JOY UNIVERSITY

Established vide Tamil Nadu State Pvt. Universities Act 2019

SCHOOL OF COMPUTATIONAL INTELLIGENCE

Outcome Based Curriculum Framework with CBCS

for

BACHELOR OF TECHNOLOGY
COMPUTER SCIENCE AND ENGINEERING
(CYBER SECURITY)

(B. Tech CSE (Cyber Security))

Students admitted from 2025 -26 onwards

JOY UNIVERSITY
semper paratus

VISION

♣ To create and nurture a multidisciplinary global university with highest academics, research and ethical standards in a creative and innovative environment.

MISSION

♣ To be a premier University of choice for all stakeholders and contribute for academic demographic dividend. To inculcate quality, integrity, team work, compassion, ethics in new generation students for catering to various needs of society.

QUALITY OBJECTIVES

- To disseminate knowledge with skills through teaching, training, seminars, workshops, conferences and symposia in Engineering and Technology, Art and Design, Management and Commerce, Allied Health Sciences, Physical and Life Sciences, Arts, Humanities and Social Sciences, Law and Agricultural Sciences to enable students to meet the current needs and trends of industries, business and society.
- To provide technical and scientific solutions to real time problems posed by industries, business and society in all Schools of Joy University.
- To inculcate quality, integrity, team work, compassion, ethics in new generation students for catering to various needs of society.
- To promote the spirit of entrepreneurship in the young generation to help and create more career opportunities in the society by incubating a nurturing technology product idea backed by Technology Business Incubation.
- To identify and nurture leadership and innovate skills in students to become future leaders to enrich society.
- To develop collaborations and partnerships with International global and reputed Universities, research establishments, Government and NGO's, industries and businesses. To support both faculties and students for international exposure.

SCHOOL OF COMPUTATIONAL SCIENCE

VISION

The SOCI envisions a 'cooperatively competitive' academic environment in the thematic areas of the school and relevant research backed by quality education to churn out graduates with professional acumen, exceptional leadership and a humane heart to meet both national and global needs.

MISSION

The SOCI offers a value-based, technology-oriented education striving to achieve high levels of academic excellence, intellectually competence and exemplary values. The tri-value system of our school is designed to deliver education through three interconnected values: **Learning, Transmutation** and **Transformation**.

PROGRAMME EDUCATIONAL OBJECTIVES

PEO1: To ensure that the graduates will have the ability and attitude to acquire new skills and adapt recent technological changes.
PEO2: To prepare the graduates to serve in the industries related to Computer Science and Engineering or to do higher education and research.
PEO3: To ensure that the graduates will work with professionalism and ethics by contributing to the advancement of the society

GRADUATE ATTRIBUTES

The Graduate Attributes of B. Tech (Cyber Security) are:

- Apply appropriate knowledge in Computer Science and Engineering to identify, formulate, analyze, and solve complex engineering problems in order to reach substantive conclusions.
- Self-learn and engage in use of advanced computing tools.
- Develop sustainable computing solutions in broader economic, societal and environmental contexts.
- Think critically, creatively and analytically as a computer scientist, whilst being able to work effectively, independently and collaboratively as part of a team in research, technology development and entrepreneurial ventures.
- Apply evolving ethics and privacy laws across various domains and territories.
- Effectively communicate engineering concepts and ideas to peers in written or oral forms.
- Be motivated to engage in independent and life-long learning in the broadest context of evolving technological challenges.

PROGRAMME OUTCOMES

On completion of the **B. Tech (Cyber Security) Programme,** students should be able to:

PO1: Engineering knowledge: Apply the knowledge of mathematics, science, engineering

fundamentals and an engineering specialization to the solution of complex engineering problems.

PO2: Problem analysis: Identify, formulate, review research literature, and analyse complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

PO3: Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

PO4: Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

PO5: Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of the limitations.

PO6: The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

PO7: Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

PO8: Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

PO9: Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings

PO10: Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

PO11: Project management and finance: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

PO12: Life-long learning: Recognize the need for and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

PROGRAM SPECIFIC OUTCOMES

PSO 1: Ability to identify and mitigate security vulnerabilities in networks, systems, and applications.

PSO 2: Proficiency in implementing and managing security protocols to protect sensitive data.

PSO 3: Skill in conducting risk assessments and responding to cyber security threats and incidents.

Summary of Credits

Semester	I	II	III	IV	V	VI	VII	VIII	Total
Credits	20	21	21	20	24	20	21	21	168
Contact Hrs./Week	24	24	24	22	26	22	19	6	167

SEMESTER WISE CREDIT STRUCTURE

Sl. No.	Category of Courses	1st Year		2nd Year		3rd Year		4th Year		Total
		Sem I	Sem II	Sem III	Sem IV	Sem V	Sem VI	Sem VII	Sem VIII	
1.	Departmental Core	8	4	20	11	12	11	8	0	74
2.	Departmental Specific Electives	0	0	0	6	6	6	6	6	30
3.	Open Electives	0	0	0	0	3	3	3	0	9
4.	Applied Sciences	8	14	0	0	0	0	0	0	22
5.	Internships/ Field Visits	0	0	0	0	0	0	2	0	2
6.	Project	0	0	0	0	0	0	2	15	17
7.	Skill Enhancement Course	0	1	0	3	3	0	0	0	7
8.	Ability Enhancement Courses (AECC)	3	0	0	0	0	0	0	0	3
9.	Value-Added Course	1	2	1	0	0	0	0	0	4
Total		**20**	**21**	**21**	**20**	**24**	**20**	**21**	**21**	**168**

School of Computational Science

B. Tech (Cyber Security)

Semester – I
(Total Credits: 20)

SI.No	Course Code	Course Title	L	T	P	Contact Hrs / Wk	Credits
1.	25BTCY111	**Core Course** Fundamentals of Computing	3	0	0	3	3
2.	25BTCY112	**Core Course** Introduction to Programming	3	0	0	3	3
3.	25BTCY113	**Applied Science** Mathematics I	3	1	0	4	4
4.	25BTCY114	**Applied Science** Physics I	3	1	0	4	4
5.	25AEEN911	**Ability Enhancement Compulsory Course (AECC)** Effective Communication	3	0	0	3	3
6.	25BTCY911	**Value-Added Course** Performing Arts/Sports (Non-Graded)	3	0	0	3	1
7.	25BTCY211	**Core Course** Fundamentals of Computing Lab	0	0	2	2	1
8.	25BTCY212	**Core Course** Introduction to Programming Lab	0	0	2	2	1
		Total	**18**	**2**	**4**	**24**	**20**

Semester – II

(Total Credits: 21)

SI.No	Course Code	Course Title	L	T	P	Contact Hrs / Wk	Credits
1.	25BTCY121	**Core Course** Python Programming	3	0	0	3	3
2.	25BTCY122	**Applied Science** Probability, Statistics and Stochastic Processes	3	0	0	3	3
3.	25BTCY123	**Applied Science** Mathematics II	3	1	0	4	4
4.	25BTCY124	**Applied Science** Physics II	3	0	0	3	3
5	25BTCY125	**Applied Science** Discrete Structures for Computer Science	3	0	0	3	3
6	25EVST921	**Value Added Course** Environmental Science	2	0	0	2	2
7	25BTCY221	**Core Course** Python Programming Lab	0	0	2	2	1
8	25BTCY222	**Applied Science** Physics Lab	0	0	2	2	1
9	25BTCY223	**Skill Enhancement Course** Extended Reality and its Application Lab (from TANSAM)	0	0	2	2	1
		TOTAL	**17**	**1**	**6**	**24**	**21**

emester – III

(Total Credits: 21)

SI.No	Course Code	Course Title	L	T	P	Contact Hrs / Wk	Credits
1.	25BTCY131	**Core Course** Fundamentals of Information and Data Security	3	0	0	3	3
2.	25BTCY132	**Core Course** Signals and Systems	3	0	0	3	3
3.	25BTCY133	**Core Course** Computer Networks	3	0	0	3	3
4.	25BTCY134	**Core Course** Data Structures and Algorithms	3	0	0	3	3
5.	25BTCY135	**Core Course** Object Oriented Programming with Java	3	0	0	3	3
6.	25BTCY231	**Core Course** Data Structures and Algorithms Lab	0	0	2	2	1
7.	25BTCY232	**Core Course** Programming with Java Lab	0	0	2	2	1
8.	25BTCY233	**Core Course** Computer Networks Lab	0	0	2	2	1
9.	25BTCY931	**Value Added Course** Indian Constitution	1	0	0	1	1
10.	25BTCY136	**Core Course** Professional Ethics	2	0	0	2	2
		Total	**18**	**0**	**6**	**24**	**21**

Semester – IV

(Total Credits: 20)

SI.No	Course Code	Course Title	L	T	P	Contact Hrs / Wk	Credits
1.	25BTCY141	**Core Course** Cryptography and Network security	3	0	0	3	3
2.	25BTCY142	**Core Course** Database Management Systems	3	0	0	3	3
3.	25BTCY143	**Core Course** Computer organization and Architecture	3	0	0	3	3
4.	25BTCY841	**Skill Enhancement Course** Engineering Economics and Foreign Trade	3	0	0	3	3
5.		**Discipline Specific Elective I**	3	0	0	3	3
6	25BTCY341	Continual Learning					
7	25BTCY342	Social Network Analysis					
8	25BTCY343	Number Theory in Cryptography					
9		**Discipline Specific Elective II**	3	0	0	3	3
10	25BTCY344	Approximation Algorithms					
11	25BTCY345	Block Chain and its Applications					
12	25BTCY346	Game Theory					
13	25BTCY241	**Core Course** Cryptography and Network security Lab	0	0	2	2	1
14	25BTCY242	**Core Course** Database Management Systems Lab	0	0	2	2	1
		Total	18	0	4	22	20

Semester – V

(Total Credits: 24)

SI.No	Course Code	Course Title	L	T	P	Contact Hrs / Wk	Credits
1.	25BTCY151	**Core Course** Introduction to Blockchain and Cryptocurrency	3	0	0	3	3
2.	25BTCY152	**Core Course** Malware Analysis	3	0	0	3	3
3.	25BTCY153	**Core Course** Theory of Computation	3	1	0	4	4
4.		**Discipline Specific Elective III**	3	0	0	3	3
	25BTCY351	Semantic Web Technology					
	25BTCY352	Web Application Security					
	25BTCY353	Web data Mining					
5		**Discipline Specific Elective IV**	3	0	0	3	3
	25BTCY354	Modern Cryptography					
	25BTCY355	Evolutionary Computation					
	25BTCY356	Biometric Security					
6		**Open Electives – I**	3	0	0	3	3
	25BTCY051	Artificial Intelligence					
	25BTCY052	Python Programming					
	25BTCY053	Computed Networks					
7	25BTCY851	**Skill Enhancement Course** Principles of Management	3	0	0	3	3
8	25BTCY251	**Core Course** Malware Analysis Lab	0	0	2	2	1
9	25BTCY252	**Core Course** Introduction to Blockchain and Cryptocurrency Lab	0	0	2	2	1
		Total	**21**	**1**	**4**	**26**	**24**

Semester – VI

(Total Credits: 20)

Sl.No	Course Code	Course Title	L	T	P	Contact Hrs / Wk	Credits
1.	25BTCY161	**Core Course** Natural Language Processing	3	0	0	3	3
2.	25BTCY162	**Core Course** Compiler Design	3	0	0	3	3
3.	25BTCY163	**Core Course** Web Technology	3	0	0	3	3
4.		**Discipline Specific Elective V**	3	0	0	3	3
	25BTCY361	Cyber Criminology and Cyber crimes					
	25BTCY362	Design of Internet of Things					
	25BTCY363	Augmented Intelligence					
5		**Discipline Specific Elective VI**	3	0	0	3	3
	25BTCY364	Reverse Engineering					
	25BTCY365	Digital Forensics					
	25BTCY366	Cyber Threat Intelligence					
6		**Open Electives – II**	3	0	0	3	3
	25BTCY061	A I Tools					
	25BTCY062	IoT					
	25BTCY063	Cyber Security					
6	25BTCY261	**Core Course** Natural Language Processing Lab	0	0	2	2	1
7	25BTCY262	**Core Course** Compiler Design Lab	0	0	2	2	1
		Total	**18**	**0**	**4**	**22**	**20**

Semester – VII

(Total Credits: 21)

SI.No	Course Code	Course Title	L	T	P	Contact Hrs / Wk	Credits
1.	25BTCY171	**Core Course** High Performance Computing	3	0	0	3	3
2.	25BTCY172	**Core Course** Ethical Hacking and Penetration Testing	3	0	0	3	3
3.		**Discipline Specific Elective VII**	3	0	0	3	3
	25BTCY371	Security Information and Event Management					
	25BTCY372	Secure Software Development					
	25BTCY373	Nature Inspired Computing					
4		**Discipline Specific Elective VIII**	3	0	0	3	3
	25BTCY374	Machine Learning for Cybersecurity					
	25BTCY375	Natural Language Processing for Security					
	25BTCY376	Cloud Security and Governance					
5	25BTCY571	Mini Project	0	0	0	0	2
6	25BTCY471	Industrial Internship	0	0	0	0	2
7		**Open Electives - III**	3	0	0	3	3
	25BTCY071	Advanced Python programming					
	25BTCY072	Optimisation Algorithms					
	25BTCY073	Computing (latest)					
8	25BTCY271	**Core Course** High Performance Computing Lab	0	0	2	2	1
9	25BTCY272	**Core Course** Ethical Hacking and Penetration Testing Lab	0	0	2	2	1
		Total	**15**	**0**	**4**	**19**	**21**

Semester – VIII

(Total Credits: 21)

SI.No	Course Code	Course Title	L	T	P	Contact Hrs / Wk	Credits
1.	25BTCY581	Cybersecurity Capstone Project	-	-	-	-	15
2.		**Discipline Specific Elective IX**	3	0	0	3	3
	25BTCY381	Mobile and IoT Security					
	25BTCY382	Security in Edge and Fog Computing					
	25BTCY383	Security in Software Defined Networks (SDN)					
3.		**Discipline Specific Elective X**	3	0	0	3	3
	25BTCY384	Research Methodology in Security					
	25BTCY385	Cyber Laws and Digital Evidence					
	25BTCY386	Security Risk Management					
		Total	**6**	**0**	**0**	**6**	**21**

Semester I

Programme	BTech CSE- Cyber Security	Programme Code	BTCY		
Course Code	25BTCY 111	Number of Hours/Week	3		
Semester	I	Max. Marks	100		
Year	I	Credits	3		
Course					
Course Title	FUNDAMENTALS OF COMPUTING		L	T	P
			3	0	0

L-Lecture Hours T-Tutorial Hours P-Practical Hours

COURSE OBJECTIVES:

The main learning objective of this course is to prepare the students for:

- To have a comprehensive understanding of a foundational understanding of computer systems.
- To learn about various number systems including decimal, binary, octal, and hexadecimal
- To develop a comprehensive grasp of how computers function, the types of software used and the significance of networking in today's digital world.
- To explore various types of software applications including operating systems, word processors, database management systems and Internet

UNIT	TOPICS	HOURS
I	**Introduction to Computer** Evolution of Computers, Generations of Computers, Classification of Computers, The Computer System, Computing Concepts, Applications of Computers. Memory and storage systems Computer Software and Hardware components and its requirements- Storage Devices, Computer Viruses Types Of Viruses – Spreading of Virus, Prevention of Computer Virus, Virus Detection, Computer Security, Maintenance, Desktop functions, Dialog boxes, Single Document Interface (SDI), Multiple Document Interface (MDI), Windows Controls, Main Menu Display, Categories of Menus, Main and Context Sensitive Menus, Booting/Shutting Down.	9
II	**Microsoft software** MS DOS, MS Word System, MS Excel System, MS Power point System, MS Access System, MS Publisher. Number System Decimal Number System, Binary Number System, Octal Number System, Hexadecimal Number System, BCD, XS,3, Gray Code, Alphanumeric Codes,(ASCII, EBCDIC).	9
III	**Computer Software**	9

	Machine language, Mnemonics, High level Language, Assembler, Compiler, Interpreter, System Development Programs, System Management Programs , Standard Application Programs , Unique Application Programs, Problem Solving, Structuring the Logic.	
IV	**Memory management** Introduction, History, Functions, Process, Memory File, Management Device, Security Management, Types of Operating Systems, Providing User Interface, Popular Operating Systems.	**9**
V	**THE INTERNET AND WORLD WIDE WEB** History of the Internet-The Internet Applications-Understanding World Wide Web-Web Browsers-Browsing the Internet-Using a Search Engine-Email Service-Protocols used in the Internet. DATA COMMUNICATIONS AND NETWORKS Introduction-Data Communication Using Modem-Computer Networks-Network Topologies-Network Protocols and Software-Applications of Network.	**9**

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1: Understand the basic concepts of computers.

CO2: Analyze the basics of number systems.

CO3: Apply system development programs to create and manage simple software projects.

CO4: Analyze the performance of different memory management techniques and their impact on system efficiency.

CO5: Evaluate the knowledge of Internet history to understand current Internet technologies and to solve problems in communication and information access.

Text Books:

1. Fundamentals of Computers, E.Balagurusamy, Tata McGraw Hill Education Private Limited, 2009.

Reference Books:

1. Introduction to Computer Fundamentals, Bright Siaw Afriyie, Second edition, Trafford Publishing, Canada, 2003-2006.
2. Computer Fundamentals, P. K. Sinha, BPB Publications, Sixth Edition, 2004.
3. Operating System Concepts, Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, Wiley publishers, Nineth edition, 2013.
4. Computer Networks, Andrew S. Tanenbaum, David J. Wetherall, Fifth edition, Prentice Hall, 2011.
5. Computing Fundamentals: Introduction to Computers, Faithe Wempen, Wiley 2014.

Mapping of Course Outcomes (COs) with PSOs

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO1 0	PO1 1	PO1 2	PSO 1	PSO 2	PSO 3
CO 1	0	1	1	0	0	0	2	0	0	0	1	3	2	3	3
CO 2	3	3	0	2	3	0	0	0	0	0	1	3	0	0	1
CO 3	3	3	3	2	2	0	0	0	0	0	3	3	1	1	1
CO 4	2	3	1	3	2	0	0	0	0	0	1	3	2	1	1
C05	3	3	2	3	3	0	0	0	0	0	1	3	3	3	3

3 – high, 2 – Average, 1 - low , 0-null

Programme	B.Tech CSE-Cyber Security	Programme Code	BTCY
Course Code	25BTCY112	Number of Hours/Week	3
Semester	I	Max. Marks	100
Year	I	Credits	3

Course

Course Title	INTRODUCTION TO PROGRAMMING	L	T	P
		3	0	0

COURSE OBJECTIVES:

The main aim of this course is to prepare the students for:

- To learn the fundamental concepts of programming, including algorithms, flowcharts, and the logical approach to problem solving that is applicable to any programming language.
- To acquire comprehensive understanding of the syntax, semantics and the basic constructs of C language.
- To learn using arrays, pointers, and dynamic memory allocation which are key to understanding data structure and memory management.
- To build a foundation for advanced programming and software development.
- To develop skills to handle complex programming challenges such as file handling, debugging.

UNIT	TOPICS	HOURS
I	**Introduction to programming** Algorithm, Formalism, Flow chart, Assembly language, Introduction to program, Program components, structure, Execution path, Programming paradigms introdution, Syntax and Semantics	9
II	**Introduction to C language** History of C, Prerequisites of C, Features and its applications, Structure of C, Preprocessor directives, Data types and constants, variables and its types, Tokens, Identifiers and format specifiers, Operators and Enums, Data I/O, Decision making and Branching, Loop Introdcution, programs with looping structure, Control Flow programs with control flow	9
III	**Array and Strings** Introduction to Array, Initialization, Single dimensional array, Multidimensional array, String, Functions with string: Read, Display string and string functions, String Arrays.	9
IV	**Functions and Pointers** Function Introduction, Function calling, Return type, Function types, Recursion, Types of Recursion, Introduction to Pointers, Types, Programming exercises with pointers.	9
V	**Structures and Unions** Introduction to structure and simple program using structure concepts, Introduction to Union and programs with union, Storage Classes- Introduction to DMA, Introduction to Pre-processor	9

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

Acquire foundational knowledge of programming including Algorithm, Flowcharts, assembly language basics, program structure.

Understand C language fundamentals

Apply various types of arrays and string manipulation technique to manage and process data in programming scenarios

Analyze and experiment with functions, develop recursive solutions and pointers to solve complex problems.

Develop modular programs using control structures, unions

Text Books

1. "Introduction to Programming Languages" Arvind Kumar Bansal, First Edition, CRC Press, Taylor and Francis group, 2014.
2. "C Programming Language", Brian Kernighan and Dennis Ritchie, Prentice Hall Software, 1988.
3. "Programming with C", Byron Gottfried, Schaum's outlines, Second Edition, Tata McGraw-Hill publishers, 1998.

Reference Books

1. **"**Programming in ANSI C", E**.** Balagurusamy**,** Third edition**,** Tata McGraw-Hill Publishers**,** 2004**.**
2. **"**The Logic of Programming"**,** Eric C.R**.**Hehner**,** Prentice hall of India**,** 1991**.**
3. **"**The Complete Reference C", Herbert Schildt**,** McGraw Hill, Fourth edition **,** 2017.

Mapping of Course Outcomes (COs) with PSOs

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PS O1	PS O2	PS O3
CO1	3	2	2	3	2	1	0	0	0	0	1	3	0	0	0
CO2	3	3	0	0	0	0	1	0	0	0	0	3	1	0	0
CO3	3	2	2	0	0	1	1	0	0	0	0	3	0	1	1
CO4	3	2	2	0	0	0	0	0	0	0	0	3	1	0	1
C05	3	3	2	2	2	0	0	0	0	0	0	3	3	0	1

3 – high, 2 – Average, 1 - low , 0-null

Programme	B.Tech CSE-Cyber Security	Programme Code	BTCY
Course Code	25BTCY 113	Number of Hours/Week	4
Semester	I	Max. Marks	100
Year	I	Credits	4

Course

Course Title	MATHEMATICS-I	L	T	P
		3	1	0

COURSE OBJECTIVES:

The main learning objective of this course is to prepare the students for:

- To recall and remember basics of matrices, complex numbers, and differential calculus.
- To understand the concepts of basic mathematical methods for matrices, complex numbers and differential calculus.
- To apply methods to solve engineering problems.
- To analyze engineering problems and evaluate.
- To solve and evaluate the problems using matrices, complex numbers, and differential calculus.

