characterization - Methods for Handling Deadlocks - Deadlock Prevention - Deadlock Avoidance - Deadlock Detection - Recovery from Deadlock.

UNIT III STORAGE MANAGEMENT 9

Main Memory – Background, Swapping, Contiguous Memory Allocation - Paging - Segmentation - Segmentation with Paging - 32 and 64 Bit Architecture Examples - Virtual Memory – Background - Demand Paging - Page Replacement - Allocation - Thrashing - Allocating Kernel Memory - OS Examples.

UNIT IV FILE SYSTEMS AND I/O SYSTEMS 9

Mass Storage System – Overview of Mass Storage Structure - Disk Structure - Disk Scheduling and Management - Swap Space Management - File-System Interface - File Concept - Access Methods - Directory Structure - Directory Organization - File System Mounting - File Sharing and Protection - File System Implementation- File System Structure - Directory Implementation - Allocation Methods - Free Space Management - Efficiency and Performance - Recovery - I/O Systems – I/O Hardware - Application I/O Interface - Kernel I/O Subsystem - Streams - Performance.

UNIT V CASE STUDY 9

Linux System - Design Principles - Kernel Modules - Process Management - Scheduling - Memory Management - Input-Output Management - File System - Inter-Process Communication - Mobile OS - iOS and Android - Architecture and SDK Framework - Media Layer - Services Layer - Core OS Layer - File System.

TOTAL : 45 PERIODS

TEXT BOOK :

1. Abraham Silberschatz, Peter Baer Galvin and Greg Gagne, "Operating System Concepts", 9th Edition, John Wiley and Sons Inc., 2012.
2 William Stallings, "Operating Systems – Internals and Design Principles",7th Edition, Prentice Hall, 2011

REFERENCES :

1. Ramez Elmasri, A. Gil Carrick, David Levine, "Operating Systems – A Spiral Approach", Tata McGraw Hill Edition, 2010.
2. AchyutS.Godbole, Atul Kahate, "Operating Systems", McGraw Hill Education, 2016.
3. Andrew S. Tanenbaum, "Modern Operating Systems", Second Edition, Pearson Education, 2004.
4. Gary Nutt, "Operating Systems", Third Edition, Pearson Education, 2004.
5. Harvey M. Deitel, "Operating Systems", Third Edition, Pearson Education, 2004.

WEB REFERENCES :

1. https://nptel.ac.in/courses/106/106/106106144/
2. https://www.coursera.org/courses?query=operating%20system
3. https://www.computerhope.com/jargon/o/os.html
4. https://www.os-book.com/OS9/slide-dir/
5. http://web.iitd.ac.in/~minati/MTL458.html

ONLINE RESOURCES:

1. https://www.udacity.com/course/introduction-to-operating-systems--ud923
2. https://freevideolectures.com/course/3670/introduction-to-operating-systems

OUTCOMES:

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

1. Understand the basic concepts and functions of the operating system. (K2)
2. Analyze various scheduling algorithms. (K4)
3. Understand deadlock, prevention and avoidance algorithms. (K2)
4. Compare and contrast various memory management schemes. (K4)
5. Understand the functionality of file systems (K2)
6. Understand the performance of administrative tasks on Linux servers. (K2)

CO-PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	1	-	1	-	1	1	-	-	-	1	2	2
CO2	3	3	3	2	2	-	1	1	-	-	-	1	2	2
CO3	3	3	2	2	2	-	1	1	-	-	-	1	2	2
CO4	2	2	3	2	2	-	1	1	-	-	-	1	2	2
CO5	3	3	3	2	2	-	1	1	-	-	-	1	2	2
CO6	3	3	2	2	2	-	1	1	-	-	-	1	2	2

SEMESTER - IV

20CSPC402 SDG NO. 4&9	DATABASE MANAGEMENT SYSTEMS	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To design a database using ER diagrams, convert them to Relational Databases and to write SQL Queries
- To understand the fundamental concepts of Transaction Processing, Concurrency Control techniques and Recovery procedures
- To understand the Internal Storage structures and about the Query Processing Techniques
- To have an introductory knowledge about the Object Databases, XML Databases and NoSQL Databases

UNIT I DATABASE DESIGN **7**

Purpose of Database System – Views of Data –Database System Architecture-Data Models– Entity Relationship Model – ER Diagrams – Enhanced ER Model.

UNIT II RELATIONAL DATABASES **11**

Introduction to Relational Databases – Relational Model-ER-to-Relational Mapping– Keys –Relational Algebra – SQL Fundamentals – Advanced SQL features – Embedded SQL– Dynamic SQL-Functional Dependencies – Non-loss Decomposition – First – Second - Third Normal Forms - Dependency Preservation – Boyce/CoddNormal Form – Multi Valued Dependencies and Fourth Normal Form – Join Dependencies and Fifth Normal Form.

UNIT III TRANSACTIONS **9**

Transaction Concepts – ACID Properties – Schedules – Serializability – Concurrency Control – Need for Concurrency – Locking Protocols – Two Phase Locking – Deadlock – Transaction Recovery – Save Points – Isolation Levels – SQL Facilities for Concurrency and Recovery.

UNIT IV IMPLEMENTATION TECHNIQUES **9**

RAID – File Organization – Organization of Records in Files – Indexing and Hashing –Ordered Indices – B+ Tree Index Files – B Tree Index Files – Static Hashing – Dynamic Hashing – Query Processing Overview – Algorithms for SELECT and JOIN operations – Query optimization using Heuristics - Cost Estimation.

UNIT V ADVANCED TOPICS **9**

Distributed Databases – Architecture - Data Storage - Transaction Processing –

Object Based Databases - Object Database Concepts – Object Relational Features - ODMG Object Model – ODL - OQL – XML Databases - XML Hierarchical Model – DTD - XML Schema –Xquery.

TOTAL: 45 PERIODS

TEXT BOOKS:

1. Abraham Silberschatz, Henry F. Korth, S. Sudharshan, "Database System Concepts", Seventh Edition, Tata McGraw Hill, 2020.
2. RamezElmasri, Shamkant B. Navathe, "Fundamentals of Database Systems", Seventh Edition, Pearson Education, 2016.

REFERENCES:

1. C.J.Date, A.Kannan, S.Swamynathan, "An Introduction to Database Systems", Eighth Edition, Pearson Education, 2006.
2. Raghu Ramakrishnan, "Database Management Systems", Fourth Edition, McGraw-Hill Education, 2015.
3. G.K.Gupta,"Database Management Systems", Tata McGraw Hill, 2011.

WEB REFERENCES:

1. https://swayam.gov.in/nd1_noc19_cs46/
2. http://www.nptelvideos.in/2012/11/database-management-system.html
3. https://www.classcentral.com/course/swayam-database-management-system-9914
4. http://learnsql.com
5. https://www.w3schools.com/sql/default.asp
6. https://www.khanacademy.org/computing/computer-programming/sql

OUTCOMES:

Upon completion of the course, the student should be able to

1. Discuss the concepts of database to apply the Relational, ER model for design and SQL for implementation of the database. (K2)
2. Recognize and identify the use of normalization and functional dependencies to reine the database system. (K1)
3. Demonstrate various SQL queries for the Transaction Processing & Locking using concept of Concurrency control. (K2)
4. Build the query processing techniques for the optimization of SQL queries. (K3)
5. Implement the indexing and hashing techniques for the organisation of database records. (K3)

6. Illustrate how the advanced databases differ from the traditional databases. (K2)

CO- PO, PSO MAPPING :

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	2	1	1	1	2	1	0	0	0	0	0	0	2	2
CO2	2	2	2	2	1	1	0	0	0	0	0	0	2	2
CO3	2	1	2	1	2	1	0	0	0	0	0	0	2	2
CO4	2	2	2	2	1	1	0	0	0	0	0	0	2	2
CO5	2	2	2	2	1	1	0	0	0	0	0	0	2	2
CO6	2	2	2	1	2	1	0	0	0	0	0	0	2	2

SEMESTER - IV

20SCPC401 SDG NO. 4	CRYPTOGRAPHY & CYBER SECURITY	L	T	P	C
		3	0	0	3

OBJECTIVES:

- Learn to analyze the security of in-built cryptosystems.
- Know the fundamental mathematical concepts related to security.
- Develop cryptographic algorithms for information security.
- Comprehend the various types of data integrity and authentication schemes
- Understand cyber crimes and cyber security.

UNIT I INTRODUCTION TO SECURITY **9**

Computer Security Concepts – The OSI Security Architecture – Security Attacks – Security Services and Mechanisms – A Model for Network Security – Classical encryption techniques: Substitution techniques, Transposition techniques, Steganography – Foundations of modern cryptography: Perfect security – Information Theory – Product Cryptosystem – Cryptanalysis.

UNIT II SYMMETRIC CIPHERS **9**

Number theory – Algebraic Structures – Modular Arithmetic - Euclid's algorithm – Congruence and matrices – Group, Rings, Fields, Finite Fields SYMMETRIC KEY CIPHERS: SDES – Block Ciphers – DES, Strength of DES – Differential and linear cryptanalysis – Block cipher design principles – Block

cipher mode of operation – Evaluation criteria for AES – Pseudorandom Number Generators – RC4 – Key distribution.

UNIT III ASYMMETRIC CRYPTOGRAPHY 9

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 distribution – Key management – Diffie Hellman key exchange -– Elliptic curve arithmetic – Elliptic curve cryptography.

UNIT IVINTEGRITY AND AUTHENTICATION ALGORITHMS 9

Authentication requirement – Authentication function – MAC – Hash function – Security of hash function: HMAC, CMAC – SHA – Digital signature and authentication protocols – DSS – Schnorr Digital Signature Scheme – ElGamal cryptosystem – Entity Authentication: Biometrics, Passwords, Challenge Response protocols – Authentication applications – Kerberos MUTUAL TRUST: Key management and distribution – Symmetric key distribution using symmetric and asymmetric encryption – Distribution of public keys – X.509 Certificates.

UNIT V CYBER CRIMES AND CYBER SECURITY 9

Cyber Crime and Information Security – classifications of Cyber Crimes – Tools and Methods – Password Cracking, Keyloggers, Spywares, SQL Injection – Network Access Control – Cloud Security – Web Security – Wireless Security

TOTAL: 45 PERIODS

TEXT BOOKS:

1. William Stallings, "Cryptography and Network Security - Principles and Practice", Seventh Edition, Pearson Education, 2017.
2. Nina Godbole, Sunit Belapure, "Cyber Security: Understanding Cyber crimes, Computer Forensics and Legal Perspectives", First Edition, Wiley India, 2011.

REFERENCES:

1. Behrouz A. Ferouzan, Debdeep Mukhopadhyay, "Cryptography and Network Security", 3rd Edition, Tata Mc Graw Hill, 2015.
2. Charles Pfleeger, Shari Pfleeger, Jonathan Margulies, "Security in Computing", Fifth Edition, Prentice Hall, New Delhi, 2015.

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the fundamentals of networks security, security architecture, threats and vulnerabilities
2. Apply the different cryptographic operations of symmetric cryptographic algorithms
3. Apply the different cryptographic operations of public key cryptography
4. Apply the various Authentication schemes to simulate different applications.
5. Understand various cyber crimes and cyber security.

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	1	0	0	0	0	0	0	0	0	0	0	1
CO2	3	3	1	0	0	0	0	0	0	0	0	0	0	1
CO3	2	3	0	1	0	0	0	0	0	0	0	0	0	1
CO4	2	3	0	2	0	0	0	0	0	0	0	0	0	1
CO5	1	2	0	1	0	0	0	0	0	0	0	0	0	1
CO6	1	2	1	2	0	0	0	0	0	0	0	0	0	1

SEMESTER - IV

20ITPC401 SDG NO. 4	DESIGN AND ANALYSIS OF ALGORITHMS	L	T	P	C
		2	1	0	3

OBJECTIVES:

- To understand and apply the algorithm analysis techniques
- To critically analyze the efficiency of alternative algorithmic solutions for the same problem
- To understand different algorithm design techniques
- To understand the limitations of Algorithmic power

UNIT I INTRODUCTION **10**

Notion of an Algorithm – Fundamentals of Algorithmic Problem Solving – Important Problem Types – Fundamentals of the Analysis of Algorithmic

Efficiency –Asymptotic Notations and their properties - Analysis Framework – Empirical analysis - Mathematical analysis for Recursive and Non-recursive algorithms – Visualization.

UNIT II BRUTE FORCE AND DIVIDE-AND-CONQUER 9

Brute Force – Computing an – String Matching - Closest-Pair and Convex-Hull Problems - Exhaustive Search - Travelling Salesman Problem - Knapsack Problem - Assignment Problem.

Divide and Conquer Methodology – Binary Search – Merge sort – Quick sort – Heap Sort - Multiplication of Large Integers – Closest-Pair and Convex - Hull Problems.

UNIT III DYNAMIC PROGRAMMING AND GREEDY TECHNIQUES 9

Dynamic programming – Principle of optimality - Coin Changing Problem - Computing a Binomial Coefficient – Floyd's Algorithm – Multi Stage Graph - Optimal Binary Search Trees – Knapsack Problem and Memory functions - Greedy Technique – Container Loading Problem - Prim's Algorithm and Kruskal's Algorithm – 0/1 Knapsack Problem - Optimal Merge pattern - Huffman Trees.

UNIT IV ITERATIVE IMPROVEMENT 8

The Simplex Method - The Maximum-Flow Problem – Maximum Matching in Bipartite Graphs - Stable Marriage problem.

UNIT V COPING WITH THE LIMITATIONS OF ALGORITHM POWER 9

Lower - Bound Arguments - P, NP, NP - Complete and NP-Hard Problems- Backtracking – n-Queen Problem - Hamiltonian Circuit Problem – Subset Sum Problem. Branch and Bound – LIFO Search and FIFO Search - Assignment Problem – Knapsack Problem – Travelling Salesman Problem - Approximation Algorithms for NP-Hard Problems – Travelling Salesman Problem – Knapsack Problem.

TOTAL: 45 PERIODS

TEXT BOOKS:

1. AnanyLevitin, "Introduction to the Design and Analysis of Algorithms", Third Edition, Pearson Education, 2012.
2. Ellis Horowitz, Sartaj Sahni and Sanguthevar Rajasekaran, "Computer Algorithms/ C++", Second Edition, Universities Press, 2007.

REFERENCES:

1. Thomas H.Cormen, Charles E.Leiserson, Ronald L. Rivest and Clifford Stein, "Introduction to Algorithms", Third Edition, PHI Learning Private Limited, 2012.

2. Alfred V.Aho, John E. Hopcroft and Jeffrey D. Ullman, "Data Structures and Algorithms", Pearson Education, Reprint 2006.
3. Harsh Bhasin, "Algorithms Design and Analysis", Oxford university press, 2016.
4. S. Sridhar, "Design and Analysis of Algorithms", Oxford university press, 2014.

WEB REFERENCES:

1. https://nptel.ac.in/courses/106101060
2. https://www.cse.iitm.ac.in/course_details.php?arg=OTI
3. https://swayam.gov.in/nd1_noc19_cs47/previ

ONLINE RESOURCES:

1. https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-046j-design-and-analysis-of-algorithms-spring-2015/
2. http://www.learnalgorithms.in/
3. https://courses.cs.vt.edu/ csonline/Algorithms/Lessons/
4. http://openclassroom.stanford.edu/MainFolder/Course Page.php?course=IntroToAlgorithms.

OUTCOMES:

Upon completion of the course, the student should be able to

1. Review the fundamentals of algorithmic problem solving and analyzing efficiency of algorithms [K2]
2. Apply mathematical formulation,complexity analysis and methodologies to solve recurrence relations for algorithms [K3]
3. Compare the time complexities of various algorithms [K3]
4. Critically analyze the different algorithm design techniques for a given problem [K3]
5. Illustrate NP class problems and formulate solutions using standard approach [K2]
6. Articulate solutions for real life problems using algorithm design principles [K3]

CO-PO, PSO MAPPING :

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	1	0	0	0	0	0	0	0	0	0	0	1
CO2	3	3	1	0	0	0	0	0	0	0	0	0	0	1
CO3	2	3	0	1	0	0	0	0	0	0	0	0	0	1
CO4	2	3	0	2	0	0	0	0	0	0	0	0	0	1
CO5	1	2	0	1	0	0	0	0	0	0	0	0	0	1
CO6	1	2	1	2	0	0	0	0	0	0	0	0	0	1

SEMESTER - IV

20SCPL401 SDG NO. 4 & 9	CRYPTOGRAPHY & CYBER SECURITY LABORATORY	L	T	P	C
		0	0	3	1.5

OBJECTIVES:

- Learn different cipher techniques.
- Implement the algorithms DES, AES, RSA and Diffie-Hellman.
- Implement hashing techniques such as SHA-1, MD-5.
- Develop a digital signature scheme.

PRACTICAL EXERCISES:

1. Write a program to implement the following cipher techniques to perform encryption and decryption
2. Caesar Cipher
3. Playfair Cipher
4. Hill Cipher
5. Write a program to implement the following transposition techniques
6. Rail fence technique –Row major transformation
7. Rail fence technique - Column major transformation
8. Write a program to implement DES algorithm
9. Write a program to implement AES algorithm
10. Write a program to implement RSA Encryption algorithm
11. Write a program to implement the Diffie-Hellman Key Exchange mechanism. Consider one of the parties as Alice and the other party as bob.

12. Write a program to calculate the message digest of a text using the SHA-1 algorithm.
13. Write a program to calculate the message digest of a text using the MD-5 algorithm.

TOTAL: 45 PERIODS

OUTCOMES:

On completion of this laboratory course, the student should be able to

1. Develop a code for classical encryption techniques.
2. Build a symmetric and asymmetric algorithms.
3. Construct a code for various Authentication schemes.
4. Apply the principles of digital signature.

CO-PO,PSO MAPPING :

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	1	-	1	-	-	-	-	-	-	1	2	2
CO2	3	3	3	2	1	1	1	2	2	2	1	2	2	2
CO3	3	3	3	3	1	2	1	2	2	2	2	2	2	2
CO4	3	3	3	2	1	-	-	1	1	1	1	2	2	2
CO5	3	3	3	2	1	-	-	1	1	1	1	1	2	2
CO6	3	3	2	2	1	-	-	1	1	1	1	1	2	2

SEMESTER - IV

20CSPL401 SDG NO. 4 & 9	OPERATING SYSTEMS LABORATORY	L	T	P	C
		0	0	3	1.5

OBJECTIVES:

- To learn Unix commands and Shell programming
- To implement various CPU scheduling algorithm, Process Creation and Interprocess Communication
- To implement Deadlock avoidance and Deadlock Detection algorithms
- To implement Page Replacement algorithms and File strategies

LIST OF EXPERIMENTS :

1. Basics of UNIX commands & Administrator commands (man, uptime, users, service, pkill, pmap, wget, free, Shutdown commands, ping, su, who, env).

2. Write programs using the following system calls of UNIX operating system fork, exec, getpid, exit, wait, close, stat, opendir, readdir.
3. Write programs to simulate UNIX commands like cp, ls, grep, etc.
4. Shell Programming.
5. Write programs to implement the various CPU Scheduling Algorithms.
6. Implementation of Semaphores.
7. Implementation of Shared memory and IPC.
8. Implementation of Bankers Algorithm for Deadlock Avoidance.
9. Implementation of Deadlock Detection Algorithm.
10. Write program to implement Threading & Synchronization Applications.
11. Implementation of the following Memory Allocation Methods for fixed partition
    a) First Fit b) Worst Fit c) Best Fit
12. Implementation of Paging Technique of Memory Management.
13. Implementation of the following Page Replacement Algorithms
    a) FIFO b) LRU c) LFU
14. Implementation of the various File Organization Techniques.
15. Implementation of the following File Allocation Strategies
    a) Sequential b) Indexed c) Linked

TOTAL: 45 PERIODS

LAB REQUIREMENTS

1. Standalone desktops with C / C++ / Java / Equivalent compiler 30 Nos. with Linux OS

OUTCOMES:

On completion of this laboratory course, the student should be able to

1. Compare the performance of various CPU Scheduling Algorithms (K4)
2. Implement Deadlock avoidance and Detection Algorithms (K2)
3. Implement Semaphores. Create processes and implement IPC (K2)
4. Analyze the performance of the various Page Replacement Algorithms (K4)
5. Implement File Organization and File Allocation Strategies (K2)
6. Implement File Allocation Strategies (K2)

CO-PO,PSO MAPPING :

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	1	-	1	-	-	-	-	-	-	1	2	2
CO2	3	3	3	2	1	1	1	2	2	2	1	2	2	2
CO3	3	3	3	3	1	2	1	2	2	2	2	2	2	2
CO4	3	3	3	2	1	-	-	1	1	1	1	2	2	2
CO5	3	3	3	2	1	-	-	1	1	1	1	1	2	2
CO6	3	3	2	2	1	-	-	1	1	1	1	1	2	2

SEMESTER - IV

20CSPL402 SDG NO. 4&9	DATABASE MANAGEMENT SYSTEMS LABORATORY	L	T	P	C
		0	0	3	1.5

OBJECTIVES:

- To learn the use of Data Definition, Data Manipulation Commands, Nested and Join queries
- To understand Functions, Procedures and Procedural extensions of databases
- To be familiar with the use of a Front End tool
- To understand design and implementation of typical Database applications

LIST OF EXPERIMENTS :

1. Data Definition Commands, Data Manipulation Commands for inserting, deleting, updating and retrieving Tables and Transaction Control statements.
2. Database Querying – Simple queries, Nested queries, Sub queries and Joins.
3. Implementation of Views, Sequences and Synonyms.
4. Database Programming: Implicit and Explicit Cursors.
5. Procedures and Functions.
6. Triggers.
7. Exception Handling.
8. Database Design using ER Modeling, Normalization and Implementation for any application.

9. Database Connectivity with Front End Tools.
10. Case Study using Real Life Database applications.

TOTAL: 45 PERIODS

LAB REQUIREMENTS

SOFTWARE

Front end: VB/VC ++/JAVA or Equivalent

Back end: Oracle / SQL / MySQL/ Postgres / DB2 or Equivalent

OUTCOMES :

On completion of this laboratory course, the student should be able to

1. Use typical data definitions and manipulation commands. (K1)
2. Design applications to test Nested and Join Queries. (K3)
3. Implement simple applications that use Views. (K3)
4. Critically analyze the use of Tables, Views, Functions and Procedures. (K4)
5. Make use of ER modeling and normalization to design and implement database. (K3)
6. Implement real life applications that require a Front-end Tool as a Team. (K3)

CO- PO, PSO MAPPING :

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	2	1	1	1	2	1	0	0	0	0	0	0	2	2
CO2	2	2	2	1	2	1	0	0	0	0	0	0	2	2
CO3	2	2	2	1	2	1	0	0	0	0	0	0	2	2
CO4	2	2	2	1	2	1	0	0	0	0	0	0	2	2
CO5	2	2	2	2	1	1	0	0	0	0	0	0	2	2
CO6	2	2	2	1	2	1	0	0	0	0	0	0	2	2

SEMESTER - IV

20CSTE401 SDG NO. 4,11&15	LIVE-IN-LAB - II	L	T	P	C
		0	0	2	1

OBJECTIVES:

- To provide opportunities for the students, expose to Industrial environment and real time work
- To offer students a glimpse into real world problems and challenges that need IT based solutions
- To improve the team building, communication and management skills of the students
- To introduce students to the vast array of literature available of the various research challenges in the field of CSE

COURSE METHODOLOGY:

1. This initiative is designed to inculcate ethical principles of research and to get involve in life-long learning process for the students.
2. The course must involve engineering design with realistic constraints. It must also include appropriate elements of the following: Engineering standards, design analysis, modeling, simulation, experimentation, prototyping, fabrication, correlation of data, and software development.
3. Project can be individual work or a group project, with maximum of 3 students. In case of group project, the individual project report of each student should specify the individual's contribution to the group project.
4. On completion of the project, the student shall submit a detailed project report. The project should be reviewed and the report shall be evaluated and the students shall appear for a viva-voce oral examination on the project approved by the Coordinator and the project guide.

EVALUATION:

1. First evaluation (Immediately after first internal examination) : 20 marks
2. Second evaluation (Immediately after second internal examination): 30marks
3. Final evaluation (Last week of the semester) : 50marks

Note: *All the three evaluations are mandatory for course completion and for awarding the final grade*

TOTAL: 45 PERIODS

OUTCOMES:

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

1. Conduct literature survey to identify the gap and an application oriented research problem in the specific domain(K4)
2. Design and validate the proposed system using simulation(K6)
3. Prototype the proposed system(K5)
4. Analyze the obtained results and prepare a technical report(K4)
5. Publish the work in journals and apply for the patents.(K3)
6. Prepare for industrial environment and real time work(K3)

CO- PO, PSO MAPPING :

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	2	2	2	2	2	2	3	2	2	3	3	3
CO2	3	3	3	2	3	3	2	2	3	3	3	3	3	3
CO3	2	2	2	1	2	1	1	1	3	2	3	3	3	2
CO4	2	2	2	1	2	1	1	1	3	2	3	3	3	2
CO5	2	2	2	1	2	1	1	1	3	2	3	3	3	2
CO6	2	2	2	2	3	2	2	2	2	2	3	3	3	3

SEMESTER - IV

20CSTP401 SDG NO. 4	SKILL ENHANCEMENT	L	T	P	C
		0	0	2	1

APTITUDE AND COGNITIVE SKILLS – PHASE 1

OBJECTIVES:

- Improve their quantitative ability.
- Improve their reasoning ability.
- Enhance their verbal ability through vocabulary building and grammar
- Equip with creative thinking and problem solving skills

UNIT I QUANTITATIVE ABILITY – III **10**

Compound Interest - Profit and Loss- Partnership - Percentage- Set Theory

UNIT II QUANTITATIVE ABILITY – IV **10**

True Discount-Ratio and Proportion - Simplification - Problems On H.C.F and L.C.M

UNIT III REASONING ABILITY – II **8**

Course of Action - Cause and Effect - Statement and Conclusion - Statement and Argument - Data Sufficiency (DS) - Statement and Assumption - Making Assumptions.

UNIT IV VERBAL ABILITY – II **10**

Change of Voice - Change of Speech - Letter and Symbol Series - Essential Part-Verbal Reasoning - Analyzing Arguments.

UNIT V CREATIVITY ABILITY – II **7**

Seating Arrangement - Direction Sense Test - Character Puzzles - Missing Letters Puzzles - Mirror &Water Images.

TOTAL : 45 PERIODS

REFERENCES:

1. Quantitative Aptitude for Competitive Exams by R. S. Agarwal
2. Quantum CAT by Sarvesh Verma
3. A Modern Approach to Logical Reasoning by R. S. Agarwal
4. Verbal Ability and Reading Comprehension by Arun sharma

ADVANCED C PROGRAMMING - PHASE 2

COURSE OBJECTIVE:

- To improve C programming skills with understanding of code organization and functional hierarchical decomposition with using complex data types.
- To understand procedural programming methods using Dynamic memory Allocation.

UNIT I INTRODUCTION TO RECURSION **9**

Introduction to Recursion, Types of Recursion - Head Recursion , Tail Recursion, Tree Recursion, Indirect Recursion and Nested Recursion . Recursion vs Looping - Analysis on efficiency of looping and recursion, Working of recursive code in main memory. Recurrence Relation , Different types of recurrence relation. Deriving time complexity and space complexity using recurrence relation.

UNIT II GROWTH FUNCTIONS AND RECURSION 9

Polynomial Equations, Compare growth functions - order growth functions, omega growth functions, theta growth functions - Constant time, Linear time, Logarithmic time, Quadratic time and exponential time. Problems on Recursions - Factorial Number, Sum of first N Natural Numbers, Nth Fibonacci Number, Exponent Function, Taylor Series, Tower of Hanoi.

UNIT III STORAGE CLASSES, THE PREPROCESSOR AND DYNAMIC MEMORY ALLOCATION 9

Storage Classes and Visibility, Automatic or local variables, Global variables, Static variables, External variables, File Inclusion, Macro Definition and Substitution, Macros with Arguments, Nesting of Macros, Conditional Compilation, Dynamic Memory Allocation, Allocating Memory with malloc, Allocating Memory with calloc, Freeing Memory, Reallocating Memory Blocks, Pointer Safety, The Concept of linked list, Inserting a node by using Recursive Programs, Sorting and Reversing a Linked List, Deleting the Specified Node in a Singly Linked List.

UNIT IV FILE MANAGEMENT 9

Defining and Opening a file, Closing Files, Input/output Operations on Files, Predefined Streams, Error Handling during I/O Operations, Random Access to Files, Command Line Arguments.

UNIT V BIT MANIPULATION 9

The hexadecimal number system, C bitwise operators, Working with individual bits, How to check if a given number is a power of 2, Count the number of ones in the binary representation of the given number, Check if the ith bit is set in the binary form of the given number, How to generate all the possible subsets of a set, Find the largest power of 2 (most significant bit in binary form), which is less than or equal to the given number N, Tricks with Bits, Applications of bit operations.