UNIT	TOPICS	HOURS
I	**Introduction to Differentiation and its applications:** Fundamentals of Differentiation, Rolle's Theorem, Mean value theorems, Taylor's and Maclaurin's theorems with remainders, Indeterminate forms and L'Hopital's rule, Maxima and Minima	10
II	**Integration and its applications:** Double integral, Triple integral, Change of order of integration, Change of variables, Beta and Gamma functions and their properties, Dirichlet's integral and its applications to area and volume, Liouville's extensions of Dirichlet's integral.	12
III	**Sequence:** Real number system, Convergence of sequence and series, Tests for convergence	8
IV	**Series:** Power series, Taylor's series, Series for exponential, trigonometric and logarithm functions, Fourier series: Half range sine and cosine series, Parseval's theorem.	8
V	**Advanced Multivariable Calculus:** Limit, continuity and partial derivatives, Directional derivatives, Total derivative, Tangent plane and normal line, Maxima, minima and saddle points, Method of Lagrange multipliers, Gradient,curl and divergence	10
VI	**Advanced Matrix Theory**: Introduction, types of matrices-symmetric, skew-symmetric, Hermitian, skew-Hermitian, orthogonal, unitary matrices, Rank of a matrix - echelon form, normal form, consistency of system of linear equations (Homogeneous and Non-Homogeneous).Inverse and rank of a matrix, rank-nullity theorem	12

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1:	Understand the concepts of mean value theorems, higher order derivative, series expansion and associated problems
CO2:	Acquire problem solving skills for finding area and volume using multiple integrals
CO3	Analyze sequences and series, including Fourier series
CO4	Apply the differentiation of functions of two variables for maximization and minimization
CO5	Evaluate basic matrix operations, linear systems of equations

Mapping of Course Outcomes (COs) with PSOs

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO 1	2	2	1	0	0	0	0	0	0	0	0	0	1	0	2
CO 2	2	2	0	0	0	0	0	0	0	0	0	0	2	1	1
CO 3	1	2	1	0	0	0	0	0	0	0	0	0	1	2	1
CO 4	2	2	2	0	1	0	0	0	0	0	0	0	1	1	1
CO 5	3	3	1	0	0	0	0	0	0	0	0	1	2	2	2

Text Books

1: Advanced Engineering Mathematics, 10th Edition, Erwin Kreyszig, 1998.

2: Calculus and Analytical Geometry, Thomas and Finney, 1996.

3: Engineering Mathematics-I, Veerarajan T., , Tata McGraw-Hill, New Delhi, 2008.

4: Higher Engineering Mathematics, Ramana B.V., , Tata McGraw Hill New Delhi, 11th Reprint, 2010.

Reference Books

1: Higher Engineering Mathematics, B.S. Grewal, Khanna Publishers, 36th Edition, 2010.

Programme	B.Tech CSE-Cyber Security	Programme Code	BTCY		
Course Code	25BTCY 114	Number of Hours/Week	4		
Semester	I	Max. Marks	100		
Year	I	Credits	4		
Course					
Course Title	PHYSICS I		L	T	P
			3	1	0

L-Lecture Hours T-Tutorial Hours P-Practical Hours

COURSE OBJECTIVES:

- To impart knowledge on the basics of the vector and scalar representation of forces and moments with Special reference to differentiation and integration methods
- To acquire knowledge on moment of inertia and angular momentum
- To impart knowledge on the concept of central force problems and uniformly accelerating systems.

UNIT	TOPICS	HOURS
I	Algebra of vectors-Describing motion: displacement, velocity, speed, acceleration; Cartesian, polar, spherical, and cylindrical polar coordinates; Mathematical tools- differentiation and integration methods, Taylor's series	12
II	Concept of inertia; concept of inertial and non-inertial frames; Newton's laws of motion; Application of Newton's laws: particles in gravitational field, simple harmonic motion, tension in a string, frictional force, viscous force, damped harmonic oscillator, forced harmonic oscillator and resonance. Concept of momentum- center of mass, conservation of momentum, momentum and flow of mass, work-energy theorem, conservative and non-conservative forces, conservation of energy, concept of power, conservation laws and particle Collisions	12
III	Concept of moment of inertia; fixed axis rotation; angular displacement, angular velocity, and angular acceleration; vector nature of angular velocity; angular momentum; torque; conservation of angular momentum; gyroscope motion	12
IV	Central forces; central force motion as one-body problem; conservation laws in central forcemotion; Kepler's laws	12
V	Galilean transformations; uniformly accelerating systems; principle of equivalence; Physics in rotating coordinate systems	12

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1: Apply the concepts of polar, rectangular, cylindrical and spherical coordinate systems.

CO2: Ability to differentiate statics and kinematics.

CO3: Demonstrate the ability to solve the problems in Newton's laws.

CO4: Appreciate to understand rotational kinetic energy & angular momentum.

CO5: Acquire adequate knowledge on conservation laws.

Text Books:

1. An Introduction to Mechanics by Daniel Kleppner, Robert Kolenkow, 2nd edition, 2006.

Reference Books:

2. Mechanics: Course of Theoretical Physics - Vol. 1, L.D. Landau and E.M. Lifshitz, Third Edition, CBS Publishers,2002.

Mapping of Course Outcomes (COs) with PSOs

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO11	PO 12	PS O1	PS O2	PS O3
CO1	2	3	0	0	0	0	0	0	0	0	0	2	0	0	0
CO2	2	0	0	1	0	0	0	0	0	0	0	0	0	0	0
CO3	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
CO4	2	1	0	0	0	0	0	0	0	0	0	0	0	0	0
C05	2	2	0	0	0	0	0	0	0	0	0	0	0	0	0

3 – high, 2 – Average, 1 - low , 0-null

Programme	B.Tech CSE-Cybersecurity	Programme Code	BTCY
Course Code	25AEEN 911	Number of Hours/Week	3
Semester	I	Max. Marks	100
Year	I	Credits	3

Course

Course Title	EFFECTIVE COMMUNICATION	L	T	P
		3	0	0

COURSE OBJECTIVES:

The main learning objective of this course is to prepare the students to:

- To define and explain the fundamental concepts, types, and processes of communication.
- To develop active listening and effective speaking skills to enhance interpersonal
- To improve reading comprehension skills through different techniques.
- To apply grammar and vocabulary rules and public communication for accurate sentence structure and effective written communication.
- To prepare and deliver effective presentations by planning, structuring, and overcoming stage fright.

UNIT	TOPICS	HOURS
I	**Introduction to Communication** Definition of Communication, Types of Communication: Formal, Informal, Oral, Written, Verbal, non-verbal, interpersonal, intrapersonal Process of Communication: Sender, Message, Channel, Receiver, Feedback Barriers: Intrapersonal, Interpersonal, Organizational Overcoming Barriers	11
II	**Listening and Speaking:** Active Listening: Types of Listening, Reasons for poor listening Traits of the good listener, Effective Speaking: Achieving Confidence, Clarity, and Fluency, Public Speaking, Drafting the Speech	10
III	**Reading and Writing:** Reading Comprehension**:** Improving Comprehension Skills, Scanning and Skimming, Predicting the Content, Understanding the Gist, PQRST Technique Grammar and Vocabulary**:** Sentence Structure, Preposition, Punctuation, Articles, Common errors and Correct Usage, Word formation: Affixes, Active and Passive Vocabulary	11
IV	**Presentation Skills** Planning: Occasion, Audience, Purpose, Thesis Statement, Material, Outlining and Structuring, Guidelines for Effective Delivery, Strategies for Reducing Stage Fright	10
V	**Practice:** Grammar Bites, English Fluency Drills	3

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

Understand the different types and processes of communication and the barriers that may arise.

Demonstrate active listening skills and strategies for confident and fluent public speaking.

Enhance reading comprehension through effective reading techniques.

Utilize proper grammar, sentence structures, and vocabulary for clear and correct written communication.

Create structured presentations, incorporating techniques to manage stage fright and engage the audience effectively.

Text Books

1. "Communication Skills", Kumar, Sanjay and Pushp Lata.. Second edition, Oxford University Press, 2015.
2. "Technical Communication: Principles and Practice", Raman, Meenakshi and Sangeetha Sharma, Fourth edition, Oxford University Press, 2022.

Reference Books

1. "Effective Communication: The Most Important Management Skill of All", Adair, John, Pan Books Publishers, 1997.
2. "Modern English Handbook", Gorrell, Robert M and Charlton Laird.. Sixth Edition, Pentice Hall Publications, 1976.
3. "GNVQ Core Skills Communication", Rose, William.. Second edition, Pitman Publishing, 1995.

Mapping of Course Outcomes (COs) with PSOs - cybersecurity

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO1 0	PO1 1	PO 12	PS O1	PS O2	PS O3
CO1	0	0	0	0	0	0	0	0	2	2	0	0	0	0	0
CO2	0	0	0	0	0	0	0	0	2	3	0	0	0	0	0
CO3	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0
CO4	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0
C05	0	0	0	0	0	0	0	0	3	3	0	0	0	0	0
3 – high, 2 – Average, 1 - low , 0-n															

Programme	BTech CSE- Cyber Security	Programme Code	BTAM		
Course Code	25BTCY 211	Number of Hours/Week	2		
Semester	I	Max. Marks	100		
Year	I	Credits	1		
Course					
Course Title	FUNDAMENTALS OF COMPUTING LAB		L	T	P
			0	0	2

L-Lecture Hours T-Tutorial Hours P-Practical Hours

LIST OF PROGRAMS

1. Basics of Microsoft Word.
2. Insert Table and Generating Chart.
3. Mail Merging.
4. Study on features of Microsoft Excel.
5. Incorporating the predefined functions in Excel.
6. Inserting table and generating chart in Excel.
7. Pivot chart, table and slicing in Excel.
8. Study on features in Microsoft PowerPoint.
9. Creating presentation incorporating the features of PowerPoint.
10. Study on HTML.
11. Basic web page design, formatting, inclusion of image and video.
12. Creation of Table.
13. Designing own web page.

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1: Understand the basic functionalities of Microsoft Word

CO2: Apply advanced Excel features for data management.

CO3: Create complex data presentations using Excel pivot tables, charts, and slicers.

CO4: Develop professional presentations using advanced PowerPoint features.

CO5: Design and develop basic web pages using HTML

Mapping of Course Outcomes (COs) with PSOs - cybersecurity

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO1 0	PO1 1	PO1 2	PSO 1	PSO2	PSO 3
CO 1	0	1	1	0	0	0	2	0	0	0	1	3	2	3	3
CO 2	3	3	0	2	3	0	0	0	0	0	1	3	0	0	1
CO 3	3	3	3	2	2	0	0	0	0	0	3	3	1	1	1
CO 4	2	3	1	3	2	0	0	0	0	0	1	3	2	1	1
CO5	3	3	2	3	3	0	0	0	0	0	1	3	3	3	3

Programme	B.Tech CSE-Cybersecurity	Programme Code	BTCY
Course Code	25BTCY212	Number of Hours/Week	2
Semester	I	Max. Marks	100
Year	I	Credits	1

INTRODUCTION TO PROGRAMMING LAB	L	T	P
	0	0	2

LIST OF PROGRAMS

1. Write a C program to print Integer, Float, Character values

2. a)Write a c program to demonstrate use of arithmetic operators
2. b)Write a C program using increment and decrement operators
3. a)Write a C program using Decision making constructs (Switch case statement)
3. b) Program to find if a number is Negative, Positive, or zero(using if..elseif..else statement)
4. C program to perform factorial of a number
5. a) Write a C program to print a message 5 times using"while" statement
5.b) Illustrate the Do-while statement using C program
5. c)Program using for loop statement
6. a) Program to implement break statement
6. b) write a program to demonstrate continue statement
7. Program to insert elements into an array and display the array elements using C language
8. Program to solve multiplication of 2 matrices
9. String
   a) Program to accept a string and display it as reverse using C language
   b) program to concatenate 2 string using C
10. Array
   a) Program to illustrate the concepts of arrays
   b) Program to illustrate pointer to 2-dimensional array
11. Program to take mark details of students and display the name of the students with highest marks using Structure concept
12. Program to implement union concept

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1 :	Acquire foundational knowledge of programming including Algorithm, Flowcharts, assembly language basics, Program structure.
CO2 :	Understand C language fundamentals
CO3 :	Apply various types of arrays and string manipulation technique to manage and process data in programming scenarios
CO4 :	Analyze and experiment with functions, develop recursive solutions and pointers to solve complex problems.
CO5 :	Develop modular programs using control structures, unions

Mapping of Course Outcomes (COs) with PSOs

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PS O1	PS O2	PS O3
CO1	3	2	2	3	2	1	0	0	0	0	1	3	0	0	0
CO2	3	3	0	0	0	0	1	0	0	0	0	3	1	0	0
CO3	3	2	2	0	0	1	1	0	0	0	0	3	0	1	1
CO4	3	2	2	0	0	0	0	0	0	0	0	3	1	0	1
C05	3	3	2	2	2	0	0	0	0	0	0	3	3	0	1

3 – high, 2 – Average, 1 - low , 0-null

Semester II

Programme	B.Tech CSE-Cybersecurity	Programme Code	BTCY
Course Code	25BTCY 121	Number of Hours/Week	3
Semester	II	Max. Marks	100
Year	II	Credits	4

Course

Course Title	PYTHON PROGRAMMING	L	T	P
		3	0	0

COURSE OBJECTIVES:

The main learning objective of this course is to prepare the students for:

- To understand the fundamentals of the Python programming language and its historical development
- To master Python basics, including data types, operators, tuples, dictionaries, and string manipulation.
- To demonstrate object-oriented concepts in Python.
- To familiarize with machine learning tools in Python.

UNIT	TOPICS	HOURS
I	**Introduction to python programming** Introduction to python; setting up python programming environment; variables; strings and its operations; special characters; striping whitespace; numbers; comments; list and its operations; indexing; looping through lists; indentation; range function; slicing a list; copying list; looping through slice;	9
II	**Python datatypes** Tuples and its operations; relational operators; conditional statements – if, if- else, if-elif-else; multiple conditional blocks; dictionaries; key-value pairs – adding, modifying, removing; looping through dictionary; list of dictionaries; dictionary in a dictionary; user input function; type casting;	9
III	**Loop and function** While loop; break and continue; functions; arguments; passing arguments – positional arguments, keyword arguments, default values; optional arguments; returning from function; passing arbitrary number of arguments; storing functions in modules; import specific function or module;	9
IV	**OOPs in python** Classes; _init_() method; instance of a class; accessing attributes; calling methods; creating multiple instances; inheritance – parent class, child class; importing classes; files – reading a file, writing to a file, appending to a file; exceptions – try-except block, else block;	9
V	**Python machine learning tools** Python tools for machine learning; python modules – numpy, pandas, matplotlib, scipy; python based machine learning libraries – pytorch, tensorflow; virtual environment; machine learning application using python tools;	9

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1 Comprehend the holistic view of programming language design and behavior

CO2 Understand the programming concepts in abstract and paradigm level.

CO3 Structure python programs for solving problems.

CO4 Develop python programs using OOP concept.

CO5 Execute ML project using python tools.

Text Book:

1. "A Hands-On, Project-Based Intro- duction to Programming", Eric Matthes. Python Crash Course, 2nd Edition:. No Starch Press, Inc., 2019.

Reference Book:

1. "AutomAte the Boring Stuff with Python", Al Sweigart.,William Pollock, 2015.

Mapping of Course Outcomes (COs) with POs PSOs

	PO_1	PO_2	PO_3	PO_4	PO_5	PO_6	PO_7	PO_8	PO_9	PO_{10}	PO_{11}	PO_{12}	PSO_1	PSO_2	PSO_3
CO_1	3	1	3	0	0	1	0	1	0	1	0	2	0	0	0
CO_2	3	3	2	3	1	2	0	2	1	1	0	2	1	0	0
CO_3	3	2	3	2	3	1	1	0	0	1	0	2	1	0	2
CO_4	3	2	3	2	1	2	1	0	1	1	0	1	2	2	1
CO_5	2	2	3	3	3	0	1	3	1	1	1	1	3	2	3

Programme	B.Tech CSE-Cybersecurity	Programme Code	BTCY
Course Code	25BTCY122	Number of Hours/Week	4
Semester	II	Max. Marks	100
Year	I	Credits	3

Core Course

Course Title	PROBABILITY, STATISTICS AND STOCHASTIC PROCESSES	L	T	P
		3	1	0

COURSE OBJECTIVES:

- **Understand fundamental probability concepts** and their applications in real-world scenarios.
- Analyze data using descriptive statistics **such as mean, variance, and standard deviation.**
- Apply probability distributions **(e.g., binomial, normal) to model and solve problems.**
- Conduct hypothesis testing and confidence intervals **to make informed statistical inferences.**
- Utilize statistical tools and software **for data analysis and decision-making in various fields.**

UNIT	TOPICS	HOURS
I	**Introduction to Probability:** Introduction to set algebra-sigma algebra-Borel sigma algebra-sequence of sets and its limits-lim-sup and lim-inf of sequence of sets; Axiomatic definition of probability-probability space-properties of probability functions-conditional probability-Bayes' rule-independence of events-continuity of probability functions-Borel Cantelli lemmas.	10
II	**Random variables**-distribution function and its property probability mass and density functions-symmetric distribution and its properties-expectation-moments moment generating function-Markov inequality-Chebyshev's inequality.	6
III	**Joint distributions**-marginal and conditional distributions-moments-independence of random variables-covariance, and correlation joint moment generating functions-additive properties of random variables-functions of random variables-ordered Statistics.	8
IV	**Special distributions**: Discrete uniform-Bernoulli-binomial-geometric negative binomial-hypergeometric-Poisson-exponential-gamma-normal-bivariate normal distribution; Population- sample-parameters-distributions of the sample mean and the sample variance for a normal population-Chi-Square-t, F distributions-law of large numbers–central limit theorem-point estimation-method of moments-maximum likelihood estimator-unbiasedness.	8
V	**Testing of hypothesis**: Null and alternate hypothesis-Neyman Pearson fundamental lemma and its applications-tests for one sample and two sample problems for normal populations-tests for proportions-confidence interval estimation-confidence interval for parameters of normal population.	10

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

- CO1: Understand Basic Probability Concepts
- CO2: Analyse Random Variables and Probability Distributions, Joint Distributions and Conditional Probability
- CO3: Implement the Central Limit Theorem and Law of Large Numbers
- CO4: Perform Hypothesis Testing and Statistical Inference, Regression and Correlation for Data Analysis
- CO5: Employ Statistical Tools in Engineering Applications

Text Books:

1. First Course in Probability, Sheldon Ross, 2022.
2. An Introduction to Probability and Statistics, V.K. Rohatgi and A.K. Md. E. Saleh, 2015.

Reference Books:

1. Introduction to Probability and Statistics, S. Milton and J.C. Arnold, 2003.
2. Introduction to Mathematical Statistics, R V Hogg, A Craig and J W McKean, 2019.

Mapping of Course Outcomes (COs) with PSOs - Cybersecurity

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO1 0	PO1 1	PO 12	PS O1	PS O2	PS O3
CO1	2	2	1	0	1	0	0	0	0	0	0	2	1	2	2
CO2	2	2	0	2	0	2	1	0	1	2	1	2	1	0	0
CO3	2	1	2	2	2	2	2	1	1	2	0	0	1	2	2
CO4	2	2	1	2	1	2	2	1	0	0	1	1	0	0	0
C05	2	0	2	2	2	2	2	2	1	1	2	2	0	1	2

3 – High, 2 – Average, 1 - low, 0-null

Programme	B.Tech CSE- Cybersecurity	Programme Code	BTCY
Course Code	25BTCY123	Number of Hours/WK	4
Semester	II	Max. Marks	100
Year	I	Credit	4

Course				
Course Title	MATHEMATICS-II	L	T	P
		3	1	0

COURSE OBJECTIVES

- To solve linear systems
- To understand vector spaces in various mathematical contexts.
- To apply linear transformations for invertibility.
- To **e**xplore Eigenvalues and Eigenvectors
- To acquire techniques for solving ordinary differential equations and methods like Laplace transforms, method of undetermined coefficients and variation of parameters.

UNIT	TOPIC	HOURS
I	**Systems of linear equations:** Elementary operations-row-reduced echelon matrices-Gauss elimination LU factorization-linear independence-rank of a matrix-solutions of linear systems- existence and uniqueness. Vector spaces: Vector space-subspaces-spanning space- bases and dimensions.	12
II	**Linear transformations:** Linear transformation-matrix representations of linear transformations- range space and rank-null space and nullity-the rank and nullity theorem- invertibility.	12
III	**Eigenvalues and eigenvectors:** Eigen values-eigenvectors and some applications of eigenvalue problems-Hermitian, skew-Hermitian, unitary matrices and their eigenvalues- eigen bases.	12
IV	**Diagonalization:** Annihilating polynomial-the minimal polynomial and the characteristic polynomial-Cayley-Hamilton theorem-real quadratic form; Inner product spaces: Inner product spaces-orthonormal bases- Gram-Schmidt process.	12
V	**Differential Equations:** Review of First Order ODE- Lipschitz condition- Picard`s theorem; Linear differential equations: Linear dependence and Wronskian-linear ODE with constant coefficients of higher order characteristic equations- Cauchy-Euler equations-method of undetermined coefficients-method of variation of parameters- solutions methods using Laplace Transform.	12

Andragogy

Class Room Lectures, Power point presentation, You Tube, Group Discussion, Seminar, Quiz, Formative Assessments, Brain storming, Activity.

Text Books:

1. "Linear Algebra", Hoffman Kunze, Prentice Hall. 1971
2. "Differential Equations", S. L Ross, Third Edition, 2007

Reference Books:

1. "Introduction to Linear Algebra", Gilbert Strang, Fifth edition, 2016
2. "Advanced Engineering Mathematics", Erwin Kreyszig, Wiley Publishers, Tenth Edition, 2011.

Mapping of Course Outcomes (COs) with PSOs

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO11	PO 12	PS O1	PS O2	PS O3
CO1	2	2	1	0	1	0	0	0	0	0	0	2	1	2	2
CO2	2	2	0	2	0	2	1	0	1	2	1	2	1	0	0
CO3	2	1	2	2	2	2	2	1	1	2	0	0	1	2	2
CO4	2	2	1	2	1	2	2	1	0	0	1	1	0	0	0
C05	2	0	2	2	2	2	2	2	1	1	2	2	0	1	2

Programme	B.Tech CSE - Cybersecurity	Programme Code	BTCY		
Course Code	25BTCY124	Number of Hours/Week	3		
Semester	II	Max. Marks	100		
Year	I	Credits	3		
Applied Science					
Course Title	PHYSICS II		L	T	P
			3	0	0

L-Lecture Hours T-Tutorial Hours P-Practical Hours

COURSE OBJECTIVES:

- To understand the working principle of various lasers, fibre optics and its applications.
- To impart knowledge on acoustics and ultrasonics and its applications.
- To provide knowledge on magnetism and superconducting phenomenon.

UNIT	TOPICS	HOURS
I	Introduction – Components of laser – Principle of laser action – Properties of laser – Spontaneous emission and stimulated emission – Einstein's coefficients – Population inversion – Types of lasers – He-Ne laser – Nd-YAG laser – Semiconductor laser – Industrial applications of laser – Medical applications of laser – Holography	9
II	Introduction – Propagation of light in optical fiber – Total internal reflection – Principle of optical fiber – Fractional Refractive index - Numerical aperture and acceptance angle – Types of optical fibers based on materials, modes of propagation and refractive index profile – Power losses in optical fibers – Fiber optic communication system – Fiber optic sensors – Temperature and Displacement – Fibre endoscope	9
III	Introduction – Classification of sound – Characteristics of musical sound – Pitch – Loudness – Quality – Intensity of sound – Weber Fechner Law – Reverberation – Reverberation Time – Sabine's Formula – Factors affecting the acoustics of a building – Absorption Coefficient – Measurement of Absorption coefficient	9
IV	Introduction – Production of ultrasonic waves – Magnetostriction Effect – Magnetostriction generator – Piezoelectric Effect – Properties of ultrasonics - Acoustic grating – Applications of ultrasonics – Industrial applications – SONAR – NDT — Medical Applications	9
V	Types of electronic materials: metals, semiconductors, and insulators, Dia, Para, Ferro magnetic materials properties, Temperature effects - Hysteresis curve, Hard and soft magnetic engineering materials - Applications: Magnetic recording and reading – Hard disc. Superconductors: Properties of superconducting materials - Type I and Type II superconductors- Applications: Maglev.	9

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1: Understand the concept of lasers and apply laser action in industries.

CO2: Explain and interpret the principle of fiber optics for different types of industrial sensors.

CO3: Discern the laws governing acoustics and implement the same in acoustic quieting.

CO4: Apply the fundamentals of ultrasonics in non-destructive testing.

CO5: Evaluate and perceive various laws governing magnetism with special reference to magnetic confinement for future power generation.

Text Books:

1. Engineering Physics, D.K. Bhattacharya and Poonam Tandon, New Delhi: Oxford University Press (2017)
2. Engineering Physics, S.Mani Naidu, New Delhi: Pearson India Education Services Pvt. Ltd., (2014)

Reference Books:

1. Engineering Physics, R.K. Gaur and S.L.Gupta, New Delhi: Dhanpat Rai Publications (P) Ltd. (2008)
2. Engineering Physics, Shatendra Sharma and Jyotsna Sharma, New Delhi: Pearson India Education Services Pvt. Ltd., (2019)
3. Engineering Physics, Dattu R. Joshi, New Delhi: Tata McGraw Hill Education Private Ltd., (2010)
4. A Textbook of Engineering Physics, M. N. Avadhanulu and P. G. Kshirsagar, New Delhi: S.Chand and Company Ltd., (2009)
5. Principles of Physics, Jearl Walker, David Halliday and Robert Resnick, Wiley India Pvt. Ltd., New Delhi (2014), Tenth Edition
6. Sears and Zemansky's University Physics with Modern Physics, Hugh D. Young and Roger A. Freedman, Pearson Education, New Delhi (2018), Fourteenth Edition.

Mapping of Course Outcomes (COs) with PSOs

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO11	PO 12	PS O1	PS O2	PS O3
CO1	2	3	0	0	0	0	0	0	0	0	0	2	0	0	0
CO2	2	0	0	2	0	0	0	0	0	0	0	0	0	0	0
CO3	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
CO4	2	1	0	0	0	0	0	0	0	0	0	0	0	2	0
C05	2	2	0	0	0	0	0	0	0	0	0	0	0	2	0

3 – high, 2 – Average, 1 - low , 0-null

Programme	B.Tech CSE- Cybersecurity	Programme Code	BTCY
Course Code	25BTCY125	Number of Hours/Wk	3
Semester	II	Max. Marks	100
Part	I	Credit	3

Applied Science

Course Title	DISCRETE STRUCTURES FOR COMPUTER SCIENCE	L	T	P
		3	0	0

COURSE OBJECTIVES

- To get familiar and understand the fundamental notions in discrete structures focusing on aspects of computer science
- To describe binary relations between two sets, combine relations using set operations and composition.
- To understand and demonstrate the basic concept of algorithm and its application in combinatorial mathematics.
- To identify the base step and the recursive or inductive step in applied problems and give a recursive and a non-recursive definition for an iterative algorithm.
- To classify the basic properties of graphs and trees and model simple applications.

UNIT	TOPIC	HOURS
I	**Set Theory and Logic** Sets – Functions – Relations - Equivalence Relation – Poset - Functions Logic: Propositional logic - Truth Tables – Tautologies - Resolution Proof System - Predicate Logic	9
II	**Induction and Combinatorics** Peano's Axioms - Mathematical Induction - Pigeon-Hole Principle - Principle of Inclusion and Exclusion - Review of Permutations and Combinations - Distribution Problems - Derangements - Bijection Principle.	9
III	**Algebraic Structures** Semi-Groups – Monoids – Groups - Subgroups and Their Properties - Cyclic Groups - Cosets - Permutation Groups - Lagrange's Theorem - Cayley's Theorem - Normal Subgroups - Homomorphism of Groups - Quotient Groups – Introduction to Rings and Fields	9
IV	**Linear Algebra and Recurrence Relations** Linear Algebra: Vector Space – Basis, Dimension, Orthogonality - Recurrence Relations: Homogeneous and Inhomogeneous Recurrences and their Solutions - Solving Recurrences Using Generating Functions.	9
V	**Graph Theory** Definitions and Basic Results - Representation of a Graph by a Matrix and Adjacency List - Trees - Cycles - Properties - Paths and Connectedness - Subgraphs - Graph Isomorphism - Operations on Graphs - Vertex and Edge Cuts - Vertex and Edge Connectivity.	9

Andragogy

- Class Room Lectures, Power point presentation, flipped classroom sessions, Group Discussion, Seminar, Quiz, Formative Assessments.
- The students can get their doubts clarified at any time whenever the faculty is available.

COURSE OUTCOMES:

On completion of this course, students will be able to

CO1: Understand the fundamental aspects of discrete and continuous mathematical structures.

CO2: Demonstrate the principles of mathematical induction to prove statements.

CO3: Differentiate between various algebraic structures and analyze their properties.

CO4: Apply logical reasoning and mathematical techniques to solve problems in set theory, algebra, and graph theory.

CO5: Construct new mathematical models and generate solutions to complex recurrence relations and graph problems.

Text Books

1. "Elements of Discrete Mathematics: A Computer Oriented Approach", C. L. Liu, D. P. Mohapatra, McGraw Hill, Third Edition, 2012.
2. "Applied Discrete Structures", Al Doerr, Ken Levasseur, LibreTexts, Third Edition, 2023

Reference Books

1. "Discrete Mathematical Structures with applications to Computer Science", Tremblay J.P. and Manohar R., McGraw Hill International Edition, 1987.
2. "Discrete Mathematics and Its Applications", Kenneth H. Rosen, Sixth Edition, Tata McGraw Hill, 2012.

Mapping of Course Outcomes (COs) with PSOs

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PS O1	PS O2	PS O3
CO1	2	1	0	0	1	2	0	0	0	0	1	2	1	1	1
CO2	1	2	1	1	1	0	0	0	0	0	1	0	1	0	1
CO3	2	1	1	2	0	0	0	0	0	0	1	1	0	1	1
CO4	2	2	1	1	0	0	0	0	0	0	2	2	2	2	2
C05	3	2	1	2	3	0	0	0	0	0	1	1	0	2	1

3 – high, 2 – Average, 1 - low , 0-null

Programme	B.Tech CSE- Cybersecurity	Programme Code	BTCY		
Course Code	25EVST921	Number of Hours/WK	2		
Semester	II	Max. Marks	100		
Year	I	Credits	2		
Course					
Course Title	ENVIRONMENTAL SCIENCE	L	T	P	
		2	0	0	

Course Objective

The main learning objective of this course is to prepare the students to:

- To understand the Environmental Foundations
- To differentiate between renewable and non-renewable resources and assess the impacts of land use changes, land degradation, and water resource exploitation.
- To study the causes and effects of pollution and its impacts on earth
- To analyse the population causes, its effects and control measures.

UNIT	TOPIC	HOURS
I	**Introduction to Environmental studies** Definition and Scope of Environmental Studies - Interdisciplinary Nature of Environmental Science-Historical Perspectives on Environmental Issues- Principles of Sustainability and Sustainable Development, Ecosystem- Structure and functions of ecosystem--Aquatic ecosystems	6
II	**Natural Resources- Renewable and Non-renewable Resources** Land resources and land use change, Land degradation, soil erosion, Desertification-Deforestation- exploitation of surface and ground water, floods, droughts, conflicts over water Energy resources: Renewable and non-renewable energy sources, use of alternate energy sources, growing energy needs, case studies.	6
III	**Biodiversity and Conservation** Levels of biological diversity- genetic, species and ecosystem diversity, Biogeographic zones of India; Biodiversity patterns and global biodiversity hot spots**.**	6
IV	**Environmental Pollution** Environmental pollution: types, causes, effects and controls; Air, water, soil and noise pollution - Nuclear hazards and human health risks-Solid waste management: Control measures of urban and industrial waste. Pollution case studies, Climate change, global warming, ozone layer depletion, acid rain and impacts on human communities and agriculture, Environment Laws: Environment Protection Act; Wildlife Protection Act; Forest Conservation Act. International agreements: Montreal and Kyoto protocols and Convention on Biological Diversity (CBD), Nature reserves, tribal populations and rights, and human wildlife conflicts in Indian context.	6
V	**Human Communities and the Environment** Human population growth: Impacts on environment, human health and welfare-Resettlement and rehabilitation of project affected persons, Disaster management: floods, earthquake, cyclones and landslides, Environmental movements- Chipko, Silent valley, Bishnoi's of Rajasthan	6

Andragogy

Class Room Lectures, Power point presentation, You Tube, Group Discussion, Seminar, Quiz, Formative Assessments, Brain storming, Activity.

COURSE OUTCOMES:

CO1: Define environmental studies and its interdisciplinary nature
CO2: Analyze the structure and functions of various ecosystems, including aquatic ecosystems.
CO3: Evaluate the growing energy needs and the role of alternative energy sources
CO4: Understand levels of biodiversity (genetic, species, and ecosystem) and identify biodiversity hotspots, with a focus on conservation strategies.
CO5: Evaluate the effects of human population growth on the environment and the importance of disaster management, resettlement, and environmental movements

Textbooks

1. Environmental and Sustainable Development, Keiji Ujikawa, Mikio Ishiwatari, Eric van Hullebusch, 1st Edition, springer publishers, 2022
2. Environmental Science: Toward A Sustainable Future, Dorothy F. Bourse and Richard T. Wright, 13th edition,Pearson publishers, 2017.
3. Social Learning in Environmental Management: Towards a Sustainable Future, Meg Keen, Valerie A. Brown, Rob Dyball, 2005

Reference Books:

1. "Waste Water Treatment", Rao, M.N., Datta, A.K.,Oxford and IBH Publishing Co. Pvt. Ltd, 1987.
2. "Fundamentals of Ecology", Odum, E.P., Odum, H.T., and Andrews, J., Saunders, Philadelphia, 1971.

Mapping of Course Outcomes (COs) with PSOs

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO11	PO 12	PS O1	PS O2	PS O3
CO1	0	0	1	0	0	0	2	0	0	0	0	0	0	0	0
CO2	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0
CO3	0	1	1	0	0	0	1	0	0	0	0	0	0	0	0
CO4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C05	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

3 – high, 2 – Average, 1 - low , 0-null

Programme	BTech CSE- Cyber Security	Programme Code	BTCY
Course Code	25BTCY221	Number of Hours/WK	2
Semester	II	Max. Marks	100
Year	II	Credit	1

Course Title	PYTHON PROGRAMMING LABORATORY	L	T	P
		0	0	2

COURSE OBJECTIVE:

The main learning objective of this course is to prepare the students for:

- To learn fundamentals in python programming language
- To introduce python modules for application
- To familiarize python framework for machine learning applications
- To develop machine learning application using python
- To implement research topic as part of python

project List of experiments:

S.NO	TITLE
1	Implement basic algebraic problems to get into python programming
2	Implement string manipulations problems using python
3	Implement problems using python datatypes such as tuple, list, dictionary etc.
4	Implement problems for python loops, conditional statements and functions
5	Implement object oriented programming concepts in python to solve different problems
6	Implement problems for python file manipulations
7	Implement standard machine learning algorithms using python frameworks such as TensorFlow, PyTorch etc.
8	Implement adavanced problems using python tools in a virtual environment as part of python project

Course outcome:

On successful completion of this course, the student will be able to

CO1 : Develop basic coding skills in python
CO2 : Understand python datatypes, modules, frameworks etc.
CO3 : Implement standard ML algorithms using python tools
CO4 : Apply python frameworks for ML applications
CO5 : Create ML model for existing problems

Mapping of Course Outcomes (COs) with POs PSOs

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO1 0	PO1 1	PO 12	PS O1	PS O2	PS O3
CO1	**3**	**1**	**3**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**2**	**2**	**0**	**0**
CO2	**3**	**3**	**2**	**3**	**1**	**2**	**0**	**2**	**1**	**1**	**0**	**2**	**2**	**0**	**0**
CO3	**3**	**2**	**3**	**2**	**3**	**1**	**1**	**0**	**0**	**1**	**0**	**2**	**3**	**1**	**1**
CO4	**3**	**2**	**3**	**2**	**1**	**2**	**1**	**0**	**1**	**1**	**0**	**1**	**3**	**1**	**1**
CO5	**2**	**2**	**3**	**3**	**3**	**0**	**1**	**3**	**1**	**1**	**1**	**1**	**3**	**3**	**3**

Programme	**B.Tech CSE- Cyber Security**	**Programme Code**	**BTCY**
Course Code	**25BTCY 222**	**Number of Hours/Week**	**2**
Semester	**II**	**Max. Marks**	**100**
Year	**II**	**Credits**	**1**

Course

Course Title	**PHYSICS LAB**	**L**	**T**	**P**
		0	**0**	**2**

L-Lecture Hours T-Tutorial Hours P-Practical Hours

At the end of the courses, the student will be able to

- Understand the concept of lasers and its action in industries.
- Explain the principle of fiber optics for different types of industrial sensors.
- Apply the basics of Lasers and Optical fibers.
- Study the principles and applications of acoustics.
- Discern the laws governing acoustics and its applications in acoustic quieting.
- Relate the application of light in optical devices.

	List of experiments	
1	Wavelength Determination – LASER diffraction	
2	Particle size Determination – LASER diffraction	
3	Attenuation of an Optical fibre– Fibre Optic Cable	
4	Numerical Aperture measurement of an Optical Fibre– Fibre Optic cable	
5	Determination of Planck's constant – LED	
6	Reverberation Time of a hall - Acoustics	
7	Refractive index of a prism – Spectrometer	
8	Wavelength of Mercury spectrum – Diffraction grating – Spectrometer	

Mapping of Course Outcomes (COs) with PSOs - cybersecurity

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO1 0	PO1 1	PO 12	PS O1	PS O2	PS O3
CO1	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0
CO2	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0
CO3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CO4	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0
C05	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0

3 – high, 2 – Average, 1 - low , 0-null

Semester III

SEMESTER - III

Programme	**B. Tech CSE- Cybersecurity**	**Programme Code**	**BTCY**		
Course Code	**25BTCY131**	**Number of Hours/Week**	**3**		
Semester	**III**	**Max. Marks**	**100**		
Year	**II**	**Credits**	**3**		
Course					
Course Title	**FUNDAMENTALS OF INFORMATION AND DATA SECURITY**		**L**	**T**	**P**
			3	**0**	**0**

L-Lecture Hours T-Tutorial Hours P-Practical Hours

COURSE OBJECTIVES:

- **Define** the fundamental goals, key concepts, and terminology of information security, and **differentiate** between various types of security threats, attacks, and control mechanisms.
- **Explain** the core principles of modern cryptography, including symmetric and asymmetric encryption, hash functions, and digital signatures, and **analyze** their practical applications in technologies like SSL/TLS and VPNs.
- **Compare and contrast** different access control models (DAC, MAC, RBAC) and **evaluate** various authentication methods (passwords, biometrics, tokens) and identity management solutions (SSO, Federated Identity).
- **Identify** and **describe** common software security vulnerabilities (e.g., OWASP Top 10) and **apply** secure coding practices and tools throughout the Secure Software Development Lifecycle (SDLC) to mitigate risks.
- **Explain** the components of an information security governance program, including security policies, risk management, and incident response procedures, and **recognize** the importance of compliance and regulatory requirements.

UNIT	TOPICS	HOURS
I	Introduction to Information Security Overview of Information Security, Key Concepts and Terminology, Goals of Information Security, Security Threats and Attacks, Security Controls and Countermeasures	**9**
II	Cryptography Principles of Cryptography, Symmetric and Asymmetric Encryption, Hash Functions and Message Digests, Digital Signatures and Certificates, Cryptographic Applications: SSL/TLS, PGP, VPNs	**9**
III	Access Control and Authentication Access Control Models, DAC, MAC, RBAC, Authentication Methods, Passwords, Biometrics, Tokens, Single Sign On (SSO) and Federated Identity, Role Based Access Control (RBAC), Access Control Lists (ACLs) and Permissions	**9**
IV	Security in Software Development Secure Software Development Lifecycle (SDLC), Common Software Security Vulnerabilities (OWASP Top 10), Secure Coding Practices, Code Review and Static Analysis Tools, Secure Development Frameworks and Libraries	**9**
V	Security Management and Governance Security Policies, Standards, and Procedures, Risk Management and Assessment Security Incident Handling and Response, Security Awareness and Training Compliance and Regulatory Requirements.	**9**

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1: Understand the Information security system, mechanisms and CIA triad

CO2: Apply the different cryptographic operations of symmetric, asymmetric algorithms, authentication schemes

CO3: Evaluate and differentiate access control models along with various authentication methods.

CO4: Assess and Enhance security in SDLC by applying code reviews and utilizing static analysis tools.

CO5: Create and evaluate comprehensive security policies, Implement governance frameworks, ensure compliance to manage organizational security risks.

Text Books:

1. Principles of Information Security, Michael E. Whitman and Herbert J. Mattord, 6th edition, 2017.
2. Cryptography and Network Security: Principles and Practices, William Stallings, 7th edition, 2017.

Reference Books:

1. CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide, Mike Chapple, James Michael Stewart, Darril Gibson, 8th edition, 2018.
2. Security Engineering: A Guide to Building Dependable Distributed Systems, Ross J. Anderson, 2 nd edition, 2018.

Mapping of Course Outcomes (COs) with PSOs

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO1 0	PO1 1	PO 12	PSO1	PS O2	PS O3
CO1	2	3	0	0	0	0	0	0	0	2	0	0	2	1	1
CO2	3	3	0	2	2	0	0	0	0	0	0	0	2	1	1
CO3	0	0	3	0	3	0	0	0	0	0	2	0	3	2	2
CO4	0	0	0	2	2	2	0	0	0	0	0	0	1	1	1
C05	2	2	2	0	0	0	0	0	0	0	0	0	1	1	1

3 – high, 2 – Average, 1 - low , 0-null

Programme	B.Tech CSE-Cybersecurity	Programme Code	BTCY		
Course Code	25BTCY132	Number of Hours/Week	3		
Semester	III	Max. Marks	100		
Year	II	Credits	3		
Course					
Course Title	SIGNALS AND SYSTEMS		L	T	P
			3	0	0

COURSE OBJECTIVES:

The main aim of learning this course is:

- Understanding the fundamental characteristics of signals and systems.
- Understanding the concepts of vector space, inner product space and orthogonal series.
- Understanding signals and systems in terms of both the time and transform domains, taking advantage of the complementary insights and tools that these different perspectives provide.
- Development of the mathematical skills to solve problems involving convolution, filtering, modulation and sampling.

UNIT	TOPICS	HOURS
I	**Classification of Signals:** Continuous-time vs discrete-time signals, analog vs digital signals, energy and power signals, deterministic vs random signals. Signal Operations: Scaling, time shifting, time inversion, and time scaling of signals. Signal Properties: Symmetry (even and odd signals), periodicity of signals, and absolute integrability. Elementary Signals: Unit step, unit impulse, ramp, exponential, sinusoidal signals.	9
II	**Systems:** Classification of Systems: Continuous-time vs discrete-time systems, linear vs nonlinear systems, causal vs non-causal systems, time-invariant vs time-varying systems, stable vs unstable systems. System Properties: Linearity, time/shift invariance, causality, and stability. LTI and LSI Systems: Continuous-time linear time-invariant (LTI) systems, discrete-time linear shift-invariant (LSI) systems. Impulse and Step Response: Impulse response and step response of systems. Response to Arbitrary Input: Convolution in continuous and discrete time domains. System Representation: Representation of systems using differential equations for continuous-time systems and difference equations for discrete-time systems.	9
III	**Fourier Series and Transforms:**Fourier Series Representation: Fourier series representation of continuous-time periodic signals, Fourier series of discrete-time periodic signals, properties of Fourier series. Continuous-Time Fourier Transform (CTFT): Fourier transform of continuous-time signals, properties of CTFT (linearity, time shifting, time scaling, etc.), Parseval's theorem, and time-bandwidth product. Discrete-Time Fourier Transform (DTFT): Fourier transform of discrete-time signals, properties of DTFT (linearity, time shifting, time scaling, etc.). Relationships among Fourier Representations: Relationship between Fourier series, CTFT, and DTFT.	9
IV	**Laplace Transform and Sampling:** Laplace Transform: Definition of	9

	the Laplace transform, region of convergence (ROC), properties of Laplace transforms (linearity, time shifting, scaling, initial value theorem, final value theorem, etc.), inverse Laplace transform. Sampling: Sampling theorem for bandlimited signals, aliasing in the sampling process, and Nyquist rate. Signal Reconstruction: Ideal signal reconstruction using interpolators, zero-order hold, and first-order hold methods.	
V	**Z-Transform and Discrete Fourier Transform:**Z-Transform: Definition of the z-transform, region of convergence (ROC) for z-transform, properties of the z-transform (linearity, time shifting, scaling, etc.), inverse z-transform (using partial fraction expansion and power series methods). Discrete Fourier Transform (DFT): Definition and properties of the DFT, relationship between DFT and DTFT, computation of DFT, inverse DFT.	**9**

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1 : To Understand different types of signals-continuous and discrete, odd and ever, periodic and aperiodic etc

CO2 : Be able to classify systems based on their properties

CO3 : To familiarize the concepts of transform based continuous time and discrete time

CO4 : Analyze continuous time and discreet time signals and systems by using appropriate mathematical tools

CO5 : Determine Fourier transforms for continuous-time and discrete-time signals (or impulse response functions), and understand how to interpret and plot Fourier transform magnitude and phase functions

Text Books:

1. Stuart Russell and Peter Norvig. Artificial Intelligence: A Modern Approach. Prentice Hall Press, USA, 3rd edition, 2009

Reference Books:

1. Ian J. Goodfellow, Yoshua Bengio, and Aaron Courville. Deep Learning. MIT Press, Cambridge, MA, USA, 2016.
2. Gilbert Strang. Introduction to Linear Algebra. Wellesley-Cambridge Press, USA, 5th edition, 2016.