TOTAL : 45 PERIODS

REFERENCES:

1. R. G. Dromey, "How to Solve It By Computer", Pearson, 1982
2. A.R. Bradley, "Programming for Engineers", Springer, 2011
3. Kernighan and Ritchie, "The C Programming Language", (2nd ed.) Prentice Hall, 1988

COURSE OUTCOMES :

Upon completion of this course, the students should be able to:

1. Analyze their quantitative ability. (K4)
2. Understand the ability of arithmetic reasoning along with creative thinking and problem solving skills. (K2)
3. Create their verbal ability through vocabulary building and grammar. (K6)
4. Evaluate code organization and functional hierarchical decomposition with complex data types. (K5)
5. Understand C programming skills to apply advanced structured and procedural programming. (K2)
6. Apply Various File and Bit Manipulation algorithms in Problem Solving. (K3)

CO- PO & PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	-	-	-	-	3	2	-	3	2	3	-	2	-	-
CO2	-	-	-	-	3	2	-	3	2	3	-	2	-	-
CO3	-	-	-	-	3	2	-	-	1	3	-	2	-	-
CO4	-	-	-	-	3	2	-	3	3	3	-	2	2	2
CO5	-	-	-	-	3	2	-	-	2	3	-	2	2	2
CO6	-	-	-	-	3	2	-	-	2	3	-	2	2	2

SEMESTER - V

20SCPC503 SDG NO. 9, 16	CYBER ATTACKS	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To understand the fundamentals of cyber security.
- To recognize different types of cyber threats and attacks.
- Understand cyber threat intelligence concepts and methodologies.
- To develop skills in incident detection and response.
- To develop skills in incident detection and response.
- To explore techniques for mitigating cyber threats.

UNIT I INTRODUCTION TO CYBER ATTACKS 9

Introduction –Terminologies - cyber attacks – Types of cyber crimes – Cyber stalking - Cyber Terrorism – Phishing – Software piracy – DoS– Spoofing

UNIT II SOCIAL ENGINEERING ATTACKS AND OSINT 9

Social engineering-Types of SE attacks, Pretexting, Phishing - Phishing Techniques- Impersonation- Human -Based Social Engineering Attacks-Quid Pro Quo- Tailgating, OSINT - Introduction to OSINT, OSINT methodologies-Overview of popular OSINT tools and their applications-Shodan- Maltego, the Harvester.

UNIT III MALWARE 9

Introduction to Malware-Malware Lifecycle-Types of Malware- Viruses, Worms, Trojans, Ransomware , Spyware, Rootkits, Fileless Malware, Zero-Day Exploits- Characteristics and Behaviors of Malware, impacts, prevention.

UNIT IV NETWORK VULNERABILITY AND SCANING 9

Introduction to Network Vulnerabilities- Common Network Vulnerabilities-Network Scanning Methods, Port Scanning and uses- Vulnerability Scanning and tools, Network Discovery and Enumeration.

UNIT V WEB ATTACKS WITH APPLICATIONS 9

Web attacks -Types, Cross-Site Scripting, Cross-Site Request Forgery (CSRF)-Click Jacking, Security Misconfigurations -Directory Traversal, Brute Force Attacks, Tools and applications.

TOTAL : 45 Hours

TEXT BOOKS:

1. "Cybersecurity Essentials" by Charles J. Brooks.
2. "Principles of Computer Security" by Conklin, White, Williams, Davis, and Cothren.
3. "Cryptography and Network Security: Principles and Practice" by William Stallings.
4. "Cybersecurity Operations Handbook" by J.W. Rittiaghouse and William Hancock.

REFERENECS:

1. "Introduction to Computer Security" by Matt Bishop.
2. "Network Security Essentials" by William Stallings.
3. "Practical Intrusion Analysis: Prevention and Detection for the Twenty-First Century" by Ryan Trost.
4. "Software Security: Building Security In" by Gary McGraw.

OUTCOMES:

Upon completion of the course, the student should be able to

1. Acquire knowledge of cyber threat intelligence frameworks.(K1)
2. Develop skills in incident detection and response. .(K2)
3. Apply techniques for mitigating cyber threats effectively. Understand the importance of secure software development. .(K2)
4. Implement techniques for ensuring application security. .(K3)
5. Apply secure coding principles in software development. .(K3)
6. Apply penetration testing methodologies to identify vulnerabilities. .(K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	3	3	1	1	1	-	1	-	1	-	2	2
CO2	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO3	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO4	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO5	3	3	3	3	3	1	1	1	2	3	1	-	2	2
CO6	3	3	2	3	3	2	-	-	-	-	-	-	1	1

SEMESTER - V

20SCPC501 SDG NO. 9, 16	SECURE CODING	L	T	P	C
		3	0	0	3

OBJECTIVES:

- Understand the importance of secure computing in modern IT environments.
- Explore the principles of secure system design and architecture.
- Analyze social engineering attacks and prevention techniques.
- Analyze social engineering attacks and prevention techniques.
- Implement secure coding practices and web application firewalls.

UNIT I INTRODUCTION TO SECURE CODING 8

Overview and importance of Secure Coding-Common security vulnerabilities in software-Secure Software Development Lifecycle (SDLC)-Integrating security into the development process-Principles of Secure Coding-Least privilege principle-Defence in depth-Principle of least astonishment.

UNIT II COMMON VULNERABILITIES AND BEST PRACTICES 9

Common Software Vulnerabilities=Buffer overflows-Injection vulnerabilities (SQL, XSS, CSRF)-Insecure file handling-Input Validation and Sanitization-Importance of proper input validation-Techniques for input sanitization-Error Handling and Logging-Secure error handling-Importance of effective logging.

UNIT III AUTHENTICATION AND AUTHORIZATION 9

Secure Authentication-Password policies and encryption-Multi-factor authentication-Authorization and Access Controls-Role-based access control-Principle of least privilege in authorization-Session Management-Secure session handling-Session fixation and hijacking prevention.

UNIT IV SECURE CODING PRACTICES FOR WEB APPLICATIONS 9

Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF)-Prevention techniques-Content Security Policy (CSP)-Secure Communication-TLS/SSL best practices-Secure handling of sensitive data-Secure File Handling-File upload/download security-Preventing path traversal attacks.

UNIT V ADVANCED TOPICS AND TOOLS FOR SECURE CODING 10

Code Review and Static Analysis-Importance of code reviews-Using static analysis tools-Security Testing-Penetration testing-Dynamic application

security testing (DAST)-3 Secure DevOps and Continuous Integration-Integrating security into DevOps processes-Continuous security testing.

TOTAL 45 HOURS

TEXT BOOKS:

1. "Cybersecurity: The Essential Body of Knowledge" by Dan Shoemaker, Wm. Arthur Conklin, and David O'Bryan.
2. "Hacking: The Art of Exploitation" by Jon Erickson.
3. "Network Security Essentials" by William Stallings
4. "Future Crimes: Inside the Digital Underground and the Battle for Our Connected World" by Marc Goodman

REFERENCES:

1. Hacking: The Art of Exploitation" by Jon Erickson
2. "Web Security Testing Cookbook" by Paco Hope and Ben Walther
3. "Software Fault Tolerance Techniques and Implementation" by Laura L. Pullum
4. "Secure Software Development: A Security Programmer's Guide" by Jason Grembi

OUTCOMES:

Upon completion of the course, the student should be able to

1. Gain a foundational understanding of secure computing principles. (K1)
2. Evaluate and implement secure design practices in computing systems. (K2)
3. Apply cryptographic principles to protect information. (K2)
4. Implement encryption algorithms in various computing scenarios. (K3)
5. Implement and configure network security measures. (K3)
6. Analyse and respond to network security incidents. (K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	3	3	1	1	1	-	1	-	1	-	2	2
CO2	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO3	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO4	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO5	3	3	3	3	3	1	1	1	2	3	1	-	2	2
CO6	3	3	2	3	3	2	-	-	-	-	-	-	1	1

SEMESTER - V

20SCPC502 SDG NO. 4,9,16	FUNDAMENTALS OF QUANTIZATION	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To provide students with a comprehensive understanding of the principles and techniques of quantization.
- To enable students to apply quantization concepts in signal processing, data compression, and digital communication.
- To familiarize students with advanced topics in quantization and their practical applications.
- To equip students with the skills to analyze and evaluate the effects of quantization in various systems.
- To encourage students to explore emerging trends and research directions in quantization.

Unit I Introduction to Quantization **9**

Overview of Quantization-Quantization Process and its Importance-Quantization Techniques-Quantization Error Analysis

Unit II Quantization in Signal Processing **9**

Basics of Signal Processing-Discrete and Continuous Signals-Quantization of Analog Signals-Quantization of Digital Signals

Unit III Quantization in Data Compression and Digital Communication **9**

Introduction to Data Compression-Role of Quantization in Data Compression-Lossy and Lossless Compression-Quantization in Image and Video Compression- Principles of Digital Communication-Quantization in Analog-to-Digital Conversion-Quantization Noise in Communication Systems-Impact of Quantization on Communication Quality

Unit IV Quantization and Cryptography Protocols **9**

Introduction to Cryptography - symmetric and Asymmetric Cryptography-Cryptographic hash Functions-Secure Communication protocols- Public Key Infrastructure (KPK) – Digital Signature and Certificates.

Unit V Applications of Quantization and Cryptography 9

Vector Quantization-Adaptive Quantization Techniques-Quantization in Machine Learning and Artificial Intelligence-Recent Developments and Trends in Quantization- Quantization in Secure Communications Systems-Quantization and Cryptography in IoT and Cloud Computing.

TOTAL: 45 PERIODS

TEXT BOOKS:

1. "Quantization Noise: Roundoff Error in Digital Computation, Signal Processing, Control, and Communications" by Bernard Widrow and István Kollár
2. "Digital Signal Processing: Principles, Algorithms, and Applications" by John G. Proakis and Dimitris G. Manolakis
3. Cryptography and Network Security: Principles and Practice" by William Stallings

REFERENCE BOOKS:

1. Quantization and Coding: Bridging the Gap Between Theory and Practice" by Dante Del Corso and Giancarlo Ferrante.
2. Introduction to Modern Cryptography" by Jonathan Katz and Yehuda Lindell

NPTEL Course Link:

1. Fundamentals of Quantization and Cryptography

OUTCOMES:

Upon completion of the course, the student should be able to

1. 1. Understand the fundamental concepts of quantization and Cryptography its applications in various domains.(K1)
2. Apply different quantization techniques to analog, Cryptography and digital signals.(K2)
3. Analyze the impact of quantization on data compression and communication systems.(K2)
4. Evaluate advanced quantization methods such as vector quantization and adaptive techniques.(K2)
5. Integrate quantization principles into real-world scenarios in fields like machine learning and artificial intelligence.(K3)
6. Critically assess recent advancements and trends in the field of quantization.(K2)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	3	3	1	1	1	-	1	-	1	-	2	2
CO2	2	3	3	2	3	1	1	-	2	-	1	-	-	2
CO3	3	2	3	3	2	1	1	-	2	-	1	-	2	2
CO4	2	3	2	3	3	1	1	-	2	-	1	-	-	2
CO5	2	3	3	3	2	1	1	1	2	3	1	-	2	2
CO6	3	3	2	3	2	2	-	-	-	-	-	-	1	1

SEMESTER - V

20SCPL501 SDG NO. 9,11,16	SECURE CODING LABORATORY	L	T	P	C
		0	0	3	1.5

OBJECTIVES:

- Understand fundamental principles and practices of secure coding.
- Implement secure coding techniques to prevent common vulnerabilities such as injection attacks, cross-site scripting (XSS), and authentication flaws.
- Analyze code for potential security weaknesses and apply appropriate mitigations.
- Demonstrate proficiency in using security tools and frameworks to enhance code security.
- Develop a proactive mindset towards security, emphasizing the importance of secure coding practices throughout the software development lifecycle.

LIST OF EXPERIMENTS:

1. Implement and test SQL injection prevention techniques like parameterized queries and input validation using OWASP ZAP or Burp Suite
2. Implement and test XSS prevention techniques like output encoding, input validation, and Content Security Policy (CSP) using OWASP ZAP or Burp Suite
3. Implement techniques like password hashing, salting, and multi-factor authentication using OWASP ZAP or Burp Suite
4. Implement techniques like session token rotation, session expiration, and secure cookie attributes using OWASP ZAP or Burp Suite

5. Implement techniques like file type validation, content-type checking, and secure file storage using OWASP ZAP or Burp Suite
6. Implement Buffer overflow vulnerabilities using GDB tools
7. To identify security mis-configurations using Nmap, Nesses tools
8. To encrypt and decrypt data using OpenSSL or PyCrypto
9. Role-based access control (RBAC) and attribute-based access control (ABAC) models using Metasploit or OWASP ZAP to exploit access control vulnerabilities.
10. Demonstrate Gauntlt or OWASP tools can be used to automate security testing processes and identify vulnerabilities in code.
11. Discuss remediation techniques and analyze the results of static code analysis using SonarQube or Checkmarx tools.
12. Analyze the scan results and prioritize vulnerabilities based on severity using Nessus or OpenVAS tools.
13. Securing APIs, including input validation, authentication, and access control using Postman or OWASP.
14. To perform dynamic application security testing using tools like OWASP ZAP or Burp Suite.

OUTCOMES:

Upon completion of the course, the student should be able to

1. Identify and explain common security vulnerabilities in software applications.
2. Apply secure coding principles to develop resilient and robust software systems.
3. Evaluate code for security flaws and implement effective counter measures.
4. Utilize secure coding frameworks and libraries to enhance application security.
5. Collaborate effectively with peers to address security challenges in coding assignments.
6. Demonstrate a comprehensive understanding of secure coding best practices through practical application and assessment.

SEMESTER - V

20SCPL502 SDG NO. 9,11,16	CYBER ATTACK LABORATORY	L	T	P	C
		0	0	3	1.5

OBJECTIVES:

- Develop practical skills in cyber security tools and techniques through experiential learning.
- Gain insight into the methodologies and tactics used by attackers to exploit vulnerabilities and compromise systems.
- Learn to implement and assess defense mechanisms and countermeasures to protect against cyber threats.
- Foster critical thinking and problem-solving abilities necessary for identifying, analyzing, and mitigating cyber threats.
- Promote ethical and responsible conduct in cyber security practices, emphasizing the importance of legal compliance and respect for privacy.

LIST OF EXPERIMENTS:

1. Network Enumeration Using Nmap for network discovery, service detection, and vulnerability scanning.
2. Employing OWASP ZAP to identify security vulnerabilities in web applications, such as SQL injection, cross-site scripting (XSS), and CSRF.
3. Developing and launching exploits against vulnerable systems using the Metasploit Framework.
4. Analyzing and assessing the security of wireless networks, including capturing packets, cracking WEP/WPA/WPA2 keys, and detecting rogue access points.
5. Analyzing malware samples in a controlled environment to understand their behavior, capabilities, and potential impact using Cuckoo Sandbox
6. Analyzing network traffic to detect suspicious activities, identify anomalies, and investigate security incidents using Wireshark.
7. Conducting comprehensive vulnerability assessments to identify weaknesses and misconfigurations in network infrastructure and systems.
8. Employing Hashcat to perform offline password cracking using various techniques, including brute-force, dictionary attacks, and mask attacks.
9. Configuring and deploying Snort IDS to monitor network traffic for signs of intrusion, malicious activities, and policy violations.
10. Conducting digital forensic investigations to collect, analyze, and preserve evidence from storage devices and digital media using Autopsy.
11. Simulating social engineering attacks, such as phishing, spear-phishing, and credential harvesting, using the SET framework.

12. Utilizing Sysinternals Suite tools (e.g., Process Explorer, Process Monitor) for endpoint security assessment, troubleshooting, and malware analysis on Windows systems.
13. Disassembling and analyzing binary executables to understand their functionality, identify vulnerabilities, and reverse engineer malware using Ghidra or IDA Pro.
14. Simulating incident response scenarios, sharing threat intelligence, and collaborating on incident handling using MISP (Malware Information Sharing Platform).
15. Assessing and improving the security posture of web servers by identifying and mitigating vulnerabilities using Burp Suite's web application security testing capabilities.

OUTCOMES:

Upon completion of the course, the student should be able to

1. Demonstrate proficiency in using a variety of cyber security tools and technologies for attack simulation, vulnerability assessment, and defense implementation.
2. Develop a comprehensive understanding of common cyber attack techniques, including reconnaissance, exploitation, privilege escalation, and data exfiltration.
3. Understand the principles of risk assessment and management in cyber security, including the identification, analysis, and prioritization of security risks.
4. Acquire skills in incident detection, response, and handling, including incident triage, containment, eradication, and recovery.
5. Enhance security awareness among participants, empowering them to recognize and mitigate cyber threats effectively.
6. Apply security best practices and principles in various domains, including network security, web application security, endpoint security, and social engineering prevention.

SEMESTER - VI

20SCPC601 SDG NO. 9,11,16	DISTRIBUTED AND CLOUD SECURITY	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To introduce students to the fundamental concepts of distributed systems and cloud computing.
- To familiarize students with security challenges and considerations specific to distributed and cloud environments.
- To equip students with the knowledge and skills to implement robust authentication, access control, and data security mechanisms in cloud deployments.
- To provide students with practical experience in designing and securing network infrastructure for cloud environments.
- To enable students to develop compliance, auditing, and incident response strategies for ensuring the security and resilience of distributed systems.

UNIT I INTRODUCTION TO DISTRIBUTED SYSTEMS AND CLOUD COMPUTING 9

Overview of distributed systems and cloud computing - Characteristics and architecture of distributed systems - Cloud service models: IaaS, PaaS, SaaS - Security challenges in distributed and cloud environments - Introduction to virtualization and containerization technologies

UNIT II AUTHENTICATION AND ACCESS CONTROL IN CLOUD ENVIRONMENTS 9

Authentication mechanisms in distributed and cloud systems - Single sign-on (SSO) and federated identity management - Access control models: Role-based access control (RBAC), attribute-based access control (ABAC) - Identity as a service (IDaaS) solutions - Best practices for securing authentication and access control in cloud environments

UNIT III DATA SECURITY AND PRIVACY IN DISTRIBUTED SYSTEMS 9

Data encryption techniques for distributed and cloud storage - Secure data transfer protocols (e.g., SSL/TLS, SSH) - Data masking and tokenization for privacy protection - Data residency and compliance requirements in distributed systems - Techniques for ensuring data integrity and confidentiality in distributed environments

UNIT IV NETWORK SECURITY IN CLOUD INFRASTRUCTURE 9

Securing virtual networks and subnets in cloud environments - Intrusion detection and prevention systems (IDS/IPS) - Network segmentation and isolation techniques - Secure communication protocols for inter-cloud and intra-cloud communication - Distributed denial of service (DDoS) mitigation strategies

UNIT V COMPLIANCE, AUDITING, AND INCIDENT RESPONSE IN CLOUD ENVIRONMENTS 9

Regulatory compliance requirements for cloud deployments (e.g., GDPR, HIPAA, PCI DSS) - Cloud auditing and monitoring tools and techniques - Incident response planning and management in distributed and cloud environments - Forensic analysis and investigation in cloud-based incidents - Disaster recovery and business continuity planning for distributed systems

TOTAL: 45 PERIODS

TEXT BOOKS:

1. "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance" by Tim Mather, Subra Kumaraswamy, and Shahed Latif
2. "Distributed Systems: Principles and Paradigms" by Andrew S. Tanenbaum and Maarten Van Steen

REFERENCE:

1. "Cloud Computing Security: Foundations and Challenges" by John R. Vacca

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the fundamental concepts and principles of distributed systems and cloud computing. (K1)
2. Implement secure authentication and access control mechanisms in cloud environments.(K2)
3. Apply encryption and privacy-enhancing techniques to secure data in distributed systems.(K2)
4. Design and implement network security measures for cloud infrastructure.(K3)
5. Ensure compliance with regulatory requirements and industry standards in cloud deployments.(K3)
6. Develop incident response and disaster recovery plans for mitigating security risks in distributed systems.(K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	3	3	1	1	1	-	1	-	1	-	2	2
CO2	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO3	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO4	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO5	3	3	3	3	3	1	1	1	2	3	1	-	2	2
CO6	3	3	2	3	3	2	-	-	-	-	-	-	1	1

SEMESTER - VI

20SCPC602 SDG NO. 4&9	QUANTUM ALGORITHM	L	T	P	C
		3	0	0	3

OBJECTIVES:

- Introduce students to the principles and basics of quantum computing.
- Provide a comprehensive understanding of key quantum algorithms and their underlying concepts.
- Offer hands-on experience in implementing quantum algorithms using programming languages such as Qiskit or Cirq.
- Encourage exploration of real-world applications and case studies of quantum algorithms.
- Stimulate discussion and collaboration on research opportunities and challenges in quantum algorithm development.

Unit I Introduction to Quantum Computing **9**

Fundamentals of Quantum Mechanics-Basics of Quantum Computation-Quantum Gates and Circuits-Quantum Parallelism and Superposition

Unit II Quantum Search Algorithms **9**

Grover's Algorithm-Grover's Search for Unsorted Databases-Applications of Grover's Algorithm

Unit III Quantum Fourier Transform and Shor's Algorithm **9**

Quantum Fourier Transform (QFT)-Period Finding and Factoring Problem-Shor's Algorithm for Integer Factorization

Unit IV Quantum Simulation **9**

Quantum Simulation Basics-Applications of Quantum Simulation in Chemistry and Physics-Quantum Approximate Optimization Algorithm (QAOA)

Unit V Quantum Machine Learning **9**

Quantum Enhancements in Machine Learning-Quantum Support Vector Machines (QSVM)-Quantum Neural Networks

TOTAL: 45 PERIODS

TEXT BOOK:

1. "Quantum Computation and Quantum Information" by Michael A. Nielsen and Isaac L. Chuang

REFERENCE BOOK:

1. "Quantum Computing: A Gentle Introduction" by Eleanor Rieffel and Wolfgang Polak

NPTEL Course Link:

1. NPTEL - Quantum Algorithms

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the principles of quantum computing and quantum algorithms.(k1)
2. Analyze and implement basic quantum algorithms such as Grover's and Shor's algorithms.(K2)
3. Explore the applications of quantum algorithms in search, optimization, and machine learning.(K2)
4. Discuss the potential impact of quantum algorithms on various industries and fields.(K2)
5. Develop critical thinking skills in evaluating the efficiency and limitations of quantum algorithms.(K3)
6. Foster creativity in designing new quantum algorithms for specific problems.(K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	3	3	1	1	1	-	1	-	1	-	2	2
CO2	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO3	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO4	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO5	3	3	3	3	3	1	1	1	2	3	1	-	2	2
CO6	3	3	2	3	3	2	-	-	-	-	-	-	1	1

SEMESTER - VI

20SCPC603 SDG NO. 16	CYBER LAW AND ETHICS	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To provide students with a solid foundation in cyber law principles and ethics.
- To familiarize students with the legal framework and regulatory landscape surrounding cyber activities.
- To explore ethical issues and dilemmas encountered in cybersecurity practices.
- To equip students with the knowledge and skills to navigate legal and ethical challenges in cyberspace.
- To prepare students for careers in cyber law enforcement, governance, and compliance roles.

UNIT I INTRODUCTION TO CYBER LAW AND ETHICS 9

Overview of cyber law and its significance in the digital age - Historical development and evolution of cyber law - Fundamental principles and concepts of cyber law - Ethical considerations in cyberspace - International treaties and conventions related to cyber law and ethics

UNIT II LEGAL FRAMEWORK FOR CYBER SECURITY 9

Cybercrime and its classification: hacking, malware, phishing, etc. - Analysis of cyber laws and regulations in different jurisdictions - Legal frameworks for data protection and privacy - Intellectual property rights and digital copyrights - Jurisdictional issues and challenges in cyber law enforcement

UNIT III REGULATION OF CYBER ACTIVITIES 9

Cybersecurity laws and regulations governing government agencies and private organizations - Compliance requirements for securing personal and sensitive data - Regulatory frameworks for critical infrastructure protection - Cybersecurity incident reporting and breach notification laws - Role of regulatory authorities and enforcement agencies in cyber law enforcement

UNIT IV ETHICAL ISSUES IN CYBER SECURITY 9

Ethical principles and values in cybersecurity - Ethical considerations in vulnerability disclosure and responsible disclosure policies - Ethical dilemmas in penetration testing and ethical hacking - Professional codes of conduct for cybersecurity professionals - Case studies and real-world scenarios highlighting ethical issues in cybersecurity

UNIT V CYBER LAW ENFORCEMENT AND GOVERNANCE 9

Investigation and prosecution of cybercrimes - Cyber forensic techniques and tools for digital evidence collection and analysis - Challenges in cyber law enforcement and international cooperation - Role of government agencies, law enforcement, and judiciary in cyber law governance - Cybersecurity policy development and implementation at national and international levels

TOTAL: 45 PERIODS

TEXT BOOKS:

1. "Cyber Law in India" by R.K. Jena
2. "Cyber Law: Indian Perspective" by Jayanta Kumar Panda

REFERENCE:

1. "The Law of Cybercrimes and Their Investigations" by George Curtis

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the legal framework and regulatory environment governing cyberspace.(K2)

2. Analyze and interpret cyber laws and regulations applicable to various cyber activities.(K1)
3. Evaluate ethical issues and dilemmas in cybersecurity practices and decision-making.(K2)
4. Apply ethical principles and professional codes of conduct in cybersecurity roles and responsibilities. (K2)
5. Demonstrate knowledge of cyber law enforcement processes and procedures. (K3)
6. Develop a comprehensive understanding of cyber law governance and policy-making. (K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	3	3	1	1	1	-	1	-	1	-	2	2
CO2	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO3	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO4	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO5	3	3	3	3	3	1	1	1	2	3	1	-	2	2
CO6	3	3	2	3	3	2	-	-	-	-	-	-	1	1

SEMESTER - VI

20SCPC604 SDG NO. 16	PENETRATION TESTING & ETHICAL HACKING	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To provide students with a comprehensive understanding of penetration testing and ethical hacking principles and methodologies.
- To equip students with the knowledge and skills to identify and exploit vulnerabilities in target systems and networks.
- To train students in conducting penetration tests and ethical hacking activities in a controlled and ethical manner.
- To enable students to prepare professional penetration testing reports and communicate findings effectively to stakeholders.
- To prepare students for careers in cybersecurity as penetration testers and ethical hackers.

UNIT I INTRODUCTION TO PENETRATION TESTING AND ETHICAL HACKING 9

Overview of penetration testing and ethical hacking - Understanding the ethical and legal implications of hacking - Introduction to common penetration testing methodologies (e.g., PTES, OWASP) - Setting up a penetration testing lab environment - Tools and techniques used in penetration testing and ethical hacking

UNIT II INFORMATION GATHERING AND FOOTPRINTING 9

Techniques for gathering information about target systems and networks - Open-source intelligence (OSINT) gathering methods - Footprinting and reconnaissance to identify potential attack vectors - Tools for information gathering and footprinting (e.g., Nmap, Maltego) - Documenting and analyzing gathered information for penetration testing purposes

UNIT III SCANNING AND ENUMERATION 9

Port scanning techniques and methodologies (e.g., TCP, UDP, SYN) - Service enumeration and fingerprinting - Vulnerability scanning and assessment using automated tools (e.g., Nessus, OpenVAS) - Manual enumeration techniques for identifying system weaknesses - Analyzing scan results and prioritizing vulnerabilities for exploitation

UNIT IV EXPLOITATION AND POST-EXPLOITATION 9

Exploiting vulnerabilities to gain unauthorized access to target systems - Common exploitation techniques (e.g., buffer overflows, SQL injection, XSS) - Privilege escalation and maintaining access to compromised systems - Post-exploitation activities: data exfiltration, lateral movement, and pivoting – Mitigation strategies and countermeasures for exploited vulnerabilities

UNIT V REPORTING, REMEDIATION, AND COMPLIANCE 9

Documentation and reporting of penetration testing findings - Prioritizing and communicating identified vulnerabilities to stakeholders - Developing comprehensive penetration testing reports - Recommendations for vulnerability remediation and risk mitigation - Compliance requirements and ethical considerations in penetration testing

TOTAL: 45 PERIODS

TEXT BOOKS:

1. "Penetration Testing: A Hands-On Introduction to Hacking" by Georgia Weidman
2. "The Hacker Playbook 3: Practical Guide to Penetration Testing" by Peter Kim

REFERENCE:

1. "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" by Dafydd Stuttard and Marcus Pinto

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the principles and methodologies of penetration testing and ethical hacking. (K2)
2. Demonstrate proficiency in information gathering, footprinting, and reconnaissance techniques.(K1)
3. Identify and exploit vulnerabilities in target systems and networks.(K1)
4. Conduct post-exploitation activities while maintaining ethical and legal standards.(K2)
5. Prepare comprehensive penetration testing reports and provide recommendations for vulnerability remediation.(K3)
6. Comply with ethical guidelines and legal requirements in penetration testing and ethical hacking practices.(K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	3	3	1	1	1	-	1	-	1	-	2	2
CO2	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO3	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO4	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO5	3	3	3	3	3	1	1	1	2	3	1	-	2	2
CO6	3	3	2	3	3	2	-	-	-	-	-	-	1	1

SEMESTER - VI

20SCPL601 SDG NO. 9,11,16	CLOUD SECURITY LABORATORY	L	T	P	C
		0	0	3	1.5

OBJECTIVES:

- Develop practical skills in configuring, monitoring, and securing cloud environments using industry-leading tools and techniques.
- Gain a deep understanding of cloud security principles, including shared responsibility models, identity and access management, encryption, and network security.
- Learn to identify, assess, and mitigate security risks associated with cloud services, applications, and data storage.
- Prepare participants to effectively detect, respond to, and recover from security incidents in cloud environments through simulated scenarios and exercises.
- Familiarize participants with regulatory compliance requirements, security standards, and best practices applicable to cloud computing, emphasizing the importance of governance and compliance frameworks.

LIST OF EXPERIMENTS:

1. Analyzing the configuration of AWS resources for compliance with security best practices using AWS Config.
2. Reviewing the security configurations of Azure resources and identifying security vulnerabilities using Azure Security Center.
3. Assessing the permissions and access controls configured in GCP projects using IAM roles and policies.
4. Monitoring network traffic within cloud environments to detect suspicious activities and potential security breaches.
5. Evaluating the security configuration of Amazon S3 buckets for data exposure risks and access control mis-configurations using AWS Trusted Advisor.
6. Scanning Docker containers and Kubernetes clusters for security vulnerabilities and misconfigurations using Docker Bench for Security.
7. Assessing and managing the security posture of cloud environments, including resource misconfigurations, compliance violations, and security risks.
8. Assessing the security of cloud workloads and virtual machines for vulnerabilities and compliance issues using native security assessment tools.
9. Implementing data encryption and managing cryptographic keys to protect sensitive data stored in cloud environments.