Mapping of Course Outcomes (COs) with PSOs

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO11	PO 12	PS O1	PS O2	PS O3
CO1	2	0	2	2	0	0	0	0	0	0	0	0	2	1	2
CO2	2	2	0	0	0	0	0	0	0	0	0	0	2	0	2
CO3	2	0	3	3	2	3	0	1	2	0	2	1	1	0	2
CO4	2	2	2	2	2	3	0	1	2	0	2	1	1	0	1
C05	0	0	0	2	1	1	1	1	1	1	2	1	1	0	1

3 – high, 2 – Average, 1 - low , 0-null

Programme	B.Tech CSE-Cybersecurity	Programme Code	BTCY		
Course Code	25BTCY133	Number of Hours/Week	3		
Semester	III	Max. Marks	100		
Year	II	Credits	4		
Course					
Course Title	COMPUTER NETWORKS		L	T	P
			3	0	0

COURSE OBJECTIVES:

The main learning objective of this course is to prepare the students for:

- To understand the concepts of Computer network
- To impart knowledge about networking and inter networking devices
- To analyze the issues met in every layer

UNIT	TOPICS	HOURS
I	**Introduction** – Network Hardware - Software - Reference Models - OSI and TCP/IP Models - Example Networks: Internet, ATM, Ethernet and Wireless LANs - Physical Layer - Theoretical Basis for Data Communication - Guided Transmission Media.	12
II	**Wireless Transmission** - Communication Satellites - Telephone System: Structure, Local Loop, Trunks and Multiplexing and Switching. Data Link Layer: Design Issues - Error Detection and Correction.	10
III	**Elementary Data Link Protocols** - Sliding Window Protocols - Data Link Layer in the Internet - Medium Access Layer - Channel Allocation Problem - Multiple Access Protocols - Bluetooth.	8
IV	**Network Layer** - Design Issues - Routing Algorithms - Congestion Control Algorithms - IP Protocol - IP Addresses - Internet Control Protocols.	8
V	**Transport Layer** - Services - Connection Management - Addressing, Establishing and Releasing a Connection - Simple Transport Protocol - Internet Transport Protocols (ITP) - Network Security: Cryptography.	8

COURSE OUTCOMES:

At the end of the course

- Learn various principles & concepts of Computer networks.
- Analyze different network models.
- Evaluate the data flow through TCP/IP & ISO Layers.
- Assess key networking protocols and their hierarchical relationship In the conceptual model like TCP/IP and OSI
- Identify networking and inter-networking devices

Text book:

1. "Computer Networks", A. S. Tanenbaum, Prentice-Hall of India, Fourth Edition. 2008.

Reference books:

1. "Data and Computer Communications", Stallings, Pearson Education, Seventh Edition, 2012.
2. "Data Communications and Networking", B. A. Forouzan, , Tata McGraw Hill, Fourth Edition, 2007.
3. "Data Communications, Computer Networks and Open Systems", F. Halsall, Pearson Education 2008.

4. “Data Networks”, D. Bertsekas and R. Gallagher, PHI, Second Edition, 2008
5. “Communication Networks”, Lamarca, Tata McGraw Hill, 2002.

Mapping of Course Outcomes (COs) with PSOs

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO11	PO 12	PS O1	PS O2	PS O3
CO1	3	2	0	2	3	1	0	2	1	1	0	2	2	2	0
CO2	3	3	2	2	3	1	0	2	1	2	1	2	2	3	3
CO3	3	3	3	3	2	1	1	2	2	1	1	3	2	3	3
CO4	2	3	3	3	3	2	2	3	2	2	2	3	3	3	3
C05	2	3	3	3	3	2	2	3	2	2	2	3	3	3	3

Programme	B.Tech CSE-Cybersecurity	Programme Code	BTCY
Course Code	25BTCY134	Number of Hours/Week	3
Semester	III	Max. Marks	100
Year	II	Credits	4

Course				
Course Title	DATA STRUCTURE AND ALGORITHMS	L	T	P
		3	0	0

COURSE OBJECTIVES:

The main learning objective of this course is to prepare the students for:

- To Comprehensive understanding of fundamental data structures and algorithms.
- To equip algorithms with the skills to analyze and implement various computational techniques.
- To select appropriate data structures for solving complex problems and optimize algorithm performance.
- To gain insight into advanced topics such as dynamic programming and NP-completeness.

UNIT	TOPICS	HOURS
I	**Introduction to Data Structures Algorithms**- asymptotic notations and analysis- Analysing Algorithms - Insertion sort, Divide and Conquer approach, Sorting, Building Heaps, Heap sort, Quick sort, Analysis of sorting algorithms,	12
II	**Elementary data structures**- Stacks and Queues, linked lists and its operations, Hash Tables - Direct and Open addressing Tree data structure - Tree Traversals-Binary Search Trees-Red Black Trees - Red-black trees and its operations. B-Tree-Insertion-Deletion.	10
III	**Dynamic programming** Memoization, Tabulation, Rod Cutting, Matrix Chain Multiplication, Longest common subsequence, Greedy Algorithms- Introducing greedy approach, activity selection problem, Huffman codes, Graphs, Trees and Algorithms	8
IV	**Introducing spanning trees** Minimum spanning tree, algorithms, Kruskal, Prims, Bellman-Ford algorithm, Single source shortest path in directed acyclic graphs, Dijkstra's algorithms, Floyd-Warshall algorithm	8
V	**NP-Completeness** Polynomial time, Verification algorithms, NP-Complete, NP-Hard	7

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1: Understand the Fundamental Data Structures.
CO2: Apply the concept of stack, queue, list, binary search tree and Red black tree.
CO3: Analyze dynamic programming, greedy algorithms and binary search trees including tree traversals, insertions and deletions.
CO4: Utilize graph representations and perform operations.
CO5: Evaluate the implications of computational complexity for algorithm design and problem-solving strategies including approaches for handling NP-Complete and NP- Hard problems.

Text Books:

1. Cormen, Thomas H., Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. Introduction to algorithms. MIT press, 2022.
2. Data Structures And Algorithms In C++, 2nd Edition by Michael T. Goodrich, 2014.
3. Data Structures and Algorithms Made Easy by Narasimha Karumanchi, 20323.
4. Fundamentals of Data Structures by Ellis Horowitz and Sartaj Sahni, 1978.

ReferenceBooks:

1. Chitra.A, Rajan.P.T , (2016*), Data Structures*, Vijay Nicol Imprints Pvt Ltd, McGraw-Hill Education of India Pvt Ltd, India, SecondEdition.
2. Pai.G.A.V,(2009), *Data Structures andAlgorithms*,TMH.
3. Samanta.D , (2006), *Classic Data Structures*, Prentice Hall of India Pvt Ltd, NewDelhi

Mapping of Course Outcomes (COs) with PSOs

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO1 0	PO1 1	PO 12	PS O1	PS O2	PS O3
CO1	3	2	2	2	3	1	1	2	1	1	0	2	3	2	2
CO2	3	3	3	2	3	1	1	2	1	2	1	2	3	3	2
CO3	3	3	3	3	2	1	1	2	2	2	1	3	3	3	3
CO4	3	3	3	3	3	2	2	3	2	2	2	3	3	3	3
C05	3	3	3	3	3	2	2	3	2	2	2	3	3	3	3

3 – high, 2 – Average, 1 - low , 0-null

Programme	B.Tech CSE-Cybersecurity	Programme Code	BTCY		
Course Code	25BTCY135	Number of Hours/Week	3		
Semester	III	Max. Marks	100		
Year	II	Credits	3		
Course					
Course Title	OBJECT ORIENTED PROGRAMMING WITH JAVA		L	T	P
			3	0	0

L-Lecture Hours **T-Tutorial Hours** **P-Practical Hours**

COURSE OBJECTIVES:

- To demonstrate a clear understanding of the necessity and principles of Object-oriented programming.
- To create applications focusing on Object oriented programming concepts.
- To manage memory using pointers leveraging C++ streams and STL container.
- To develop reusable and modular code using the concepts learned.
- To write diversified solutions using C++ language.

UNIT	TOPICS	HOURS
I	**Basics of Java Programming**: Introduction to Java: Features, JVM, JDK, and JRE.-Writing, compiling, and executing Java programs.-Data types, variables, and operators.-Control structures: Decision-making , loops .-Arrays and Strings: Declaration, initialization, and operations.	9
II	**Object-Oriented Programming in Java Classes and Objects:** Declaration, instantiation, and initialization.-Methods: Static, instance, and parameterized methods -Constructors and destructors. Inheritance: Single, multilevel, hierarchical, and overriding. Polymorphism: Compile-time and runtime. Encapsulation and abstraction. Interfaces and abstract classes.	8
III	**Exception Handling and Multithreading Exception handling:** Try-catch block, multiple catch, finally, throw, and throws. Built in exceptions and user-defined exceptions. Multithreading: Thread lifecycle, creating threads -Thread class, Runnable interface. Thread synchronization and inter-thread communication.	9
IV	**File I/O and Streams** Reading and writing files using FileReader, FileWriter, BufferedReader, and BufferedWriter. Byte and character streams. Serialization and deserialization	9
V	**GUI Programming and Event Handling** Introduction to AWT and Swing-Layout managers -FlowLayout, GridLayout, BorderLayout.Event handling: ActionListener, MouseListener, KeyListener. Creating simple GUI applications.	9

COURSE OUTCOMES:

CO 1: Recall the concepts of structured programming.
CO 2: Understand the differences between structure programming and object-oriented programming
CO 3: Able to execute C++ programs utilizing member functions
CO 4: Implement operator and function overloading to extend the capabilities of the programs
CO 5: Create classes and objects employing data abstraction, encapsulation, inheritance and polymorphism in real-world scenarios.

Text Books

1. "Elements of Discrete Mathematics: A Computer Oriented Approach", C. L. Liu, D. P. Mohapatra, McGraw Hill, Third Edition, 2012.
2. "Applied Discrete Structures", Al Doerr, Ken Levasseur, LibreTexts, Third Edition, 2023.

Reference Books

3. "Discrete Mathematical Structures with applications to Computer Science", Tremblay J.P. and Manohar R., McGraw Hill International Edition, 1987.
4. "Discrete Mathematics and Its Applications", Kenneth H. Rosen, Sixth Edition, Tata McGraw Hill, 2012.

Mapping of Course Outcomes (COs) with PSOs

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PS O1	PS O2	PS O3
CO1	1	1	1	1	2	0	0	0	1	0	2	2	1	1	1
CO2	2	2	2	1	2	0	0	0	1	0	2	2	1	1	1
CO3	1	2	3	1	2	0	0	0	1	0	2	3	1	2	1
CO4	1	2	3	2	2	0	0	0	1	0	2	3	2	2	1
C05	1	2	3	1	2	0	0	0	1	0	3	3	3	3	2

3 – high, 2 – Average, 1 - low , 0-null

Programme	B.Tech CSE-Cybersecurity	Programme Code	BTCY		
Course Code	25BTCY231	Number of Hours/Week	2		
Semester	III	Max. Marks	100		
Year	II	Credits			
Course					
Course Title	DATA STRUCTURE AND ALGORITHMS LAB		L	T	P
			0	0	2

L-Lecture Hours T-Tutorial Hours P-Practical Hours

COURSE OBJECTIVES:

- To implement basic data structures like arrays linked lists, stacks, and queues.
- To develop skills in implementing algorithms for searching and sorting.
- To gain hands-on experience with tree and graph data structures.
- To apply recursion and dynamic memory management in problem-solving.
- To understand the practical implications of algorithm efficiency and optimization.

Programs:

1. Program for Insertion sort.
2. Program for Quick sort.
3. Program for Merge sort.
4. Program for Heap sort.
5. Implementation of a stack using an array with push and pop operations.
6. Implementation of swap () function using stack.
7. Implementation of swap () function using queue.
8. Singly linked list with basic operations.
9. Double linked list with basic operations.
10. Hash table using direct addressing.
11. Hash table using indirect addressing.
12. Binary search tree with insertion and traversal.
13. Graphs
    a. Depth First Search (DFS)
    b. Breadth First Search (BFS)
    c. Dijkstra's Algorithm (Shortest Path in Weighted Graph)
    d. Kruskal's Algorithm (Minimum Spanning Tree)
14. Tree Algorithms
    a. Binary Search Tree (BST) Operations
    b. AVL Tree (Balanced BST) Insertions
15. Verifying a Solution for the Knapsack Problem.

Course Outcomes:

By learning Data Structures and Algorithms, students will be able to

CO1 : Demonstrate the implementation of basic data structures in real-world problems.
CO2 : Apply various searching and sorting techniques in practical scenarios.
CO3 : Implement tree and graph algorithms effectively.
CO4 : Solve complex problems using recursion and dynamic memory management.
CO5 : Analyze and optimize algorithms for better performance in practical applications.

Mapping of Course Outcomes (COs) with PSOs

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO1 0	PO1 1	PO 12	PS O1	PS O2	PS O3
CO1	3	2	2	2	3	1	1	2	1	1	0	2	3	2	2
CO2	3	3	3	2	3	1	1	2	1	2	1	2	3	3	2
CO3	3	3	3	3	2	1	1	2	2	2	1	3	3	3	3
CO4	3	3	3	3	3	2	2	3	2	2	2	3	3	3	3
C05	3	3	3	3	3	2	2	3	2	2	2	3	3	3	3

3 – high, 2 – Average, 1 - low , 0-null

B.Tech CSE-Cybersecurity	Programme Code	BTCY		
25BTCY232	Number of Hours/Week	2		
III	Max. Marks	100		
II	Credits			
PROGRAMMING WITH JAVA LAB		L	T	P
		0	0	2

TOPICS

1. Write a Java program to calculate the factorial of a number using loops.
2. Implement a program to demonstrate the use of arrays and string operations (reverse, concatenate, length).
3. Create a program to find the largest and smallest numbers in an array.
4. Create a class Student with properties name, rollNumber, and marks. Write methods to calculate and display the grade.
5. Demonstrate single and multilevel inheritance using classes for Shape, Rectangle, and Square.
6. Implement polymorphism using method overloading and method overriding.
7. Write a program to handle ArrayIndexOutOfBoundsException and NumberFormatException.
8. Create a multithreaded program to calculate the sum of odd and even numbers in an array using two threads.
9. Demonstrate thread synchronization by simulating a producer-consumer problem.
10. Write a program to copy the contents of one text file to another using FileReader and FileWriter.
11. Implement a program to serialize and deserialize an object of a class Employee.
12. Create a program to count the number of words and characters in a text file.
13. Create a simple calculator using AWT/Swing with basic arithmetic operations.
14. Develop a GUI application to accept student details and display them in a table format.
15. Create a Java Swing application to simulate a login screen with username and password validation.

COURSE OUTCOMES

CO1: Demonstrate an understanding of the foundational principles of structured programming.
CO2: Differentiate between structured programming and object-oriented programming paradigms. **CO3:** Develop C++ programs using member functions effectively.
CO4: Apply operator and function overloading techniques to enhance program functionality.
CO5: Implement classes and objects using principles of data abstraction, encapsulation, inheritance, and polymorphism in real-world applications.

Mapping of Course Outcomes (COs) with PSOs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	1	1	1	1	2	0	0	0	1	0	2	2	1	1	1
CO2	2	2	2	1	2	0	0	0	1	0	2	2	1	1	1
CO3	1	2	3	1	2	0	0	0	1	0	2	3	1	2	1
CO4	1	2	3	2	2	0	0	0	1	0	2	3	2	2	1
C05	1	2	3	1	2	0	0	0	1	0	3	3	3	3	2

3 – high, 2 – Average, 1 - low , 0-null

Programme	B.Tech CSE-Cybersecurity	Programme Code	BTCY		
Course Code	25BTCY233	Number of Hours/Week	2		
Semester	III	Max. Marks	100		
Year	II	Credits			
Course					
Course Title	COMPUTER NETWORKS LAB		L	T	P
			0	0	2

COURSE OBJECTIVES:

The main learning objective of this course is to prepare the students for:

- To understand the concepts of Computer network
- To impart knowledge about networking and inter networking devices
- To analyze the issues met in every layer

TOPICS

1. Implement the data link layer framing methods such as character, character stuffing and bit stuffing.
2. Implement on a data set of characters the three CRC polynomials – CRC 12, CRC 16 and CRC CCIP.
3. Implement Dijkstra‘s algorithm to compute the Shortest path thru a graph.
4. Take an example subnet graph with weights indicating delay between nodes. Now obtain Routing

table art each node using distance vector routing algorithm

5. Take an example subnet of hosts. Obtain broadcast tree for it.
6. Take a 64 bit playing text and encrypt the same using DES algorithm.
7. Write a program to break the above DES coding
8. Using RSA algorithm encrypt a text data and decrypt the same.

Mapping of Course Outcomes (COs) with PSOs

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO11	PO 12	PS O1	PS O2	PS O3
CO1	3	2	0	2	3	1	0	2	1	1	0	2	2	2	0
CO2	3	3	2	2	3	1	0	2	1	2	1	2	2	3	3
CO3	3	3	3	3	2	1	1	2	2	1	1	3	2	3	3
CO4	2	3	3	3	3	2	2	3	2	2	2	3	3	3	3
C05	2	3	3	3	3	2	2	3	2	2	2	3	3	3	3

3 – high, 2 – Average, 1 - low, 0-null

Programme	B.Tech CSE-Cybersecurity	Programme Code	BTCY
Course Code	25BTCY136	Number of Hours/Week	2
Semester	III	Max. Marks	100
Year	II	Credits	

Course

Course Title	PROFESSIONAL ETHICS	L	T	P
		2	0	0

COURSE OBJECTIVES:

The main learning objective of this course is to prepare the students for:

- To identify and understand key concepts of human values, including ethics, integrity, and professional responsibility.
- To explore moral theories and frameworks related to engineering ethics, and analyze how these impact decision-making.
- To evaluate the role of engineers in society through the lens of social experimentation, responsibility, and professional codes of conduct.
- To assess safety and risk management principles, rights and responsibilities, including intellectual property and occupational ethics.

UNIT	TOPICS	HOURS
I	**Human Values** Morals, values and Ethics – Integrity – Work ethic – Service learning – Civic virtue – Respect for others – Living peacefully – Caring – Sharing – Honesty – Courage – Valuing time – Cooperation – Commitment – Empathy – Self-confidence – Character - Spirituality – Introduction to Yoga and meditation for professional excellence and stress management.	6
II	**Engineering Ethics** Senses of Engineering Ethics – Variety of moral issues – Types of inquiry – Moral dilemmas – Moral Autonomy – Kohlberg's theory – Gilligan's theory – Consensus and Controversy – Models of professional roles - Theories about right action – Self-interest, Customs and Religion – Uses of Ethical Theories.	6
III	**Engineering as Social Experimentation** Engineering as Experimentation – Engineers as responsible Experimenters – Codes of Ethics – A Balanced Outlook on Law.	6
IV	**Safety, Responsibilities and Rights** Safety and Risk – Assessment of Safety and Risk – Risk Benefit Analysis and Reducing Risk - Respect for Authority – Collective Bargaining – Confidentiality – Conflicts of Interest – Occupational Crime – Professional Rights – Employee Rights – Intellectual Property Rights (IPR) – Discrimination.	6
V	**Global issues** Multinational Corporations – Environmental Ethics – Computer Ethics – Weapons Development – Engineers as Managers – Consulting Engineers – Engineers as Expert Witnesses and Advisors – Moral Leadership –Code of Conduct – Corporate Social Responsibility.	6

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

Recognize the significance of human values and ethics in personal and professional life.

Analyze various moral theories and ethical dilemmas in various practices.

Evaluate the responsibilities of engineers as experimenters and decision-makers within legal and ethical frameworks.

Assess risk and safety issues, including intellectual property and employee rights in various contexts.

Apply ethical theories and frameworks to make informed decisions.

Text Books:

1. "A Textbook on Professional Ethics and Human Values" Naagarazan, R.S., New Age International Limited Publishers: New Delhi, 2006.

Reference Books:

1. "Engineering Ethics ǁ", Charles B. Fleddermann, - Pearson Prentice Hall, New Jersey, 2004.
2. "Engineering Ethics – Concepts and Cases ǁ", Charles E. Harris, Michael S. Pritchard and Michael J. Rabins, Cengage Learning, 2009.

Mapping of Course Outcomes (COs) with PSOs - cybersecurity

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO1 0	PO1 1	PO 12	PS O1	PS O2	PS O3
CO1	0	0	0	0	0	2	0	0	2	2	0	0	0	0	0
CO2	0	0	0	0	0	0	0	0	0	3	0	0	0	0	2
CO3	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0
CO4	0	0	0	0	0	0	0	0	0	3	0	0	0	0	3
C05	0	0	0	0	0	0	2	0	0	3	0	0	0	0	0

3 – high, 2 – Average, 1 - low , 0-null

Semester IV

SEMESTER - IV

Programme	**B.Tech CSE-Cybersecurity**	**Programme Code**	**BTCY**
Course Code	**25BTCY141**	**Number of Hours/Week**	**3**
Semester	**IV**	**Max. Marks**	**100**
Year	**II**	**Credits**	**3**

Course				
Course Title	**CRYPTOGRAPHY, CRYPTANALYSIS AND NETWORK SECURITY**	**L**	**T**	**P**
		3	**0**	**0**

COURSE OBJECTIVES:

The main learning objective of this course is to prepare the students for:

- To understand basics of Cryptography and Network Security.
- To be able to secure a message over insecure channel by various means.
- To learn about how to maintain the Confidentiality, Integrity and Availability of a data.
- To understand various protocols for network security to protect against the threats in the networks.