10. Evaluating CASB solutions for monitoring and enforcing security policies across cloud applications and services.
11. Configuring and managing web application firewalls (WAFs) to protect cloud applications from common web-based attacks and threats.
12. Assessing the security of serverless applications and functions deployed on cloud platforms for vulnerabilities and misconfigurations.
13. Configuring and testing distributed denial-of-service (DDoS) protection mechanisms to safeguard cloud applications and services from DDoS attacks.
14. Simulating cloud security incidents and practicing incident response procedures to effectively detect, analyze, and mitigate security threats.
15. Automating compliance checks and auditing cloud resources against regulatory standards and industry best practices using cloud-native compliance frameworks.

OUTCOMES:

Upon completion of the course, the student should be able to

1. Demonstrate proficiency in using a variety of cloud security tools and platforms, including AWS, Azure, and Google Cloud, for security configuration, monitoring, and management.
2. Develop a comprehensive understanding of cloud security concepts, architectures, and technologies, encompassing identity and access management, data encryption, network security, and compliance.
3. Apply security controls and best practices to secure cloud environments effectively, including configuring access controls, encryption, logging, monitoring, and intrusion detection/prevention systems.
4. Acquire skills in detecting, analyzing, and responding to security incidents in cloud environments, including incident triage, containment, eradication, and recovery procedures.
5. Ensure adherence to regulatory compliance requirements, industry standards, and organizational policies governing cloud security, including data protection regulations, compliance frameworks, and security certifications.
6. Enhance security awareness among participants, empowering them to recognize and mitigate cloud security risks effectively, and promoting a culture of security within organizations utilizing cloud services.

SEMESTER - VI

20SCPL602 SDG NO. 9,11,16	PENETRATION TESTING LABORATORY	L	T	P	C
		0	0	3	1.5

OBJECTIVES:

- Provide participants with practical experience in conducting penetration tests using current cyber security tools and techniques, enhancing their technical skills in offensive security.
- Familiarize participants with various penetration testing methodologies, frameworks, and best practices employed in the identification and exploitation of security vulnerabilities.
- Knowledge and skills to perform comprehensive vulnerability assessments and penetration tests across different target environments, including networks, applications, and wireless networks.
- Foster critical thinking and problem-solving abilities necessary for identifying, analyzing, and exploiting security weaknesses in target systems and networks.
- Promote ethical and responsible conduct in penetration testing practices, emphasizing the importance of obtaining proper authorization, respecting privacy, and adhering to legal and ethical guidelines.

LIST OF EXPERIMENTS:

1. Performing vulnerability scans to identify security weaknesses and misconfigurations in network devices, servers, and applications using OpenVAS.
2. Exploiting identified vulnerabilities to gain unauthorized access to systems and execute payloads using the Metasploit Framework.
3. Assessing the security posture of web applications by identifying common vulnerabilities such as SQL injection, cross-site scripting (XSS), and CSRF using Burp Suite.
4. Assessing the security of wireless networks by capturing and analyzing Wi-Fi traffic, and exploiting vulnerabilities to gain unauthorized access using Aircrack-ng.
5. Simulating social engineering attacks, such as phishing, spear-phishing, and credential harvesting, using the SET framework.
6. Employing Hashcat to perform offline password cracking using techniques such as brute-force, dictionary attacks, and rule-based attacks.
7. Conducting man-in-the-middle attacks and exploiting vulnerabilities in Wi-Fi networks using the Wi-Fi Pineapple tool.

8. Demonstrating techniques to escalate privileges on Windows and Linux systems, such as exploiting misconfigured permissions, weak service configurations, and kernel vulnerabilities.
9. Assessing the physical security controls of a facility by attempting to gain unauthorized access through methods like tailgating, lockpicking, and bypassing access control systems.
10. Identifying Internet of Things (IoT) devices using Shodan and exploiting vulnerabilities in IoT protocols and firmware using specialized tools.
11. Analyzing and exploiting buffer overflow vulnerabilities in binary executables using debugging tools like GDB and Immunity Debugger.
12. Demonstrating post-exploitation techniques to maintain persistent access, escalate privileges, and exfiltrate data using offensive frameworks like Empire and Cobalt Strike.
13. Exploring various methods to exfiltrate sensitive data from compromised systems, including covert channels, steganography, and encrypted tunnels.
14. Conducting a simulated attack scenario where a red team attempts to breach the defenses of a network while a blue team defends and detects the intrusion, followed by a debriefing and lessons learned session.

OUTCOMES:

Upon completion of the course, the student should be able to

1. Demonstrate proficiency in using a variety of penetration testing tools and techniques, including network scanning, vulnerability assessment, exploitation, and post-exploitation activities.
2. Develop a comprehensive understanding of penetration testing methodologies, including reconnaissance, enumeration, vulnerability analysis, exploitation, and reporting.
3. To identify, assess, and exploit security vulnerabilities in target systems and networks, including common web application vulnerabilities, misconfigurations, and weaknesses in network protocols.
4. Gain proficiency in documenting penetration test findings, including vulnerabilities discovered, exploitation techniques used, and recommendations for remediation, in clear and concise reports.
5. Prepare participants to effectively respond to security incidents discovered during penetration testing activities, including incident triage, containment, eradication, and recovery procedures.
6. Enhance security awareness among participants by providing insights into the mindset and tactics of attackers, enabling them to better defend against cyber threats and implement proactive security measures.

SEMESTER - VII

20SCPC701 SDG NO. 4,9,16	QUANTUM CRYPTOGRAPHY	L	T	P	C
		3	0	0	3

OBJECTIVES:

- Understand the fundamental principles of quantum mechanics relevant to cryptography.
- Analyze and implement various quantum key distribution protocols.
- Evaluate the security and efficiency of quantum cryptographic algorithms.
- Explore the integration of quantum communication networks with classical systems.
- Investigate advanced topics and emerging trends in quantum cryptography.

Unit I Introduction to Quantum Cryptography **9**

Overview of classical cryptography-Basic concepts of quantum mechanics-Introduction to qubits and quantum states-Quantum entanglement and superposition-The concept of quantum key distribution (QKD)-BB84 Protocol: Theory and implementation

Unit II Quantum Key Distribution Protocols **9**

Detailed study of BB84 Protocol-B92 Protocol-E91 Protocol-Device-independent QKD-Security proofs of QKD protocols-Practical implementations and challenges in QKD

Unit III Quantum Cryptographic Algorithms **9**

Quantum algorithms: Shor's algorithm and Grover's algorithm-Quantum-safe cryptographic algorithms-Post-quantum cryptography-Applications of quantum cryptographic algorithms

Unit IV Quantum Communication and Network Security **9**

Quantum teleportation-Quantum error correction-Quantum repeaters-Quantum communication networks-Security issues in quantum communication-Integration with classical communication networks.

Unit V Advanced Topics and Future Directions in Quantum Cryptography **9**

Advanced QKD protocols-Quantum coin flipping-Quantum bit commitment-Quantum blockchain-Future trends in quantum cryptography-Ethical and societal implications of quantum technologies.

TOTAL : 45 PERIODS

TEXT BOOKS:

1. "Quantum Computation and Quantum Information" by Michael A. Nielsen and Isaac L. Chuang
2. "Quantum Cryptography and Secret-Key Distillation" by Gilles van Assche

REFERENCE BOOKS:

1. "Introduction to Quantum Cryptography" by Thomas Beth and Gerd Leuchs
2. "Quantum Cryptography: An Applied Approach" by Marco Lanzagorta and Jeffrey Uhlmann

NPTEL RESOURCES:

1. NPTEL Course on Quantum Cryptography
2. NPTEL Lecture Series on Quantum Computing

OUTCOMES:

Upon completion of the course, the student should be able to

1. Demonstrate a comprehensive understanding of quantum mechanics and its application in cryptography.(K1)
2. Apply quantum key distribution protocols and evaluate their security measures.(K2)
3. Analyze quantum algorithms and post-quantum cryptographic techniques.(K2)
4. Design and implement secure quantum communication networks.(K3)
5. Critically assess advanced quantum cryptographic protocols and future trends.(K3)
6. Discuss the ethical and societal implications of quantum cryptography.(K2)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	3	3	1	1	1	-	1	-	1	-	2	2
CO2	3	3	3	2	3	1	1	-	2	-	1	-	2	2
CO3	3	3	3	2	3	1	1	-	2	-	1	-	2	2
CO4	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO5	3	3	3	2	3	1	1	1	2	3	1	-	2	2
CO6	3	3	2	2	3	2	-	-	-	-	-	-	1	1

SEMESTER - VII

20SCPC702 SDG NO.4,11,9, 16	CYBER FORENSICS	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To provide foundational knowledge of cyber forensics and its importance in modern society.
- To develop skills in the collection, preservation, and analysis of digital evidence.
- To understand the legal and ethical considerations in cyber forensics.
- To train students in the use of forensic tools and software.
- To apply theoretical knowledge through case studies and practical scenarios.

Unit I Introduction to Cyber Forensics **9**

Overview of Cyber Forensics-Definition, scope, and importance-Types of digital crimes and cyber threat-Cyber Crime Investigation-Legal and ethical aspects-Role of cyber forensics in investigations-Digital Evidence-Types of digital evidence-Principles of digital evidence handling

Unit II Digital Evidence Collection and Preservation **9**

Evidence Collection Techniques-Acquisition of digital evidence-Tools and methods for -evidence collection-Preservation of Digital Evidence-Chain of custody-Storage and preservation methods-Forensic Imaging-Creating forensic copies-Tools and best practices

Unit III Data Recovery and Analysis **9**

Data Recovery Techniques-Deleted file recovery-Recovering data from damaged devices-Forensic Data Analysis-Techniques for analyzing digital evidence-Use of forensic tools (e.g., EnCase, FTK)-Network Forensics-Monitoring and analyzing network traffic-Tools and techniques for network forensics

Unit IV Mobile and Cloud Forensics **9**

Mobile Device Forensics-Tools and techniques for mobile forensics-Challenges in mobile forensics-Cloud Forensics-Collecting and analyzing evidence from cloud environments-Legal and technical challenges in cloud forensics-Emerging Trends in Forensics-IoT forensics-AI and machine learning in cyber forensics

Unit V Reporting and Presentation of Findings **9**

Documentation and Reporting-Writing forensic reports-Importance of clear and concise reporting-Expert Testimony-Presenting findings in court-Preparing for cross-examination-Case Studies-Analysis of real-world cyber forensics cases-Lessons learned and best practices

TOTAL : 45 PERIODS

TEXT BOOKS:

1. "Guide to Computer Forensics and Investigations" by Bill Nelson, Amelia Phillips, and Christopher Steuart
2. "Digital Forensics and Cyber Crime: A Primer" by Joshua I. James and Frank Breitinger
3. "Computer Forensics: Cybercriminals, Laws, and Evidence" by Marie-Helen Maras

REFERENCE BOOKS:

1. "Digital Forensics: Incident Response and Computer Forensics" by Jason Luttgens, Matthew Pepe, and Kevin Mandia
2. "Network Forensics: Tracking Hackers through Cyberspace" by Sherri Davidoff and Jonathan Ham

NPTEL COURSES:

1. NPTEL Course: Introduction to Cyber Security
2. NPTEL Course: Computer and Network Security

OUTCOMES:

Upon completion of the course, the student should be able to

1. Explain the types and impacts of digital crimes and cyber threats.(K1)
2. Analyze legal and ethical issues in cyber forensics.(K2)
3. Demonstrate skills in the collection, preservation, and analysis of digital evidence.(K3)
4. Use various cyber forensic tools effectively.(K2)
5. Apply forensic techniques to mobile devices and cloud environments.(K3)
6. Prepare and present forensic findings in legal and professional settings.(K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	3	3	1	1	1	-	1	-	1	-	2	2
CO2	3	3	3	2	3	1	1	-	2	-	1	-	2	2
CO3	3	3	3	2	3	1	1	-	2	-	1	-	2	2
CO4	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO5	3	3	3	3	3	1	1	1	2	3	1	-	2	2
CO6	3	3	2	3	3	2	-	-	-	-	-	-	1	1

SEMESTER - VII

20SCPC703 SDG NO.8,9,16,17	BLOCK CHAIN TECHNOLOGY	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To provide a foundational understanding of blockchain technology and its significance.
- To equip students with the skills to develop and deploy blockchain applications.
- To explore and analyze the application of blockchain in various industries.
- To understand the challenges faced in blockchain implementation and explore potential solutions.
- To encourage innovation and exploration of future trends in blockchain technology

Unit I Introduction to Blockchain Technology 9

Overview of Blockchain-Definition and history-Key characteristics and benefits-Types of blockchain: public, private, consortium-Blockchain Architecture-Components of blockchain: blocks, chains, nodes-Consensus mechanisms: Proof of Work, Proof of Stake, and others-Cryptographic Foundations-Hash functions-Digital signatures-Public and private keys

Unit II Blockchain Platforms and Development 9

Bitcoin and Ethereum-Overview of Bitcoin: structure, transaction flow, mining-Ethereum: smart contracts and DApps-Smart Contracts-Definition and characteristics-Writing and deploying smart contracts-Use cases and limitations-Blockchain Development Tools-Introduction to development tools like Remix, Truffle, Ganache-Setting up a development environment

Unit III Blockchain Use Cases and Applications **9**

Financial Services-Crypto currencies and digital payments-Decentralized finance (DeFi)-Cross-border payments-Supply Chain Management-Tracking and tracing goods-Enhancing transparency and efficiency-Other Industries-Healthcare, real estate, and government services-Case studies of successful block chain implementations

Unit IV Challenges and Future Trends **9**

Scalability and Performance-Issues related to scalability-Solutions and improvements (e.g., sharding, layer 2 solutions)-Security and Privacy-Common vulnerabilities and attacks-Enhancing privacy on the blockchain-Regulatory and Ethical Issues-Legal challenges and regulatory frameworks-Ethical considerations in blockchain deployment

Unit V Hands-on Projects and Emerging Trends **9**

Project Development-Planning and developing a blockchain project-Testing and deploying blockchain applications-Emerging Trends-Blockchain and IoT-Integration with AI and machine learning-Future of Blockchain-Predictions and potential developments-Impact on various industries

TOTAL : 45 PERIODS

TEXT BOOKS:

1. "Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications" by Imran Bashir
2. "Blockchain Basics: A Non-Technical Introduction in 25 Steps" by Daniel Drescher
3. "Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World" by Don Tapscott and Alex Tapscott

REFERENCE BOOKS:

1. "Blockchain: Blueprint for a New Economy" by Melanie Swan
2. "Ethereum Smart Contract Development: Build Blockchain-Based Decentralized Applications Using Solidity" by Mayukh Mukhopadhyay

NPTEL COURSES:

1. NPTEL Course: Blockchain Architecture Design and Use Cases
2. NPTEL Course: Blockchain and its Applications

OUTCOMES:

Upon completion of the course, the student should be able to

1. Explain the fundamental concepts and components of blockchain technology.(K1)
2. Demonstrate knowledge of major blockchain platforms and the development of smart contracts.(K2)
3. Analyze and apply blockchain solutions in different industries.(K2)
4. Identify and address scalability, security, and regulatory challenges in blockchain deployment.(K2)
5. Develop and deploy blockchain applications through hands-on projects.(K2)
6. Evaluate emerging trends and predict future impacts of blockchain technology.(K2)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	2	3	1	1	1	-	1	-	1	-	2	2
CO2	3	3	3	2	3	1	1	-	2	-	1	-	3	2
CO3	2	2	2	2	3	1	1	-	2	-	1	-	2	2
CO4	2	2	3	3	3	1	1	-	2	-	1	-	3	2
CO5	2	2	2	3	3	1	1	1	2	3	1	-	2	2
CO6	3	3	2	3	3	2	-	-	-	-	-	-	1	1

SEMESTER - VII

20SCPL701 SDG NO. 9,11,16	QUANTUM LABORATORY	L	T	P	C
		0	0	3	1.5

OBJECTIVES:

- Provide participants with a foundational understanding of quantum mechanics, quantum algorithms, and quantum information theory as they relate to quantum computing.
- Familiarize participants with quantum computing frameworks, quantum programming languages, and simulation tools to facilitate hands-on experimentation and exploration.

- Introduce participants to quantum cryptographic principles and protocols for secure communication, key distribution, and data protection in the context of quantum computing.
- Enable participants to develop, analyze, and optimize quantum algorithms for various applications, including cryptography, optimization, and machine learning.
- Explore real-world applications of quantum computing in cybersecurity, finance, optimization, and scientific research to demonstrate the potential impact and capabilities of quantum technology.

LIST OF EXPERIMENTS:

1. Implementing and analyzing QKD protocols like BB84 or E91 for secure key distribution, ensuring quantum-safe communication channels.
2. Simulating quantum-resistant cryptographic algorithms such as lattice-based cryptography or hash-based cryptography to evaluate their security and performance.
3. Assessing the randomness and unpredictability of quantum-generated random numbers for cryptographic applications.
4. Implementing and benchmarking post-quantum cryptographic algorithms such as NTRUEncrypt or Lattice-based schemes for encryption and digital signatures.
5. Evaluating the resistance of hash functions against quantum attacks, including testing for collision resistance and pre-image resistance.
6. Designing and analyzing authentication protocols resilient to quantum attacks, ensuring secure authentication in a post-quantum era.
7. Developing and testing SMPC protocols resilient to quantum attacks, allowing secure computation on sensitive data without revealing inputs.
8. Analyzing the resilience of blockchain consensus mechanisms against quantum attacks, exploring quantum-safe alternatives to traditional proof-of-work or proof-of-stake.
9. Investigating the potential of quantum computing for enhancing anomaly detection and threat identification in network traffic analysis.
10. Evaluating the security and efficiency of quantum-resistant digital signature schemes such as hash-based signatures or multivariate cryptography.
11. Exploring quantum machine learning algorithms for improving malware detection, anomaly detection, and threat intelligence analysis.
12. Designing and testing quantum-resistant versions of the TLS protocol to secure communication over the internet in a post-quantum world.

13. Conducting cryptanalysis experiments to assess the security of classical cryptographic algorithms against quantum attacks, such as Shor's algorithm for integer factorization.
14. Investigating quantum-enhanced techniques for secure and efficient key generation, distribution, and management in cryptographic systems.
15. Developing privacy-preserving data sharing protocols resilient to quantum attacks, enabling secure collaboration and data exchange in quantum-threatened environments.

OUTCOMES:

Upon completion of the course, the student should be able to

1. Demonstrate proficiency in fundamental quantum computing concepts, quantum gates, quantum circuits, and quantum algorithms, as well as practical skills in using quantum computing tools and simulators.
2. Gain a deep understanding of quantum cryptographic principles, including quantum key distribution (QKD), quantum-resistant cryptography, and quantum-safe protocols for secure communication.
3. Acquire the ability to develop, analyze, and implement quantum algorithms for solving computational problems efficiently on quantum computers, leveraging principles of superposition, entanglement, and interference.
4. Evaluate the potential applications and limitations of quantum computing in various domains, including cryptography, optimization, machine learning, and scientific simulations.
5. Develop critical thinking and problem-solving skills necessary for tackling complex computational problems using quantum computing approaches, including algorithm design, optimization, and error mitigation.
6. Consider the ethical implications, societal impacts, and potential risks associated with the development and deployment of quantum technologies, including privacy concerns, security vulnerabilities, and algorithmic biases. (K2)

CO-PO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	2	3	2	2	1	-		-	1	-	1	-	2	-
CO2	2	3	2	2		-		-	2	-	1	-	2	-
CO3	3	2	3	2		-	-	-	2	-	1	-	2	-
CO4	3	2	3	2	3	-	-	-	2	-	1	-	2	-
CO5	3	2	2	2	3	-	-	1	2	3	1	-	2	-
CO6	2	2	2	2	2	-	-	-	-	-	-	-	1	-

SEMESTER - VII

20SCPL702 SDG NO. 9,11,16	CYBER FORENSICS LABORATORY	L	T	P	C
		0	0	3	1.5

OBJECTIVES:

- Provide participants with practical, hands-on experience in conducting cyber forensics investigations using current tools and techniques.
- Familiarize participants with established forensic methodologies, procedures, and best practices for collecting, preserving, analyzing, and presenting digital evidence.
- Develop technical proficiency in utilizing cyber forensics tools and software applications for data acquisition, analysis, and reporting in various forensic scenarios.
- Foster critical thinking and problem-solving skills necessary for identifying, analyzing, and interpreting digital evidence to reconstruct cybercrime incidents and support legal proceedings.
- Emphasize the importance of ethical conduct and adherence to legal requirements, standards, and regulations governing cyber forensics investigations, including privacy rights and chain of custody protocols.

LIST OF EXPERIMENTS:

1. Creating forensic disk images of storage devices and analyzing them for evidence of digital crimes using FTK Imager.
2. Extracting and analyzing volatile memory (RAM) dumps for forensic artifacts, such as processes, network connections, and malware, using the Volatility framework.

3. Recovering deleted or fragmented files from disk images or storage devices using file carving tools like Scalpel or Foremost.
4. Capturing and analyzing network traffic to identify malicious activities, data exfiltration, or unauthorized access using Wireshark.
5. Extracting and analyzing digital evidence from mobile devices, including call logs, messages, images, and application data using forensic tools like Cellebrite UFED or Oxygen Forensic Detective.
6. Collecting, analyzing, and preserving email evidence from email servers or email client applications using forensic tools like MailXaminer or Examine Forensic Email Collector.
7. Extracting browsing history, cookies, downloads, and other artifacts from web browsers like Google Chrome or Mozilla Firefox using specialized forensic tools.
8. Analyzing Windows registry hives for evidence of malicious activity, system configuration changes, or user actions using forensic tools like Registry Explorer or Registry Recon.
9. Creating forensic timelines of system events and user activities from various sources, including log files, registry entries, and file system metadata using forensic tools like Log2Timeline or Plaso.
10. Extracting and analyzing metadata embedded in digital files (e.g., images, documents) to gather information about their creation, modification, and source using tools like ExifTool or Metadata Extractor.
11. Extracting and analyzing data from SQLite databases found on computer systems or mobile devices using forensic tools like SQLite Forensic Explorer.
12. Analyzing malware samples in a controlled environment to understand their behavior, capabilities, and impact on systems using malware analysis platforms like REMnux or Cuckoo Sandbox.
13. Detecting hidden information or malware concealed within digital files using steganography detection tools like StegExpose or StegDetect.
14. Investigating transactions and activities on blockchain networks (e.g., Bitcoin, Ethereum) to trace cryptocurrency transactions and identify illicit or fraudulent activities using blockchain forensics tools like Chainalysis or Elliptic.
15. Collecting, analyzing, and preserving digital evidence stored in cloud services (e.g., Google Drive, Dropbox) using forensic tools like Magnet AXIOM or FTK (Forensic Toolkit).

OUTCOMES:

Upon completion of the course, the student should be able to

1. Demonstrate proficiency in applying cyber forensics techniques, including disk imaging, memory forensics, network packet analysis, mobile device forensics, and malware analysis, to investigate cyber incidents and digital crimes. (K1)
2. Develop a comprehensive understanding of forensic processes, including evidence identification, collection, preservation, examination, analysis, and documentation, following established forensic principles and methodologies. (K2)
3. Acquire skills in analyzing digital evidence to reconstruct cybercrime incidents, identify perpetrators, attribute malicious activities, and support legal proceedings through accurate and reliable data interpretation. (K2)
4. Develop effective report writing and presentation skills for documenting forensic findings, methodologies, analysis results, and conclusions in a clear, concise, and legally defensible manner suitable for judicial review. (K3)
5. Enhance incident response capabilities by leveraging cyber forensics techniques to rapidly detect, contain, eradicate, and recover from security incidents, minimizing the impact and preventing future occurrences. (K3)
6. Encourage continual learning and professional development in the field of cyber forensics by fostering a culture of research, innovation, and collaboration, staying updated with emerging trends, technologies, and threats in cybersecurity. (K2)

CO-PO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	2	3	2	2	1	-		-	1	-	1	-	2	-
CO2	2	2	3	2	-	-		-	2	-	1	-	2	-
CO3	3	2	3	2	-	-	-	-	2	-	1	-	2	-
CO4	3	2	3	2	3	-	-	-	2	-	1	-	2	-
CO5	-	-	-	-	-	-	-	1	2	3	1	-	2	-
CO6	2	2	2	2	2	-	-	-	-	-	-	-	1	-

PROFESSIONAL ELECTIVES - I

20SCEL501 SDG NO. 4	FOUNDATION OF DATA SCIENCE	L	T	P	C
		3	0	0	3

OBJECTIVES:

- Able to apply fundamental algorithmic ideas to process data.
- Learn to apply hypotheses and data into action able predictions.
- Document and transfer the results and effectively communicate the findings using visualization techniques.

Module 1: INTRODUCTION TO DATA SCIENCE 6

Data science process–roles, stages in data science project–working with data from files– working with relational databases.

Module 2: EXPLORING AND MANAGING DATA SCIENCE 7

Exploring data – managing data – cleaning and sampling for modeling and validation – introduction to NoSQL.

Module 3: MODELING METHOD 8

Choosing and evaluating models – mapping problems to machine learning, evaluating clustering models, validating models–cluster analysis–K-means algorithm, Naïve Bayes–Memorization Methods–Linear and logistic regression–unsupervised methods.

Module 4: INTRODUCTION TO R 8

Reading and getting data into R–ordered and unordered factors–arrays and matrices–lists and data frames–reading data from files–probability distributions–statistical models in R-manipulating objects–data distribution.

Module 5: MAP REDUCE 8

Introduction–distributed file system–algorithms using map reduce, Matrix-Vector Multiplication by Map Reduce – Hadoop - Understanding the Map Reduce architecture- Writing Hadoop Map Reduce Programs - Loading data into HDFS-Executing the Map phase-Shuffling and sorting-Reducing phase execution.

Module 6: DELIVERING RESULTS 8

Documentation and deployment–producing effective presentations – Introduction to graphical analysis – plot() function – displaying multivariate

data – matrix plots – multiple plots in one window - exporting graph – using graphics parameters. Cases Studies

TOTAL: 45 PERIODS

TEXT BOOKS:

1. Nina Zumel, John Mount, "Practical Data Science with R", Manning Publications,2014.
2. JureLeskovec, Anand Rajaraman, JeffreyD.Ullman, "Mining of Massive Datasets", Cambridge UniversityPress,2014.

REFERENCES:

1. Mark Gardener,"BeginningR-The Statistical Programming Language",JohnWiley&Sons,Inc.,2012.
2. W.N.Venables,D.M.Smith and theR Core Team," An Introductionto R",Network Theory Ltd, Second Edition,2013.
3. Tony Ojeda, Sean Patrick Murphy, Benjamin Bengfort,Abhijit Dasgupta," Practical Data Science Cook book", Packet Publishing Ltd.,2014.
4. NathanYau, "VisualizeThis:The Flowing Data Guide to Design,Visualization,and Statistics",Wiley,2011.
5. Borislublinsky, Kevint.Smith, Alexey Yakubovich," Professional Hadoop Solutions", Wiley ,ISBN:9788126551071, 2015.

WEB REFERENCES:

1. http://www.johndcook.com/R_language_for_programmers.html
2. http://bigdatauniversity.com/
3. http://home.ubalt.edu/ntsbarsh/stat-data/topics.htm#rintroduction

ONLINE RESOURCES:

1. https://freevideolectures.com/search/foundation-of-data-science/
2. https://www.simplilearn.com/big-data-and-analytics/senior-data-scientist-masters-program-training

OUTCOMES:

Upon completion of the course, the student should be able to

1. Develop to obtain, clean/process and transform data.(K1)
2. Analyze and interpret data using an ethically responsible approach.(K3)
3. Use appropriate models of analysis, assess the quality of input, derive insight from results ,and investigate potential issues.(K3)
4. Apply computing theory, languages and algorithms, as well as mathematical and statistical models, and the principles of optimization to appropriately formulate and used at a analyses.(K3)

5. Formulate and use appropriate models of data analysis to solve hidden solutions to business-related challenges.(K2)
6. Employ the techniques related to the area of data science in several statistical analysis methods.(K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	1	2	2	-	2	-	-	-	-	2	2	3	2
CO2	3	1	3	2	-	2	-	-	-	-	2	2	3	2
CO3	3	1	3	2	-	2	-	-	-	-	2	2	3	2
CO4	3	1	3	2	3	2	-	-	-	-	2	2	3	2
CO5	3	1	3	2	3	2	-	-	2	3	2	2	3	2
CO6	3	1	3	2	3	2	-	-	2	3	2	2	3	2

PROFESSIONAL ELECTIVES - I

20CSEL502 SDG NO. 4&9	NO SQL DATABASE	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To define, compare and use the four types of NoSQL Databases
- To demonstrate an understanding of the detailed architecture, define objects, load data, query data and performance tune Column-oriented NoSQL databases.
- To understand Data Analytics and Cloud in the context of NoSql
- To explain the detailed architecture, define objects, load data, query data and performance Document-oriented NoSQL databases.

Module 1: INTRODUCTION TO NoSQL DATABASES 7

Overview of NoSQL Databases -Comparison of relational databases to new NoSQL stores, MongoDB, Cassandra, HBASE, Neo4j use and deployment and Application.

Module 2: RDBMS APPROACH AND CHALLENGES TO NoSQL 6

RDBMS approach, Challenges NoSQL approach, Key-Value and Document DataModels, Aggregate-Oriented Databases.