UNIT	TOPICS	HOURS
I	**Introduction to Cryptography and Block Ciphers** Introduction to security attacks - services and mechanism - introduction to cryptography - Conventional Encryption: Conventional encryption model – classical encryption techniques - substitution ciphers and transposition ciphers – cryptanalysis – steganography - stream and blockciphers - Modern Block Ciphers: Block ciphers principals - Shannon's theory of confusion anddiffusion - fiestal structure – data encryption standard(DES) - strength of DES - differential and linearcrypt analysis of DES - block cipher modes of operations - triple DES – AES.	8
II	**Confidentiality and Modular Arithmetic** Confidentiality using conventional encryption - traffic confidentiality - key distribution - random number generation - Introduction to graph - ring and field - prime and relative prime numbers - modular arithmetic - Fermat's and Euler's theorem - primality testing - Euclid's Algorithm - Chinese Remainder theorem - discrete algorithms.	8
III	**Public key cryptography and Authentication requirements** Principles of public key crypto systems - RSA algorithm - security of RSA – key management – Diffle-Hellman key exchange algorithm - introductory idea of Elliptic curve cryptography – Elgamel encryption - Message Authentication and Hash Function: Authentication requirements - authentication functions – message authentication code - hash functions - birthday attacks – security of hash functions and MACS.	8
IV	**Integrity checks and Authentication algorithms** MD5 message digest algorithm - Secure hash algorithm (SHA) Digital Signatures-Digital Signatures - authentication protocols - digital signature standards (DSS) - proof of digital signature algorithm - Authentication Applications: Kerberos and X.509 - directory authentication service - electronic mail security-pretty good privacy (PGP) - S/MIME.	8
V	**IP Security and Key Management** IP Security: Architecture - Authentication header - Encapsulating security payloads - combining security associations - key management. Unit VI (Web and System Security) Web Security: Secure socket layer and transport layer security – secure electronic transaction (SET) - System Security: Intruders - Viruses and	8

	related threads - firewall design principals – trusted systems.	

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

- Provide security of the data over the network.
- Implement various networking protocols.
- Protect any network from the threats in the world
- Research in the emerging areas of cryptography and network security.
- Implement the security in real time systems

Text Books:

1. William Stallings, "Cryptography and Network security- Principles and Practices", Pearson/PHI, 8th edition, 2020.
2. Wade Trappe, Lawrence C Washington, "Introduction to Cryptography with coding theory", Pearson, 3rd edition, 2020.

Reference Books:

1. "Modern Cryptography – Theory and Practice", W. Mao, Pearson Education, 1st edition, 2003.
2. "Security in computing", Charles P. Pfleeger, Shari Lawrence Pfleeger –Prentice Hall of India, 5th edition, 2015.

Mapping of Course Outcomes (COs) with PSO

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO11	PO 12	PS O1	PS O2	PS O3
CO1	0	1	0	0	0	2	0	0	2	2	0	0	0	1	0
CO2	2	0	0	0	0	0	0	0	0	3	0	0	0	0	2
CO3	0	3	0	0	0	0	1	0	0	3	0	0	0	0	0
CO4	0	0	1	0	0	0	0	0	0	3	0	0	2	0	3
C05	0	0	0	0	0	0	2	0	0	3	0	0	0	0	0

3 – high, 2 – Average, 1 - low , 0-null

Programme	B.Tech CSE-Cybersecurity	Programme Code	BTCY
Course Code	25BTCY142	Number of Hours/Week	3
Semester	IV	Max. Marks	100
Year	II	Credits	3

Course

Course Title	DATABASE MANAGEMENT SYSTEMS	L	T	P
		3	0	0

COURSE OBJECTIVES:

The main learning objective of this course is to prepare the students for:

- To learn data models, conceptualize and depict a database system using ER diagram
- To understand the internal storage structures in a physical DB design
- To know the fundamental concepts of transaction processing techniques
- To understand the concept of Database Design in Normalization techniques
- To know the manipulation of SQL Queries

UNIT	TOPICS	HOURS
I	**Data base System Applications**, Purpose of Database Systems, View of Data, Data Abstraction, Instances and Schemas, data Models , the ER Model , Relational Model , Other Models , Database Languages , DDL , DML , database Access for applications Programs, data base Users and Administrator , Transaction Management , data base Architecture, Storage Manager , the Query Processor Data base design and ER diagrams , ER Model, Entities, Attributes and Entity sets , Relationships and Relationship sets , ER Design Issues, Concept Design , Conceptual Design for University Enterprise. Introduction to the Relational Model, Structure, Database Schema, Keys, Schema Diagrams.	9
II	**Relational Query Languages,** Relational Operations. Relational Algebra, Selection and projection set operations, renaming, Joins, Division, Examples of Algebra overviews, Relational calculus , Tuple relational Calculus , Domain relational calculus. Overview of the SQL Query Language, Basic Structure of SQL Queries, Set Operations, Aggregate Functions, GROUPBY, HAVING, Nested Sub queries, Views, Triggers.	9
III	**Normalization,** Introduction, Non loss decomposition and functional dependencies, First, Second, and third normal forms, dependency preservation, Boyee/Codd normal form. Higher Normal Forms, Introduction, Multi,valued dependencies and Fourth normal form, Join dependencies and Fifth normal form	9
IV	**Transaction State**, Implementation of Atomicity and Durability, Concurrent, Executions, Serializability, Recoverability, Implementation of Isolation, testing for serializability, Lock Based Protocols, Timestamp Based Protocols, Validation, Based Protocols, Multiple Granularity. Recovery and Atomicity, Log Based Recovery, Recovery with Concurrent Transactions, Buffer Management, Failure with loss of nonvolatile storage,Advance Recovery systems, Remote Backup systems.	9
V	**File organization**, various kinds of indexes. Query Processing, Measures of query cost, Selection operation, Projection operation, Join operation, set operation and aggregate operation , Relational Query Optimization , Transacting SQL queries , Estimating the cost , Equivalence Rules.	9

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1 Install a relational database management system
CO2 Master the basics of SQL and construct queries using SQL
CO3 Design large database with optimal query processing
CO4 Develop efficient storage scheme for saving and retrieving Records and Files

CO5 Design the database with normalization techniques

Text Books

1. "Data base System Concepts", Silberschatz, Korth, McGraw hill, Sixth Edition, 2010
2. "Data base Management Systems" , Raghurama Krishnan, Johannes Gehrke, TATA McGrawHill Third Edition, 2003.

Reference Books

1. "Fundamentals of Database Systems", Elmasri Navathe Pearson Education, 2015
2. "An Introduction to Database systems", C.J. Date, A.Kannan, S.Swami Nadhan, Pearson, Eight Edition,2019.

Mapping of Course Outcomes (COs) with PSOs

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO11	PO 12	PS O1	PS O2	PS O3
CO1	2	0	2	2	0	0	0	0	0	0	0	0	1	0	0
CO2	2	2	0	0	0	0	0	0	0	0	0	0	0	0	2
CO3	2	0	3	3	2	3	0	1	2	0	2	1	0	0	0
CO4	2	2	2	2	2	3	0	1	2	0	2	1	1	1	3
C05	0	0	0	2	1	1	1	1	1	1	2	1	2	0	0

3 – high, 2 – Average, 1 - low , 0-null

Programme	B.Tech CSE-Cybersecurity	Programme Code	BTCY
Course Code	25BTCY143	Number of Hours/Week	3
Semester	IV	Max. Marks	100
Year	II	Credits	3

Course

Course Title	COMPUTER ORGANIZATION AND ARCHITECTURE	L	T	P
		3	0	0

COURSE OBJECTIVES:

The main learning objective of this course is to prepare the students for:

- To understand the basic hardware and software issues of computer organization
- To understand the representation of data at machine level
- To understand how computations are performed at machine level
- To understand the memory hierarchies, cache memories and virtual memories
- To learn the different ways of communication with I/O devices

UNIT	TOPICS	HOURS
I	**Introduction**, Technologies for building Processors and Memory, Performance, The Power Wall, Operations of the Computer Hardware, Operands Signed and Unsigned numbers, Representing Instructions, Logical Operations, Instructions for Making Decisions	10
II	**MIPS Addressing** for 32, Bit Immediates and Addresses, Parallelism and Instructions: Synchronization, Translating and Starting a Program, Addition and Subtraction, Multiplication, Division, Floating Point, Parallelism and Computer Arithmetic: Subword Parallelism, Streaming SIMD Extensions and Advanced Vector Extensions in x86.	9
III	**Logic Design Conventions** - Building a Datapath, A Simple Implementation Scheme, overview of Pipelining, Pipelined Datapath, Data Hazards: Forwarding versus Stalling, Control Hazards, Exception, Parallelism via Instructions, The ARM Cortex–A8 and Intel Core i7 Pipelines, Instruction, Level Parallelism and Matrix Multiply Hardware Design language.	10
IV	**Memory Technologies**, Basics of Caches, Measuring and Improving Cache Performance, dependable memory hierarchy, Virtual Machines, Virtual Memory, Using FSM to Control a Simple Cache, Parallelism and Memory Hierarchy: Redundant Arrays of Inexpensive Disks, Advanced Material: Implementing Cache Controllers.	10
V	**Disk Storage and Dependability**, Parallelism and Memory Hierarchy: RAID levels, performance of storage systems, Introduction to multi-threading clusters, message passing multiprocessors.	7

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1 Understand the architecture and functionality of central processing unit

CO2 Analyze the abstraction of various components of a computer

CO3 Analyze the hardware and software issues and the interfacing

CO4 Work out the trade-offs involved in designing a modern computer system

CO5 Understand the various memory systems and I/O communication

Text Books:

1. "Computer Organization and Design, The Hardware/Software Interface", David A. Patterson, John L. Hennessey, fifth edition, Morgan Kauffman/Elsevier, 2014.
2. "Computer Organization and Architecture", Smruti Ranjan Sarangi, McGraw Hill Education, 2015.

Reference Books:

1. "Computer Organization", V. Carl Hamacher, Zvonko G. Varanesic, Safat G. Zaky, Sixth Edition, McGrawHill Inc., 2012.
2. "Computer Organization and Architecture", William Stallings, Eighth Edition, Pearson Education, 2010.

Mapping of Course Outcomes (COs) with PSOs - cybersecurity

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PS O1	PS O2	PS O3
CO1	2	1	1	2	1	2	2	1	2	2	1	3	3	2	1
CO2	3	3	1	2	3	1	2	2	2	2	1	3	2	1	1
CO3	3	3	3	2	2	1	1	1	1	1	3	3	3	3	2
CO4	2	3	1	3	2	2	2	2	1	1	1	3	3	2	2
C05	3	3	2	3	2	2	1	1	1	1	1	3	3	2	2

3 – high, 2 – Average, 1 - low , 0-null

Programme	B.Tech CSE-Cybersecurity	Programme Code	BTCY		
Course Code	25BTCY841	Number of Hours/Week	3		
Semester	IV	Max. Marks	100		
Year	II	Credits	3		
Course					
Course Title	ENGINEERING ECONOMICS & FOREIGN TRADE		L	T	P
			3	0	0

L-Lecture Hours T-Tutorial Hours P-Practical Hours

COURSE OBJECTIVES:

- **Explain** fundamental economic concepts such as scarcity, efficiency, and opportunity cost, and **analyze** how societies address basic economic problems using models like the Production Possibility Frontier (PPF).
- **Analyze** consumer and producer behavior by examining the forces of demand and supply, **evaluate** market equilibrium, and **differentiate** between short-run and long-run production and cost functions.
- **Compare and contrast** various market structures (perfect competition, monopoly, oligopoly) in product and factor markets, and **assess** their implications for market efficiency, pricing, and general equilibrium.
- **Apply** engineering economics principles to estimate and **classify** costs (e.g., fixed, variable, sunk, life-cycle costs) and **utilize** estimation models and cost indexes for effective project decision-making.
- **Describe** the fundamentals of international trade, including the balance of trade and balance of payments, and **evaluate** the advantages, disadvantages, and global impact of market globalization.

UNIT	TOPICS	HOURS
I	**Introduction** The themes of economics – scarcity and efficiency – three fundamental economic problems – society's capability – Production possibility frontiers (PPF) – Productive efficiency Vs economic efficiency – economic growth & stability – Micro economies and Macro economies – the role of markets and government – Positive Vs negative externalities.	9
II	**Consumer and Producer Behaviour** Market – Demand and Supply – Determinants – Market equilibrium – elasticity of demand and supply – consumer behavior – consumer equilibrium – Approaches to consumer behavior – Production – Short-run and long-run Production Function – Returns to scale – economies Vs diseconomies of scale – Analysis of cost – Short- run and long-run cost function – Relation between Production and cost function	9

III	**Product and Factor Market** Product market – perfect and imperfect market – different market structures – Firm's equilibrium and supply – Market efficiency – Economic costs of imperfect competition – factor market – Land, Labour and capital – Demand and supply – determination of factor price – Interaction of product and factor market – General equilibrium and efficiency of competitive markets.	**9**
IV	**Engineering Costs & Estimation** Fixed, Variable, Marginal & Average Costs, Sunk Costs, Opportunity Costs, Recurring And Nonrecurring Costs, Incremental Costs, Cash Costs vs Book Costs, Life-Cycle Costs; Types Of Estimate, Estimating Models - Per-Unit Model, Segmenting Model, Cost Indexes, Power-Sizing Model. Inflation, Types of Index, Composite vs Commodity Indexes, Use of Price Indexes In Engineering Economic Analysis.	**9**
V	**Foreign Trade** Introduction, Definition of Foreign Trade, balance of Trade, difference between international and domestic business, Advantages and Disadvantages of International Business, Globalization of Markets, Trends in Globalization, Effects and Benefits of Globalization, balance of payment and foreign exchange.	**9**

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1:	Understand the fundamental themes of economics
CO2:	Demonstrate market dynamics including demand and supply and their determinants.
CO3:	Appraise the firm equilibrium and supply in relation to market efficiency.
CO4:	Illustrate the different engineering cost concepts, including fixed, variable, and opportunity costs, and apply these concepts to perform break-even analysis.
CO5:	Evaluate the globalization trends, balance of payments and foreign exchange dynamics.

Text Books:

Textbook:

1. Karl E. Case and Ray C. fair, Principles of Economics, 7th edition, Pearson, Education Asia, New Delhi, 2022.

Reference Books:

1. Paul A. Samuelson, William D. Nordhaus, Sudip Chaudhuri and Anindya Sen, Economics, 19thedition, Tata McGraw Hill, New Delhi, 2021
2. William Boyes and Michael Melvin, Textbook of economics, Biztantra, 2022.
3. N. Gregory Mankiw, Principles of Economics, 8th edition, Thomson learning, New Delhi,2021.

Mapping of Course Outcomes (COs) with PSOs

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO1 0	PO1 1	PO 12	PS O1	PS O2	PS O3
CO1	0	1	0	1	0	0	0	0	1	0	1	0	0	0	0
CO2	0	1	0	1	0	1	0	0	1	0	1	0	0	0	0
CO3	0	1	0	1	0	0	0	0	1	0	1	0	0	0	0
CO4	0	1	0	1	0	0	0	0	1	0	2	0	0	0	0
C05	0	1	0	1	0	0	0	0	1	0	1	0	0	0	0

3 – high, 2 – Average, 1 - low , 0-null

Discipline Specific Elective - I

Programme	B. Tech CSE Cyber Security	Programme Code	BTCY
Course Code	25BTCY341	Number of Hours/ Week	3
Semester	IV (Discipline Specific Elective I)	Max. Marks	100
Year	II	Credits	3

Course

Course Title	CONTINUAL LEARNING	L	T	P
		3	0	0

COURSE OBJECTIVES:

The main aim of this course is to prepare the students for:

- To understand the fundamental concepts and significance of Continual Learning (CL).
- To understand Regularization-based approaches like EWC (Elastic Weight Consolidation) and Synaptic Intelligence (SI).
- To investigate Natural Language Processing (NLP) models with CL, including Transformer-based methods.
- To explore Federated Continual Learning (FCL) and its role in Edge AI & Distributed Learning.
- To identify open challenges and limitations of existing CL models.

UNIT	TOPICS	HOURS
I	**Introduction to Continual Learning (CL):** Definition and Scope of Continual Learning - Key Challenges: Catastrophic Forgetting, Plasticity - Stability Tradeoff, Transfer & Retention of Knowledge Comparison with Related Fields: Online Learning, Meta - Learning, Incremental Learning, Types of CL Paradigms: Task-incremental, Class - incremental, Domain-incremental, Online Learning Applications: Robotics, Healthcare, Finance, Autonomous Systems, NLP.	10
II	**Approaches & Strategies for Continual Learning:** Replay - based Methods: Experience Replay, Generative Replay - Memory - Augmented Neural Networks (MANN), Regularization -based Methods: Elastic Weight Consolidation (EWC) - Synaptic Intelligence (SI)- Learning without Forgetting (LwF), Architectural Strategies: Progressive Neural Networks - PackNet & PathNet - Dynamic Expansion Models.	9
III	**Continual Learning in Deep Learning & NLP:** Computer Vision Applications- Incremental Image Classification- Domain Adaptation for CL, Natural Language Processing (NLP)- Transfer Learning in NLP- Transformer-based CL (Adapter Layers, Prompt Learning) - Self-Supervised Learning in Continual Learning.	9

IV	**Reinforcement Learning & Federated Continual Learning:** Continual Learning in Reinforcement Learning (RL) : Policy Gradient Methods & Zero- shot Transfer - Curriculum Learning & Lifelong RL, Federated Continual Learning (FCL): CL in Edge AI & Distributed Systems- Privacy-Preserving Continual Learning.	9
V	**Challenges, Ethical Considerations & Future Directions:** Challenges in Continual Learning: Model Adaptation & Forgetting Mitigation - Bias & Fairness in Continual Learning Models - Industry Applications & Emerging Trends Future of Continual Learning in AI & Robotics	8

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

- **CO1 :** Understand Fundamentals of Continual Learning
- **CO2 :** Apply and Compare Different Continual Learning Strategies
- **CO3 :** Implement Continual Learning in Deep Learning and NLP
- **CO4 :** Explore Reinforcement Learning & Federated Continual Learning
- **CO5 :** Analyze Ethical Considerations & Future Research in Continual Learning

Text Books:

1. Lifelong Machine Learning, Author: Zhiyuan Chen & Bing Liu, Publisher: Morgan & Claypool Publishers, Year: 2018, ISBN: 978-1681733173.
2. Ethics of Artificial Intelligence and Robotics – Markus D. Dubber, Oxford University Press, Publication Date: June 30, 2020, ISBN-13: 978-0190067397.
3. NeurIPS, ICML Research Papers on Ethical AI & Continual Learning.

Reference Books:

1. The Oxford Handbook of Ethics of AI," Editors: Markus D. Dubber, Frank Pasquale, Sunit Das, Publisher: Oxford University Press .Year: 2020, ISBN: 978-0190067397.
2. Transformers for NLP: Build and Train Deep Learning Models for Natural Language Processing, Author: Denis Rothman, Publisher: Packt Publishing, Year: 2021, ISBN: 978-1800208973.

Mapping of Course Outcomes (CO's) with PO's & PSO's

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PS O1	PS O2	PS O3
CO1	3	3	2	2	2	2	1	2	2	3	2	3
CO2	3	3	3	3	3	2	1	2	2	2	3	3
CO3	3	3	3	3	3	2	1	1	2	2	3	3
CO4	3	3	3	3	3	2	2	1	2	3	3	3
CO5	3	2	2	2	2	3	3	3	2	3	2	2

3 – High, 2 – Average, 1 - Low , 0-Null

Programme	B. Tech CSE Cyber Security	Programme Code	BTCY		
Course Code	25BTCY342	Number of Hours/Week	3		
Semester	IV	Max. Marks	100		
Year	II	Credits	3		
Course					
Course Title	SOCIAL NETWORK ANALYSIS		L	T	P
			3	0	0

COURSE OBJECTIVES:

The main learning objective of this course is to prepare the students for:

- Explain the evolution of the Semantic Web, its limitations, and the role of social web platforms in network analysis.
- Apply ontology-based knowledge representation and advanced modelling techniques to social network data.
- Analyse and extract insights from web communities and study their evolution using archival data.
- Evaluate human behaviour in social networks and address privacy, trust, and reputation challenges.
- Utilize visualization techniques and graph theory to analyse and interpret social networks in practical scenarios.

UNIT	TOPICS	HOURS
I	**Unit-I: INTRODUCTION** Introduction to Semantic Web: Limitations of current Web – Development of Semantic Web.Emergence of the Social Web – Social Network analysis: Development of Social Network.Analysis – Key concepts and measures in network analysis – Electronic sources for network.	9
II	**Unit-II: MODELLING, AGGREGATING AND KNOWLEDGEREPRESENTATION** Ontology and their role in the Semantic Web: Ontology-based knowledge Representation –Language – Modelling and aggregating social network data: State-of-the-art in network data.social relationships – Aggregating and reasoning with social network data – Advanced.Representations.	9
III	**Unit-III: EXTRACTION AND MINING COMMUNITIES IN WEB SOCIAL** **NETWORKS:**Extracting evolution of Web Community from a Series of Web Archive – Detecting.	9
IV	**Unit-V: VISUALIZATION AND APPLICATIONS OF SOCIAL NETWORKS** Graph theory – Centrality – Clustering – Node-Edge Diagrams – Matrix representation –Visualizing online social networks, visualizing social networks with matrix-based.representations – Matrix and Node-Link Diagrams – Hybrid representations – Applications –Cover networks – Community welfare – Collaboration networks – Co-Citation networks.	9
V	**Unit-V: PREDICTING HUMAN BEHAVIOR AND PRIVACY ISSUES** Understanding and predicting human behaviour 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 modelsbased on subjective logic – Trust network analysis – Trust transitivity analysis – Combining Trust and reputation – Trust derivation based on trust comparisons.	9

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1: Illustrate the Evolution of the Semantic Web and Social Web Platforms
CO2: Apply Ontology-Based Knowledge Representation and Modeling Techniques
CO3: Extract Insights from Web Communities and Evaluate Evolution
CO4: Assess Human Behavior and Address Privacy, Trust, and Reputation Challenges
CO5: Employ Graph Theory and Visualization Techniques for Social Network Analysis

Text Books:

1. **Semantic Web for the Working Ontologist**: Effective Modeling in RDFS and OWL, **Authors**: Dean Allemang, James Hendle, **Publisher**: Morgan Kaufmann, **Edition**: 2nd Edition (2011)

Reference Books:

1. **The Semantic Web: A Guide to the Future of XML, Web Services, and Knowledge Management**, **Authors**: Tim Berners-Lee, James Hendler, Ora Lassila, **Publisher**: Morgan Kaufmann, **Edition**: 1st Edition (2001)

PO and PSO Mapping Table

CO-PO-PSO Mapping Table:(**B. Tech Cyber security)**

CO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO3
CO1	3	2	1	2	2	1	2	3	2	2	1	1	1	1	1
CO2	3	3	3	2	3	2	2	2	3	3	2	2	2	3	2
CO3	2	3	3	3	3	2	2	2	3	3	2	2	3	3	3
CO4	3	2	2	3	2	2	3	3	2	3	2	3	3	2	3
Co5	3	3	3	2	3	3	3	3	3	3	3	3	3	3	3

3 – high, 2 – Average, 1 - Low , 0-Null

Programme	B.Tech-CSE Cyber Security	Programme Code	BTCY		
Course Code	25BTCY343	Number of Hours/Week	3		
Semester	IV	Max. Marks	100		
Year	II	Credits	3		
Course					
Course Title	NUMBER THERORY IN CRYPTOGRAPHY		L	T	P
			3	0	0

COURSE OBJECTIVES:

- Provide a foundational understanding of cryptographic principles and algorithms
- Explore key concepts in number theory and their application in cryptography.
- Equip students with practical skills in implementing encryption, key exchange, and digital signature protocols.

UNIT	TOPICS	HOURS
I	**Introduction to Cryptography and Computational Complexity.** Basics of Cryptography, Definitions and principles of cryptography, Symmetric vs Asymmetric Encryption, Complexity of Computation, Time and Space complexity, Big O notation in cryptography, Number Theory in Cryptography, Divisibility, prime numbers, greatest common divisor (GCD)	9
II	**Modular Arithmetic and Euclid's Algorithm** Modular Arithmetic- Introduction to Modulo operation, Operations in modular arithmetic, Euclid's Algorithm: GCD and its computation, Extended Euclidean Algorithm, Application in key generation, Chinese Remainder Theorem: Solving simultaneous modular equations, Application in RSA and speeding up decryption, Fermat's Little Theorem: Modular exponentiation and primality testing, Applications in Diffie-Hellman and RSA.	9
III	**Prime Numbers and Factorization** Prime Numbers- Primality testing algorithms, Prime Factorization, Cryptosystems based on Prime Factorization: RSA key generation, encryption, and decryption Applications and attacks related to prime factorization, Pollard's Rho Algorithm	9
IV	**Discrete Logarithms and Diffie-Hellman Key Exchange** Discrete Logarithms, Diffie-Hellman Key Exchange Protocol, Elgamal Cryptosystem: Public key encryption using discrete logarithms, Digital signatures based on DLP	9
V	**Elliptic Curve Cryptography and Advanced Topics** Introduction to Elliptic Curves, Elliptic Curve Discrete Logarithm Problem (ECDLP), Elliptic Curve Digital Signature Algorithm (ECDSA), Zero Knowledge Proofs, Advanced Cryptographic Techniques	9

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1: Understand and Apply Basic Concepts of Cryptography and Number Theory
CO2 : Implement and Solve Problems Using Modular Arithmetic and Euclid's Algorithm
CO3: Understand and Apply Prime Factorization in Cryptographic Systems
CO4: Analyze and Solve Discrete Logarithm Problems in Key Exchange Protocols
CO5: Implement and Understand Elliptic Curve Cryptography (ECC) and Advanced Topics

Text Book

1. N. Koblitz, A Course in Number Theory and Cryptography, Springer 2006.

2. L. C. Washington, Elliptic curves: number theory and cryptography, Chapman & Hall/CRC, 2003.

3. I. Niven, H.S. Zuckerman, H.L. Montgomery, An Introduction to theory of numbers, Wiley, 2006.

Reference Books

1. William Stallings , "Cryptography and Network Security Principles and Practice", Pearson Education Inc., 6th Edition, 2014, ISBN: 978-93- 325-1877-3
2. Handbook of Applied Cryptography, A. Menzes, P. van Oorschot and S. Vanstone. Scribes: Rakesh Yarlagadda, Ravi Ranjan
3. D. Hankerson, A. Menezes and S. Vanstone, Guide to elliptic curve cryptography, Springer-Verlag, 2004.
4. J. Pipher, J. Hoffstein and J. H. Silverman, An Introduction to Mathematical Cryptography, Springer-Verlag, 2008.

Mapping of Course Outcomes (COs) with PSOs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	2	2	3	2	1	2	1	3	2	1	3	2	2	0
CO2	2	3	3	3	2	1	1	2	2	3	2	2	3	2	2
CO3	3	3	2	3	2	1	2	2	2	3	1	3	3	2	1
CO4	3	3	3	3	3	2	2	1	3	3	2	3	3	2	2
C05	3	3	2	3	3	2	2	2	3	3	2	3	3	3	3

3 – high, 2 – Average, 1 - low , 0-null

Discipline Specific Elective - II

Programme	B.Tech CSE Cyber Security	Programme Code	BTCY		
Course Code	25BTCY344	Number of Hours/Week	3		
Semester	IV	Max. Marks	100		
Year	II	Credits	3		
Course					
Course Title	APPROXIMATION ALGORITHM		L	T	P
			3	0	0

COURSE OBJECTIVES:

The main aim of this course is to prepare the students for:

- To understand the basics of approximation algorithm technique
- To understand the different types of algorithm and searching methods
- To infer about rounding of linear programs using deterministic and randomized
- To infer about primal-dual method
- Evaluate with cut and matrices method

UNIT	TOPICS	HOURS
I	**An Introduction to the Techniques – An introduction to approximation algorithms** – The whats and whys of approximation algorithms – An introduction to the techniques and to linear programming – A deterministic rounding algorithm – Rounding a dual solution - constructing a dual solution: the primal-dual method – A greedy algorithm – A randomized rounding algorithm	9
II	**Greedy algorithm and local search:** Scheduling jobs with deadlines on a single machine – the k-center problem – Scheduling jobs on identical parallel machines – the travelling salesman problem – maximizing float in bank accounts – finding minimum-degree spanning trees – edge colouring. **Rounding data and dynamic programming**: the knapsack problem – scheduling jobs on identical parallel machines – the bit-packing problem	9
III	**Deterministic rounding of linear programs:** Minimizing the sum of completion times on a single machine – minimizing the weighed sum of completion times on a single machine – Solving large linear programs in polynomial time – the prize-collecting Steiner tree problem – the uncapacitated facility location problem – the bin-packing problem. **Random sampling and randomized rounding of linear programs:** Simple algorithms for MAX SAT and MAX CUT – Derandomization - Flipping biased coins - Randomized rounding - Choosing the better of two solutions - Non-linear randomized rounding - the prize-collecting Steiner tree problem - The uncapacitated facility location problem- Scheduling a single machine with release dates - Chernoff bounds - Integer multicommodity flows - Random sampling and coloring dense 3-colorable graphs	9
IV	**Randomized rounding of semi definite programs:** A brief introduction to semidefinite programming - Finding large cuts - Approximating quadratic programs - Finding a correlation clustering - Coloring 3-colorable graphs. **The primal-dual method:** The set cover problem: a review - Choosing variables to increase - Cleaning up the primal solution - Increasing multiple variables at once - Strengthening inequalities - The uncapacitated facility location problem	9

	- Lagrangean relaxation and the k-median problem	
V	**Cuts and metrics:** The multiway cut problem and a minimum-cut-based algorithm - The multiway cut problem and an LP rounding algorithm - The multicut problem - Balanced cuts - Probabilistic approximation of metrics by tree metrics - An application of tree metrics: Buy-at-bulk network design - Spreading metrics, tree metrics, and linear arrangement	**9**

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1 : To understand the basics of approximation algorithm technique
CO2 : To understand the different types of algorithm and searching methods
CO3 : To infer about rounding of linear programs using deterministic and randomized
CO4 : To infer about primal-dual method
CO5 : Evaluate with cut and matrices method

Text Book

1. The Design of Approximation Algorithm, David.P. Williamsons, David. B.Shmoys, Cambridge University Press, 2010

Reference Books

1. Approximation Algorithms, Vijay V. Varirani, Springer, 2003
2. NP-Hard Problems and Approximation Algorithm, Springer, 2022

Mapping of Cos with POs and PSOs for B. Tech

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6
CO1	3	2	2	3	2	2	3	2	2	3	2	2	2	2	3	1	2	2
CO2	3	3	3	2	3	2	3	3	3	2	3	2	2	2	2	1	1	3
CO3	3	3	2	3	2	2	3	3	2	3	2	2	3	3	2	3	3	2
CO4	3	2	2	3	1	2	3	2	2	3	1	2	3	3	2	1	1	3
CO5	3	2	2	2	1	2	3	2	2	2	1	2	3	3	3	1	2	1

3 – High, 2 – Average, 1 - low, 0 - null

Programme	B.Tech CSE Cyber Security	Programme Code	BTCY		
Course Code	25BTCY345	Number of Hours/Week	3		
Semester	IV	Max. Marks	100		
Year	II	Credits	3		
Course					
Course Title	BLOCK CHAIN AND ITS APPLICATIONS		L	T	P
			3	0	0

COURSE OBJECTIVES:

The main aim of this course is to prepare the students for:

- To understand the basics of blockchain
- To interpret the decentralization in blockchain
- To categorize the symmetric cryptography
- To estimate block chain and its application
- To evaluate bitcoin networks and payments

UNIT	TOPICS	HOURS
I	Block chain – The growth of blockchain technology – Distributed systems – The history of blockchain and bitcoin – Types of blockchain – Consensus	9
II	Decentralization – Decentralization using blockchain – methods of decentralization – Routes to decentralization – Blockchain and full ecosystem decentralization – Smarts contracts – Decentralizaed organizations – Platforms for decentralization	9
III	Symmetric Cryptography – Working with openSSL command – Introduction – Cryptography – Confidentiality – Integrity – Authentication – Non-repudiation – Accountability – Symmetric cryptography – Stream ciphers – Block ciphers – Data encryption standard – Advanced encryption standard	9
IV	Introducing bitcoin – Bitcoin – Digital keys and addresses – Transactions – Blockchain – Mining	9
V	Bitcoin network and payments – The bitcoin network – wallets – Bitcoin payments – innovation in bitcoin	9

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1 : To understand the basics of blockchain
CO2 : To interpret the decentralization in blockchain
CO3 : To categorize the symmetric cryptography
CO4 : To estimate block chain and its application
CO5 : To evaluate bitcoin networks and payments

Text Book

1. **Mastering bitcoin**, Imran Bashir, Second Edition, packt, Birmingham, Mumbai, 2018

Reference Books

1. **Blockchain basics: A non-technical introduction in 25 steps,** Daniel Drescher, Apress, 2017
2. **Blockchain for Enterprise Application Developers,** Ambadas Tulajadas Chondari, Arshad Sarfaz Ariff, Sham M R, Wiley, 2020

Mapping of Cos with POs and PSOs for B. Tech

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6
CO1	3	2	2	3	2	2	3	2	2	3	2	2	2	2	3	1	2	2
CO2	3	3	3	2	3	2	3	3	3	2	3	2	2	2	2	1	1	3
CO3	3	3	2	3	2	2	3	3	2	3	2	2	3	3	2	3	3	2
CO4	3	2	2	3	1	2	3	2	2	3	1	2	3	3	2	1	1	3
CO5	3	2	2	2	1	2	3	2	2	2	1	2	3	3	3	1	2	1

3 – High, 2 – Average, 1 - low, 0 - null

Programme	B. Tech Cybersecurity	Programme Code	BTCY
Course Code	25BTCY346	Number of Hours/ Week	3
Semester	IV (Discipline Specific Elective II)	Max. Marks	100
Year	II	Credits	3

Course

Course Title	GAME THEORY	L	T	P
		3	0	0

COURSE OBJECTIVES:

The main aim of this course is to prepare the students for:

- To Understand fundamental concepts, types of games, Nash equilibrium, and strategic decision-making.
- To Analyze sequential games, backward induction, Subgame Perfect Equilibrium, and applications in auctions.
- To Study repeated games, Bayesian Nash Equilibrium, mechanism design, and auction theory.
- To Explore evolutionarily stable strategies, replicator dynamics, learning in games, and AI applications.
- To Learn cooperative game solutions, Shapley value, market design, and real-world applications in networks and economics.

UNIT	TOPICS	HOURS
I	**Introduction to Game Theory and Strategic Form Games:** Definition of games and strategic interactions- Types of games: Cooperative vs. Non-Cooperative, Static vs. Dynamic, Zero-Sum vs. Non-Zero-Sum-Nash Equilibrium in pure and mixed strategies- Dominant and dominated strategies-Best response functions- Applications in Economics, Computer Science, and Engineering.	10
II	**Extensive Form Games and Subgame Perfection:** Representation of sequential games (Game trees, Information sets)- Backward Induction and Subgame Perfect Equilibrium-Games with Perfect and Imperfect Information-Bargaining games and strategic moves- Applications in Auctions and Negotiations.	9

III	**Repeated and Bayesian Games :** Infinitely repeated games and the Folk Theorem Stochastic and Markov Games- Bayesian Games and Nash Equilibrium in Bayesian settings- Mechanism Design: Incentive Compatibility, Revelation Principle - Auction Theory: First-price, Second-price, VCG Mechanism.	9
IV	**Evolutionary Game Theory and Learning in Games**: Evolutionarily Stable Strategies (ESS) - Replicator Dynamics - Adaptive and Learning Strategies in Games (Fictitious Play, Regret Minimization) - Computational complexity of finding equilibria- Game theory in Machine Learning and AI.	**9**
V	**Cooperative Game Theory and Applications:** The Core, Shapley Value, and Bargaining Solutions -Matching Games and Market Design - Coalition formation and cost-sharing- Case studies: Network Routing, Cybersecurity, Blockchain Economics	**8**

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1 : Understand fundamental game theory concepts, including types of games and strategic interactions.

CO2 : Represent and solve sequential games using extensive form and backward induction.

CO3 : Analyze repeated games and determine long-term strategic interactions using the Folk Theorem.

CO4 : Explore learning-based approaches and computational complexity in game theory.

CO5 : Apply game theory concepts to real-world applications in economics, networks, and cybersecurity.

Text Books:

1. **Martin J. Osborne,** *An Introduction to Game Theory*, **Publisher:** Oxford University Press, **Edition:** 1st Edition, 2004, **ISBN:** 9780195128956.

2. **Robert Gibbons** *A Primer in Game Theory*, **Publisher:** Pearson Education, **Edition:** 1st Edition, 1992, **ISBN:** 9780135699146.

3. **Roger B. Myerson,** *Game Theory: Analysis of Conflict*, **Publisher:** Harvard University Press, **Edition:** 1st Edition, 1991, **ISBN:** 9780674341166.

Reference Books:

1. **Drew Fudenberg & Jean Tirole, "***Game Theory",* **Publisher:** MIT Press, **Edition:** 1st Edition, 1991 , **ISBN:** 9780262061414.

2. **Tamer Başar & Geert Jan Olsder,** *Dynamic Noncooperative Game Theory,* **Publisher:** SIAM (Society for Industrial and Applied Mathematics), **Edition:** 2nd Edition, 1999 **ISBN:** 9780898714296

3. **Yoav Shoham & Kevin Leyton-Brown,** *Multiagent Systems: Algorithmic, Game- Theoretic, and Logical Foundations* **Publisher:** Cambridge University Press **Edition:** 1st Edition, 2009 **ISBN:** 9780521899437

4. **John von Neumann & Oskar Morgenstern** *Theory of Games and Economic Behavior* **Publisher:** Princeton University Press **Edition:** 60th Anniversary Edition, 2007 **ISBN:** 9780691130613

Mapping of Course Outcomes (CO's) with PO's & PSO's

	PO 1	**PO 2**	**PO 3**	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	**PSO1**	**PSO2**	**PSO3**
CO 1	3	3	2	2	2	1	1	1	2	2	2	2
CO 2	3	3	3	3	2	1	1	1	2	2	2	2
CO 3	3	3	2	3	2	1	2	1	2	3	3	3
CO 4	3	3	2	3	3	1	2	1	2	3	3	3
CO 5	3	3	3	3	3	2	3	2	3	3	3	3

3 – High, 2 – Average, 1 - Low , 0-Null

Programme	B.Tech CSE-Cybersecurity	Programme Code	BTCY
Course Code	25BTCY241	Number of Hours/Week	2
Semester	IV	Max. Marks	100
Year	II	Credits	1

Course				
Course Title	CRYPTOGRAPHY, CRYPTANALYSIS AND NETWORK SECURITY LAB	L	T	P
		0	0	2

COURSE OBJECTIVES:

The main learning objective of this course is to prepare the students for:

- To understand basics of Cryptography and Network Security.
- To be able to secure a message over insecure channel by various means.
- To learn about how to maintain the Confidentiality, Integrity and Availability of a data.
- To understand various protocols for network security to protect against the threats in the networks.

List of Experiments

1) Write a C program that contains a string(char pointer) with a value\Hello World'. The programsshould XOR each character in thisstring with 0 and display the result.

2)) Write a C program that contains a string (char pointer) with a value \Hello World'. The program should AND or and XOR each character in this string with 127 and display the result.

3) Write a Java program to perform encryption and decryption using the following algorithms: i. Ceaser Cipher ii. Substitution Cipher iii. Hill Cipher

4) Write a Java program to implement the DES algorithm logic.

5) Write a C/JAVA program to implement the Blowfish algorithm logic.

6) Write a C/JAVA program to implement the Rijndael algorithm logic.

7) Write the RC4 logic in Java Using Java Cryptography, encrypt text "Hello world" usingBlowfish. Create your own key using Java key tool.

8) Write a Java program to implement RSA Algorithm.

9) Implement the Diffie-Hellman Key Exchange mechanism using HTML and JavaScript.

10) Calculate the message digest of a text using the SHA-1 algorithm in JAVA.

11) Calculate the message digest of a text using the MD5 algorithm in JAVA

On successful completion of this course, the student will be able to

- Provide security of the data over the network.
- Implement various networking protocols.
- Protect any network from the threats in the world
- Research in the emerging areas of cryptography and network security.
- Implement the security in real time systems

Mapping of Course Outcomes (COs) with PSO

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO11	PO 12	PS O1	PS O2	PS O3
CO1	0	1	0	0	0	2	0	0	2	2	0	0	0	1	0
CO2	2	0	0	0	0	0	0	0	0	3	0	0	0	0	2
CO3	0	3	0	0	0	0	1	0	0	3	0	0	0	0	0
CO4	0	0	1	0	0	0	0	0	0	3	0	0	2	0	3
C05	0	0	0	0	0	0	2	0	0	3	0	0	0	0	0

3 – high, 2 – Average, 1 - low , 0-null

Programme	B.Tech CSE- Cybersecurity	Programme Code	BTCY (P)		
Course Code	25BTCY242	Number of Hours/Week	2		
Semester	IV	Max. Marks	100		
Year	II	Credits	1		
Course					
Course Title	DATABASE MANAGEMENT SYSTEMS LAB		L	T	P
			0	0	2

L-Lecture Hours T-Tutorial Hours P-Practical Hours

COURSE OBJECTIVES:

The main learning objective of this course is to prepare the students for:

- Understand and Apply SQL DDL and DML Commands
- Utilize SQL Functions and Operators Effectively
- Implement SQL Joins and Advanced Clauses
- Work with Constraints, Views, and Subqueries in SQL
- Master Database Management and PL/SQL Concepts

Programs

1. DDL commands of SQL with suitable examples
   Create table
   Alter table
   Drop Table

2. DML commands of SQL with suitable examples
   Insert
   Update
   Delete

3. Different types of function with suitable examples
   Number function
   Aggregate Function
   Character Function
   Conversion Function
   Date Function

4. Different types of operators in SQL
   Arithmetic Operators
   Logical Operators
   Comparison Operator
   Special Operator
   Set Operation

5. Different types of Joins
   Inner Join
   Outer Join
   Natural Join etc..

6. Study and Implementation of
   Group By & having clause
   Order by clause
   Indexing

7. Study & Implementation of
   Sub queries
   Views

8. Different types of constraints

9. Database Backup & Recovery commands.
 Rollback, Commit, Savepoint.

10. Creating Database /Table Space
Managing Users: Create User, Delete User
Managing roles:-Grant, Revoke

11. PL/SQL

12. SQL Triggers

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1: Understand and apply SQL Data Definition Language (DDL) commands.

CO2: Understand and execute SQL Data Manipulation Language (DML) commands.

CO3: Apply different SQL functions to manipulate and retrieve data.

CO4: Understand and apply different types of constraints in SQL.

CO5: Design and implement SQL triggers for automated actions.

Mapping of Course Outcomes (COs) with PSOs

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO11	PO 12	PSO1	PSO2	PSO3
CO1	2	0	2	2	0	0	0	0	0	0	0	0	1	0	0
CO2	2	2	0	0	0	0	0	0	0	0	0	0	0	0	2
CO3	2	0	3	3	2	3	0	1	2	0	2	1	0	0	0
CO4	2	2	2	2	2	3	0	1	2	0	2	1	1	1	3
C05	0	0	0	2	1	1	1	1	1	1	2	1	2	0	0

3 – high, 2 – Average, 1 - low , 0-null

Semester V

Programme	B.Tech CSE(Cyber Security)	Programme Code	BTCY		
Course Code	25BTCY151	Number of Hours/Week	3		
Semester	V	Max. Marks	100		
Year	III	Credits	3		
Course					
Course Title	INTRODUCTION TO BLOCKCHAIN AND CRYPTOCURRENCY		L	T	P
			3	0	0

COURSE OBJECTIVES:

- Introduce the basics of Blockchain technology and cryptocurrency.
- Understand blockchain structure, consensus models, and public vs. private blockchains.
- Explore key cryptographic techniques such as hash functions and digital signatures.
- Learn about Bitcoin transactions, mining, and Proof of Work (PoW).
- Examine blockchain applications and permissioned systems, with a focus on smart contracts using Hyperledger Fabric and Ethereum.

UNIT	TOPICS	HOURS
I	**Introduction** Overview of Blockchain, Public Ledgers, Bitcoin, Smart Contracts, Block in a Blockchain, Transactions, Distributed Consensus, Public vs Private Blockchain, Understanding Crypto currency to Blockchain, Permissioned Model of Blockchain, Overview of Security aspects of Blockchain, Basic Crypto Primitives: Cryptographic Hash Function, Properties of a hash function, Hash pointer and Merkle tree, Digital Signature, Public Key Cryptography, A basic cryptocurrency.	9
II	**Blockchain With Crypto Currency** Bitcoin and Blockchain: Creation of coins, Payments and double spending, Bitcoin Scripts, Bitcoin P2P Network, Transaction in Bitcoin Network, Block Mining, Block propagation and block relay. Working with Consensus in Bitcoin: Distributed consensus in open environments, Consensus in a Bitcoin network, Proof of Work (PoW) – basic introduction, HashcashPoW, Bitcoin PoW, Attacks on PoW and the monopoly problem, Proof of Stake, Proof of Burn and Proof of Elapsed Time, The life of a Bitcoin Miner, Mining Difficulty, Mining Pool.	9
III	**Permissioned blockchain and Consensus mechanisms.** Permissioned Blockchain: Permissioned model and use cases, Design issues for Permissioned blockchains, Execute contracts, State machine replication, Overview of Consensus models for permissioned blockchain, Distributed consensus in closed environment, Paxos, RAFT Consensus, Byzantine general problem, Byzantine fault tolerant system, Lamport-Shostak-Pease BFT Algorithm, BFT over Asynchronous systems.	9
IV	**Blockchain and Cryptocurrency Applications** Cross-Border Payments, Know Your Customer (KYC) and Blockchain, Blockchain in Food Security, Mortgage over Blockchain, Supply Chain Financing and Blockchain, Identity, Smart Property, and Digital Transactions, Transactions, Payments, and Market Mechanisms, Multi-Party Lotteries	9

	on Blockchain	
V	**Blockchain Frameworks and Smart Contract Development** Hyperledger Fabric- Architecture, Identities and Policies, Membership and Access Control, Channels, Transaction Validation, Writing smart contract using Hyperledger Fabric, Writing smart contract using Ethereum, Overview of Ripple and Corda.	**9**

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1: Understand the fundamentals of blockchain, cryptographic techniques, and consensus models.