Module 3: DATABASE FOR MODERN WEB 8

Replication and sharding, Map Reduce on databases. Distribution Models, Single Server, Sharding, Master-Slave Replication, Peer-to-Peer Replication, Combining Sharding and Replication Document Databases, Scaling, Suitable Use Cases, Web Analytics or Real-Time Analytics, E-Commerce Applications, Complex Transactions Spanning Different Operations, Queries against Varying Aggregate Structure

Module 4: COLUMN- ORIENTED NOSQL DATABASES 8

Column- oriented NoSQL databases using Apache HBASE, Column-oriented NoSQL databases using Apache Cassandra, Architecture of HBASE, Column-Family Data Store, Features, Consistency, Transactions, Availability, Query Features, Scaling, Suitable Use Cases, Event Logging, Content Management Systems, Blogging Platforms, Counters, Expiring Usage.

Module 5: KEY VALUE DATABASE DESIGNS 8

NoSQL Key/Value databases using Riak, Key-Value Databases, Key-Value Store, Key-Value Store Features, Consistency, Transactions, Query Features, Structure of Data, Scaling, Suitable Use Cases, Storing Session Information, User Profiles, Preferences, Shopping Cart Data, Relationships among Data, Multi operation Transactions, Query by Data, Operations by Sets.

Module 6: GRAPH DATABASE DESIGN 8

Graph NoSQL databases using Neo4, NoSQL database development tools and programming languages, Graph Databases, Features, Consistency, Transactions, Availability, Query Features, Scaling, Suitable Use Cases, Connected Data, Routing, Dispatch, and Location-Based Services, Recommendation Engines.

TOTAL:45PERIODS

TEXT BOOKS:

1. Pramod J. Sadalage & Martin Fowler," No SQL Distilled: A Brief Guide to the Emerging World of Polyglot Persistence", Addison- Wesley, Fist Edition,2013.
2. Andreas Meier &Michael Kaufmann, “SQL & NoSQL Databases: Models,Languages,ConsistencyOptionsandArchitecturesforBigDataManagement”,Springer2019.

REFERENCES:

1. Redmond, E. & Jim Wilson R." A Guide to Modern Databases and the No SQL Movement Edition,"Second Edition, 2018.

2. "MongoDB: The Definitive Guide (2nd ed.). Upper Saddle River", NJ:PearsonEducationIndia,Inc.ISBN-13:978-1449344689ISBN-10:1449344682.
3. Andreas Meier, Michael Kaufmann, "SQL & NoSQL Databases Models,languages,Consistencyoptionsandarchitecturesforbigdatamanagement",SpringerVieweg,2019.
4. ShashankTiwari,"ProfessionalNoSQL",Wrox,2011.
5. DanSullivan,"NoSQLforMereMortals",AddisonWesley,2015.

WEB REFERENCES:

1. https://www.mongodb.com/nosql-explained
2. https://en.wikipedia.org/wiki/NoSQL
3. https://docs.microsoft.com/en-us/dotnet/architecture/microservices/microservice-dddcqrs-patterns/nosql-database-persistence-infrastructure

ONLINE RESOURCES:

1. https://www.w3resource.com/mongodb/nosql.php
2. https://www.couchbase.com/resources/why-nosql

OUTCOMES:

Upon completion of the course, the student should be able to

1. Evaluate NoSQL database development tools and programming languages.(K1)
2. Demonstrateanunderstandingofthedetailedarchitecture,defineobjects, load data, query data and performance tune Column-oriented NoSQL databases.(K1)
3. Define, compare and use the four types of NoSQL Databases (Document-oriented, Key Value Pairs, Column-oriented and Graph).(K3)
4. Perform hands-on NoSql database lab assignments by using the four NoSQL database types via products such as Cassandra, Hadoop Hbase,MongoDB,andNeo4J.(K3)
5. Perform CRUD operations (create, read, update and delete) on data in NoSQL environment.(K5)
6. Explore the emergence, requirements and benefits of a NoSQL database.(K4)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	3	2	2	-	-	-	-	-	-	-	3	2
CO2	3	3	2	2	3	-	-	-	-	1	-	-	3	3
CO3	3	3	3	2	3	1	-	-	2	2	-	-	2	2
CO4	3	3	3	3	3	2	-	-	-	3	-	-	3	2
CO5	3	3	3	2	3	-	-	-	-	1	-	-	2	2
CO6	3	3	2	2	2	2	-	-	2	3	-	-	3	2

PROFESSIONAL ELECTIVES - I

20CSEL503 SDG NO. 4,9,11,12	INTERNET OF THINGS	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To understand Smart Objects, IoT Architectures and IoT protocols
- To build simple IoT Systems using Arduino and RaspberryPi
- To understand Data Analytics and Cloud in the context of IoT
- To develop IoT infrastructure for popular applications

Module 1: FUNDAMENTALS OF INTERNET OF THINGS 8

Evolution of Internet of Things - Enabling Technologies – IoT Architectures: one M2M-IoT World Forum (IoTWF) and Alternative IoT models–Simplified IoT Architecture and Core IoT Functional Stack-Fog, Edge and Cloud in IoT–Functional Blocks of an IoT Ecosystem – Sensors - Actuators - Smart Objects and Connecting Smart Objects.

Module 2: IOT PROTOCOLS 8

IoT Access Technologies- Physical and MACLayers –Topology and Security of IEEE802.15.4, 802.15.4g, 802.15.4e, 1901.2a ,802.11ah and LoRa WAN–Network Layer-IP Versions-Constrained Nodes and Constrained Networks–Optimizing IP for IoT- From 6 LoWPAN to 6 Lo-Routing Over Low Power and Lossy Networks–Application Transport Methods- Supervisory Control and Data Acquisition–Application Layer Protocols-CoAP and MQTT.

Module 3: DESIGN AND DEVELOPMENT 8

Design Methodology-Embedded Computing Logic- Microcontroller- System on Chips-IoT System Building Blocks – Arduino-Board Details-IDE

Programming-RaspberryPi-Interfaces and Raspberry Pi with Python Programming.

Module 4: DATA ANALYTICS AND SUPPORTING SERVICES 8

Structured Vs Unstructured Data and Data in Motion Vs Data in Rest–Role of Machine Learning – No SQL Databases – Hadoop Ecosystem – Apache Kafka, Apache Spark – Edge Streaming Analytics and Network Analytics – Xively Cloud for IoT, Python Web Application Framework – Django – AWS for IoT –System Management with NETCONF-YANG

Module 5: CASE STUDIES 7

Cisco IoT System - IBM Watson IoT Platform – Manufacturing – Converged Plant wide Ethernet Model (CPwE)

Module 6: INDUSTRIAL APPLICATIONS 6

Power Utility Industry – Grid Blocks Reference Model-Smart and Connected Cities-Layered Architecture-Smart Lighting-Smart Parking Architecture and Smart Traffic Control

TOTAL: 45 PERIODS

TEXT BOOKS:

1. DavidHanes, GonzaloSalgueiro,P atrick Grossetete, RobBarton and JeromeHenry, "IoTFundamentals:NetworkingTechnologies,Protocols and Use Cases for Internet of Things",CiscoPress,2017.
2. Rajkamal," Internet of Things: Architecture, Design Principles And Applications",McGraw Hill Higher Education,2017.

REFERENCES:

1. Arshdeep Bahga, Vijay Madisetti, "Internet of Things–AHands-on approach", Universities Press, 2011.
2. Olivier Hersent, David Boswarthick, Omar Elloumi, "The Internet of Things – Key Applications and Protocols", Wiley,2012.
3. JanHoller, Vlasios Tsiatsis, Catherine Mulligan, Stamatis, Karnouskos, Stefan Aves and David Boyle,"From Machine-to-Machine to the Internet of Things and Introduction to a New Age of Intelligence", Elsevier, 2014.
4. Dieter Uckelmann, Mark Harrison, Michahelles, Florian (Eds), "Architecting the Internet of T hings", Springer, 2011.
5. Michael Margolis, Arduino Cookbook,"Recipes to Begin, Expand and Enhance Your Projects, 2nd Edition, O'Reilly Media, 2011.

WEB REFERENCES:

1. https://www.arenasolutions.com/blog/10-valuable-iot-web-resources/
2. https://nevonprojects.com/iot-projects/
3. https://www.skyfilabs.com/blog/list-of-latest-iot-projects-for-engineering-students

ONLINE RESOURCES:

1. https://www.arenasolutions.com/blog/10-valuable-iot-web-resources/
2. https://nevonprojects.com/iot-projects/

OUTCOMES:

Upon completion of the course, the student should be able to

1. Interpret the concept of IoT, its Components and its architecture.(K2)
2. Learn the design methods of various protocols.(K2)
3. Build the design methodology for a IoT system using Raspberry.(K3)
4. Apply the Data analytics and Support sevicting tool related to IoT.(K3)
5. Experiment the case study and application of IoT in real time scenario.(K3)
6. Illustrate the solutions for various distributed applications using the Bigdata technologies.(K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	2	3	1	2	1	0	0	0	0	0	2	3	2	2
CO2	2	3	1	2	1	0	0	0	0	0	2	3	2	2
CO3	3	2	3	0	3	0	0	0	0	0	2	1	3	3
CO4	2	3	2	3	2	0	0	0	0	0	1	1	3	3
CO5	2	3	3	3	2	2	2	2	1	2	1	2	3	3
CO6	2	3	3	3	3	2	3	2	1	2	1	2	3	3

PROFESSIONAL ELECTIVES - I

20CSEL504 SDG NO. 4	IOT ARCHITECTURE, NETWORK AND SECURITY	L	T	P	C
		3	0	0	3

OBJECTIVES:

- Understand the fundamentals of the Internet of Things.
- Learn about the basics of IOT protocols.
- Build a small low-cost embedded system using RaspberryPi.
- Apply the concept of Internet of Things in the world.

Module 1: INTRODUCTION TO IoT **8**

Internet of Things- Physical Design- Logical Design - IoT Enabling Technologies - IoT Levels & Deployment Templates - Domain Specific IoTs- IoT and M2M - IoT System Management with NETCONF – YANG- IoT Platforms Design Methodology.

Module 2: IoT ARCHITECTURE **8**

M2MHigh – level ETSI Architecture – IETF Architecture for IoT – OGC Architecture - IoT Reference Model - Domain Model - Information Model - Functional Model- Communication Model- IoT Reference Architecture.

Module 3: IoT PROTOCOLS **8**

Protocol Standardization for IoT– Efforts– M2M and WSN Protocols – SCADA and RFID Protocols – Unified Data Standards – Protocols – IEEE 802.15.4 –BACNet Protocol–Modbus–Zigbee Architecture– Network layer– 6 LoWPAN-CoAP– Security.

Module 4: BUILDING IoT WITH RASPBERRY PI & ARDUINO **8**

Building IOT with RASPBERRY PI- IoT Systems- Logical Design using Python - IoT Physical Devices & End points- IoT Device- Building blocks - Raspberry Pi - Board - Linux on Raspberry Pi- Raspberry Pi Interfaces - Programming Raspberry Pi with Python- Other IoT Platforms - Arduino.

Module 5: IOT REAL - WORLD APPLICATIONS **7**

Real World Design Constraints- Applications- Asset Management, Industrial Automation, Smart Grid, Commercial Building Automation, Smart Cities - Participatory Sensing- Data Analytics for IoT

Module 6: IOT TOOLS **6**

Software & Management Tools for IoT Cloud Storage Models & Communication APIs- Cloud for IoT - Amazon Web Services for IoT.

TOTAL:45PERIODS

TEXT BOOKS:

1. David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Rob Barton and Jerome Henry, "IoT Fundamentals: Networking Technologies, Protocols and Use Cases for Internet of Things", Cisco Press, 2017.
2. Arshdeep Bahga, Vijay Madisetti, "Internet of Things – A hands-on approach" ,Word Press,2015

REFERENCES:

1. Olivier Hersent, David Boswarthick, Omar Elloumi , "The Internet of Things – Key applications and Protocols", Wiley, 2012 (for Unit2).
2. Jan Holler, Vlasios Tsiatsis, Catherine Mulligan, Stamatis, Karnouskos, Stefan Aves and David Boyle,"FromMachine-to-Machine to the Internet of Things-Introduction to a New Age of Intelligence'', Elsevier ,2014.
3. Honbo Zhou, "The Internet of Things in the Cloud: A Middleware Perspective ", CRC Press, 2012.
4. Dieter Uckelmann, Mark Harrison, Michahelles, Florian(Eds), "Architecting the Internet of Things", Springer, 2011.
5. Michael Margolis, Arduino Cookbook, "Recipes to Begin, Expand, and Enhance Your Projects", 2nd Edition, O'Reilly Media, 2011.

ONLINERESOURCES:

1. https://www.arduino.cc/
2. https://www.ibm.com/smarterplanet/us/en/?ca=v_smarterplanet
3. https://www.cisco.com/c/en/us/solutions/internet-of-things/resources/case-studies.html

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the fundamentals of the Internet of Things (K2)
2. Discuss various networking protocols for IoT (K2)
3. Interpret web services to access/control IoT devices (K2)
4. Construct a small low cost embedded system using Raspberry Pi (K3)
5. Extend an IoT application and connect to the cloud (K2)
6. Demonstrate applications of IoT in real time scenarios (K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	2	2	2	1	-	-	-	-	-	-	-	-	-	1
CO2	2	2	2	1	-	-	-	-	-	-	-	-	-	1
CO3	3	2	2	1	1	-	-	-	-	-	-	-	-	1
CO4	3	3	3	1	2	1	-	-	-	-	-	-	1	2
CO5	3	3	3	1	2	1	-	-		-	-	-	1	2
CO6	3	3	3	2	2	1	1	1	1	1	1	1	1	2

PROFESSIONAL ELECTIVES - I

20CSEL505 SDG NO. 4 & 9	SOFTWARE TESTING	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To learn the criteria and design of Test Cases
- To learn the design of Test Cases
- To understand Test Management and Test Automation Techniques
- To apply Test Metrics and Measurements

Module 1: INTRODUCTION 8

Testing as an Engineering Activity – Testing as a Process – Testing Maturity Model- Basic Definitions – Software Testing Principles – The Tester's Role in a Software Development Organization – Origins of Defects – Cost of Defects –Defect Classes – The Defect Repository and Test Design – Defect Examples- Developer / Tester Support of Developing a Defect Repository.

Module 2: TEST CASE DESIGN STRATEGIES 8

Test Case Design Strategies – Using Black Box Approach to Test Case Design – Boundary Value Analysis– Equivalence Class Partitioning – State Based Testing – Cause - Effect Graphing – Compatibility Testing – User Documentation Testing – Domain Testing - Random Testing – Requirements Based Testing – Using White Box Approach to Test design – Test Adequacy Criteria – Static Testing Vs. Structural Testing – Code Functional Testing – Coverage and Control Flow Graphs – Covering Code Logic – Paths – Code Complexity Testing – Additional White Box Testing Approaches.

Module 3: LEVELS OF TESTING 8

The Need for Levels of Testing – Unit Test – Unit Test Planning – Designing the Unit Tests – The Test Harness – Running the Unit Tests and Recording Results – Integration Tests – Designing Integration Tests – Integration Test Planning – Scenario Testing – Defect Bash Elimination System Testing – Acceptance Testing – Performance Testing – Regression Testing – Internationalization Testing – AdHoc Testing – Alpha, Beta Tests – Testing Object Oriented Systems – Usability and Accessibility Testing – Configuration Testing – Compatibility Testing – Testing the Documentation – Website Testing.

Module 4: TEST MANAGEMENT 7

People and Organizational Issues in Testing – Organization Structures for Testing Teams – Testing Services – Test Planning – Test Plan Components –Test Plan Attachments – Locating Test Items – Test Management

Module 5: TEST PROCESS 6

TestProcess – Reporting Test Results – Introducing the Test Specialist – Skills Needed by a Test Specialist – Building a Testing Group- The Structure of Testing Group- The- Technical Training Program.

Module 6: TEST AUTOMATION 8

Software Test Automation – Skills needed for Automation– Scope of Automation – Design and Architecture for Automation – Requirements for a Test Tool – Challenges in Automation – Test Metrics and Measurements –Project, Progress and Productivity Metrics.

TOTAL:45PERIODS

TEXT BOOKS:

1. Srinivasan Desikan and Gopalaswamy Ramesh, "Software Testing–Principles and Practices", Pearson Education, 2006.
2. Ron Patton, "Software Testing Second Edition", Sams Publishing, Pearson Education, 2007.

REFERENCES:

1. Ilene Burnstein, "Practical Software Testing", Springer International Edition, 2003.
2. Edward Kit, "Software Testing in the Real World–Improving the Process", Pearson Education, 1995.
3. Boris Beizer, "Software Testing Techniques" 2nd Edition, Van Nostrand Reinhold, NewYork, 1990.

4. AdityaP. Mathur"Foundations of Software Testing-Fundamental Algorithms and Techniques", Dorling Kindersley (India)Pvt.Ltd., Pearson Education,2008.
5. Naresh chauhan - software testing principles and practices, 2nd edition, oxford University Press, 2017.

WEB REFERENCE:

1. https://nptel.ac.in/courses/106/105/106105150/

ONLINERESOURCES:

1. https://www.javatpoint.com/software-testing-tutorial
2. https://www.toolsqa.com/software-testing-tutorial/

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand about the Software Testing Principles and Defect Classes (K2)
2. Apply test cases suitable for software development for different domains (K3)
3. Discuss the various Levels of Tsting (K2)
4. Identify suitable tests to be carried out (K2)
5. Discuss the concepts of Test plan and its skillset (K2)
6. Apply automatic testing tools and discuss the various test metrics and measurements (K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	2	1	-	-	-	-	-	-	-	-	2	-	2	3
CO2	2	3	3	-	-	-	-	-	2	-	1	-	3	3
CO3	2	3	3	-	-	-	-	-	3	-	1	2	3	3
CO4	2	3	3	-	-	-	-	-	3	-	3	3	3	3
CO5	-	2	1	-	-	-	-	-	2	-	2	-	3	3
CO6	3	2	2	-	-	-	-	-	1	2	2	2	3	3

PROFESSIONAL ELECTIVES - I

20CSEL506 SDG NO. 4,9,16	INFORMATION RETRIEVAL TECHNIQUES	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To provide an understanding of core principles and architectures of IR systems.
- To equip students with skills for developing efficient and scalable indexing and searching techniques.
- To familiarize students with advanced IR concepts, including ML and deep learning.
- To explore practical applications and ethical considerations in IR.
- To encourage research and innovation in the field of IR.

Module 1: Introduction to Information Retrieval 8

Basics of Information Retrieval- Components and Architecture of IR Systems-Types of IR Systems (Web, Enterprise, Digital Library, etc.)-Boolean, Vector Space, and Probabilistic Models-Evaluation Metrics: Precision, Recall, F-Measure, MAP

Module 2: Query Processing and Transformation 7

Query Languages and Syntax-Query Expansion Techniques-Relevance Feedback and Rocchio Algorithm-Stemming and Lemmatization Techniques-Thesaurus Construction and Ontology Integration

Module 3: Indexing Techniques 8

Inverted Index Construction and Maintenance-Compression Techniques for Indexing-Dynamic Indexing-Hashing and Signature Files-Distributed and Parallel Indexing

Module 4: Web and Multimedia Information Retrieval 7

Crawling and Web Search Engines-Link Analysis: PageRank, HITS Algorithm-Multimedia Content Search: Image, Video, and Audio Retrieval-Semantic Web and Metadata Standards-Recommender Systems

Module 5: Advanced Topics in IR 8

Machine Learning for IR: RankNet, Lambda MART-Natural Language Processing in IR-Cross-Language Information Retrieval-Deep Learning in IR: BERT, Transformers for Search-Personalized and Context-Aware Retrieval.

Module 6: Applications and Trends in IR **7**

IR Applications in E-Commerce and Healthcare-Research Trends in IR-Ethical Issues in Information Retrieval-Case Studies and Real-World IR Systems-Future of IR: AI Integration

TOTAL:45PERIODS

TEXT BOOKS:

1. Introduction to Information Retrieval" by Christopher D. Manning, Prabhakar Raghavan, and Hinrich Schütze, Cambridge University Press, 2008.
2. "Search Engines: Information Retrieval in Practice" by W. Bruce Croft, Donald Metzler, and Trevor Strohman, Pearson Education, 2

REFERENCES:

1. "Modern Information Retrieval: The Concepts and Technology behind Search" by Ricardo Baeza-Yates and Berthier Ribeiro-Neto, Addison-Wesley, 2011.
2. "Foundations of Multidimensional and Metric Data Structures" by Hanan Samet, Morgan Kaufmann, 2006.

NPTEL LINK

1. Information Retrieval - IIT KharagpurNPTEL Link
2. Text Information Retrieval - IIT Bombay

OUTCOMES:

Upon completion of the course, the student should be able to

1. Develop and evaluate information retrieval models and metrics.
2. Apply techniques for query processing and relevance feedback.
3. Design and implement efficient indexing systems.
4. Leverage modern tools like machine learning and NLP in IR systems.
5. Address challenges in web and multimedia information retrieval.
6. Innovate and analyse ethical implications in real-world IR applications.

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	3	3	1	1	1	-	1	-	1	-	2	2
CO2	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO3	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO4	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO5	3	3	3	3	3	1	1	1	2	3	1	-	2	2
CO6	3	3	2	3	3	2	-	-	-	-	-	-	1	1

PROFESSIONAL ELECTIVES - I

20CSEL507 SDG NO. 4&15	BIOINFORMATICS	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To analyze the need for Bio informatics Technologies
- To be familiar with the modeling techniques
- To learn micro array analysis
- To implement Pattern Matching and Visualization

MODULE 1: INTRODUCTION **8**

Need for Bioinformatics Technologies–OverviewofBioinformatics Technologies - Structural Bioinformatics – Data Format and Processing –Secondary Resources and Applications – Role of Structural Bioinformatics - Biological Data Integration System.

MODULE II: DATA WAREHOUSING AND DATA MINING IN BIOINFORMATICS **8**

Bioinformatics Data – Data Warehousing Architecture – DataQuality – Biomedical Data Analysis – DNA Data Analysis – Protein Data Analysis –Machine Learning – Neural Network Architecture - Applications in Bio informatics.

MODULE III: MODELING FOR BIO INFORMATICS **8**

Hidden Markov Modeling for Biological Data Analysis – Sequence Identification –Sequence Classification – Multiple Alignment Generation

–Comparative Modeling – Protein Modeling – Genomic Modeling – Probabilistic Modeling – Bayesian Networks – Boolean Networks - Molecular Modeling – Computer Programs for Molecular Modeling.

MODULE IV: PATTERN MATCHING 6

Gene Regulation – Motif Recognition – Motif Detection – Strategies for MotifDetection

MODULE V: VISUALIZATION 7

Visualization – Fractal Analysis – DNA Walk Models – One Dimension – Two Dimension – Higher Dimension – Game Representation of Biological Sequences – DNA – Protein - Amino Acid Sequences.

MODULE VI: MICRO ARRAY ANALYSIS 8

Microarray Technology for Genome Expression Study – Image Analysis for Data Extraction – Preprocessing – Segmentation –Gridding– Spot Extraction – Normalization – Filtering – Cluster Analysis – Gene Network Analysis – Scientific Data Management Systems – Cost Matrix– Evaluation Model – Benchmark – Tradeoffs.

TOTAL:45PERIODS

TEXT BOOKS:

1. Yi-Ping Phoebe Chen (Ed), "BioInformatics Technologies", First IndianReprint,SpringerVerlag,2007.
2. JinXiong,"EssentialBioinformatics",CambridgeUniversityPress,2012.

REFERENCES:

1. Bryan Bergeron, "Bio Informatics Computing", Second Edition, Pearson Education India,2003.
2. Arthur M Lesk, "Introduction to Bioinformatics", Second Edition, OxfordUniversityPress,2005.
3. David W. Mount, "Bioinformatics: Sequence and Genome Analysis", Second Edition, Cold Spring Harbor Laboratory Press, U.S., 2004.
4. Andreas D. Baxevanis, B.F.Francis Ouellette, "Bioinformatics: A Practical Guide to the Analysis of Genes and Proteins", Second Edition, Wiley Interscience, 2001.
5. Mitchell L Model, "Bio informatics Programming Using Python", O'ReillyMedia,2009.

ONLINE RESOURCES:

1. https://www.classcentral.com/subjects/bioinformatics
2. https://mooc-list.com/tags/bioinformatis?_cf_chi_jschi_tk
3. https://www.udemy.com/topic/bioinformatics/?utm_source=adwords?

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the basic concepts of Bio informatics and its significance in bio logical data analysis. (K2)
2. Describe the history, scope and importance of Bio informatics and role of the internet in bio informatics. (K1)
3. Elaborate the methods to characterize and manage the different types of biological data. (K2)
4. Discuss the classification of biological databases. (K1)
5. Explore the basics of sequence alignment and analysis. (K3)
6. Describe- how bio informatics methods can be used to relate sequence, structure and functions. (K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	2	2	2	1	1	2	1	-	1	-	-	2	2	2
CO2	2	3	3	2	2	2	2	1	1	-	1	2	2	2
CO3	3	3	3	3	3	2	2	1	3	1	2	3	2	2
CO4	3	3	3	3	3	2	2	1	3	1	2	3	2	2
CO5	2	3	1	2	3	2	2	1	3	1	2	3	2	2
CO6	3	1	1	2	-	-	-	-	1	2	-	1	2	1

PROFESSIONAL ELECTIVES - I

20CSEL508 SDG NO. 4	SOFTWARE QUALITY ASSURANCE	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To impart knowledge of fundamental concepts in software quality assurance and testing.
- To familiarize students with international standards and best practices in SQA.
- To equip students with the skills to apply quality models and tools effectively.
- To enhance the ability to analyze and improve software processes.
- To explore advanced techniques and tools in ensuring quality in innovative domains.

Module 1: Introduction to Software Quality Assurance 8

Definition and Importance of SQA-SQA Framework and Standards (ISO, CMMI, IEEE)-Quality Attributes: Reliability, Usability, Maintainability, and Security-Cost of Quality and ROI in Software Quality-Roles and Responsibilities in Quality Assurance

Module 2: Software Development Life Cycle (SDLC) and Quality 7

SQA in Various SDLC Phases (Requirements, Design, Coding, Testing, Maintenance)-Verification and Validation (V&V) Practices-Quality Factors in Agile and DevOps Practices-Risk Management in Software Quality

Module 3: Software Testing 10

Fundamentals of Software Testing-Types of Testing: Unit Testing, Integration Testing, System Testing, Regression Testing-Test Automation: Tools and Techniques-Test Metrics and Test Reporting- Emerging Trends: AI in Testing

Module 4: Process Improvement and Quality Models 7

Process Improvement Models: Six Sigma, Lean, and TQM-Software Quality Models: McCall's, Boehm's, and ISO 25010-Benchmarking and Best Practices-Continuous Improvement Strategies

Module 5: Tools for Quality Assurance 7

Static and Dynamic Analysis Tools-Defect Tracking Tools (JIRA, Bugzilla)-Configuration Management Tools (Git, SVN)-Case Studies on Tool Implementation

Module 6: Advanced Topics in Software Quality 6

Quality in Emerging Areas: Cloud, IoT, AI, Blockchain-Legal and Ethical Aspects of Quality in Software-SQA Auditing and Certification Processes-SQA in Startups and SMEs

TOTAL:45PERIODS

TEXT BOOKS:

1. "Software Quality Assurance: From Theory to Implementation" by Daniel Galin (2018, Pearson Education).
2. "Foundations of Software Testing" by Dorothy Graham, Rex Black, and Erik Van Veenendaal (2019, Cengage Learning).

REFERENCE BOOKS:

1. "Effective Software Testing" by Elfriede Dustin (2020, Addison-Wesley).
2. "Metrics and Models in Software Quality Engineering" by Stephen H. Kan (2017, Pearson Education).

NPTEL RESOURCES

1. NPTEL Course: Software Testing by Prof. Rajib Mall, IIT Kharagpur.
2. NPTEL Course: Agile Software Development by Prof. Sangeeta Sabharwal, IIT Roorkee.

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the principles and processes of SQA. (K2)
2. Identify quality requirements in various SDLC phases. (K1)
3. Apply testing techniques and automation tools. (K3)
4. Analyze software processes and recommend improvements. (K4)
5. Implement quality frameworks and industry best practices. . (K3)
6. Evaluate software quality in emerging technologies. (K4)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	3	3	1	1	1	-	1	-	1	-	2	2
CO2	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO3	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO4	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO5	3	3	3	3	3	1	1	1	2	3	1	-	2	2
CO6	3	3	2	3	3	2	-	-	-	-	-	-	1	1

PROFESSIONAL ELECTIVES - I

20CSEL509 SDG NO. 4,9	FUNDAMENTALS OF EDGE AND SOFT COMPUTING	L	T	P	C
		3	0	0	3

OBJECTIVES:

- Understand Soft Computing concepts, technologies, and applications
- Understand the underlying principle of soft computing with its usage in various application
- Develop the skills to gain a basic understanding of neural network theory and fuzzy logic theory
- Understand different soft computing tools to solve real life problems.
- Develop application on different soft computing techniques like Fuzzy, GA and Neural network

Module 1: INTRODUCTION TO SOFT COMPUTING 8

ARTIFICIAL NEURAL NETWORKS Basic concepts - Single layer perceptron - Multilayer Perceptron - Supervised and Unsupervised learning – Back propagation networks - Kohnen's self-organizing networks - Hopfield network.

Module 2: FUZZY SYSTEMS 8

Fuzzy sets, Fuzzy Relations and Fuzzy reasoning, Fuzzy functions - Decomposition - Fuzzy automata and languages - Fuzzy control methods - Fuzzy decision making.