CO2 : Learn about cryptocurrency mechanisms, Bitcoin transactions, and Proof of Work

CO3: Apply various consensus models and understand distributed consensus in blockchains.

CO4: Explore real-world blockchain applications in payments, security, and identity management.

CO5: Develop smart contracts using frameworks like Hyperledger Fabric and Ethereum.

Text Book

1. Dhillon, V., Metcalf, D., and Hooper, M, Blockchain enabled applications, 2017, 1st Proceedings of the 65th Academic Council (17.03.2022) 1042 Edition, CA: Apress, Berkeley.

2. Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions" by Joseph J. Bambara, Paul R. Allen, Kedar Iyer, Rene Madsen, Solomon Lederer, and Michael Wuehler

3. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder, Agenda Item 65/39 - Annexure - 35 Proceedings of the 65th Academic Council (17.03.2022) 1047 Bitcoin and cryptocurrency technologies: a comprehensive introduction, 2016, Princeton University Press

Reference Books

1. Diedrich, H., “Ethereum: Blockchains, digital assets, smart contracts, decentralized autonomous organizations”, 2016, 1st Edition, Wildfire publishing, Sydney

2. Cryptography and Network Security: Principles and Practices, William Stallings, 7th edition, 2017

3. Bashir, I., "Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained", 2nd Edition, Packt Publishing Ltd, March 30, 2018.

Mapping of Course Outcomes (COs) with PSOs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	2	2	3	3	2	2	1	2	2	2	3	3	3	2
CO2	3	3	2	3	3	2	2	1	2	2	2	3	3	3	2
CO3	3	3	3	3	3	3	2	2	2	2	3	3	3	2	3
CO4	3	3	3	3	3	3	3	2	2	2	3	3	3	3	3
CO5	3	3	3	3	3	3	3	2	2	3	3	3	3	3	3

3 – high, 2 – Average, 1 - low, 0-null

Programme	B.Tech-CSE Cyber Security	Programme Code	BTCY		
Course Code	25BTCY152	Number of Hours/Week	3		
Semester	V	Max. Marks	100		
Year	III	Credits	3		
Course					
Course Title	MALWARE ANALYSIS		L	T	P
			3	0	0

COURSE OBJECTIVES:

- Equip students with the skills to analyse and detect malware using both static and dynamic techniques.
- Identify malicious software, assemble an analysis toolkit.
- Understand various detection methods to uncover and mitigate threats effectively

UNIT	TOPICS	HOURS
I	**Introduction to Malware and Basic Analysis Techniques** Introduction to malware, OS security concepts, malware threats, evolution of malware, malware types – viruses, rootkits, worms, bots, Trojans, spyware, adware, logic bombs, basic malware analysis, static malware analysis, dynamic malware analysis**.**	9
II	**Malware Analysis Techniques** Assembling a toolkit for effective malware analysis - examining static properties of suspicious programs - performing behavioural analysis of malicious Windows executables - performing static and dynamic code analysis of malicious Windows executables -interacting with malware in a lab to derive additional behavioural characteristics.	9
III	**Static Malware Analysis** Architecture of X86 - Main Memory, Instructions, Opcodes and Endianness, Operands, Registers, Simple Instructions, The Stack, Conditionals, Branching, Rep Instructions, C Main Method and Offsets, Antivirus Scanning - Fingerprint for Malware, Portable Executable File Format, The PE File Headers and Sections.	9
IV	**Dynamic Malware Analysis** Malware Sandbox - running malware, Monitoring with Process Monitor, Packet Sniffing with Wireshark, source-level vs. assembly level debuggers, Kernel vs. User-Mode Debugging, OLLYDBG - Breakpoints, Tracing, Exception Handling, Patching	9
V	**Malware Behaviour and Detection Strategies** Downloaders, Backdoors, Credential Stealers, Persistence Mechanisms, Privilege Escalation, Covert malware launching, Launchers, Process Injection, Process Replacement, Hook Injection, Detours, APC injection, Signature-based techniques: malware signatures, packed malware signature, metamorphic and polymorphic malware signature, non-signature-based techniques: similarity-based techniques, machine-learning methods, invariant inferences	9

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1: Identify and classify various types of malwares based on behavior and structure.

CO2 : Effectively use static and dynamic analysis techniques to examine and detect malicious software

CO3: Develop a strong understanding of malware analysis tools and how to set up a controlled analysis environment.

CO4: Apply malware detection methods, including signature-based and machine-learning techniques, to identify and mitigate threats.

CO5: Demonstrate the ability to analyze and interpret malicious code, recognizing key indicators of compromise and suspicious activity.

Text Book

1. Practical malware analysis, "The Hands-On Guide to Dissecting Malicious Software", by Michael Sikorski and Andrew Honig ISBN-10: 159327-290-1, ISBN-13: 978-1-59327-290-6, 2012.

2. Dang, Gazet and Bachaalany, "Practical Reverse Engineering", Wiley,2014

Reference Books

1. Computer viruses: From theory to applications by Filiol, Eric Springer Science & Business Media, 2006

Mapping of Course Outcomes (COs) with PSOs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	3	2	1	2	1	2	0	0	2	0	3	3	1	1
CO2	3	3	3	2	3	2	3	0	0	2	2	3	2	1	2
CO3	3	2	2	3	3	2	2	1	1	3	0	3	3	1	2
CO4	3	3	3	2	3	1	2	1	1	3	0	3	2	2	3
C05	2	2	3	3	3	2	3	0	0	2	2	3	3	3	2

3 – high, 2 – Average, 1 - low , 0-null

Programme	B. Tech CSE Cyber Security	Programme Code	BTCY		
Course Code	25BTCY153	Number of Hours/Week	3		
Semester	V	Max. Marks	100		
Year	III	Credits	3		
Course					
Course Title	THEORY OF COMPUTATION		L	T	P
			3	1	0

COURSE OBJECTIVES:

The main learning objective of this course is to prepare the students for:

- To give an overview of the theoretical foundations of computer science from the perspective of formal languages.
- To illustrate finite state machines to solve problems in computing
- To familiarize Regular grammars and Context Free Grammar.
- To solve various problems by normal form techniques, Push Down Automata and Turing Machines

UNIT	TOPICS	HOURS
I	**Introduction-Finite Automata** Introduction to Computation and Formal Languages- Syntax and Semantics- Finite Automata- Alphabets - Strings and Languages - Automata and Grammars - Deterministic Finite Automata (DFA) - Formal Definition - Simplified notation: State transition graph - Transition table - Language of DFA - Nondeterministic Finite Automata (NFA) - NFA with epsilon transition - Language of NFA - Equivalence of NFA and DFA - Minimization of Finite Automata - Distinguishing one string from other - Myhill-Nerode Theorem.	9
II	**Regular Expression (RE)** Definition - Operators of regular expression and their precedence - Algebraic laws for Regular expressions - Kleen's Theorem - Regular expression to FA - DFA to Regular expression - Arden Theorem - Non Regular Languages - Pumping Lemma for regular Languages. Application of Pumping Lemma - Closure properties of Regular Languages - Decision properties of Regular Languages - FA with output: Moore and Mealy machine - Equivalence of Moore and Mealy Machine - Applications and Limitation of FA.	9
III	**Context Free Grammar (CFG) and Context Free Languages** Definition - Examples - Derivation - Derivation trees - Ambiguity in Grammar - Inherent ambiguity - Ambiguous to Unambiguous CFG - Useless symbols - Simplification of CFGs - Normal forms for CFGs: CNF and GNF - Closure properties of CFLs - Decision Properties of CFLs: Emptiness - Finiteness and Membership - Pumping lemma for CFLs.	9
IV	**Push Down Automata (PDA)** Description and definition - Instantaneous Description - Language of	9

	PDA - Acceptance by Final state - Acceptance by empty stack - Deterministic PDA - Equivalence of acceptance by empty stack and final state - Conversion of CFG to PDA and PDA to CFG.	
V	**Turing Machines (TM) and Undecidability** Basic model - definition and representation - Instantaneous Description - Language acceptance by TM - Variants of Turing Machine - TM as Computer of Integer functions - Universal TM - Church's Thesis - Recursive and recursively enumerable languages - Halting problem - Introduction to Undecidability - Undecidable problems about TMs - Post correspondence problem (PCP) - Modified PCP and undecidable nature of post correspondence problem - Introduction to recursive function theory.	**9**

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1 : Design finite automata or regular expression for any tokenization task

CO2 : Construct a context free grammar for parsing any language

CO3 : Design Turing machine for any language

CO4 : Conclude the decidable / undecidable nature of any language

CO5 : Apply mathematical and formal techniques for solving real-world problems

Text Book:

1. John E. Hopcroft, Rajeev Motwani, Jeffrey D. Ullman, Introduction to Automata Theory Languages and Computation, 3rd edition, Pearson Education, India, 2007

Reference Books:

1. K. L. P Mishra, N. Chandrashekaran, Theory of Computer Science-Automata Languages and Computation, 2nd edition, Prentice Hall of India, India, 2003

CO-PO-PSO Mapping Table :(B. Tech):

CO/PO/PSO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO3
CO1	3	2	1	1	2	2	1	1	3	2	2	1	3	2	1
CO2	2	3	2	1	3	2	3	1	2	3	1	2	2	3	2
CO3	3	2	3	2	2	3	1	1	2	2	3	2	3	2	2
CO4	2	3	2	3	2	1	2	2	3	3	2	3	2	1	3
CO5	1	1	2	3	1	2	3	3	1	1	3	2	1	2	3

Discipline Specific Elective - III

Programme	B. Tech CSE Cyber Security	Programme Code	BTCY		
Course Code	25BTCY351	Number of Hours/Week	3		
Semester	V	Max. Marks	100		
Year	III	Credits	3		
Course Title	SEMANTIC WEB TECHNOLOGY		L	T	P
			3	0	0

COURSE OBJECTIVES:

The main learning objectives of this course are to:

1. To learn Web Intelligence.
2. To learn Knowledge Representation for the Semantic Web. 3.
3. To learn Ontology Engineering.
4. To learn Semantic Web Applications, Services and Technology.
5. Apply Semantic Web Technologies in Real-World Applications:

UNIT	TOPICS	HOURS
I	UNIT - I Introduction: Introduction to Semantic Web, the Business Case for the Semantic Web, XML and Its Impact on the Enterprise.	9
II	UNIT - II Web Services: Uses, Basics of Web Services, SOAP, UDDI, Orchestrating Web Services, Securing Web Services, Grid Enabled and Semantic Web of Web Services.	9
III	UNIT - III Resource Description Framework: Features, Capturing Knowledge with RDF. XML Technologies: XPath, The Style Sheet Family: XSL, XSLT, and XSL FO, XQuery, XLink, XPointer, XInclude, XMLBase, XHTML, XForms, SVG	9
IV	UNIT - IV Taxonomies and Ontologies: Overview of Taxonomies, Defining the Ontology Spectrum, Topic Maps, Overview of Ontologies, Syntax, Structure, Semantics, and Pragmatics, Expressing Ontologies Logically, Knowledge Representation.	9
V	UNIT - V Semantic Web Application: Semantic Web Services, e-Learning, Semantic Bioinformatics, Enterprise Application Integration, Knowledge Base. Semantic Search Technology: Search Engines, Semantic Search, Semantic Search Technology, Web Search Agents, Semantic Methods, Latent Semantic Index Search, TAP, Swoogle.	9

Course Outcomes

CO1: Understand the characteristics of Semantic Web.

CO2: Apply SOAP and UDDI to web services

CO3: Handle multiple web services using Orchestration

CO4: Create documents using XML

CO5: Construct and use Ontologies

Text Books:

Thinking on the Web - Berners Lee, Godel and Turing, Wiley Interscience.

Reference Books

1. The Semantic Web: A Guide to the Future of XML, Web Services, and Knowledge Management by Michael C. Daconta, Leo J. Obrst, Kevin T. Smith, Wiley Publishing
2. Semantic Web Technologies, Trends and Research in Ontology Based Systems, J.Davies, R.Studer, P.Warren, John Wiley & Sons
3. 3. Semantic Web and Semantic Web Services - Liyang Lu Chapman and Hall/CRC Publishers, (Taylor & Francis Group)

CO-PO-PSO Mapping Table:(**B. tech Cybersecurity)**

CO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO3
CO1	3	2	2	2	3	2	1	2	2	3	2	3	2	1	1
CO2	3	3	3	3	3	2	2	2	3	2	2	2	3	2	3
CO3	3	3	2	2	3	2	3	3	3	3	3	3	2	2	3
CO4	2	3	3	2	3	2	2	2	2	3	2	3	2	3	2
Co5	3	3	2	3	3	3	3	3	3	3	2	3	3	3	3

Programme	**B.Tech CSE-Cybersecurity**	**Programme Code**	**BTCY**
Course Code	**25BTCY352**	**Number of Hours/WK**	**3**
Semester	**V**	**Max. Marks**	**100**
Year	**III**	**Credits**	**3**

Course Title	**WEB APPLICATION SECURITY**	**L**	**T**	**P**
		3	**0**	**0**

L-Lecture Hours T-Tutorial Hours P-Practical Hours

COURSE OBJECTIVES

- To understand web security fundamentals and vulnerabilities.
- To learn subdomain, API, and authentication security.
- To explore common web attacks like XSS, CSRF, and SQL Injection.
- To analyze security risks and prevention techniques.
- To apply secure coding and basic vulnerability testing.

UNIT	TOPIC	HOURS
I	**Introduction to Web Application Security:** Basics of Web Security – Information Gathering – Web Application Mapping – Structure of Modern Web Applications – Web Servers & Databases – Authentication & Authorization Basics – Common Security Risks.	**9**
II	**Subdomain and API Analysis:** Basics of Subdomains – Identifying Multiple Applications on a Domain – API Security – Endpoint Discovery – Authentication Mechanisms – Secure vs. Insecure Web Architectures – Common Vulnerabilities & Exposures (CVE).	**9**
III	**Web Application Attacks - Part 1:** Introduction to Web Exploits – Cross-Site Scripting (XSS) – Stored XSS & Reflected XSS – Cross- Site Request Forgery (CSRF) – Query Parameter Tampering – Basic SQL Injection Attacks.	**9**
IV	**Web Application Attacks - Part 2:** Command Injection – Code Injection – Basic Denial of Service (DoS) – Exploiting Weak Authentication – Introduction to Security Misconfigurations.	**9**
V	**Defensive Security & Secure Web Development:** Basics of Secure Software Development – Secure Authentication & Hashing – Basics of SSL/TLS – Secure Coding Practices – Introduction to Vulnerability Testing – Fundamentals of Bug Bounty Programs – Preventing Common Web Attacks.	**9**

Andragogy

Class Room Lectures, Power point presentation, You Tube, Group Discussion, Seminar, Quiz, Formative Assessments, Brain storming, Activity.

COURSE OUTCOMES:

On successful completion of this course, the student will be able to:

CO1	Define web security principles, classify authentication methods, and illustrate authorization techniques.
CO2	Detect subdomain and API vulnerabilities, categorize security weaknesses, and assess their impact on web applications.
CO3	Investigate web attacks, implement XSS, CSRF, and SQL Injection techniques in a controlled environment, and evaluate their risks.
CO4	Examine security risks, analyze misconfigurations, and propose mitigation strategies.
CO5	Implement secure coding practices, conduct vulnerability testing, and validate security controls in web applications.

Text book:

1. "Web Application Security- Exploitation and Countermeasures for Modern Web Applications", Andrew Hoffman, O'Reilly Media, 1st Edition, 2020.

References:

1. "The Web Applications Hackers Handbook", D. Stuttard and M. Pinto, Wiley, 2nd Edition, 2011.
2. "Web Security for Developers: Real Threats, Practical Defense", Malcolm McDonald, No Starch Press, 2020.

Mapping of Course Outcomes (CO's) with PO's & PSO's

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	3	2	2	3	2	1	1	1	2	2	3	3	2	3
CO2	3	3	3	3	3	2	1	1	1	2	2	3	3	3	3
CO3	3	3	3	3	3	2	1	2	2	2	3	3	3	3	3
CO4	3	3	3	3	3	3	2	3	2	2	3	3	3	3	3
CO5	3	3	3	3	3	3	2	3	2	3	3	3	3	3	3

3 – High, 2 – Average, 1 – Low , 0-Null

Programme	B. Tech CSE Cyber Security	Programme Code	BTCY		
Course Code	25BTCY353	Number of Hours/Week	3		
Semester	V	Max. Marks	100		
Year	III	Credits	3		
Course					
Course Title	WEB DATA MINING		L	T	P
			3	0	0

COURSE OBJECTIVES:

The main learning objectives of this course are to prepare students to:

1. **Understand Data Mining Concepts and Functionalities:** Learn the foundational principles of data mining, including pre-processing techniques like cleaning, integration, reduction, and discretization, along with the architecture and classification of data mining systems.
2. **Explore Association Rule Mining:** Study efficient algorithms for frequent item set mining, discover various types of association rules, and perform correlation and constraint-based analysis for meaningful data insights.
3. **Master Classification and Prediction Techniques:**Analyze methods like decision trees, Bayesian classifiers, backpropagation, support vector machines, and ensemble techniques to develop accurate classification and prediction models.
4. **Analyze Clustering Techniques and Outlier Detection:** Examine clustering methods, such as partitioning, hierarchical, density-based, and model-based techniques, and apply these methods to high-dimensional data and outlier analysis.
5. **Mine Complex Data Types:** Explore multidimensional analysis and mining techniques for complex data objects, including spatial, multimedia, text, and web data, for advanced data mining applications.

UNIT	TOPICS	HOURS
I	**Introduction:** Basic Data Mining Tasks – Data Mining Versus Knowledge Discovery in Data Bases – Data Mining Issues – Data Mining Matrices – Social Implications of Data Mining – Data Mining from Data Base Perspective.	9
II	**Neural Networks:** Data Mining Techniques – a Statistical Perspective on data mining – Similarity Measures – Decision Trees – Neural Networks – Genetic Algorithms.	9
III	**Fuzzy Systems** Classification: Introduction – Statistical – Based Algorithms – Distance Based Algorithms – Decision.	9
IV	**Genetic Algorithm:** Clustering Tree – Based Algorithms – Neural Network Based Algorithms – Rule Based .Algorithms – Combining Techniques: Introduction – Similarity and Distance Measures –Outliers – Hierarchical Algorithms. Partitioned Algorithms.	9
V	**Hybrid Systems:** Association Rules: Introduction - Large Item Sets – Basic Algorithms – Parallel &Distributed .Algorithms – Comparing Approaches – Incremental Rules – Advanced Association Rules .Techniques – Measuring the Quality of Rules.	9

Course Outcomes

pon successful completion of this course, the student will be able to:

CO1: Understanding Data Mining Techniques and Their Applications
CO2: Mastery of Machine Learning Algorithms for Data Mining
CO3: Critical Analysis of Data Mining Issues and Social Implications
CO4: Expertise in Hybrid and Combined Data Mining Approaches
CO5: Application of Data Mining Techniques for Real-World Problems

Text Books:

1. Jiawei Han & Micheline Kamber, "Data Mining Concepts & Techniques", 2011, 3rd Edition.

Reference Books:

1. Margaret H.Dunbam, "Data Mining Introductory and Advanced Topics", Pearson,Education 2003.

CO-PO-PSO Mapping Table:(B. tech Cybersecurity)

CO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO3
CO1	3	3	2	2	3	2	1	1	2	2	3	1	2	2	2
CO2	3	3	3	3	3	3	2	2	3	3	3	2	3	3	3
CO3	2	2	3	2	2	3	3	2	3	2	3	3	2	3	3
CO4	3	3	2	3	3	3	3	3	3	3	2	3	3	3	2
C05	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3

3 – high, 2 – Average, 1 - Low , 0-Null

Discipline Specific Elective - IV

Programme	B.Tech CSE Cyber Security	Programme Code	BTCY		
Course Code	25BTCY354	Number of Hours/Week	3		
Semester	V	Max. Marks	100		
Year	III	Credits	3		
Course					
Course Title	MODERN CRYPTOGRAPHY		L	T	P
			3	0	0

COURSE OBJECTIVES:

- Introduce symmetric and asymmetric cryptography concepts and security notions.
- Analyze attack models, provable security, and pseudo-random functions.
- Explore block ciphers, message authentication, and public key signature schemes.
- Study cryptographic protocols, zero-knowledge proofs, and their applications.

UNIT	TOPICS	HOURS
I	**Introduction** Basics of Symmetric Key Cryptography, Basics of Asymmetric Key Cryptography, Hardness of Functions. Notions of Semantic Security (SS) and Message Indistinguishability (MI): Proof of Equivalence of SS and MI, Hard Core Predicate, Trap-door permutation, Goldwasser- Micali Encryption. Goldreich-Levin Theorem: Relation between Hardcore Predicates and Trap-door permutation	9
II	**Formal Notions of Attacks** Attacks under Message Indistinguishability: Chosen Plaintext Attack (IND-CPA), Chosen Ciphertext Attacks (IND-CCA1 and IND-CCA2), Attacks under Message Non-malleability: NM-CPA and NM-CCA2, Inter-relations among the attack model	9
III	**Provable Security in Cryptography** Provable Security and asymmetric cryptography, hash functions. One-way functions: Weak and Strong one-way functions. Pseudo-random Generators (PRG): Blum-Micali-Yao Construction, Construction of more powerful PRG, Relation between One-way functions and PRG, Pseudorandom Functions (PRF)	9
IV	**Building A Pseudorandom Permutation** The Luby Rackoff Construction: Formal Definition, Application of the Luby Rackoff Construction to the construction of Block Ciphers, The DES in the light of Luby Rackoff Construction.	9
V	**Message Authentication** Left or Right Security (LOR). Formal Definition of Weak and Strong MACs, Using a PRF as a MAC, Variable length MAC, Public Key Signature Schemes: Formal Definitions, Signing and Verification, Formal Proofs of Security of Full Domain Hashing. Assumptions for Public Key Signature Schemes: One-way functions Imply Secure One-time Signatures. Shamir's Secret Sharing Scheme. Formally Analyzing Cryptographic Protocols. Zero Knowledge Proofs and Protocols	9

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1 : Understand the fundamentals of symmetric and asymmetric cryptography, semantic security, and hardness of functions.

CO2 : Analyze various cryptographic attack models, including chosen plaintext and chosen ciphertext attacks.