Module 3: NEURO FUZZY MODELING 8

Adaptive networks based Fuzzy inference systems - Classification and Regression Trees - Data clustering algorithms - Rule based structure identification - Neuro-Fuzzy controls - Simulated annealing – Evolutionary computation

Module 4: GENETIC ALGORITHMS 7

Survival of the Fittest - Fitness Computations - Cross over - Mutation - Reproduction -Rankmethod – Rankspacemethod

Module 5: ADVANCED APPLICATIONS 8

Optimization of traveling salesman problem using Genetic Algorithm, Genetic algorithm-based Internet Search Techniques, Soft computing-based hybrid fuzzy controller,

Module 6: MATLAB APPLICATIONS **6**

Introduction to MATLAB

TOTAL:45PERIODS

TEXT BOOKS:

1. J.S.R.Jang, C.T.Sun and E.Mizutani, "Neuro-Fuzzy and Soft Computing", Pearson Education2004.
2. Melanie Mitchell, "An Introduction to Genetic Algorithm", MIT Press, 1999.

REFERENCES:

1. Laurene Fausett, "Fundamentals of Neural Networks", Prentice Hall, 2004.
2. D.E.Goldberg, "Genetic Algorithms: Search, Optimization and Machine Learning", Addison Wesley, 2000.

WEB REFERENCES:

1. https://nptel.ac.in/courses/106/105/106105173/
2. https://www.coursera.org/lecture/machine-learning-sas/introduction-to-neural-networks-tqN4q
3. http://www.myreaders.info/html/soft_computing.html

OUTCOMES:

Upon completion of the course, the student should be able to

1. Comprehend the fuzzy logic and the concept of fuzziness involved in various systems and fuzzy set theory. (K2)
2. Realize the concepts of fuzzy sets, knowledge representation using fuzzy rules, approximate reasoning, fuzzy inference systems, and fuzzy logic. (K2)
3. Apply basics of Fuzzy logic and neural network. (K3)
4. Describe genetic algorithms and other random search procedures useful while seeking global optimum in self learning situations. (K2)
5. Appreciate appropriate learning rules for each of the architectures and learn several neural network paradigms and its applications. (K2)
6. Apply modern software tools to solve real problems using a soft computing approach (K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	1	0	0	0	0	0	0	0	0	0	1	2
CO2	3	3	3	1	2	0	0	0	0	0	0	0	1	2
CO3	3	3	3	3	3	0	0	0	0	0	0	0	2	2
CO4	3	3	3	2	3	0	0	0	0	0	0	1	3	3
CO5	3	3	3	3	3	0	0	0	0	0	2	1	3	3
CO6	3	3	3	3	3	2	1	2	2	0	2	2	3	3

PROFESSIONAL ELECTIVES - I

20CSEL519 SDG NO. 4	INFORMATION STORAGE AND MANAGEMENT	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To understand the basic components of Storage System Environment
- To learn about the Storage Area Network Characteristics and Components
- To illustrate merging technologies in Storage Area Network
- To learn about the different backup and recovery Topologies and their role in providing disaster recovery

Module 1: STORAGE SYSTEMS 8

Introduction to Information Storage and Management: Information Storage, Evolution of Storage Technology and Architecture – Data Center Infrastructure-Key Challenges in Managing Information - Information Lifecycle – Storage System Environment - Components of the Host - RAID - Implementation of RAID - RAID Array Components - RAID Levels - RAID Comparison – RAID Impaction Disk Performance – Hot Spares - Intelligent Storage System – Components – Intelligent Storage Array.

Module 2: STORAGE NETWORKING TECHNOLOGIES 8

Direct – Attached to rage and Introduction to SCSI – Types of DAS – DAS Benefits and Limitations - Disk Drive Interfaces - Introduction to Parallel SCSI – SCSI Command Model - Storage Area Networks - Fiber Channel - SAN Evolution -SAN Components - Fiber Channel Connectivity - Fiber Channel Ports – Fiber Channel Architecture - Zoning - Fiber Channel Login Types - Fiber Channel Topologies – Network Attached Storage – Benefits of NAS – File I/O Components of NAS – NAS Implementations – NAS File Sharing Protocols – NAS I/O Operations.

Module 3: ADVANCED STORAGE NETWORKING 8

IP SAN - iSCSI - FCIP - Content - Addressed Storage - Fixed Content and Archives – Types ofArchives – Features and BenefitsofCAS – CAS Architecture – Object Storage and Retrieve alin CAS- CAS Examples-

Module 4: VIRTUALIZATION 6

Storage Virtualization – Forms of Virtualization – NIA Storage Virtualization Taxonomy – Storage Virtualization Configurations - Storage Virtualization Challenges - Types of Storage Virtualization.

Module 5: BUSINESS CONTINUITY 8

Introduction to Business Continuity-Information Availability-BC Terminology - BC Planning Lifecycle - Failure Analysis - Business Impact Analysis-BC Technology Solutions – Backup and Recovery-Backup Purpose – Considerations – Granularity-Recovery Considerations-Backup Methods and Process-Backup and Restore Operations-Backup Topologies - Backup in NAS Environments-Backup Technologies.

Module 6: REPLICATION 7

Local Replication-Source and Target-Uses of Local Replicas-Data Consistency-Local Replication Technologies-Restore and Restart Considerations-Creating Multiple Replicas-Management Interface-Remote Replication - Modes of Remote Replication and its Technologies – Network Infrastructure.

TOTAL: 45 PERIODS

TEXT BOOKS:

1. EMC Corporation, “Information Storage and Management”, Wiley Publication, India, 2009.
2. Robert Spalding, "Storage Networks: The Complete Reference", Tata McGrawHill, Osborne, 2003

REFERENCES:

1. Marc Farley, “Building Storage Networks”, Tata McGrawHill, Osborne, 2001.
2. Meeta Gupta, “Storage Area Networks Fundamentals”, Pearson Education Limited, 2002.

WEB REFERENCES:

1. https://www.coursera.org/courses?query=data%20storage
2. https://www.springpeople.com/information-storage-management-training
3. https://nptel.ac.in/courses/106105175/

ONLINE RESOURCES:

1. https://www.sciencedirect.com/topics/computer-science/storage-management
2. https://www.communitydoor.org.au/technology/information-storage-and-management-systems

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the logical and the physical components of a Storage infrastructure with virtualization techniques. (K2)
2. Classify the different types of RAID implementations and Intelligent Storage System. (K2)
3. Discuss the architecture of storage networking technologies such as DAS, SAN,IPSAN, NAS. (K1)
4. Apply the various storage architectures and compare the key elements in classic and virtualized environments. (K3)
5. Illustrate the business continuity solutions with different backup and recovery techniques. (K3)
6. Demonstrate the Information Storage System Environment- by applying various archives for managing fixed content and different replication technologies. (K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	0	0	0	0	0	0	0	0	0	0
CO2	3	3	0	1	0	0	0	0	0	0	0	2
CO3	3	3	0	1	0	0	0	0	0	0	0	2
CO4	1	2	0	2	0	0	0	0	0	0	0	0
CO5	2	1	0	3	0	0	0	0	0	0	0	2
CO6	2	0	0	0	0	0	0	0	0	0	0	3

PROFESSIONAL ELECTIVES - II

20SCEL601 SDG NO. 4	INTRUSION DETECTION SYSTEMS	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To provide an in–depth introduction to the science and art of intrusion detection.
- To study the methodology, Techniques, and tools for monitoring events in computer network.
- To provide the study of preventing and detecting unwanted process activity and recovering from malicious behaviour.
- To compare alternative tools and approaches for Intrusion Detection through quantitative analysis.
- To Identify and describe the parts of all intrusion detection systems and characterize new and emerging IDS technologies

MODULEI: INTRODUCTION 9

Network Attacks, Attack Taxonomies, Probes, IP Sweep and Port Sweep, N Map, M Scan, SAINT, Satan, Privilege Escalation Attacks, Denial of Service(DoS) and Distributed Denial of Service (DDoS) Attacks, Worms Attacks, Routing Attacks

MODULE II: DETECTION APPROACHES 9

Detection Approaches, Misuse Detection, Pattern Matching, Rule–based Techniques, State–based Techniques, Techniques based on Data Mining, Anomaly Detection, Advanced Statistical Models, Rule based Techniques, Biological Models, Learning Models, Specification – based Detection, Hybrid Detection

MODULE III: DATA COLLECTION AND THEORETICAL FOUNDATION 9

Data Collection, Data Collection for Host–Based IDSs, Audit Logs, System Call Sequences and Data Collection for Network–Based IDSs, Theoretical Foundation of Detection, Taxonomy of Anomaly Detection Systems, Fuzzy Logic, Architecture and Implementation, Centralized, Distributed, Intelligent Agents, Mobile Agents and Cooperative Intrusion Detection

MODULE IV: ALERT MANAGEMENT AND CORRELATION 9

Alert Management and Correlation, Data Fusion, Alert Correlation, Pre process, Correlation Techniques, Post process, Alert Correlation

Architectures, Validation of Alert Correlation System, Cooperative Intrusion Detection, Basic Principles of Information Sharing and Cooperation Based on Goal – tree Representation of Attack Strategies.

MODULE V: EVALUATION CRITERIA 6

Evaluation Criteria, Accuracy, False Positive and Negative, Confusion Matrix, Precision, Recall, and F–Measure, ROC Curves, The Base–Rate Fallacy, Performance, Completeness, Timely Response

MODULE VI : EVALUATION CRITERIA II 3

Intrusion Tolerance and Attack Resistance, Redundant and Fault Tolerance Design and Test, Evaluation and Data Sets

TOTAL: 45 PERIODS

TEXT BOOKS:

1. Ali A. Ghorbani, Network Intrusion Detection and prevention concepts and techniques,Springer,2010.

REFERENCES:

1. PeterSzor, The Art of Computer Virus Research and Defense, Symantec Press, 2010, ISBN0–321–30545–3.
2. Markus Jakobsson and Zulfikar Ramzan, Crimeware, Understanding New Attacks and Defenses, Symantec Press, 2008, ISBN:978–0–321–50195–0.
3. Roberto Di Pietro, Luigi V.Mancini, Intrusion Detection System, Springer, 2008.

OUTCOMES:

Upon completion of the course, the student should be able to

1. Learn fundamentals and history of Intrusion Detection system. (K1)
2. Apply knowledge of Intrusion Detection in order to avoid common pitfall in the creation and evaluation of new intrusion detection system. (K3)
3. Able to explore the principles and techniques used in intrusion detection. (K3)
4. Able to apply intrusion detection tools and techniques. (K2)
5. Preparation to become an independent researcher in intrusion detection. (K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	1	2	2	-	2	-	-	-	-	2	2	3	2
CO2	3	1	3	2	-	2	-	-	-	-	2	2	3	2
CO3	3	1	3	2	-	2	-	-	-	-	2	2	3	2
CO4	3	1	3	2	3	2	-	-	-	-	2	2	3	2
CO5	3	1	3	2	3	2	-	-	2	3	2	2	3	2
CO6	3	1	3	2	3	2	-	-	2	3	2	2	3	2

PROFESSIONAL ELECTIVES - II

20SCEL602 SDG NO. 4	VULNERABILITY DISCOVERY & EXPLOIT DEVELOPMENT	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To focus on a comprehensive coverage of software exploitation.
- To present different domains of code Exploitation
- How they can be used together to test the security of an application.
- To Search for vulnerabilities in closed–source applications
- To Learn about exploits in various operating systems and Wireless environment

MODULE 1: INTRODUCTION TO VULNERABILITY DISCOVERY 9

Background: Vulnerability Discovery Methodologies – Fuzzing Methods and Fuzzer Types, Data Representation and Analysis – Requirements for Effective Fuzzing.

Vulnerability Issues: Operating System Vulnerabilities – Application Vulnerabilities – Connectivity and Dependence – Vulnerability assessment for natural disaster, technological hazards, and terrorist threats.

MODULE 2: ADVANCED FUZZY TECHNOLOGIES 9

Targets and Automation: Automation and Data Generation – Environment Variable and Argument Fuzzing – Web Application and Server Fuzzing – File Format Fuzzing – Network Protocol Fuzzing – Web Browser Fuzzing – In–Memory Fuzzing. Advanced Fuzzy Technologies– Fuzzing Frameworks – Automated Protocol Dissection – Fuzzer Tracking – Intelligent Fault Detection.

MODULE 3: LINUX EXPLOITATION 9

Advanced Linux Exploitation: Linux heap management, constructs, and environment, Navigating the heap – Abusing macros such as unlink() and frontlink() – Function pointer overwrites – Using IDA for Linux application exploitation – Patch Diffing, – One day Exploits and Return Oriented Shell code.

Microsoft patch management process and Patch Tuesday – Obtaining patches and patch extraction – Binary diffing with BinDiff, patchdiff2, turbodiff, and darungrim – Triggering patched vulnerabilities– Writing one–day exploits – Handling modern exploit mitigation controls.

MODULE 4 : WINDOWS EXPLOITATION 9

Windows Kernel Debugging and Exploitation: Understanding the Windows Kernel, WinDbg, Analysing Kernel Vulnerabilities and Kernel vulnerability types, Kernel exploitation techniques. Windows Heap Overflows and Client–Side Exploitation: Windows heap management, constructs, and environment – Browser–based and client–side exploitation, Remedial heap spraying, vftable/vtable behavior, Modern heap spraying to determine address predictability, Use–After– Free attacks and dangling pointers, Determining exploitability, Defeating ASLR, DEP, and other common exploit mitigation controls

MODULE 5: ANDROID AND iOS EXPLOITATION 9

Android Exploitation: Android Basics, Android Security Model, Introduction to ARM, Android Development Tools, Android Security Assessment Tools, Exploiting Applications, Protecting Applications, Native Exploitation and Analysis.

MODULE 6: IOS EXPLORATION II

iOS Exploitation: Introduction to iOS hacking, iOS User Space Exploitation, iOS Kernel Debugging and Exploitation.

TOTAL:45PERIODS

TEXT BOOKS:

1. "Hack I.T.– Security Through Penetration Testing", T.J. Klevinsky, Scott Laliberte and Ajay
2. Gupta, Addison– Wesley, ISBN:0–201–71956–8
3. "Managing Risk and Information Security", Malcolm Harkins, Apress, 2012.
4. "Metasploit: The Penetration Tester's Guide", David Kennedy, Jim O' Gorman, Devon Kearns, Mati Aharoni

REFERENCE BOOKS:

1. "Professional Penetration Testing: Creating and Operating a Formal Hacking Lab", Thomas Wilhelm

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand how to exploit a program and different types of software exploitation techniques (K1)
2. Understand the exploit development process(K2)
3. Search for vulnerabilities in closed–source applications(K3)
4. Learn about exploits in various operating systems and Wireless environment Write their own exploits for vulnerable applications(K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	1	2	2	-	2	-	-	-	-	2	2	3	2
CO2	3	1	3	2	-	2	-	-	-	-	2	2	3	2
CO3	3	1	3	2	-	2	-	-	-	-	2	2	3	2
CO4	3	1	3	2	3	2	-	-	-	-	2	2	3	2
CO5	3	1	3	2	3	2	-	-	2	3	2	2	3	2
CO6	3	1	3	2	3	2	-	-	2	3	2	2	3	2

PROFESSIONAL ELECTIVES - II

20SCEL603 SDG NO. 4	BIOMETRIC SECURITY	L	T	P	C
		3	0	0	3

OBJECTIVES:

- Introduce Bio–metric and traditional authentication methods.
- Describe the background theory of image processing required in biometric security
- Classify algorithms related to various bio metrics
- Evaluate the performance of various biometric systems.
- Study the challenges and limitations associated with bio–metrics security

MODULE I: INTRODUCTION **9**

Introduction and Definitions of bio–metrics, Traditional authenticated methods and technologies. Introduction to Image Processing, Image Enhancement Techniques: Spatial Domain Methods: Smoothing, sharpening filters, Laplacian filters, Frequency domain filters, Smoothing and sharpening filters.

MODULE II: IMAGE ANALYSIS **9**

Image Restoration & Reconstruction: Model of Image Degradation / restoration process, Noise models, spatial filtering, inverse filtering, Minimum mean square Error filtering.

MODULE III: IMAGE EXTRACTION **9**

Introduction to image segmentation: Image edge detection: Introduction to edge detection, types of edge detectors. Introduction to image feature extraction.

MODULE 4: TECHNOLOGIES IN BIO–METRIC **9**

Bio–metric technologies: Fingerprint, Face, Iris, Hand Geometry, Gait recognition, Ear, Voice, Palm print, On–Line Signature Verification, 3D Face Recognition, Dental Identification and DNA.

MODULE 5: BIO–METRIC SYSTEMS **5**

Multi bio–metrics Introduction– Sources of Multiple Evidence, Acquisition and Processing Architecture–Fusion levels – sensor–level, feature–level, score–level, rank–level, decision–level fusion;

MODULE 6 : BIO-METRIC SECURITY **4**

Security of biometric systems–introduction, Adversary attacks, attacks at the user interface, attacks on biometric processing,attacks on the template Database – Casestudyof3DfacerecognitionandDNAmatching

TOTAL:45PERIODS

TEXT BOOKS:

1. Gonzalez, R.C. and Woods, R.E., Digital Image Processing. 2nd ed. India: Person Education, 2009
2. AnilJain, Arun A. Ross, Karthik Nandakumar, Introduction to biometric, Springer, 2011.

REFERENCES:

1. J. Wayman, A.K. Jain, D. Maltoni, and D. Maio(Eds.), Biometric Systems: Technology, Design and Performance Evaluation, Springer, 2004.
2. PaulReid, Biometrics for network security, Hand book of Pearson, 2004.
3. A. K. Jain, R. Bolle, S. Pankanti (Eds.), BIO METRICS: Personal Identification inNetworkedSociety,KluwerAcademicPublishers,1999.

OUTCOMES:

Upon completion of the course, the student should be able to

1. A good understanding of the various modules constituting a bio–metric system.(K2)
2. Familiarity with different bio–metric traits and to appreciate their relative significance.(K1)
3. A good knowledge of the feature sets used to represent some of the popular bio–metric traits.(K3)
4. Evaluate and design security systems incorporating bio–metrics.(K3)
5. Understand the Law and the use of multi bio–metrics systems(K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	1	2	2	-	2	-	-	-	-	2	2	3	2
CO2	3	1	3	2	-	2	-	-	-	-	2	2	3	2
CO3	3	1	3	2	-	2	-	-	-	-	2	2	3	2
CO4	3	1	3	2	3	2	-	-	-	-	2	2	3	2
CO5	3	1	3	2	3	2	-	-	2	3	2	2	3	2
CO6	3	1	3	2	3	2	-	-	2	3	2	2	3	2

PROFESSIONAL ELECTIVES - II

20SCEL604 SDG NO. 4	CYBER THREAT INTELLIGENCE	L	T	P	C
		3	0	0	3

OBJECTIVES:

- Leaders can guide organizations in accurately accessing threats,
- Risks, and vulnerabilities
- To minimize the potential for incidents and,
- when necessary, provide more thoughtful responses
- To Providers of threat indicators

MODULE I : DEFINING CYBER THREAT INTELLIGENCE 9

The Need for Cyber Threat Intelligence: The menace of targeted attacks, The monitor–and–respond strategy, Why the strategy is failing, Cyber Threat Intelligence Deined, Key Characteristics: Adversary based, Risk focused, Process oriented, Tailored for diverse consumers, The Beneits of Cyber Threat Intelligence

MODULE II : DEVELOPING CYBER THREAT INTELLIGENCE REQUIREMENTS 9

Assets That Must Be Prioritized: Personal information, Intellectual property, Conidential business information, Credentials and IT systems information, Operational systems. Adversaries: Cybercriminals, Competitors and cyber espionage agents, Hack activists. Intelligence Consumers: Tactical users, Operational users, Strategic users

MODULE III : COLLECTING CYBER THREAT INFORMATION 9

Threat Indicators, File hashes and reputation data, Technical sources: honey pots and scanners, Industry sources: malware and reputation feeds. Level 2: Threat Data Feeds, Cyber threat statistics, reports, and surveys, Malware analysis. Level 3: Strategic Cyber Threat Intelligence, Monitoring the underground, Motivation and intentions, Tactics, techniques, and procedures

MODULE IV : ANALYZING AND DISSEMINATING CYBER THREAT INTELLIGENCE 9

Information versus Intelligence, Validation and Prioritization: Risk scores, Tags for context, Human assessment. Interpretation and Analysis: Reports, Analyst skills, Intelligence platform, Customization. Dissemination: Automated feeds and APIs, Searchable knowledge base,Tailored reports.

MODULE V: SOURCE SOFTWARE DEVELOPMENT 6

Types of Partners: Providers of threat indicators, Providers of threat data feeds, Providers of comprehensive cyber threat intelligence. Important Selection Criteria: Global and cultural reach, Historical data and knowledge, Range of intelligence deliverables

MODULE VI: API'S INTEGRATION 3

APIs and integrations, Intelligence platform, knowledge base, and portal, Client services, Access to experts. Intelligence–drivenSecurity.

TOTAL: 45 PERIODS

TEXT BOOKS:

1. Jon Friedman. Mark Bouchard, CISSP. Foreword by John P. Watters, Cyber ThreatIntelligence,DefinitiveGuideTM,2015.
2. Scott J. Roberts, Rebekah Brown, Intelligence–Driven Incident Response: Outwitting the Adversary, O'Reilly Media, 2017.

REFERENCES:

1. Henry Dalziel, How to Define and Build an Effective CyberThreat Intelligence Capability Elsevier Science & Technology, 2014.
2. John Robertson, Ahmad Diab, Ericsson Marin, Eric Nunes, Vivin Paliath,J ana Shakarian, Paulo Shakarian, Dark Web Cyber Threat Intelligence Mining Cambridge University Press, 2017.
3. Bob Gourley, The Cyber Threat, Create space Independent Pub, 2014.

OUTCOMES:

Upon completion of the course, the student should be able to

1. Study of different Cyber Threat. (K2)
2. Study the technique to Develop Cyber Threat Intelligence Requirements. (K1)
3. Can Collect Cyber Threat Information. (K3)
4. Help in Analyzing and Disseminating Cyber Threat Intelligence.(K3)
5. Study of Open-Source Software Development. (K2)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	3	3	1	1	1	-	1	-	1	-	2	2
CO2	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO3	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO4	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO5	3	3	3	3	3	1	1	1	2	3	1	-	2	2
CO6	3	3	2	3	3	2	-	-	-	-	-	-	1	1

PROFESSIONAL ELECTIVES - II

20SCEL605 SDG NO. 4	SOCIAL NETWORK ANALYSIS	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To understand the concept of semantic web and related applications.
- To learn knowledge representation using ontology.
- To understand human behavior in social web and related communities.
- To understand privacy issues in online social networks.
- To learn visualization of social networks.

MODULE 1: INTRODUCTION **9**

Introduction to Semantic Web: Limitations of current Web – Development of SemanticWeb – Emergence of the Social Web – Social Network analysis: Development of Social Network Analysis – Key concepts and measures in network analysis– Electronic sourcesfor network analysis: Electronic discussion networks, Blogs and online communities –Web–based networks

MODULE 2 : MODELLING, AGGREGATING AND KNOWLEDGE REPRESENTATION **9**

Ontology and the irrole in the Semantic Web: Ontology–based knowledge Representation – Ontology Languages for the Semantic Web: Resource Description Framework–Web Ontology Language– Modelling and aggregating social network data: State–of–the–art in network data representation – Ontological representation of social individuals–Ontological representation of social relationships–Aggregating and reasoning with social network data.

MODULE 3 : EXTRACTION AND MINING COMMUNITIES IN WEB SOCIAL NETWORKS **9**

Extracting evolution of Web Community from a Series of Web Archive – Detecting communities in social networks – Definition of community – Evaluating communities –Methods for community detection and mining–Applications of community mining algorithms–Tools for detecting communities social network infrastructures and communities– Decentralized online social networks.

MODULE 4 : PREDICTING HUMAN BEHAVIOUR AND PRIVACY ISSUES **9**

Understanding and predicting human behavior for social communities– User data management – Inference and Distribution – Enabling new human

experiences – Reality mining – Context – Awareness – Privacy in online social networks – Trust in online environment – Trust models based on subjective logic – Trust network analysis – Trust transitivity analysis – Combining trust and reputation – Trust derivation based on trust comparisons–Attack spectrum and counter measures.

MODULE 5 : VISUALIZATION AND APPLICATIONS OF SOCIAL NETWORKS **9**

Graph theory – Centrality – Clustering – Node–Edge Diagrams – Matrix representation –Visualizing online social networks, Visualizing social networks with matrix–based representations.

MODULE 6: HYBRID REPRESENTATION **3**

Matrix and Node–Link Diagrams– Hybrid representations– Cover networks– Community welfare–Collaboration networks–Co–Citation networks.

TOTAL : 45PERIODS

TEXT BOOKS:

1. Peter Mika,– Social Networks and the Semantic Web, First Edition, Springer 2007.
2. Borko Furht, Handbook of Social Network Technologies and Applications, 1st Edition, Springer, 2010.

REFERENCE BOOKS:

1. GuandongXu, Yanchun Zhang and LinLi,– Web Mining and Social Networking–Techniques and applications, First Edition,Springer,2011.
2. DionGoh and Schubert Foo, –Social information Retrieval Systems: Emerging Technologies and Applications for Searching the Web Effectively, IGIGlobal Snippet,2008.

OUTCOMES:

Upon completion of the course, the student should be able to

1. Develop semantic web related applications. (K1)
2. Represent knowledge using ontology. (K3)
3. Predict human behavior in social web and related communities.(K2)
4. Learn Visualize social networks.(K3)
5. Understand privacy issues in online social networks, the knowledge representation and applications of social networks.(K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	3	3	1	1	1	-	1	-	1	-	2	2
CO2	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO3	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO4	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO5	3	3	3	3	3	1	1	1	2	3	1	-	2	2
CO6	3	3	2	3	3	2	-	-	-	-	-	-	1	1

PROFESSIONAL ELECTIVES - II

20SCEL606 SDG NO. 4	MALWARE ANALYSIS & REVERSE ENGINEERING	L	T	P	C
		3	0	0	3

OBJECTIVES:

- Provides the basic knowledge in overall process and methodology of analyzing malware
- Provides a foundation for using IDA Pro and performing in–depth analysis of malware.
- Explains the basics of debugging and how to use a debugger for malware analysts.
- Describes common malware functionality and shows how to recognize that functionality when analyzing malware.
- Demonstrates techniques used by malware to make it difficult to analyze in a virtual machine and how to bypass those techniques

MODULE 1 : BASIC ANALYSIS **9**

Basic Static Techniques, Antivirus Scanning– Static Analysis in practice–Malware Analysis in Virtual, Machines, Basic Dynamic Analysis.

MODULE 2 : ADVANCED STATIC ANALYSIS **9**

A Crash Course in x86 Disassembly, IDA Pro, Recognizing C Code Constructs in Assembly Analyzing Malicious Windows Programs

MODULE 3 : ADVANCED DYNAMIC ANALYSIS **9**

Debugging, vi Brief Contents, Olly Dbg, Kernel Debugging with WinDbg–Drivers and Kernel code–Rootkits–Loading drivers

MODULE 4 : MALWARE FUNCTIONALITY 9

Malware Behavior– Backdoors, Covert Malware Launching, Data Encoding, Malware–Focused Network Signatures

MODULE 5 : ANTI–REVERSE–ENGINEERING 6

Anti–Disassembly–Defeating Disassembly algorithm, Anti– Debugging,

MODULE 6: ANTI–REVERSE–ENGINEERING II 3

Anti–Virtual Machine Techniques, Packers and Unpacking

TOTAL: 45 PERIODS

TEXT BOOKS:

1. Michael Sikorski and AndrewHonig,"Practical Malware Analysis: TheHands–On Guide to Dissecting Malicious Software", No Starch Press,2012.

REFERENCES:

1. Jamie Butler and Greg Hoglund," Rootkits: Subverting the Windows Kernel",Addison–Wesley,2005.
2. Dang, Gazet, Bachaalany," Practical Reverse Engineering",Wiley,2014.
3. Reverend Bill Blunden, "The Rootkit Arsenal: Escape and Evasion in the Dar Corners of the System" Second Edition, Jones& Bartlett, 2012.

OUTCOMES:

Upon completion of the course, the student should be able to

1. Possess the skills necessary to carry out independent analysis of modern malware samples using both static and dynamic analysis techniques. (K2)
2. Understand the x86 assembly language to provide a foundation for using IDA Pro and performing in–depth analysis of malware. (K1)
3. Achieve proficiency with industry standard tools including OllyDbg and WinDBG (K3)
4. Identify the common malware functionality by analysing the network behaviour (K2)
5. Apply techniques and concepts to unpack, extract, decrypt, or bypass new anti-analysis techniques in future malware samples. (K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	3	3	1	1	1	-	1	-	1	-	2	2
CO2	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO3	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO4	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO5	3	3	3	3	3	1	1	1	2	3	1	-	2	2
CO6	3	3	2	3	3	2	-	-	-	-	-	-	1	1

PROFESSIONAL ELECTIVES - II

20SCEL607 SDG NO. 4	QUANTUM-RESISTANT BLOCKCHAIN	L	T	P	C
		3	0	0	3

OBJECTIVES:

- Introduce students to the basic concepts of quantum computing and cryptography.
- Analyze the impact of quantum computing on traditional cryptographic algorithms.
- Provide students with the knowledge and skills to implement quantum-resistant cryptographic solutions.
- Foster critical thinking regarding the development and adoption of quantum-resistant cryptography.
- Promote interdisciplinary understanding of the intersection between quantum computing and cryptography.

MODULE 1 : INTRODUCTION TO QUANTUM COMPUTING AND CRYPTOGRAPHY 9

Overview of Quantum Computing: Basic concepts, -quantum bits (qubits)-quantum gates, superposition, and entanglement-Classical Cryptography Overview: Basics of classical cryptography algorithms and their vulnerabilities to quantum attacks-Quantum Cryptography Fundamentals:

Quantum key distribution (QKD)-quantum-resistant cryptographic primitives, and post-quantum cryptography-Sustainable Development Goals (SDGs): SDG 9 - Industry, Innovation, and Infrastructure.

MODULE 2: POST-QUANTUM CRYPTOGRAPHIC PRIMITIVES 9

Lattice-based Cryptography: Lattice problems, lattice-based cryptographic primitives (LWE, NTRUEncrypt), and security parameters-Code-based Cryptography: Error-correcting codes, code-based cryptographic primitives (McEliece, Niederreiter), and security analysis-Hash-based Cryptography: Merkle trees, hash-based signatures (Merkle Signature Scheme), and security considerations-Sustainable Development Goals (SDGs): SDG 16 - Peace, Justice, and Strong Institutions.

MODULE 3: QUANTUM KEY DISTRIBUTION (QKD) AND QUANTUM SECURE COMMUNICATION 9

Quantum Key Distribution Protocols: BB84 protocol, E91 protocol, security analysis, and implementation challenges-Quantum Secure Communication: Quantum teleportation, quantum repeaters, and quantum network architecture-Practical Considerations: Implementation challenges, experimental setups, and real-world applications-Sustainable Development Goals (SDGs): SDG 17 - Partnerships for the Goals.

MODULE 4: CRYPTANALYSIS OF QUANTUM-RESISTANT CRYPTOGRAPHY 9

Quantum Cryptanalysis Techniques: Shor's algorithm, Grover's algorithm, quantum collision finding, and quantum period finding-Security Analysis: Attacks on post-quantum cryptographic primitives, quantum oracle models, and quantum-resistant security proofs

MODULE 5: IMPLEMENTATION AND DEPLOYMENT OF QUANTUM-RESISTANT CRYPTOGRAPHY 6

Transitioning to Quantum-resistant-Cryptography: Challenges-Practical Considerations: Quantum resources required for cryptanalysis.

MODULE 6: CRYPT ANALYSIS 3

complexity analysis- cryptanalysis challenges-Sustainable Development Goals (SDGs): SDG 4 - Quality Education

TOTAL:45PERIODS

TEXT BOOKS:

1. "Quantum Computing for Computer Scientists" by Noson S. Yanofsky and Mirco A. Mannucci.
2. "Post-Quantum Cryptography" by Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen.
3. "Lattice-Based Cryptography" by Vadim Lyubashevsky, Chris Peikert, and Oded Regev.
4. "Code-Based Cryptography" by Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen.
5. "Quantum Communication and Quantum Networking" by Mark M. Wilde.

REFERENCE BOOKS:

1. "Quantum Cryptography and Secret-Key Distillation" by Norbert Lütkenhaus.
2. "Hash-Based Cryptography" by Johannes Buchmann, Erik Dahmen, and Andreas Hülsing.
3. "Quantum Algorithms via Linear Algebra: A Primer" by Richard J. Lipton and Kenneth W. Regan.

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the fundamental principles of quantum computing and its implications for cryptography. (K2)
2. Analyze the vulnerabilities of classical cryptographic algorithms against quantum attacks. (K2)
3. Evaluate the principles and practical applications of quantum key distribution. (K1)
4. Explore post-quantum cryptographic primitives and their potential applications. (K2)
5. Identify the challenges and opportunities in transitioning to quantum-resistant cryptography. (K3)
6. Apply quantum-resistant cryptographic techniques to real-world scenarios. (K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	1	0	0	0	0	0	0	0	0	0	1	2
CO2	3	3	3	1	2	0	0	0	0	0	0	0	1	2
CO3	3	3	3	3	3	0	0	0	0	0	0	0	2	2
CO4	3	3	3	2	3	0	0	0	0	0	0	1	3	3
CO5	3	3	3	3	3	0	0	0	0	0	2	1	3	3
CO6	3	3	3	3	3	2	1	2	2	0	2	2	3	3

PROFESSIONAL ELECTIVES - II

20SCEL608 SDG NO. 4 & 9	QUANTUM-RESISTANT CRYPTOGRAPHY	L	T	P	C
		3	0	0	3

OBJECTIVES:

- Introduce students to the basic concepts of blockchain technology.
- Analyze the potential threats posed by quantum computing to blockchain security.
- Provide students with the knowledge and skills to implement quantum-resistant solutions in blockchain systems.
- Foster critical thinking regarding the security implications of quantum computing for blockchain technology.
- Promote interdisciplinary understanding of the convergence of blockchain and quantum computing.

MODULE 1: INTRODUCTION TO QUANTUM-RESISTANT CRYPTOGRAPHY 9

Overview of Classical Cryptography - Its Vulnerabilities to Quantum Attacks Introduction to Quantum Computing and Shor's Algorithm-Need for Quantum-Resistant Cryptography-Principles and Requirements of Quantum-Resistant Cryptography-Overview of Quantum-Resistant Cryptographic Algorithms

MODULE 2: LATTICE-BASED CRYPTOGRAPHY 9

Introduction to Lattices and Lattice Problems-Fundamentals of Lattice-Based Cryptography-Lattice-Based Encryption Schemes: NTRUEncrypt, Ring-LWE Lattice-Based Signature Schemes- BLISS, NTRUSign-Security Analysis of Lattice-Based Cryptography

MODULE 3: CODE-BASED CRYPTOGRAPHY 9

Introduction to Error-Correcting Codes-Code-Based Encryption Schemes: McEliece Cryptosystem- Code-Based Signature Schemes- Niederreiter Crypto system- Security Analysis of Code-Based Cryptography-Applications and Limitations of Code-Based Cryptography

MODULE 4: MULTI VARIATE POLYNOMIAL CRYPTOGRAPHY 9

Introduction to Multi variate Polynomials-Multivariate Polynomial Encryption Schemes-Multivariate Polynomial Signature Schemes-Security Analysis of Multi variate Polynomial Cryptography-Comparison with Other Quantum-Resistant Cryptographic Approaches

MODULE 5: HASH-BASED CRYPTOGRAPHY AND OTHER APPROACHES 9

Introduction to Hash-Based Cryptography-Merkle Trees and Merkle Signature Schemes-Other Quantum-Resistant Cryptographic Approaches-Hybrid Crypto systems

MODULE 6: HASH-BASED CRYPTOGRAPHY AND OTHER APPROACHES II 3

Combining Classical and Quantum-Resistant Techniques- Future Directions and Challenges in Quantum-Resistant Cryptography

TOTAL:45 PERIODS

TEXT BOOKS:

1. "Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications" by Imran Bashir.
2. "Quantum Computing for Computer Scientists" by Noson S. Yanofsky and Mirco A. Mannucci.
3. "Post-Quantum Cryptography" by Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen.
4. "Blockchain Basics: A Non-Technical Introduction in 25 Steps" by Daniel Drescher.

REFERENCE BOOKS:

1. "Block chain Basics: A Non-Technical Introduction in 25 Steps" by Daniel Drescher.
2. NPTEL Link: Block chain Technology – NPTEL
3. "Quantum Cryptography and Secret-Key Distillation" by Norbert Lütkenhaus.
4. NPTEL Link: Block chain Data Management - NPTEL

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the fundamentals of block chain technology and its decentralized nature. (K1)
2. Analyze the potential impact of quantum computing on block chain security.(K2)
3. Identify the vulnerabilities of existing block chain systems to quantum attacks.(K3)
4. Explore the challenges and opportunities in integrating quantum-resistant solutions into block chain technology.(K2)
5. Develop strategies for enhancing the security and resilience of block chain networks against quantum threats.(K3)
6. Collaborate effectively in interdisciplinary teams to address the intersection of block chain and quantum computing(K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	1	0	0	0	0	0	0	0	0	0	1	2
CO2	3	3	3	1	2	0	0	0	0	0	0	0	1	2
CO3	3	3	3	3	3	0	0	0	0	0	0	0	2	2
CO4	3	3	3	2	3	0	0	0	0	0	0	1	3	3
CO5	3	3	3	3	3	0	0	0	0	0	2	1	3	3
CO6	3	3	3	3	3	2	1	2	2	0	2	2	3	3

PROFESSIONAL ELECTIVES - II

20SCEL610 SDG NO. 4 & 9	QUANTUM INFORMATION THEORY	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To provide students with a solid foundation in quantum mechanics and its applications to information theory.
- To introduce students to advanced concepts in quantum information processing, including quantum algorithms and cryptography.
- To enable students to analyze and solve problems related to quantum communication and computation.
- To explore the potential impact of quantum information technology on society, economy, and sustainability.

- To foster critical thinking and ethical reasoning regarding the development and deployment of quantum information technology.

MODULE 1: INTRODUCTION TO QUANTUM MECHANICS AND INFORMATION THEORY 10

Basic principles of quantum mechanics- Quantum states and operators=Quantum measurements and observables - Introduction to classical information theory-Classical vs. quantum information processing

MODULE 2: QUANTUM STATES AND QUANTUM OPERATIONS 10

Quantum states and density operators-Entanglement and Bell states-Quantum operations and channels-Quantum circuit model-No-cloning theorem and quantum teleportation

MODULE 3: QUANTUM ENTANGLEMENT AND QUANTUM COMMUNICATION 10

Entanglement measures and quantification-Quantum teleportation protocol-Quantum dense coding-Quantum key distribution (QKD) protocols-Quantum error correction and fault-tolerant quantum computation

MODULE 4: QUANTUM ALGORITHMS AND COMPLEXITY 10

Quantum algorithms: Shor's algorithm, Grover's algorithm-Quantum complexity classes-Quantum simulation algorithms-Quantum Fourier transform and its applications-Quantum supremacy and quantum advantage

MODULE 5: QUANTUM CRYPTOGRAPHY AND QUANTUM INFORMATION APPLICATIONS 5

Quantum cryptography protocols: BB84, E91-Quantum secure direct communication-Quantum computing and its applications in various fields

MODULE 6: INFORMATION APLLICATIONS II 4

Quantum machine learning and optimization algorithms-Ethical considerations and societal implications of quantum information technology

TOTAL: 45 PERIODS

TEXT BOOKS:

1. "Quantum Computation and Quantum Information" by Michael A. Nielsen and Isaac L. Chuang.
2. "Quantum Information Theory and Quantum Statistics" by E. T. Jaynes and F. W. Cummings.

REFERENCE BOOKS:

1. "Quantum Computing: An Applied Approach" by Jack D. Hidary.
2. "Quantum Information Theory: Mathematical Foundation" by Mark M. Wilde.

NPTEL Links:

1. Quantum Mechanics and Quantum Computing

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the fundamental principles of quantum mechanics and their relevance to quantum information processing.(K2)
2. Analyze and manipulate quantum states, operations, and entanglement for various quantum information tasks.(K3)
3. Design and implement quantum communication protocols and algorithms, including quantum cryptography and error correction.(K2)
4. Evaluate the potential applications of quantum information technology in diverse fields, such as cryptography, computing, and simulation.(K3)
5. Critically assess the ethical and societal implications of quantum information technology deployment.(K3)
6. Collaborate effectively and communicate ideas related to quantum information theory in interdisciplinary contexts.(K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	1	0	0	0	0	0	0	0	0	0	1	2
CO2	3	3	3	1	2	0	0	0	0	0	0	0	1	2
CO3	3	3	3	3	3	0	0	0	0	0	0	0	2	2
CO4	3	3	3	2	3	0	0	0	0	0	0	1	3	3
CO5	3	3	3	3	3	0	0	0	0	0	2	1	3	3
CO6	3	3	3	3	3	2	1	2	2	0	2	2	3	3

PROFESSIONAL ELECTIVES - II

20SCEL609 SDG NO. 4	SOCIAL ENGINEERING	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To provide students with a comprehensive understanding of social engineering concepts, including its history, psychology, and techniques.
- To familiarize students with various social engineering tactics and their real-world applications through case studies and examples.
- To equip students with the knowledge and skills to develop and implement effective social engineering prevention and mitigation strategies.
- To raise awareness among students about the ethical considerations and legal implications associated with social engineering practices.
- To encourage critical thinking and ethical decision-making in dealing with social engineering challenges in cyber security.

MODULE 1: INTRODUCTION TO SOCIAL ENGINEERING 9

Understanding Social Engineering Concepts-History and Evolution of Social Engineering-Psychology Behind Social Engineering Attacks-Common Social Engineering Techniques Real-world Examples and Case Studies

MODULE 2: PSYCHOLOGICAL PRINCIPLES IN SOCIAL ENGINEERING 9

Understanding Human Behavior and Decision Making-Influence and Persuasion Techniques-Cognitive Biases Exploited in Social Engineering-Emotional Manipulation Tactics-Social Engineering in the Context of Maslow's Hierarchy of Needs

MODULE 3: SOCIAL ENGINEERING TACTICS AND TECHNIQUES 9

Phishing Attacks: Types and Variants-Pretexting and Impersonation Techniques-Baiting, Tailgating, and Shoulder Surfing-Dumpster Diving and Physical Security Exploits-Online and Offline Reconnaissance Methods

MODULE 4: SOCIAL ENGINEERING PREVENTION AND MITIGATION 9

Awareness and Training Programs-Developing Security Policies and Procedures-Technology Solutions for Social Engineering Defense-Incident Response and Reporting Mechanisms-Social Engineering Red Team Exercises

MODULE 5: ETHICAL AND LEGAL ASPECTS OF SOCIAL ENGINEERING 5

Ethical Considerations in Social Engineering Research and Practice-Legal Frameworks and Regulations Related to Social Engineering-Case Studies of Ethical and Unethical Social Engineering

MODULE 6: PROFESSIONAL PRACTICES II 4

Practices-Professional Codes of Conduct for Security Practitioners-Emerging Trends and Future Directions in Social Engineering

TOTAL:45PERIODS

TEXT BOOKS:

1. "The Art of Deception: Controlling the Human Element of Security" by Kevin D. Mitnick.
2. "Social Engineering: The Science of Human Hacking" by Christopher Hadnagy.
3. "Influence: The Psychology of Persuasion" by Robert B. Cialdini.

Reference Book:

1. "Social Engineering in IT Security: Tools, Tactics, and Techniques" by Sharon Conheady.

NPTEL Course Link:

1. Social Engineering in Cybersecurity - NPTEL

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the fundamental concepts and principles of social engineering in cybersecurity. (K2)
2. Analyze the psychological aspects behind social engineering attacks and their impact on human behaviour.(K1)
3. Identify various social engineering tactics and techniques used by attackers to exploit vulnerabilities.(K2)
4. Develop strategies and countermeasures to prevent and mitigate social engineering attacks.(K3)
5. Evaluate the ethical and legal implications of social engineering practices in cybersecurity. (K3)
6. Apply knowledge and skills learned to assess, defend against, and respond to social engineering threats effectively.(K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	3	3	1	1	1	-	1	-	1	-	2	2
CO2	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO3	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO4	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO5	3	3	3	3	3	1	1	1	2	3	1	-	2	2
CO6	3	3	2	3	3	2	-	-	-	-	-	-	1	1

PROFESSIONAL ELECTIVES - III

20SCEL701 SDG NO. 4&9	QUANTUM COMMUNICATION	L	T	P	C
		3	0	0	3

OBJECTIVES:

- Introduce students to the fundamentals of quantum mechanics and information theory.
- Provide an in-depth understanding of quantum communication protocols and technologies.
- Foster critical thinking skills in analyzing security aspects and challenges in quantum communication.
- Encourage hands-on experience in designing and implementing basic quantum communication systems.
- Explore the societal and ethical implications of quantum communication technologies.

Module 1: Introduction to Quantum Communication 8

Introduction to Quantum Mechanics and Information Theory-Basics of Quantum Cryptography -Quantum Key Distribution (QKD) Protocols: BB84, E91 -Security in Quantum Communication

Module 2: Quantum Entanglement and Teleportation 7

Entanglement and Bell's Inequality - Quantum Teleportation Protocol - Applications of Entanglement in Quantum Communication

Module 3: Quantum Communication Protocols 7

Quantum Repeaters - Quantum Error Correction - Quantum Secure Direct Communication (QSDC) - Quantum Communication Networks

Module 4: Quantum Cryptography 8

Principles of Quantum Cryptography - Quantum Key Distribution (QKD) Systems and Implementations - Post-Quantum Cryptography - Challenges and Future Directions in Quantum Cryptography

Module 5: Quantum Communication Technologies 8

Quantum Communication Hardware: Quantum Repeaters, QKD Systems - Quantum Communication in Practice: Challenges and Solutions - Quantum Communication for Secure Data Transmission - Quantum Communication and Future Technologies

Module 6: Applications of Quantum Communication 7

Real-world Applications of Quantum Communication - Integration with Existing Technologies Potential Impact on Various Industries - Future Prospects of Quantum Communication

TOTAL:45 PERIODS

TEXT BOOKS:

1. "Quantum Computation and Quantum Information" by Michael A. Nielsen and Isaac L. Chuang
2. "Quantum Cryptography and Secret-Key Distillation" by Charles H. Bennett, Gilles Brassard.
3. "Introduction to Quantum Information Science" by Vlatko Vedral.
4. "Quantum Computation and Quantum Information" by Michael A. Nielsen, Isaac L. Chuang.

REFERENCE BOOK:

1. "Quantum Information and Quantum Computing" by Christopher Gerry and Peter Knight

NPTEL COURSE LINK:

1. NPTEL - Quantum Communication

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the principles of quantum mechanics underlying quantum communication.(K1)
2. Analyze different quantum communication protocols and their security implications.(K2)
3. Design and implement basic quantum communication systems.(K2)
4. Evaluate the challenges and limitations of current quantum communication technologies.(K3)
5. Explore the potential applications and future directions of quantum communication.(K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	3	3	1	1	1	-	1	-	1	-	2	2
CO2	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO3	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO4	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO5	3	3	3	3	3	1	1	1	2	3	1	-	2	2
CO6	3	3	2	3	3	2	-	-	-	-	-	-	1	1

PROFESSIONAL ELECTIVES - III

20SCEL702 SDG NO. 4&9	POST-QUANTUM CRYPTOGRAPHY	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To introduce students to the concept of post-quantum cryptography and its importance in the era of quantum computing.
- To provide a comprehensive understanding of various post-quantum cryptographic approaches and their underlying mathematical principles.
- To enable students to design and implement post-quantum cryptographic algorithms for secure communication.
- To equip students with the skills to analyze the security of post-quantum cryptographic schemes against quantum attacks.
- To foster critical thinking and discussion on the potential applications, challenges, and future directions of post-quantum cryptography.

Module 1: Introduction to Classical Cryptography and Quantum Computing **7**

Classical cryptographic primitives and protocols - Limitations of classical cryptography against quantum attacks - Introduction to quantum computing and its potential impact on cryptography

Module 2: Mathematical Background for Post-Quantum Cryptography **7**

Algebraic structures used in post-quantum cryptography: lattices, codes, multivariate polynomials, hash functions - Mathematical hardness assumptions underlying post-quantum cryptographic schemes

Module 3: Lattice-Based Cryptography 8

Basics of lattice-based cryptography - Lattice-based cryptographic primitives: Learning with Errors (LWE), ring-LWE - Lattice-based signature schemes and encryption schemes - Security analysis and parameter selection for lattice-based cryptography

Module 4: Code-Based Cryptography 8

Code-based cryptographic primitives: McEliece encryption, Niederreiter encryption, and code-based signature schemes - Security analysis and parameter selection for code-based cryptography

Module 5: Multivariate Polynomial Cryptography 7

Basics of multivariate polynomial cryptography - Multivariate polynomial signature schemes - Security of multivariate polynomial cryptographic schemes

Module 6: Hash-Based Signatures and Future Directions 8

Hash-based signature schemes and their security - Challenges and future directions in post-quantum cryptography - Real-world applications and implementations of post-quantum cryptographic systems.

TOTAL:45PERIODS

TEXT BOOKS:

1. Post-Quantum Cryptography: Third International Workshop, PQCrypto 2010" edited by Tanja Lange, Rachel Player, and Cristofaro Mune
2. Introduction to Modern Cryptography" by Jonathan Katz and Yehuda Lindell
3. "Introduction to Post-Quantum Cryptography" by Jintai Ding, Jason E. Gower, and Petros Wallden
4. "Post-Quantum Cryptography" by Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen
5. "Post-Quantum Cryptography: 10th International Conference, PQCrypto 2019" edited by Tanja Lange and Daniel J. Bernstein

REFERENCES:

1. Quantum Computing for Computer Scientists" by Noson S. Yanofsky and Mirco A. Mannucci
2. Cryptography and Network Security: Principles and Practice" by William Stallings
3. Public-Key Cryptography: Code Design for Code-B
4. Lattice-Based Cryptography: A Comprehensive Overview" edited by Vadim Lyubashevsky and Daniele Micciancio

5. Introduction to Coding Theory" by Ron Roth
6. The LLL Algorithm: Survey and Applications" by Phong Q. Nguyen and Brigitte Vallée
7. Cryptographic Aspects of Algebraic Lattices" by C. Gentry
8. Multivariate Public Key Cryptosystems" by Michael R. Garey, Joseph D. Murray, and David S. Johnson

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the threats posed by quantum computers to classical cryptographic algorithms. (K2)
2. Analyse and compare different post-quantum cryptographic approaches, including lattice-based, code-based, and multivariate polynomial cryptography. (K2)
3. Design and implement post-quantum cryptographic algorithms for encryption and digital signatures. (K3)
4. Evaluate the security of post-quantum cryptographic schemes against quantum attacks. (K3)
5. Discuss the potential applications and limitations of post-quantum cryptography. (K3)
6. Explore future directions and open problems in the field of post-quantum cryptography. (K2)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	3	3	1	1	1	-	1	-	1	-	2	2
CO2	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO3	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO4	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO5	3	3	3	3	3	1	1	1	2	3	1	-	2	2
CO6	3	3	2	3	3	2	-	-	-	-	-	-	1	1

PROFESSIONAL ELECTIVES - III

20SCEL703 SDG NO. 4	EMERGING TECHNOLOGIES AND POLICY IMPLICATIONS	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To introduce the fundamentals of cyber security, including threats, vulnerabilities, and legal aspects.
- To equip students with knowledge of cryptographic algorithms and network security techniques.
- To develop skills in secure coding practices and vulnerability assessment.
- To enable students to utilize advanced tools for penetration testing and digital forensics.
- To analyze emerging trends in cyber security and their policy implications.

Module 1: Fundamentals of Cyber Security **7**

Overview of Cyber Security: Definition, scope, and importance.-Threats and Attacks: Malware, phishing, denial-of-service, and insider threats - Legal and Regulatory Framework: Cyber laws, GDPR, and IT Act - Ethical Hacking and Penetration Testing Basics.

Module 2: Cryptographic Algorithms and Network Security **8**

Cryptography Fundamentals: Symmetric and asymmetric encryption - Key Management: Digital signatures and certificates - Network Security Protocols: SSL/TLS, VPNs, and firewalls - Intrusion Detection and Prevention Systems (IDPS).

Module 3: Software Security and Secure Coding Practices **7**

Secure Software Development Lifecycle (SDLC) - Common Vulnerabilities: Buffer overflows, SQL injection, and cross-site scripting - Secure Coding Guidelines: OWASP Top 10 - Static and Dynamic Application Security Testing (SAST/DAST).

Module 4: Cyber Security Tools and Forensic Investigations **8**

Cyber Security Tools: Kali Linux, Wireshark, Metasploit - Forensic Techniques: Data recovery, log analysis, and chain of custody - Case Studies: Real-world forensic investigations - Incident Response Frameworks.

Module 5: Emerging Trends in Cyber Security **8**

Artificial Intelligence and Machine Learning in Cyber Security - IoT Security Challenges and Solutions - Cloud Security: Models, risks, and mitigations - Blockchain and Zero Trust Architecture.

Module 6: Governance, Risk Management, and Compliance 7

Cyber Security Policies and Standards - Risk Assessment and Management Frameworks - Security Awareness and Training - Ethical Implications and Professional Responsibilities.

TOTAL:45 PERIODS

OUTCOMES:

Upon completion of the course, the student should be able to

1. Explain the fundamentals of cyber security and legal aspects.(K2)
2. Apply cryptographic algorithms and network security techniques.(K3)
3. Analyze software vulnerabilities and implement secure coding practices(K4)
4. Use cyber security tools for penetration testing and forensic investigations.(K3)
5. Evaluate trends like AI, IoT, and cloud security for future applications.(K4)
6. Formulate governance and ethical policies for secure organizational operations.(K4)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	2	2	2	3	3	2	1	2	2	3	2	3
CO2	3	3	3	2	3	2	2	2	2	3	2	3	3	3
CO3	3	3	3	3	3	2	2	2	2	3	3	3	3	3
CO4	2	3	3	3	3	2	2	2	2	3	2	3	3	3
CO5	3	3	3	3	3	3	3	3	2	3	2	3	3	3
CO6	3	3	3	3	3	3	3	3	3	3	3	3	3	3

PROFESSIONAL ELECTIVES - III

20SCEL704 SDG NO. 4	IT SECURITY COMPLIANCE AND DIGITAL FORENSICS	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To understand the current security landscape, including the nature of threat and vulnerabilities
- To justify the need for appropriate strategies and processes for disaster recovery and fault tolerance
- To Know about the emerging security solutions for Web and Email
- To assess the current information security compliance and network forensics security tools, evidence and investigations

Module 1: INFORMATION SECURITY FUNDAMENTALS 8

Importance of Computer and Network Security – Confidentiality – Integrity Availability- Accountability –Non- repudiation - Threats and Countermeasures- Policies and Standards – Authentication overview – Authentication credentials & protocols – Authentication services: LDAP, RADIUS, TACACS –Best practices for secure authentication – Authorization and access control models – Implementing access control on Windows and Unix

Module 2: NETWORK SECURITY 7

Best Practices for Network Security - Securing Network Transmission - Analyzing Security Requirements for Network Traffic- Defining Network Perimeters.

Module 3: SERVER SECURITY 7

Data Transmission Protection Protocols - Server Roles and Baselines - Securing Network Infrastructure Servers- Securing Domain Controllers - Securing File , Print and Application Servers.

Module 4: APPLICATION SECURITY AND DISASTER RECOVERY ASSURANCE 7

Web Browser Security - Email Security – Planning for the worst - Creating a Backup Strategy - Designing for Fault Tolerance.

Module 5: INFORMATION SECURITY COMPLIANCE 7

Develop an Information System Strategy - Integrate security into an organization – Security compliance management and auditing – Information security program metrics.

Module 6: FORENSICS AND SECURITY 9

Managing Updates - Auditing and Logging- Secure Remote Administration - Intrusion Detection - Honeypots – Forensics: Understanding Evidence - Gathering Evidence on a Live System - Preparing a Hard Drive Image - Searching for Data on a Hard Drive – Forensic Laboratories – Forensics Tools –Network Forensics : Network Security Tools – Incidence response – Network evidence and investigation.

TOTAL:45PERIODS

TEXT BOOKS:

1. Cole, Eric, Rachelle Reese, Ronald L. Krutz, and James Conley, "Network Security Fundamentals", United Kingdom: Wiley, John Sons, 2008. (ISBN No.:978- 0-470-10192-6).
2. Jason Andress, Mark Leary, "Building a Practical Information Security Program", Syngress Publication , 2017,

REFERENCES:

1. John Sommons, "The Basics of Digital Forensics - The Primer for Getting Started in Digital Forensics", Syngress Publication , 2012.
2. Joshi, James, Bruce S. Davie, and Saurabh Bagchi, "Network Security: Know It All" , United States: Morgan Kaufmann Publishers In, 2008.(ISBN No.: 978-0-12- 374463-0).
3. Ciampa, Mark. "Security Guide to Network Security Fundamentals". 4th edition, Boston, MA: Course Technology, Cengage Learning, 2011. (ISBN No. : 978-1-111- 64012-5)
4. Thomas R, "Information Security Fundamentals", 2nd edition, CRC Press. Boca Raton, FL: Auerbach Publications, 2014. (ISBN No.: 978-1- 4398-1063-7)
5. Vacca , John R . , e d . " Network and System Security " United States: Syngress Media, U.S., 2010. (ISBN No. : 978-1-59749-535-6).

OUTCOMES:

Upon completion of the course, the student should be able to

1. Remember various vulnerabilities of computer network systems, as well as the different modes of attack. (K1)
2. Understand design techniques to prevent security attacks. (K2)
3. Summarize about the emerging security solutions for Web and Email.(K2)
4. Apply and Build disaster recovery and fault tolerance systems.(K3)
5. Identify the need for information security compliance, forensics and security.(K3)
6. Understand Network Security Tools and Applications.(K2)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	1	0	0	0	0	0	0	0	0	0	1	2
CO2	3	3	3	1	2	0	0	0	0	0	0	0	1	2
CO3	3	3	3	3	3	0	0	0	0	0	0	0	2	2
CO4	3	3	3	2	3	0	0	0	0	0	0	1	3	3
CO5	3	3	3	3	3	0	0	0	0	0	2	1	3	3
CO6	3	3	3	3	3	2	1	2	2	0	2	2	3	3

PROFESSIONAL ELECTIVES - III

20SCEL705 SDG NO. 4&9	QUANTUM-SAFE NETWORK PROTOCOLS	L	T	P	C
		3	0	0	3

OBJECTIVES:

- Introduce students to the basics of quantum computing and its impact on network security.
- Analyze the vulnerabilities of classical cryptographic protocols to quantum attacks.
- Provide students with the knowledge and skills to implement quantum-safe cryptographic solutions for network protocols.
- Foster critical thinking regarding the development and adoption of quantum-safe network protocols.
- Promote interdisciplinary understanding of the convergence of quantum computing and network security.

Module 1: Introduction to Quantum-Safe Network Protocols 8

Overview of Classical Network Protocols and Security Challenges-Introduction to Quantum-Safe Cryptography-Quantum-Safe Network Protocols: Concepts and Requirements-Quantum-Safe Key Exchange Protocols-Quantum-Safe Authentication and Authorization Protocols

Module 2: Quantum-Safe Encryption and Hash Functions 7

Symmetric and Asymmetric Quantum-Safe Encryption Schemes-Quantum-Safe Hash Functions Quantum-Safe Secure Channels and Transport Layer Security (TLS)-Quantum-Safe VPN Protocols-Quantum-Safe Email and Messaging Protocols

Module 3: Quantum-Safe Routing Protocols 7

Challenges in Securing Network Routing in the Quantum Era-Quantum-Safe Routing Protocols for Internet and Intranets-Quantum-Safe Secure Multipath Routing-Quantum-Safe Routing in Wireless and Mobile Networks-Case Studies of Quantum-Safe Routing Implementations

Module 4: Quantum-Safe Security Mechanisms for Networked Systems 8

Quantum-Safe Intrusion Detection and Prevention Systems (IDPS)-Quantum-Safe Firewall and Access Control Mechanisms-Quantum-Safe Network Monitoring and Traffic Analysis-Quantum-Safe Distributed Denial of Service (DDoS) Mitigation-Quantum-Safe Network Forensics and Incident Response

Module 5: Advanced Quantum-Safe Network Protocols 7

Quantum-Safe Secure Multipath Routing (detailed exploration)-Quantum-Safe Secure Channels and Advanced VPN Protocols-Quantum-Safe Authentication in IoT and Mobile Networks-Quantum-Safe Data Integrity and Digital Signatures-Implementation Strategies for Quantum-Safe Networks

Module 6: Future Directions and Challenges in Quantum-Safe Networking 8

Emerging Trends in Quantum-Safe Network Protocols Research-Challenges in Implementing-Quantum-Safe Protocols in Real-World Networks-Regulatory and Standardization Efforts in Quantum-Safe Networking-Ethical and Policy Considerations in Quantum-Safe Networking-Opportunities and Future Directions in Quantum-Safe Networking

TOTAL:45 PERIODS

TEXT BOOKS:

1. "Quantum Computing for Computer Scientists" by Noson S. Yanofsky and Mirco A. Mannucci.
2. "Post-Quantum Cryptography" by Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen.
3. "Quantum Communication and Quantum Networking" by Mark M. Wilde.

Reference Book:

1. "Quantum Cryptography and Secret-Key Distillation" by Norbert Lütkenhaus.
2. NPTEL Link: Quantum Computing and Cryptography – NPTEL
3. Quantum-Safe Cryptography" by Bruce Schneier, Tanja Lange, and Daniel J. Bernstein.
4. NPTEL Link: Computer Networks - NPTEL

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the fundamental concepts of quantum computing and its implications for network security.(K2)
2. Analyze the vulnerabilities of classical cryptographic protocols to quantum attacks.(K2)
3. Identify the principles and components of quantum-safe cryptography. (K3)
4. Explore the challenges and opportunities in transitioning to quantum-safe network protocols.(K3)
5. Develop strategies for enhancing the security of network communication against quantum threats.(K3)
6. Collaborate effectively in interdisciplinary teams to address the intersection of quantum computing and network security.(K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	1	0	0	0	0	0	0	0	0	0	1	2
CO2	3	3	3	1	2	0	0	0	0	0	0	0	1	2
CO3	3	3	3	3	3	0	0	0	0	0	0	0	2	2
CO4	3	3	3	2	3	0	0	0	0	0	0	1	3	3
CO5	3	3	3	3	3	0	0	0	0	0	2	1	3	3
CO6	3	3	3	3	3	2	1	2	2	0	2	2	3	3

PROFESSIONAL ELECTIVES - III

20SCEL706 SDG NO. 4&9	MULTI-CORE ARCHITECTURES AND PROGRAMMING	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To understand the need for Multi-core processors and their architectures
- To understand the challenges in Parallel and Multi- threaded programming
- To learn about the various Parallel Programming paradigms
- To develop Multi-core programs and design parallel solutions

Module 1: MULTI-CORE PROCESSORS 8

Single core to Multi-core Architectures - SIMD and MIMD SystemsInterconnection Networks-Symmetric and Distributed Shared Memory Architectures- Cache Coherence - Performance Issues - Parallel Program Design.

Module 2: PARALLEL PROGRAM CHALLENGES 7

Performance - Scalability - Synchronization and Data Sharing – Data Races - Synchronization Primitives (Mutexes, Locks, Semaphores, Barriers).

Module 3: COMMUNICATION CHANNEL CHALLENGES 7

Deadlocks and LiveLocks - Communication between Threads (Condition Variables - Signals - Message Queues and Pipes).

Module 4: SHARED MEMORY PROGRAMMING WITH OpenMP 7

OpenMP Execution Model - Memory Model - OpenMP Directives - Work Sharing Constructs - Library functions - Handling Data and Functional Parallelism - Handling Loops - Performance Considerations

Module 5: DISTRIBUTED MEMORY PROGRAMMING WITH MPI 7

MPI Program Execution - MPI Constructs - Libraries - MPI Send and Receive - Point-to-Point and Collective Communication - MPI Derived Data Types - Performance Evaluation.

Module 6: PARALLEL PROGRAM DEVELOPMENT 9

Case studies - n-body Solvers - Tree Search - OpenMP and MPI Implementations and Comparison

TOTAL:45PERIODS

TEXT BOOKS:

1. Peter S. Pacheco, "An Introduction to Parallel Programming", MorganKauffman/Elsevier, 2011.
2. Darryl Gove, "Multicore Application Programming for Windows, Linux, and Oracle Solaris", Pearson, 2011 (Unit 2).

REFERENCES:

1. Michael J Quinn, "Parallel programming in C with MPI and OpenMP", Tata McGraw Hill, 2003.
2. Shameem Akhter and Jason Roberts, "Multi-core Programming", Intel Press, 2006.
3. Yan Solihin, "Fundamentals of Parallel Multicore Architecture" CRC press, 2015.
4. John L. Hennessey and David A. Patterson, " Computer Architecture – A Quantitative Approach", Morgan Kaufmann / Elsevier, 5th edition, 2012.
5. Richard Y. Kain, "Advanced Computer Architecture a Systems Design Approach", Prentice Hall, 2011.

WEB REFERENCES:

1. https://swayam.gov.in/nd1_noc19_cs45/preview

ONLINE RESOURCES:

1. https:// youtube.be/FauseE2FtUsY
2. https://slideplayer.com/slide/7106313/&9784375

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the basics of Multi-core Architectures. (K2)
2. Understand the challenges in Parallel and Multithreaded programming. (K2)
3. Explain about the various Parallel Programming paradigms and solutions.(K2)
4. Identify the issues in programming Parallel Processors.(K2)
5. Write programs using Openmp and MPI. (K3)
6. Compare and contrast programming for Serial Processors and programming for Parallel Processors.(K2)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	3	3	1	1	1	-	1	-	1	-	2	2
CO2	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO3	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO4	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO5	3	3	3	3	3	1	1	1	2	3	1	-	2	2
CO6	3	3	2	3	3	2	-	-	-	-	-	-	1	1

PROFESSIONAL ELECTIVES - III

20SCEL707 SDG NO. 4	WEB ANALYTICS	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To know the importance of qualitative data, get insights and techniques.
- To develop a customer-centric approach in dealing with data.
- To know the principles, tools and methods of web intelligence.
- To apply analytics for business situations.

Module 1: INTRODUCTION **8**

Web Analytics – Basics – Traditional Ways – Expectations – Data Collection – Click stream Data – Weblogs – Beacons – JavaScript Tags – Packet Sniffing – Outcomes data – Competitive data – Search Engine Data.

Module 2: STRATEGIES FOR ANALYTICS **7**

Qualitative Analysis – Customer Centricity – Site Visits – Surveys – Questionnaires – Website Surveys – Post visits – Creating and Running Benefits of surveys – Critical components of successful strategy.

Module 3: CONCEPTS OF WEB ANALYTICS **7**

Web Analytic concepts – URLS – Cookies – Time on site – Page views – Understand standard reports – Website content quality – Navigation reports (top pages, top destinations, site overlay).

Module 4: SEARCH OF WEB ANALYTICS 7

Search Analytics – Internal search, SEO and PPC – Measuring Email and Multichannel Marketing - Competitive intelligence and Web 2.0 Analytics – Segmentation – Connectable reports.

Module 5: GOOGLE ANALYTICS 8

Analytics - Cookies - Accounts vs Property - Tracking Code - Tracking Unique Visitors - Demographics - Page Views & Bounce Rate Acquisitions - Custom Reporting.

Module 6: ADVERTISING AND PROMOTION 8

Goals & Funnels – Filters - Ecommerce Tracking - Real Time Reports - Customer Data Alert - Adwords Linking - Adsense Linking -Attribution Modeling - Segmentation - Campaign Tracking - Multi-Channel Attribution.

TOTAL:45 PERIODS

TEXT BOOKS:

1. Avinash Kaushik, "Web Analytics 2.0: The Art of Online Accountability and Science Of Customer Centricity ", 1st edition, Sybex, 2009.
2. Jason Burby, Shane Atchison, Jim Sterne, "Actionable Web Analytics: Using Data to Make Smart Business Decisions", 1st edition, Sybex , 29 May 2007.

REFERENCES:

1. Michael Beasley, "Practical Web Analytics for User Experience: How Analytics can help you Understand your Users", Morgan Kaufmann, 2013.
2. Magy Seif El-Nasr, Anders Drachen, Alessandro Canossa, eds., "Game Analytics: Maximizing the Value of Player Data", Springer, 2013.
3. Bing Liu, "Web Data Mining: Exploring Hyperlinks, Content, and Usage Data", 2nd Edition, Springer, 2011.
4. Justin Cutroni, "Google Analytics", O'Reilly, 2010.
5. Eric Fettman, Shiraz Asif, FerasAlhlou , "Google Analytics Breakthrough", John Wiley & sons, 2016.

WEB REFERENCES:

1. https://www.simplilearn.com/web-analytics-guide-for-newbies-article
2. https://www.tutorialspoint.com/web_analytics/web_analytics_tutorial.pdf

ONLINE RESOURCES:

1 https://www.techtarget.com/searchbusinessanalytics/deinition/Webanalytics
2. https://www.optimizely.com/optimization-glossary/web-analytics/

OUTCOMES:

Upon completion of the course, the student should be able to

1. Know the concepts and terminologies related to web analytics. (K1)
2. Explore various parameters used for web analytics and their impact. (K3)
3. Explore the use of tools and techniques of web analytics. (K3)
4. Get experience on websites, web data insights and conversions. (K2)
5. Find out the applications of IoT in real time scenario.(K3)
6. List the quantifiable and measurable data of your website with the aim of understanding and optimizing the web usage.(K2)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	3	3	1	1	1	-	1	-	1	-	2	2
CO2	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO3	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO4	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO5	3	3	3	3	3	1	1	1	2	3	1	-	2	2
CO6	3	3	2	3	3	2	-	-	-	-	-	-	1	1

PROFESSIONAL ELECTIVES - III

20SCEL708 SDG NO. 4&9	QUANTUM SIDE-CHANNEL ATTACKS AND COUNTERMEASURES	L	T	P	C
		3	0	0	3

OBJECTIVES:

- Introduce students to the concepts and methodologies of side-channel attacks.
- Analyze the vulnerabilities of quantum systems to side-channel attacks.
- Provide students with a foundational understanding of quantum computing.
- Foster critical thinking regarding the development and adoption of countermeasures against side-channel attacks in quantum computing.

- Promote interdisciplinary understanding of the convergence of side-channel attacks and quantum computing.

Module 1: Introduction to Quantum Side-Channel Attacks 8

Overview of Side-Channel Attacks in Classical Cryptography - Introduction to Quantum Side-Channel Attacks - Quantum Physical Attacks: Photon Number Splitting, Time-Shift Quantum Information Leakage Channels - Case Studies of Quantum Side-Channel Attacks

Module 2: Quantum Side-Channel Analysis Fundamentals 7

Quantum Side-Channel Analysis Fundamentals - Information Theory and Quantum Leakage Metrics - Quantum Side-Channel Measurement Models - Quantum Leakage Detection and Measurement Techniques - Statistical Methods for Quantum Side-Channel Analysis

Module 3: Quantum Side-Channel Attacks on Cryptographic Systems 8

Quantum Side-Channel Attacks on Quantum Key Distribution (QKD) - Quantum Side-Channel Attacks on Quantum Cryptographic Protocols - Quantum Side-Channel Attacks on Quantum Computing Implementations - Quantum Side-Channel Attacks on Post-Quantum Cryptographic Schemes - Evaluating Vulnerabilities in Quantum Cryptographic Implementations

Module 4: Countermeasures against Quantum Side-Channel Attacks 7

Quantum Countermeasures Design Principles - Quantum Secure Implementation Techniques - Quantum Leakage Reduction Strategies - Hardware and Software Countermeasures for Quantum Systems - Evaluation and Testing of Quantum Side-Channel Countermeasures

Module 5: Emerging Trends in Quantum Side-Channel Attacks 7

Emerging Quantum Side-Channel Attack Techniques - Open Problems and Research Challenges in Quantum Side-Channel Analysis - Quantum Side-Channel Attack Defense Strategies - Ethical and Policy Considerations in Quantum Side-Channel Attacks

Module 6: Future Directions and Opportunities in Quantum Security 8

Future Directions and Opportunities in Quantum Security - Integration of Quantum Side-Channel Security with Post-Quantum Cryptography - The Role

of Quantum Side-Channel Attacks in Quantum System Design - Collaboration between Research and Industry in Quantum Side-Channel Security - Long-Term Challenges and Future Research Directions

TOTAL: 45 PERIODS

TEXT BOOKS:

1. "Introduction to Side-Channel Attacks" by Stefan Mangard, Elisabeth Oswald, and Thomas Popp.
2. "Quantum Computing for Computer Scientists" by Noson S. Yanofsky and Mirco A. Mannucci.
3. Quantum Communication and Quantum Networking" by Mark M. Wilde.
4. "Post-Quantum Cryptography" by Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen.
5. "Quantum Computing: A Gentle Introduction" by Eleanor G. Rieffel and Wolfgang H. Polak.

REFERENCE BOOKS:

1. "Quantum Information and Quantum Computing" by Mikio Nakahara and Tetsuo Ohmi.
2. NPTEL Link: Quantum Computing and Cryptography - NPTEL

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the fundamentals of side-channel attacks and their relevance to quantum computing. (K1)
2. Analyze the vulnerabilities of quantum systems to side-channel attacks. (K2)
3. Identify the basic principles and components of quantum computing. (K3)
4. Explore the challenges and opportunities in addressing side-channel attacks in quantum systems. (K2)
5. Develop strategies for mitigating side-channel attacks in quantum computing environments. (K3)
6. Collaborate effectively in interdisciplinary teams to address the intersection of side-channel attacks and quantum computing. (K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	1	0	0	0	0	0	0	0	0	0	1	2
CO2	3	3	3	1	2	0	0	0	0	0	0	0	1	2
CO3	3	3	3	3	3	0	0	0	0	0	0	0	2	2
CO4	3	3	3	2	3	0	0	0	0	0	0	1	3	3
CO5	3	3	3	3	3	0	0	0	0	0	2	1	3	3
CO6	3	3	3	3	3	2	1	2	2	0	2	2	3	3

PROFESSIONAL ELECTIVES - III

20SCEL709 SDG NO. 4&9	NATIONAL SECURITY AND CYBER SECURITY	L	T	P	C
		3	0	0	3

OBJECTIVES:

- Understand the basics of cyber security and its importance in the modern world.
- Learn and apply various cryptographic and network security techniques.
- Analyze software vulnerabilities and ensure secure software development.
- Explore advanced cyber security tools and techniques for practical applications
- Develop comprehensive governance and ethical policies in cyber security.

Module 1: Fundamentals of Cyber Security 8

Introduction to Cyber Security - Cyber Threats and Vulnerabilities - Cyber Security Principles and Frameworks - Legal and Ethical Aspects of Cyber Security

Module 2: Cryptography and Network Security 8

Basics of Cryptography - Cryptographic Algorithms - Network Security Protocols - Security in Wireless Networks

Module 3: Secure Software Development 7

Software Vulnerabilities and Secure Coding Practices - Secure Software Development Life Cycle (SDLC) - Penetration Testing - Forensic Investigations

Module 4: Advanced Topics in Cyber Security 7

Emerging Trends: AI, IoT, Cloud Security - Cyber Security Challenges in Emerging Technologies - Case Studies on Recent Cyber Security Incidents

Module 5: Cyber Security Governance and Policies 8

Governance Models in Cyber Security - Development of Cyber Security Policies - Ethical and Legal Considerations - International Cyber Security Policies

Module 6: Data Protection and Privacy 7

Data Protection Laws and Regulations - Privacy by Design - Data Breaches and Incident Response - Cyber Security in Data Governance

TOTAL:45PERIODS

TEXT BOOKS:

1. "Cyber Security Essentials" by James Graham, Richard Howard, Ryan Olson, CRC Press, 2011.
2. "Network Security Essentials" by William Stallings, Pearson, 2017.

Reference Books

1. "Principles of Information Security" by Michael E. Whitman, Herbert J. Mattord, Cengage Learning, 2018.
2. "Computer Security: Principles and Practice" by William Stallings, Lawrie Brown, Pearson, 2018.

OUTCOMES:

Upon completion of the course, the student should be able to

1. Explain the fundamentals of cyber security and legal aspects. (K2)
2. Apply cryptographic algorithms and network security techniques. (K3)
3. Analyze software vulnerabilities and implement secure coding practices. (K4)
4. Use cyber security tools for penetration testing and forensic investigations. (K3)
5. Evaluate trends like AI, IoT, and cloud security for future applications. (K4)
6. Formulate governance and ethical policies for secure organizational operations. (K4)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	1	0	0	0	0	0	0	0	0	0	1	2
CO2	3	3	3	1	2	0	0	0	0	0	0	0	1	2
CO3	3	3	3	3	3	0	0	0	0	0	0	0	2	2
CO4	3	3	3	2	3	0	0	0	0	0	0	1	3	3
CO5	3	3	3	3	3	0	0	0	0	0	2	1	3	3
CO6	3	3	3	3	3	2	1	2	2	0	2	2	3	3

PROFESSIONAL ELECTIVES - III

20SCEL710 SDG NO. 4&9	QUANTUM MACHINE LEARNING	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To provide students with a comprehensive understanding of quantum computing principles and their relevance to machine learning.
- To introduce students to advanced concepts in quantum data encoding, feature mapping, and variational quantum algorithms.
- To enable students to design and implement quantum machine learning models and algorithms for various tasks.
- To explore the potential applications of quantum machine learning in diverse fields and address ethical considerations.
- To foster critical thinking and problem-solving skills in the context of quantum machine learning research and applications.

Module 1: Introduction to Quantum Computing and Machine Learning **8**

Introduction to Classical Machine Learning Algorithms - Basic Concepts of Quantum Computing and Qubits - Quantum Parallelism and Superposition - Quantum Gates and Circuits - Overview of Quantum Machine Learning Algorithms

Module 2: Quantum Data Encoding and Feature Mapping 8

Encoding Classical Data into Quantum States - Quantum Feature Mapping Techniques - Quantum Kernel Methods for Classification and Regression - Quantum Data Encoding for Unsupervised Learning Tasks - Quantum-Enhanced Feature Extraction and Dimensionality Reduction

Module 3: Quantum Variational Algorithms 8

Variational Quantum Algorithms and Optimization - Quantum Circuit Learning and Parameterized Quantum Circuits (PQCs) - Quantum Approximate Optimization Algorithms (QAOA) - Quantum Generative Models and Variational Autoencoders - Training Quantum Models Using Gradient-Based Optimization Techniques

Module 4: Quantum Neural Networks and Quantum Support Vector Machines 9

Quantum Neural Network Architectures and Training Algorithms - Quantum Convolutional Neural Networks (QCNNs) and Quantum Gates in Neural Networks - Quantum Support Vector Machines (QSVMs) and Quantum Kernel Methods - Quantum-Enhanced Reinforcement Learning Algorithms - Applications of Quantum Neural Networks in Pattern Recognition and Optimization Problems

Module 5: Quantum Machine Learning Applications 6

Quantum Machine Learning Applications in Chemistry, Finance, and Optimization - Quantum Machine Learning for Big Data Analytics and Quantum-Enhanced Simulations

Module 6: Future Directions in Quantum Machine Learning 6

Ethical Considerations and Societal Implications of Quantum Machine Learning - Future Directions and Challenges in Quantum Machine Learning Research

TOTAL:45 PERIODS

TEXT BOOKS:

1. "Quantum Machine Learning: What Quantum Computing Means to Data Mining" by Peter Wittek.
2. "Quantum Computing: An Applied Approach" by Jack D. Hidary.

REFERENCE BOOKS:

1. "Quantum Computing for Computer Scientists" by Noson S. Yanofsky and Mirco A. Mannucci.
2. "Machine Learning: A Probabilistic Perspective" by Kevin P. Murphy.

NPTEL LINK:

1. Quantum Computing for Engineers

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the principles of quantum computing and its application to machine learning tasks. (K2)
2. Apply quantum data encoding techniques and feature mapping methods for classical data sets. (K1)
3. Design and implement variational quantum algorithms for optimization and generative modeling tasks. (K2)
4. Develop and train quantum neural networks and support vector machines for classification and regression tasks. (K2)
5. Analyze and evaluate the potential applications and societal impacts of quantum machine learning technology. (K3)
6. Collaborate effectively and communicate ideas related to quantum machine learning in interdisciplinary contexts. (K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	1	0	0	0	0	0	0	0	0	0	1	2
CO2	3	3	3	1	2	0	0	0	0	0	0	0	1	2
CO3	3	3	3	3	3	0	0	0	0	0	0	0	2	2
CO4	3	3	3	2	3	0	0	0	0	0	0	1	3	3
CO5	3	3	3	3	3	0	0	0	0	0	2	1	3	3
CO6	3	3	3	3	3	2	1	2	2	0	2	2	3	3

PROFESSIONAL ELECTIVES - IV

20CSEL801 SDG NO. 4	CYBER SECURITY POLICY AND STRATEGY	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To provide a comprehensive understanding of cyber security concepts, challenges, and strategies.
- To analyze the legal foundations governing cyber activities, including cyber crime, data protection, and intellectual property laws.
- To develop the skills necessary for formulating, implementing, and evaluating effective cyber security policies.
- To explore the legal aspects of incident response, digital forensics, and the admissibility of digital evidence.
- To examine emerging trends, future challenges, and ethical considerations in the context of cyber security policy.

Module 1: Introduction to Cyber Security 8

Overview of Cyber Security: Concepts, threats, and challenges—Historical development of cyber security policies—Role of governments, private sector, and individuals in cyber security

Module 2: National and International Cyber Security Strategies 8

Introduction to national and international cyber security strategies—Integration of cyber security in global frameworks—Role of international collaborations in strengthening cyber security

Module 3: Legal and Regulatory Foundations of Cyber Security 8

Cybercrime laws and regulations—Data protection and privacy laws—Intellectual property laws in the context of cyber security—International legal frameworks for cyber activities

Module 4: Policy Development and Risk Management 7

Process of developing cyber security policies—Implementation strategies for cyber security policies—Regulatory compliance and standards—Risk management in policy formulation

Module 5: Incident Response and Digital Forensics 7

Legal aspects of incident response—Digital forensics procedures and methodologies—Admissibility of digital evidence in legal proceedings—Case studies and real-world examples

Module 6: Emerging Trends and Future Challenges in Cyber Security **7**

Policy implications of emerging technologies (AI, IoT, blockchain)—Future challenges in cyber security—Ethical considerations in cyber security policy—Continuous learning and adaptation in the cyber security landscape

TOTAL:45 PERIODS

TEXT BOOKS:

1. "Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions" by Omar Santos and Ron Taylor.

Reference Book:

1. "Cybersecurity Policy Guidebook" by Jennifer L. Bayuk, Jason Healey, Paul Rohmeyer, Marcus H. Sachs, Jeffrey Schmidt.
2. NPTEL Cybersecurity Policy and Strategy Course

OUTCOMES:

Upon completion of the course, the student should be able to

1. Develop awareness of ethical considerations in combating cybercrime. (K2)
2. Understand the structure and components of cybercrime legislation.(K3)
3. Identify challenges in prosecuting cybercriminals.(K2)
4. Analyze privacy considerations in the context of cybercrime legislation.(K2)
5. Analyze legal challenges posed by emerging technologies in the context of cybercrime.(K1)
6. Evaluate the role of international cooperation in adapting legislation to new threats.(K2)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	1	0	0	0	0	0	0	0	0	0	1	2
CO2	3	3	3	1	2	0	0	0	0	0	0	0	1	2
CO3	3	3	3	3	3	0	0	0	0	0	0	0	2	2
CO4	3	3	3	2	3	0	0	0	0	0	0	1	3	3
CO5	3	3	3	3	3	0	0	0	0	0	2	1	3	3
CO6	3	3	3	3	3	2	1	2	2	0	2	2	3	3

PROFESSIONAL ELECTIVES - IV

20CSEL802 SDG NO. 4&9	QUANTUM AUTHENTICATION	L	T	P	C
		3	0	0	3

OBJECTIVES:

- Introduce students to the basic concepts of quantum computing and its impact on authentication.
- Analyze the vulnerabilities of classical authentication schemes to quantum attacks.
- Provide students with the knowledge and skills to implement quantum-safe authentication solutions.
- Foster critical thinking regarding the development and adoption of quantum-safe authentication methods.
- Promote interdisciplinary understanding of the convergence of quantum computing and authentication.

MODULE 1: INTRODUCTION TO QUANTUM AUTHENTICATION 9

Overview of Authentication in Classical Cryptography-Introduction to Quantum Computing and Quantum Information Theory-Authentication Requirements and Challenges in Quantum Communication-Quantum Authentication Schemes: Overview and Classification-Applications of Quantum Authentication in Secure Communication

MODULE- 2: QUANTUM KEY DISTRIBUTION (QKD) FOR AUTHENTICATION 9

Principles of Quantum Key Distribution (QKD)-Quantum Authentication Protocols Based on QKD-Security Analysis of QKD-Based Authentication Schemes- Experimental Realizations of QKD-Based Authentication Systems-Quantum Key Authentication vs. Classical Key Authentication

MODULE - 3: QUANTUM CRYPTOGRAPHY FOR AUTHENTICATION 9

Overview of Quantum Cryptography Techniques-Quantum Digital Signatures for Authentication-Quantum One-Time Passwords (QOTP)-Quantum Authentication Tokens and Smart Cards-Quantum Authentication Using Entangled States

MODULE - 4: QUANTUM AUTHENTICATION PROTOCOLS 9

BB84 Protocol and its Variants for Authentication-E91 Protocol for Quantum Authentication-B92 Protocol and its Application in Quantum Authentication-Quantum Authentication with Continuous Variable QKD-Quantum Authentication in Practical Scenarios

MODULE - 5: FUTURE DIRECTIONS AND CHALLENGES 9

Emerging Trends in Quantum Authentication Research-Challenges in Implementing Quantum Authentication Schemes-Quantum Authentication in the Post-Quantum Era-Ethical and Policy Considerations in Quantum Authentication

MODULE - 6: Applications of Quantum Authentication in Secure Communication 9

Introduction to Secure Communication - Classical vs. Quantum Authentication - OpportModuleies and Future Directions in Quantum Authentication - Integration with Existing Systems - Future Prospects

TOTAL:45 PERIODS

TEXT BOOKS:

1. "Quantum Computing for Computer Scientists" by Noson S. Yanofsky and Mirco A. Mannucci.
2. "Quantum-Safe Cryptography" by Bruce Schneier, Tanja Lange, and Daniel J. Bernstein.
3. "Post-Quantum Cryptography" by Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen.
4. "Quantum-Safe Cryptography" by Mark M. Wilde.

REFERENCE BOOK:

1. "Quantum Cryptography and Secret-Key Distillation" by Norbert Lütkenhaus.
2. NPTEL Link: Quantum Computing and Cryptography - NPTEL
3. "Quantum Information and Communication" by Stephen M. Barnett and Paul M. Radmore.

NPTEL LINK:

1. Cryptography and Network Security - NPTEL

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the fundamental principles of quantum computing and its relevance to authentication. (K2)
2. Analyze the vulnerabilities of classical authentication schemes to quantum attacks. (K2)
3. Identify the principles and components of quantum key distribution for secure authentication. (K3)

4. Explore the challenges and opportModuleies in transitioning to quantum-safe authentication methods. (K2)
5. Develop strategies for enhancing the security of authentication systems against quantum threats. (K3)
6. Collaborate effectively in interdisciplinary teams to address the intersection of quantum computing and authentication. (K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	1	0	0	0	0	0	0	0	0	0	1	2
CO2	3	3	3	1	2	0	0	0	0	0	0	0	1	2
CO3	3	3	3	3	3	0	0	0	0	0	0	0	2	2
CO4	3	3	3	2	3	0	0	0	0	0	0	1	3	3
CO5	3	3	3	3	3	0	0	0	0	0	2	1	3	3
CO6	3	3	3	3	3	2	1	2	2	0	2	2	3	3

PROFESSIONAL ELECTIVES - IV

20CSEL803 SDG NO. 4&9	QUANTUM CYBER-PHYSICAL SYSTEMS SECURITY	L	T	P	C
		3	0	0	3

OBJECTIVES:

- Introduce students to the basic concepts of quantum computing and its impact on CPS security.
- Analyze the vulnerabilities of classical CPS security mechanisms to quantum attacks.
- Provide students with an understanding of the components and challenges of cyber-physical systems.
- Foster critical thinking regarding the development and adoption of quantum-secure CPS security solutions.
- Promote interdisciplinary understanding of the convergence of quantum computing and CPS security.

MODULE 1: INTRODUCTION TO QUANTUM CYBER-PHYSICAL SYSTEMS (QCPS) 9

Overview of Cyber-Physical Systems (CPS) - Security Challenges-Introduction to Quantum Computing and Quantum Information Science-Integration of Quantum Technologies into Cyber-Physical Systems Applications

MODULE 2: QUANTUM THREATS TO CYBER-PHYSICAL SYSTEMS 9

Threat Landscape of Quantum Cyber-Physical Systems-Quantum Vulnerabilities in Critical Infrastructure-Quantum Attacks on CPS Components: Sensors, Actuators, Controllers-Quantum Communication and Control Vulnerabilities Case Studies of Quantum Attacks on Cyber-Physical Systems

MODULE 3: QUANTUM SECURITY PROTOCOLS FOR CYBER-PHYSICAL SYSTEMS 9

Introduction to Quantum Cryptography and Key Distribution-Quantum Authentication and Authorization Protocols- Quantum Secure Communication Channels in CPS-Quantum Secure Multi-Party Computation in CPS-Quantum Resilience and Recovery Mechanisms for CPS

MODULE 4: QUANTUM RESILIENCE FOR CYBER- PHYSICAL SYSTEMS 9

Quantum Resilient Architectures for CPS-Quantum Intrusion Detection and Prevention Systems (IDPS)-Quantum Secure Control and Monitoring Systems - Use Cases of Quantum Cyber-Physical Systems-Security Implications of Quantum Technologies in CPS

MODULE 5: DEFENSE MECHANISMS FOR CYBER- PHYSICAL SYSTEMS 9

Quantum Secure Firmware and Software Updates-Quantum Incident Response and Recovery Planning for CPS - Emerging Trends in Quantum Cyber-Physical Systems Security

MODULE 6: FUTURE DIRECTIONS AND CHALLENGES 9

Challenges in Implementing Quantum Security Solutions in CPS-Ethical and Policy - Considerations in Quantum CPS Security-Regulatory Frameworks and Standards for Quantum CPS Security-Research Opport Moduleies and Future Directions in Quantum CPS Security

TOTAL:45 PERIODS

TEXT BOOKS:

1. "Quantum Computing for Computer Scientists" by Noson S. Yanofsky and Mirco A. Mannucci.
2. "Cyber-Physical Systems: From Theory to Practice" by Raj Rajkumar, Dionisio de Niz, and Borzoo Bonakdarpour.
3. "Quantum Communication and Quantum Networking" by Mark M. Wilde.

4. "Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications" by Houbing Song, Glenn A. Fink, and Sabina Jeschke
5. Quantum Cybersecurity: Threats and Countermeasures" by Vladimir Akis, Pavel Lougovski, and Joshua G

REFERENCE BOOK:

1. "Quantum Cybersecurity: Threats and Countermeasures" by Vladimir Akis, Pavel Lougovski, and Joshua Gessin.
2. NPTEL Link: Quantum Computing and Cryptography – NPTEL
3. "Introduction to Modern Cryptography" by Jonathan Katz and Yehuda Lindell.
4. NPTEL Link: Computer Science and Engineering - NPTEL

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the fundamental principles of quantum computing and its relevance to CPS security. (K2)
2. Analyze the vulnerabilities of classical CPS security mechanisms to quantum attacks. (K2)
3. Identify the components and challenges of cyber-physical systems. (K3)
4. Explore the challenges and opportModuleies in achieving quantum-secure CPS security. (K3)
5. Develop strategies for enhancing the security and resilience of CPS against quantum threats. (K3)
6. Collaborate effectively in interdisciplinary teams to address the intersection of quantum computing and CPS security. (K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	1	0	0	0	0	0	0	0	0	0	1	2
CO2	3	3	3	1	2	0	0	0	0	0	0	0	1	2
CO3	3	3	3	3	3	0	0	0	0	0	0	0	2	2
CO4	3	3	3	2	3	0	0	0	0	0	0	1	3	3
CO5	3	3	3	3	3	0	0	0	0	0	2	1	3	3
CO6	3	3	3	3	3	2	1	2	2	0	2	2	3	3

PROFESSIONAL ELECTIVES - IV

20CSEL804 SDG NO. 4	CYBERCRIME LEGISLATION	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To provide a comprehensive understanding of various types and forms of cybercrime.
- To analyze national and international cybercrime laws and regulatory frameworks.
- To develop skills in handling digital evidence and utilizing digital forensics in cybercrime cases.
- To understand the importance of international cooperation and mutual legal assistance in combating cybercrime.
- To explore emerging trends and future directions in cybercrime and prepare for proactive strategies.

Module 1: Introduction to Cybercrime 8

Definition and types of cybercrime - Historical context and evolution of cyber threats - Impact of cybercrime on individuals, organizations, and nations - Overview of relevant international conventions and agreements

Module 2: Cybercrime Legislation and Regulatory Frameworks 8

Examination of national and international cybercrime laws - Comparative analysis of regulatory frameworks - Jurisdictional challenges in prosecuting cybercriminals - Role of law enforcement agencies in combating cybercrime

Module 3: Investigation and Prosecution 8

Role of law enforcement agencies in cybercrime investigations - Digital evidence collection and preservation - Challenges in prosecuting cybercriminals - Case studies of successful cybercrime investigations

Module 4: Emerging Trends in Cybercrime 7

Emerging trends in cybercrime - Challenges in keeping up with evolving cyber threats - Jurisdictional issues in prosecuting cybercriminals - Collaboration between countries in combating cybercrime

Module 5: Ethical Implications of Cybercrime 7

Ethical considerations in combating cybercrime - Human rights implications of cybercrime legislation - Public perception and awareness of cybercrime laws

Module 6: Legal Challenges and Balancing Rights 7

Legal challenges in balancing cybersecurity and individual rights - The evolving nature of cybercrime laws - Strategies for promoting public awareness and compliance - Collaborative approaches to strengthening legal frameworks

TOTAL:45 PERIODS

TEXT BOOKS:

1. Cybercrime: An Introduction" by Robert Moore.

Reference Book:

1. "Computer Crime, Investigation, and the Law" by Chuck Easttom.
2. Cybercrime and Digital Forensics: An Introduction" by Thomas Holt and Adam Bossler.

NPTEL Course Link:

1. NPTEL Cybercrime Legislation Course

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the various types and historical evolution of cybercrime.(K1)
2. Analyze and compare national and international legal frameworks for combating cybercrime.(K2)
3. Develop skills related to the investigation and prosecution of cybercrime cases.(K3)
4. Evaluate challenges and emerging trends in the field of cybercrime.(K3)
5. Assess ethical and legal implications of cybercrime legislation.(K2)
6. Relate the course content to Sustainable Development Goal 16 and, where applicable, Goal 17. (K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	1	0	0	0	0	0	0	0	0	0	1	2
CO2	3	3	3	1	2	0	0	0	0	0	0	0	1	2
CO3	3	3	3	3	3	0	0	0	0	0	0	0	2	2
CO4	3	3	3	2	3	0	0	0	0	0	0	1	3	3
CO5	3	3	3	3	3	0	0	0	0	0	2	1	3	3
CO6	3	3	3	3	3	2	1	2	2	0	2	2	3	3

PROFESSIONAL ELECTIVES - IV

20CSEL805 SDG NO. 4	REGULATORY COMPLIANCE	L	T	P	C
		3	0	0	3

OBJECTIVES:

- Provide a comprehensive understanding of regulatory compliance principles and practices.
- Analyze the impact of industry-specific regulations on business operations and innovation.
- Equip students with the knowledge of international and industry-specific standards and frameworks.
- Develop skills in risk management and aligning strategies with regulatory requirements.
- Foster an understanding of the evolving regulatory landscape and strategies for continuous improvement.

Module 1: Introduction to Regulatory Compliance 8

Definition and importance of regulatory compliance-Overview of regulatory bodies and frameworks-Role of compliance in various industries-Legal and ethical considerations in regulatory compliance

Module 2: Industry-Specific Regulations 7

In-depth study of regulations in specific industries (e.g., finance, healthcare, telecommunications)-Compliance challenges and best practices in industry-specific contexts-Regulatory impact on business operations and innovation

Module 3: Standards and Frameworks 8

Overview of international and industry-specific standards-Adoption of frameworks such as ISO 27001, NIST, and others-Integration of standards into organizational processes-Compliance audits and assessments

Module 4: Risk Management 7

Identification and assessment of compliance risks-Strategies for managing and mitigating compliance risks-Compliance risk monitoring and reporting-Aligning risk management with regulatory requirements

Module 5: Regulatory Compliance 7

Partnerships for the Goals-Linking compliance efforts with sustainability goals - Monitoring changes in regulatory requirements

Module 6: Evolving Regulatory Landscape and Future Trends 8

Anticipating and adapting to future regulatory trends-Impact of emerging technologies on regulatory compliance-Continuous improvement in compliance programs - Case studies of regulatory compliance in different sectors

TOTAL:45 PERIODS

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the fundamentals and importance of regulatory compliance. (K2)
2. Analyze industry-specific regulations and their impact on various sectors.(K3)
3. Evaluate the role of standards and frameworks in achieving regulatory compliance.(K3)
4. Develop skills in identifying, assessing, and managing compliance risks.(K2)
5. Anticipate and adapt to changes in the regulatory landscape.(K2)
6. Relate the course content to Sustainable Development Goals, focusing on peace, justice, partnerships, industry, innovation, and infrastructure.(K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	1	0	0	0	0	0	0	0	0	0	1	2
CO2	3	3	3	1	2	0	0	0	0	0	0	0	1	2
CO3	3	3	3	3	3	0	0	0	0	0	0	0	2	2
CO4	3	3	3	2	3	0	0	0	0	0	0	1	3	3
CO5	3	3	3	3	3	0	0	0	0	0	2	1	3	3
CO6	3	3	3	3	3	2	1	2	2	0	2	2	3	3

PROFESSIONAL ELECTIVES - IV

20CSEL806 SDG NO. 3,4,11	RISK MANAGEMENT AND LIABILITY	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To introduce students to the concept of risk management and its significance in various industries.
- To familiarize students with techniques for identifying, analyzing, and prioritizing risks.
- To equip students with strategies for mitigating risks and minimizing liability.
- To enable students to evaluate and improve risk management processes.
- To discuss legal and ethical issues related to risk management and liability.

Module 1: Introduction to Risk Management and Liability 8

Understanding risk and liability-Historical perspective and evolution of risk management-Types of risks: financial, operational, strategic, compliance-Legal aspects of liability and negligence-Risk assessment methodologies

Module 2: Risk Identification and Analysis

Techniques for identifying and categorizing risks-Risk analysis tools: probability, impact assessment, risk matrix, fault tree analysis-Risk register and documentation-Case studies and practical exercises

Module 3: Risk Mitigation and Control 8

Strategies for risk mitigation: risk avoidance, risk reduction, risk transfer, risk acceptance-Control measures and contingency planning-Insurance and other risk financing techniques

Module 4: Monitoring and Evaluation of Risks 8

Establishing key performance indicators (KPIs) for risk management-Risk monitoring tools and techniques-Evaluating the effectiveness of risk management strategies

Module 5: Legal Aspects of Risk Management 7

Legal frameworks governing risk management and liability-Contractual risk allocation and indemnification clauses - Role of regulations and standards in risk management

Module 6: Ethical Considerations and Corporate Responsibility 7

Ethical dilemmas in risk management-Corporate social responsibility (CSR) and risk management -Continual improvement in risk management processes

TOTAL:45 PERIODS

TEXT BOOKS:

1. "Principles of Risk Management and Insurance" by George E. Rejda and Michael McNamara
2. "Risk Management: Concepts and Guidance" by Carl L. Pritchard
3. "Legal Aspects of Risk Management" by Donald J. Weidner and David W. Case

Reference Books:

1. "Enterprise Risk Management: From Incentives to Controls" by James Lam
2. "Risk Management and Financial Institutions" by John C. Hull
3. "The Handbook of Insurance-linked Securities" edited by Pauline Barrieu and Luca Albertini

NPTEL Web Links:

NPTEL - Risk Management Course

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the fundamental concepts and principles of risk management and liability. (K1)
2. Identify and analyze various types of risks affecting organizations.(K2)
3. Develop strategies for mitigating and controlling risks.(K3)
4. Evaluate the effectiveness of risk management measures.(K3)
5. Analyze legal frameworks and ethical considerations in risk management.(K2)
6. Apply sustainable development principles to enhance risk management practices(K1)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	1	0	0	0	0	0	0	0	0	0	1	2
CO2	3	3	3	1	2	0	0	0	0	0	0	0	1	2
CO3	3	3	3	3	3	0	0	0	0	0	0	0	2	2
CO4	3	3	3	2	3	0	0	0	0	0	0	1	3	3
CO5	3	3	3	3	3	0	0	0	0	0	2	1	3	3
CO6	3	3	3	3	3	2	1	2	2	0	2	2	3	3

PROFESSIONAL ELECTIVES - IV

20CSEL802 SDG NO. 4,9&11	VIRTUAL AND AUGMENTED REALITY	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To introduce students to the concepts and challenges of national security and cyber security.
- To familiarize students with cyber threats and vulnerability assessment techniques.
- To equip students with defensive cyber security strategies and technologies.
- To enable students to understand cyber security policy and governance frameworks.
- To discuss the importance of international cooperation and diplomacy in cyber security.

Module 1: Introduction to Virtual and Augmented Reality in Cyber Security 7

Fundamentals of Virtual Reality (VR) and Augmented Reality (AR) - Overview of Cyber Security Challenges in Virtual Environments - Key Components of VR and AR Systems - Legal and Ethical Considerations in VR/AR Cyber Security

Module 2: Cryptography and Secure Communication in VR/AR Systems 8

Cryptographic Algorithms for VR/AR Applications - Secure Data Transmission in Virtual Environments - Key Management in AR Systems - Case Studies: Cryptographic Breaches in VR/AR

Module 3: Identifying and Mitigating Vulnerabilities in VR/AR Software **7**

Common Vulnerabilities in VR/AR Platforms - Secure Coding Practices for VR/AR Development - Vulnerability Assessment Tools - Software Patching and Updates

Module 4: Penetration Testing and Forensics in VR/AR Environments **8**

Introduction to Penetration Testing in VR/AR - Tools for VR/AR Forensic Investigations - Investigating Cyber Attacks in VR Systems - Practical Lab: Simulated Penetration Testing in AR

Module 5: Future Trends in Cyber Security for VR/AR **7**

Role of Artificial Intelligence in VR/AR Security - Securing IoT Devices in AR Systems - Cloud-Based VR/AR Platforms: Risks and Mitigation - Emerging Threats in VR/AR

Module 6: Governance, Policies, and Sustainable Practices in VR/AR Security **8**

Cyber Security Governance for Organizations - Developing Ethical Policies for VR/AR Systems - Sustainable Development Goals (SDGs) and VR/AR Security - Case Study: Sustainable Practices in VR Security

TOTAL:45PERIODS

TEXT BOOKS:

1. Burdea, G., & Coiffet, P. (2017). Virtual Reality Technology (3rd Edition). Wiley.
2. Stallings, W. (2020). Cryptography and Network Security: Principles and Practice (7th Edition). Pearson.

Reference Books

1. Bishop, M. (2018). Computer Security: Art and Science (2nd Edition). Addison-Wesley.
2. Craig, A. B. (2013). Understanding Augmented Reality: Concepts and Applications. Morgan Kaufmann.

NPTEL Resources

1. Cyber Security: NPTEL Web Link
2. Augmented Reality and Virtual Reality: NPTEL Web Link

OUTCOMES:

Upon completion of the course, the student should be able to

1. Explain the fundamentals of cyber security and legal aspects. K2
2. Apply cryptographic algorithms and network security techniques. K3
3. Analyze software vulnerabilities and implement secure coding practices. K4
4. Use cyber security tools for penetration testing and forensic investigations. K3
5. Evaluate trends like AI, IoT, and cloud security for future applications. K4
6. Formulate governance and ethical policies for secure organizational operations. K4

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	2	2	1	1	2	2	2	2	1	3	3	2
CO2	3	3	3	2	3	1	2	2	2	2	1	3	3	3
CO3	3	3	3	3	2	1	2	3	2	2	2	3	3	3
CO4	3	3	3	3	3	2	2	2	3	3	2	3	3	3
CO5	3	3	2	3	2	3	3	3	2	3	3	3	3	2
CO6	3	3	3	3	2	3	3	3	2	3	3	3	3	2

PROFESSIONAL ELECTIVES - IV

20CSEL808 SDG NO. 4	CYBER SECURITY AWARENESS AND EDUCATION	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To introduce students to the importance of cybersecurity awareness in today's digital age.
- To equip students with knowledge of common cyber threats and best practices for online security.
- To empower students to implement cybersecurity measures to protect themselves and others.
- To train students in designing and delivering effective cybersecurity awareness programs.
- To promote a culture of cybersecurity awareness and advocacy within organizations and communities.

Module 1: Introduction to Cyber Security Awareness 8

Importance of cyber security awareness-Basic concepts of cyber security: threats, vulnerabilities, and attacks-Impact of cyber threats on individuals, organizations, and society-Legal and ethical aspects of cyber security awareness

Module 2: Cyber Threats and Risks 8

Overview of common cyber threats: malware, phishing, ransomware-Recognizing signs of cyber-attacks and intrusions-Personal cyber security practices: password hygiene, software updates-Risk assessment and management for individuals and organizations

Module 3: Cyber Security Best Practices 7

Secure online behavior: safe browsing, social media usage-Data protection and privacy measures- Securing personal devices: computers, smart phones, tablets-Importance of strong authentication mechanisms

Module 4: Cyber Security Awareness Programs and Training 8

Designing effective cyber security awareness programs-Role of education and training in promoting cyber security awareness-Techniques for delivering cyber security awareness training: workshops, simulations

Module 5: Cyber Security Culture and Advocacy 7

Evaluation and assessment of cyber security awareness initiatives - Building a culture of cyber security awareness in organizations and commModuleies - Role of advocacy and public awareness campaigns

Module 6: Cyber Security Advocacy 7

Engaging stakeholders: government, industry, academia, and civil society - Promoting inclusivity and accessibility in cyber security education

TOTAL : 45 PERIODS

TEXT BOOKS:

1. "Cybersecurity Essentials" by Charles J. Brooks and Christopher Grow.
2. "Cybersecurity Awareness for CEOs and Management" by Raj Goel.
3. "Cybersecurity for Beginners" by Raef Meeuwisse.

REFERENCE BOOKS:

1. "Cyber Smart: Five Habits to Protect Your Family, Money, and Identity from Cyber Criminals" by Bart R. McDonough.

2. "Cybersecurity and Cyberwar: What Everyone Needs to Know" by P.W. Singer and Allan Friedman.
3. "The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations" by Ben Buchanan.

NPTEL WEB LINKS:

1. NPTEL - Cyber Security Awareness Course

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the significance of cybersecurity awareness in mitigating cyber risks.(K2)
2. Recognize common cyber threats and adopt best practices for online security.(K1)
3. Implement effective cybersecurity measures to protect personal and organizational data.(K4)
4. Design and deliver cybersecurity awareness programs and training.(K3)
5. Foster a culture of cybersecurity awareness and advocacy.(K2)
6. Apply sustainable development principles to promote inclusive cybersecurity education.(K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	1	0	0	0	0	0	0	0	0	0	1	2
CO2	3	3	3	1	2	0	0	0	0	0	0	0	1	2
CO3	3	3	3	3	3	0	0	0	0	0	0	0	2	2
CO4	3	3	3	2	3	0	0	0	0	0	0	1	3	3
CO5	3	3	3	3	3	0	0	0	0	0	2	1	3	3
CO6	3	3	3	3	3	2	1	2	2	0	2	2	3	3

PROFESSIONAL ELECTIVES - IV

20CSEL807 SDG NO. 4&9	COMPUTER VISION	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To review image processing techniques for Computer Vision
- To understand shape and region analysis
- To understand Hough Transform and its applications to detect lines, circles, ellipses
- To understand three-dimensional Image Analysis & Motion Analysis techniques

Module 1: IMAGE PROCESSING FOUNDATIONS 9

Review of Image Processing Techniques – Classical Filtering Operations – Thresholding Techniques – Edge Detection Techniques – Corner and Interest Point Detection – Mathematical Morphology – Texture.

Module 2: SHAPES AND REGIONS 7

Binary Shape Analysis – Connectedness – Object Labeling and Counting – Size Filtering – Distance Functions – Skeletons and Thinning – Deformable Shape Analysis – Boundary Tracking Procedures – Active Contours – Shape Models And Shape Recognition – Centroidal Proiles – Handling Occlusion – Boundary Length Measures – Boundary Descriptors – Chain Codes – Fourier Descriptors – Region Descriptors – Moments.

Module 3: HOUGH TRANSFORM 7

Line Detection – Hough Transform (HT) for Line Detection – Foot-of-normal Method – Line Localization – Line Fitting – Ransac for Straight Line Detection – HT Based Circular Object Detection – Accurate Center Location – Speed Problem – Ellipse Detection – Case Study: Human Iris Location– Hole Detection – Generalized Hough Transform (GHT) – Spatial Matched Filtering – GHT for Ellipse Detection – Object Location – GHT for Feature Collation.

Module 4: 3D VISION AND MOTION 7

Methods for 3D Vision – Projection Schemes – Shape from Shading – Photometric Stereo – Shape from Texture – Shape from Focus – Active Range Finding – Surface Representations – Point-based Representation – Volumetric Representations – 3D Object Recognition – 3D Reconstruction –

Module 5: 3D MOTION 8

Introduction to Motion – Triangulation – Bundle Adjustment – Translational Alignment – Parametric Motion – Spline-based Motion – Optical Flow – Layered Motion.

Module 6: APPLICATIONS 8

Application: Photo Album – Face Detection – Face Recognition – Eigenfaces – Active Appearance And 3D Shape Models of Faces Application: Surveillance – Foreground - Background Separation – Particle Filters – Chamfer Matching - Tracking - and Occlusion – Combining Views From Multiple Cameras – Human Gait Analysis Application - In-vehicle Vision System - Locating Roadway – Road Markings – Identifying Road Signs – Locating Pedestrians.

TOTAL : 45 PERIODS

TEXT BOOKS:

1. E. R. Davies, "Computer & Machine Vision", Fourth Edition, Academic Press, 2017.
2. R. Szeliski, "Computer Vision: Algorithms and Applications", Springer 2011.

REFERENCES:

1. D. L. Baggio et al., "Mastering OpenCV with Practical Computer Vision Projects", Packt Publishing, 2012.
2. Jan Erik Solem, "Programming Computer Vision with Python: Tools and algorithms for analyzing images", O'Reilly Media, 2012.
3. Mark Nixon and Alberto S. Aquado, "Feature Extraction & Image Processing for Computer Vision", Third Edition, Academic Press, 2012.
4. Simon J. D. Prince, "Computer Vision: Models, Learning and Inference", Cambridge University Press, 2012.
5. David Forsyth and Jean Ponce ," Computer Vision: A Modern Approach", Second Edition, Pearson, 2011.

WEB REFERENCES:

1. https://nptel.ac.in/courses/106105216/
2. https://nptel.ac.in/courses/106105032/
3. https://swayam.gov.in/nd1_noc19_cs58/preview
4. http://www.cse.iitd.ernet.in/~suban/vision/index.html
5. http://www.cse.iitm.ac.in/~vplab/courses/CV_DIP/PDF/INTRO_CV.pdf

ONLINE RESOURCES:

1. https://youtu.be/715uLCHt4jE
2. https://www.coursera.org/lecture/deep-learning-in-computervision/introduction-to-video-analysis-alApg
3. https://www.coursera.org/lecture/introduction-computer-visionwatson-opencv/applications-of-computer-vision-EEDvi
4. https://www.analyticsvidhya.com/blog/2020/01/computer-visionlearning-path-2020/

OUTCOMES:

Upon completion of the course, the student should be able to

1. Implement fundamental image processing techniques required for computer vision.(K3)
2. Perform shape analysis, Implement boundary tracking techniques & Apply chain codes and other region descriptors.(K3)
3. Apply Hough Transform for line, circle, and ellipse detections.(K3)
4. Apply 3D vision techniques.(K3)
5. Design of a computer vision system for identification and recognition of objects.(K4)
6. Implement motion related techniques & Develop applications using computer vision techniques.(K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	3	3	1	1	1	-	1	-	1	-	2	2
CO2	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO3	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO4	3	3	3	3	3	1	1	-	2	-	1	-	2	2
CO5	3	3	3	3	3	1	1	1	2	3	1	-	2	2
CO6	3	3	2	3	3	2	-	-	-	-	-	-	1	1

PROFESSIONAL ELECTIVES - IV

20CSEL819 SDG NO. 4	ETHICAL HACKING AND OFFENSIVE CYBER OPERATIONS	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To introduce students to the concepts and techniques of ethical hacking and offensive cyber operations.
- To equip students with practical skills for identifying and exploiting vulnerabilities.
- To train students in network attack and defense strategies.
- To discuss legal and ethical considerations in cybersecurity practices.
- To provide hands-on experience in conducting penetration tests and vulnerability assessments.

Module 1: Introduction to Ethical Hacking 8

Understanding ethical hacking and offensive cyber operations-Legal and ethical considerations in cyber security-Overview of hacking methodologies and techniques-Introduction to penetration testing and vulnerability assessment

Module 2: Reconnaissance and Footprinting 8

Techniques for gathering information about target systems and networks-Open-source intelligence (OSINT) gathering-Footprinting methodologies: network scanning, enumeration-Case studies and practical exercises

Module 3: Exploitation and post-exploitation 7

Exploiting vulnerabilities in target systems and networks-Payload delivery techniques: malware, remote code execution-Privilege escalation and maintaining access-Covering tracks and maintaining stealth

Module 4: Network Attacks and Defense 7

Common network-based attacks: DOS, DDOS - man-in-the-middle(MITM) - Network security protocols and countermeasures

Module 5: Network Attacks and Defense 7

Intrusion detection system (IDS) and Intrusion prevention systems (IPS) - Network forensics and incident response

Module 6: Legal and Regulatory Aspects 8

Laws and regulations governing offensive cyber operations-Ethical guidelines and professional standards for ethical hackers-Reporting vulnerabilities and responsible disclosure-Case studies on legal implications of cyber-attacks

TOTAL:45 PERIODS

TEXT BOOKS:

1. "The Hacker Playbook: Practical Guide to Penetration Testing" by Peter Kim.
2. "Metasploit: The Penetration Tester's Guide" by David Kennedy, Jim O'Gorman, and others.
3. "Hacking: The Art of Exploitation" by Jon Erickson.

REFERENCE BOOKS:

1. "Penetration Testing: A Hands-On Introduction to Hacking" by Georgia Weidman.
2. "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" by Dafydd Stuttard and Marcus Pinto.
3. "Gray Hat Hacking: The Ethical Hacker's Handbook" by Daniel Regalado, Shon Harris, and others.

NPTEL WEB LINKS:

1. NPTEL - Ethical Hacking and Offensive Cyber Operations Course

OUTCOMES:

Upon completion of the course, the student should be able to

1. Understand the principles and methodologies of ethical hacking and offensive cyber operations.(K2)
2. Identify and exploit vulnerabilities in target systems and networks.(K2)
3. Apply network attack and defense techniques.(K2)
4. Analyze legal and ethical considerations in cybersecurity.(K3)
5. Demonstrate proficiency in conducting penetration tests and vulnerability assessments.(K3)
6. Apply sustainable development principles to promote responsible cybersecurity practices.(K3)

CO- PO, PSO MAPPING:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	1	0	0	0	0	0	0	0	0	0	1	2
CO2	3	3	3	1	2	0	0	0	0	0	0	0	1	2
CO3	3	3	3	3	3	0	0	0	0	0	0	0	2	2
CO4	3	3	3	2	3	0	0	0	0	0	0	1	3	3
CO5	3	3	3	3	3	0	0	0	0	0	2	1	3	3
CO6	3	3	3	3	3	2	1	2	2	0	2	2	3	3

Imagine the Future and

Make it happen!

Together let's build a better world where there is NO POVERTY and ZERO HUNGER.

We have GOOD HEALTH AND WELL BEING QUALITY EDUCATION and full GENDER EQUALITY everywhere.

There is CLEAN WATER AND SANITATION for everyone. AFFORDABLE AND CLEAN ENERGY

which will help to create DECENT WORK AND ECONOMIC GROWTH. Our prosperity shall be fuelled

by investments in INDUSTRY, INNOVATION AND INFRASTRUCTURE that will help us to

REDUCE INEQUALITIES by all means. We will live in SUSTAINABLE CITIES AND COMMUNITIES.

RESPONSIBLE CONSUMPTION AND PRODUCTION will help in healing our planet.

CLIMATE ACTION will reduce global warming and we will have abundant,

flourishing LIFE BELOW WATER, rich and diverse LIFE ON LAND.

We will enjoy PEACE AND JUSTICE through STRONG INSTITUTIONS

and will build long term PARTNERSHIPS FOR THE GOALS.

For the goals to be reached, everyone needs to do their part: governments, the private sector, civil society and **People like you.**

Together we can...

Sai Prakash Leo Muthu

Chairman & CEO – Sairam Institutions

We build a Better nation through Quality education.

Sairam INSTITUTIONS

Sri

SAIRAM INSTITUTE OF TECHNOLOGY

An Autonomous Institution

Affiliated to Anna University & Approved by AICTE, New Delhi

*Accredited by **NBA** and **NAAC** "**A+**"*
***ISO** 9001:2015 Certified and MHRD **NIRF** ranked institutions*

College Campus
Sai Leo Nagar, West Tambaram,
Chennai - 600 044. Ph : 044-2251 2111

Administrative Office
"Sai Bhavan", 31B, Madley Road, T.Nagar,
Chennai - 600 017. Ph : 044-4226 7777

e-mail : sairam@sairamgroup.in

www.sairamgroup.in