CO3 : Evaluate provable security concepts, one-way functions, pseudo-random generators, and their applications.

CO4 : Examine pseudorandom permutations, block cipher constructions, and their security implications.

CO5 : Explore message authentication, public key signature schemes, cryptographic protocols, and zero-knowledge proofs.

Text Book

1. Hans Delfs and Helmut Knebl, Introduction to Cryptography: Principles and Applications, Springer Verlag.

2. Wenbo Mao, Modern Cryptography, Theory and Practice, Pearson Education (Low Priced Edition)

Reference Books

1, ShafiGoldwasser and MihirBellare, Lecture Notes on Cryptography, Available at http://citeseerx. ist. psu.edu/.

2. OdedGoldreich, Foundations of Cryptography, CRC Press (Low Priced Edition Available), Part 1 and Part 23

3. William Stallings, "Cryptography and Network Security: Principles and Practice", PHI 3rd Edition, 2006.

Mapping of Course Outcomes (COs) with PSOs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	2	2	2	2	1	1	1	1	2	1	2	3	2	2
CO2	3	3	2	3	2	1	1	1	1	2	1	2	3	2	3
CO3	3	3	3	3	3	2	2	1	1	2	2	2	3	3	2
CO4	3	2	3	3	3	1	1	1	1	2	2	2	3	3	2
CO5	3	3	3	3	3	2	2	2	1	3	2	3	3	3	3

3 – high, 2 – Average, 1 - low, 0-null

Programme	B. Tech CSE Cyber Security	Programme Code	BTCY
Course Code	25BTCY355	Number of Hours/Week	3
Semester	V	Max. Marks	100
Year	III	Credits	3

Course

Course Title	EVOLUTIONARY COMPUTATION	L	T	P
		3	0	0

COURSE OBJECTIVES:

The main learning objective of this course is to prepare the students for:

- Understand the fundamental principles of evolutionary computation and its applications.
- Develop and implement various evolutionary algorithms, including genetic algorithms, evolutionary programming, and genetic programming.
- Apply evolutionary computation techniques to solve optimization, search, and machine learning problems.
- Analyse the performance and behaviour of evolutionary algorithms.
- Explore advanced topics and recent trends in evolutionary computation.

UNIT	TOPICS	HOURS
I	**Introduction to Evolutionary Computation:** Introduction to optimization and search problems, biological evolution as inspiration, history and development of evolutionary computation, overview of evolutionary algorithms, basic terminology (population, fitness, selection, crossover, mutation).	8
II	**Genetic Algorithms (GAs):** Representation schemes (binary, real-valued, permutation), selection methods (roulette wheel, tournament selection), crossover operators (one-point, two-point, uniform), mutation operators (bit-flip, Gaussian), GA implementation and parameter tuning.	8
III	**Evolutionary Programming (EP) and Genetic Programming (GP):** Evolutionary programming: representation, mutation, and selection. Genetic programming: tree-based representation, function and terminal sets, crossover and mutation operators, applications of GP.	8
IV	**Advanced Evolutionary Algorithms and Optimization:** Particle swarm optimization (PSO), ant colony optimization (ACO), differential evolution (DE), multi-objective optimization (MOO), constraint handling techniques, applications in engineering optimization problems.	8
V	**Applications and Advanced Topics:** Evolutionary machine learning, neuroevolution, evolutionary robotics, parallel and distributed evolutionary algorithms, recent trends and research directions, case studies and real-world applications.	8

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1 : Understand the fundamental principles and concepts of evolutionary computation.

CO2 : Implement and apply genetic algorithms to solve optimization and search problems.

CO3 : Develop and utilize evolutionary programming and genetic programming techniques.

CO4 : Apply advanced evolutionary algorithms like PSO, ACO, and DE to complex optimization tasks.

CO5 : Analyze and apply evolutionary computation to emerging areas like machine learning and robotics, and understand current research trends.

Text Book:

1. Eiben, A. E., & Smith, J. E. (2015). From evolutionary computation to computational evolution: Evolving artificial life. Springer.
2. Engelbrecht, A. P. (2007). Computational intelligence: an introduction. John Wiley & Sons.
3. Mitchell, M. (1998). An introduction to genetic algorithms. MIT press.

Reference Books:

1. Goldberg, D. E. Genetic algorithms in search, optimization, and machine learning. Addison-Wesley Professional, 1989.
2. Fogel, D. B., Evolutionary computation: toward a new philosophy of machine intelligence. John Wiley & Sons, 2006
3. Kennedy, J., Eberhart, R. C., & Shi, Y. Swarm intelligence. Morgan Kaufmann, 2001.
4. Dorigo, M., & Stützle, T. Ant colony optimization. MIT press, 2004.
5. Back, T., Fogel, D. B., Michalewicz, Z., Handbook of Evolutionary Computation. Oxford University Press, 1997.

CO-PO-PSO Mapping Table :(**B. Tech)**

CO/PO /PSO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO3
CO1	**3**	**3**	**2**	**3**	**2**	**1**	**1**	**1**	**2**	**2**	**1**	**3**	**3**	**2**	**1**
CO2	**3**	**3**	**3**	**3**	**3**	**2**	**2**	**1**	**2**	**3**	**2**	**2**	**3**	**3**	**1**
CO3	**3**	**3**	**3**	**3**	**3**	**2**	**2**	**1**	**2**	**3**	**3**	**2**	**3**	**3**	**2**
CO4	**2**	**3**	**3**	**3**	**3**	**2**	**1**	**1**	**2**	**2**	**3**	**2**	**3**	**2**	**1**
C05	**2**	**2**	**3**	**3**	**3**	**2**	**2**	**1**	**2**	**3**	**3**	**3**	**3**	**3**	**2**

Programme	B.Tech-CSE(Cyber Security)	Programme Code	BTCY		
Course Code	25BTCY356	Number of Hours/Week	3		
Semester	V	Max. Marks	100		
Year	III	Credits	3		
Course					
Course Title	BIOMETRIC SECURITY		L	T	P
			3	0	0

COURSE OBJECTIVES:

- To introduce biometric systems, authentication technologies, and key modalities like fingerprints, face, iris, and voice.
- To understand system components, verification methods, and matching techniques.
- To analyze strengths, weaknesses, privacy concerns, and real-world applications of biometrics.

UNIT	TOPICS	HOURS
I	**Introduction to Biometric systems** Introduction and background, Biometric technologies, Passive biometrics, Active biometrics, Biometric systems, Enrolment, Templates, Algorithm, Verification, Biometric applications, biometric characteristics, Authentication technologies, Need for strong authentication, Protecting privacy and biometrics and policy, Biometric applications, Biometric characteristics	9
II	**Fingerprint Biometric systems** History of fingerprint pattern recognition, General description of fingerprints, Fingerprint feature processing techniques, Fingerprint sensors using RF imaging techniques, Fingerprint quality assessment, Computer enhancement and modelling of fingerprint images, Fingerprint enhancement, Feature extraction, Fingerprint classification, Fingerprint matching.	9
III	**Face recognition and hand geometry** Introduction to face recognition, Neural networks for face recognition, face recognition from correspondence maps, Hand geometry, Scanning, Feature Extraction, Adaptive Classifiers, Visual-Based Feature Extraction and Pattern Classification, Feature extraction, Types of algorithms, and Biometric fusion.	9
IV	**Iris, Voice recognition** Iris scan, Features, Components, Operation (Steps), Competing iris Scan technologies, Strength and weakness, Voice Scan, Features, Components, Operation (Steps), Competing voice Scan (facial) technologies, Strength and weakness.	9
V	**Physiological and Behavioural Biometrics** Retina scan, AFIS (Automatic Finger Print Identification Systems), Behavioural biometrics, Signature scan, Keystroke scan biometrics application, Biometric Solution Matrix, Bio privacy, Comparison of privacy factor in different biometrics technologies	9

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1 : Understand biometric technologies, authentication techniques, and the need for strong authentication.

CO2 : Analyze fingerprint recognition techniques, including feature extraction and classification.

CO3 : Evaluate face and hand geometry recognition methods, biometric fusion, and pattern classification.

CO4 : Examine iris and voice recognition technologies, their components, strengths, and weaknesses.

CO5 : Explore physiological and behavioural biometrics, privacy concerns, and biometric security applications.

Text Book

1. Nalini K Ratha and Govindraju, "Advances in Biometrics - Sensors, Algorithms And Systems", 2018, 1st edition, Springer, London..

2. "Introduction to Biometrics" by Anil K. Jain, Arun Ross, and Karthik Nandakumar

3. "Biometric Systems: Technology, Design and Performance Evaluation" by James L. Wayman, Anil K. Jain, Davide Maltoni, and Dario Maio

Reference Books

1. David Check Long, Andre beck ling and Jiankun Hun, Biometric Security, Cambridge scholar publications. 2015
2. "Handbook of Face Recognition" edited by Stan Z. Li and Anil K. Jain
3. Samir Nanavathi, Michel Thieme, and Raj Nanavathi "Biometrics -Identity verification

Mapping of Course Outcomes (COs) with PSOs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	2	0	0	2	3	2	3	0	2	0	3	3	3	3
CO2	3	3	2	3	3	0	0	0	0	0	0	2	3	3	3
CO3	3	3	3	3	3	0	0	0	0	2	0	2	3	3	3
CO4	3	2	2	3	3	0	0	0	0	2	0	2	3	3	3
CO5	3	2	2	2	2	3	3	3	0	2	0	3	3	3	3

3 – high, 2 – Average, 1 - low , 0-null

Open Electives - I

Programme	B.Tech CSE Cyber Security	Programme Code	BTCY		
Course Code	25BTCY851	Number of Hours/Week	3		
Semester	V	Max. Marks	100		
Year	III	Credits	3		
Course					
Course Title	ARTIFICIAL INTELLIGENCE		L	T	P
			3	0	0

COURSE OBJECTIVES:

- To introduce the fundamental concepts and techniques of Artificial Intelligence.
- To provide an overview of real-world AI applications across various domains.
- To explain basic algorithms in problem solving, knowledge representation, and machine learning.
- To enable students to understand ethical implications and societal impact of AI.
- To motivate students to explore AI applications in their respective fields.

UNIT	TOPICS	HOURS
I	**Introduction to Artificial Intelligence** History and evolution of AI - Definitions and characteristics of AI - Applications of AI in various domains (agriculture, healthcare, finance, smart cities, etc.) - Intelligent agents and environments - Foundations: Psychology, Philosophy, Mathematics, Computer Science	9
II	**Problem Solving and Search Techniques** Problem formulation - Uninformed search: BFS, DFS - Informed search: Heuristics, A* algorithm - Game playing: Minimax and Alpha-Beta pruning (introductory level)- Applications: Route finding, decision support	9
III	**Knowledge Representation and Reasoning** Propositional logic and first-order logic (basic concepts) - Rule-based systems and inference - Semantic networks and ontologies -Expert systems (e.g., MYCIN, DENDRAL) - Use cases: Legal decision support, medical diagnostics	9
IV	**Introduction to Machine Learning** What is machine learning? - Types: Supervised, Unsupervised, Reinforcement learning - Basic algorithms: KNN, Decision Trees, Clustering (K-Means) -Real-world examples: Email spam detection, product recommendations - Tools and platforms: Scikit-learn, Weka (basic demo-oriented)	9

V	**AI Ethics and Applications in Other Domains** AI and society: Opportunities and risks - Bias in AI and algorithmic fairness - Privacy, surveillance, and data governance - Role of AI in	**9**

	Sustainable Development Goals (SDGs) - Career pathways and interdisciplinary AI projects	

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1 : Describe the core concepts and historical development of Artificial Intelligence.
CO2 : Apply AI techniques to solve basic problems involving logic and decision-making.
CO3 : Understand the working of machine learning and data-driven AI models.
CO4 : Identify AI applications relevant to their domain (e.g., agriculture, medicine, finance, etc.).
CO5 : Evaluate ethical issues and limitations related to AI systems.

Text Book

Melanie Mitchell, *Artificial Intelligence: A Guide for Thinking Humans*

Open Educational Resource (Free PDF)

Title: *AI For Everyone (MIT OpenCourseWare)*

- Free PDF Notes and Lectures: https://ocw.mit.edu

Mapping of Course Outcomes (COs) with PSOs

3 – high, 2 – Average, 1 - low, 0-null

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	2	2	2	2	1	1	1	1	2	1	2	3	2	2
CO2	3	3	2	3	2	1	1	1	1	2	1	2	3	2	3
CO3	3	3	3	3	3	2	2	1	1	2	2	2	3	3	2
CO4	3	2	3	3	3	1	1	1	1	2	2	2	3	3	2
CO5	3	3	3	3	3	2	2	2	1	3	2	3	3	3	3

Programme	BTech. CSE Cyber Security	Programme Code	BTIA		
Course Code	25BTCY851	Number of Hours/Week	5		
Semester	V	Max. Marks	100		
Year	III	Credits	3		
Course					
Course Title	PYTHON PROGRAMMING		L	T	P
			3	0	0

COURSE OBJECTIVES:

The main learning objective of this course is to prepare the students for:

- To Understand the fundamentals of the Python programming language and its historical development
- To Master Python basics, including data types, operators, tuples, dictionaries, and string manipulation.
- To demonstrate object oriented concept in python
- To familiarize with machine learning tools in python

UNIT	TOPICS	HOURS
I	**Introduction to python programming** Introduction to python ; setting up python programming environment; variables; strings and its operations; special characters; striping whitespace; numbers; comments; list and its operations; indexing; looping through lists; indentation; range function; slicing a list; copying list; looping through slice;	9
II	**Python datatypes** Tuples and its operations; relational operators; conditional statements – if, if-else, if-elif-else; multiple conditional blocks; dictionaries; key-value pairs – adding, modifying, removing; looping through dictionary; list of dictionaries; dictionary in a dictionary; user input function; type casting;	9
III	**Loop and function** While loop; break and continue; functions; arguments; passing arguments – positional arguments, keyword arguments, default values; optional arguments; returning from function; passing arbitrary number of arguments; storing functions in modules; import specific function or module;	9
IV	**OOPs in python** Classes; __init__() method; instance of a class; accessing attributes; calling methods; creating multiple instances; inheritance – parent class, child class; importing classes; files – reading a file, writing to a file, appending to a file; exceptions – try-except block, else block;	9
V	**Python machine learning tools** Python tools for machine learning; python modules – numpy, pandas, matplotlib, scipy; python based machine learning	9

	libraries – pytorch, tensorflow; virtual environment; machine learning application using python tools;	

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1 : Comprehend the holistic view of programming language design and behavior

CO2 : Understand the programming concepts in abstract and paradigm level

CO3 : Structure python programs for solving problems

CO4 : Develop python programs using OOP concept

CO5 : Execute ML project using python tools

Text Books:

1. Eric Matthes. Python Crash Course, 2nd Edition: A Hands-On, Project-Based Intro- duction to Programming. No Starch Press, Inc., 2019.

Reference Books:

1. Al Sweigart. AutomAte the Boring Stuff with Python. William Pollock, 2015.

Programme	B. Tech CSE Cyber Security	Programme Code	BTCY
Course Code	25BTCY851	Number of Hours/Week	3
Semester	V	Max. Marks	100
Year	III	Credits	3

Course				
Course Title	COMPUTER NETWORK	L	T	P
		3	0	0

L-Lecture Hours T-Tutorial Hours P-Practical Hours

COURSE OBJECTIVES:

The main learning objective of this course is to prepare the students for:

- To understand the concept of Computer network
- To impart knowledge about networking and inter networking devices

UNIT	TOPICS	HOURS
I	UNIT - I Introduction – Network Hardware - Software - Reference Models - OSI and TCP/IP Models - Example Networks: Internet, ATM, Ethernet and Wireless LANs - Physical Layer - Theoretical Basis for Data Communication - Guided Transmission Media.	9
II	UNIT - II Wireless Transmission - Communication Satellites - Telephone System: Structure, Local Loop, Trunks and Multiplexing and Switching. Data Link Layer: Design Issues - Error Detection and Correction.	9
III	UNIT - III Elementary Data Link Protocols - Sliding Window Protocols - Data Link Layer in the Internet - Medium Access Layer - Channel Allocation Problem - Multiple Access Protocols - Bluetooth.	9
IV	UNIT - IV Network Layer - Design Issues - Routing Algorithms - Congestion Control Algorithms - IP Protocol - IP Addresses - Internet Control Protocols.	9
V	UNIT - V Transport Layer - Services - Connection Management - Addressing, Establishing and Releasing a Connection - Simple Transport Protocol - Internet Transport Protocols (ITP) - Network Security: Cryptography.	9

Andragogy

Class Room Lectures, Power point presentation, You Tube, Group Discussion, Seminar, Quiz, Formative Assessments, Brain storming, Activity.

COURSE OUTCOME:

On successful completion of this course, the student will be able to

CO1 :	To Learn various principles & concepts of Computer networks.
CO2 :	To Analyze different network models.
CO3 :	To Evaluate the data flow through TCP/IP & ISO Layers.
CO4 :	To Assess key networking protocols and their hierarchical relationship In the conceptual model like TCP/IP and OSI
CO5 :	To Identify networking and inter-networking devices

Text Book :

1. A. S. Tanenbaum, "Computer Networks", Prentice-Hall of India 2008, 4th Edition.

Reference Books:

1. Stallings, "Data and Computer Communications", Pearson Education 2012, 7th Edition.
2. B. A. Forouzan, "Data Communications and Networking", Tata McGraw Hill 2007, 4th Edition.
3. F. Halsall, "Data Communications, Computer Networks and Open Systems", Pearson Education2008.
4. D. Bertsekas and R. Gallagher, "Data Networks", PHI 2008, 2nd Edition. 5. Lamarca,"Communication Networks", Tata McGraw Hill 2002.

Programme	B. Tech CSE Cyber Security	Programme Code	BTCY		
Course Code	24BTCY252	Number of Hours/Week	2		
Semester	V	Max. Marks	100		
Year	III	Credits	1		
Course					
Course Title	MALWARE ANALYSIS LAB		L	T	P
			0	0	2

L-Lecture Hours T-Tutorial Hours P-Practical Hours

COURSE OBJECTIVES:

- Equip students with skills to analyze and detect malware using static and dynamic techniques.
- Identify malicious software and assemble an analysis toolkit.
- Understand various detection methods to uncover and mitigate threats.

Programs

xp. No.	Experiment Title	Tools / Environment Used	Mapped COs
1	**Introduction to Malware Types and Sandbox Setup**	VirtualBox/VMware, Windows VM	CO1, CO3
2	**Static Analysis: Hashing, Strings, and File Header Examination**	PEiD, Strings, HashCalc	CO1, CO2
3	**PE File Structure Analysis using PE Explorer**	PE Explorer, CFF Explorer	CO2, CO5
4	**Basic Dynamic Analysis: Monitoring with Process Monitor**	Process Monitor, Autoruns	CO2, CO5
5	**Network Traffic Analysis of Malware using Wireshark**	Wireshark, FakeNet-NG	CO2, CO4
6	**Behavioral Analysis in a Controlled Sandbox**	ANY.RUN, Joe Sandbox (or local sandbox)	CO2, CO3
7	**Debugging Malware with x64dbg/OLLYDBG – Basic Instructions**	x64dbg, OLLYDBG	CO2, CO5
8	**Analyzing Packed Malware using Unpacking Tools**	UPX, PEiD, Malware Unpacker scripts	CO2, CO4
9	**Signature-based Detection using YARA Rules**	YARA, ClamAV	CO4
10	**Machine Learning-Based Malware Detection (Feature Extraction)**	Python, scikit-learn, PE feature datasets	CO4

11	**Analysis of Persistence Mechanisms: Registry, Services, Scheduled Tasks**	Regshot, Autoruns, Sysinternals Suite	CO1, CO5
12	**Comprehensive Malware Analysis Report Writing**	All tools used previously	CO1–CO5

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1:	Identify and classify malware.
CO2 :	Use static and dynamic analysis techniques.
CO3:	Set up a malware analysis environment.
CO4:	Apply detection methods (signature-based, ML).
CO5:	Analyze and interpret malicious code.

Mapping of Course Outcomes (COs) with PSOs – B.Tech

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	2	3	2	3	1	1	2	2	2	2	3	3	3	2
CO2	3	3	2	2	3	2	1	1	2	2	2	3	3	3	3
CO3	3	3	3	3	3	1	1	2	2	2	2	3	3	2	3
CO4	3	3	3	3	3	1	2	2	2	2	3	3	3	3	3
C05	3	3	3	3	3	2	3	2	2	3	3	3	3	3	3

Programme	B.Tech CSE(Cyber Security)	Programme Code	BTCY
Course Code	25BTCY252	Number of Hours/Week	2
Semester	V	Max. Marks	100
Year	III	Credits	1

Course

Course Title	INTRODUCTION TO BLOCKCHAIN AND CRYPTOCURRENCY LABORATORY	L	T	P
		0	0	2

L-Lecture Hours T-Tutorial Hours P-Practical Hours

LIST OF PROGRAMS

1. Write the program to implement a Solidity smart contract using array and function in Remix IDE with following functions
    a. Creation of static and dynamic array
    b. Addition and deletion of array elements
    c. Finding length of a given array
    d. Printing array element in sorted order
    e. Searching a particular element in an array

2. Install a Meta mask testnet. Use the Metamask testnet for embedding wallet and transferring ethers to other wallets through a smart contract.

3. To install Truffle & Ganache and use Ethreum -Ganache to create an account and illustrate using solidity smart contract compilation and development environment

4. Deploy an Ethereum Testnet and use Web3.py for writing smart contracts.

5. Write a chain-code application in GO to alter the state of a distributed hyper ledger fabric account with assets; check to see if the asset exists; transfer assets from one account wallet to another

6. Design and develop a Blockchain based referendum system with Ethereum Blockchain. Based on the result of the referendum a series of steps have to be put in pace through a smart contract. (Innovative Experiment)

7. Creating Crypto-currency Wallet

8. Creating and Building Up Crypto Token

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1: Understand and implement Solidity smart contracts using arrays and functions in Remix IDE.

CO2 : Deploy and manage Ethereum-based wallets using MetaMask for secure transactions.

CO3: Utilize Truffle & Ganache for smart contract development, compilation, and deployment.

CO4: Develop and interact with Ethereum smart contracts using Web3.py and blockchain frameworks.

CO5: Design blockchain-based applications such as cryptocurrency wallets, tokens, and referendum systems.

Mapping of Course Outcomes (COs) with PSOs – B.Tech

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	2	3	2	3	1	1	2	2	2	2	3	3	3	2
CO2	3	3	2	2	3	2	1	1	2	2	2	3	3	3	3
CO3	3	3	3	3	3	1	1	2	2	2	2	3	3	2	3
CO4	3	3	3	3	3	1	2	2	2	2	3	3	3	3	3
C05	3	3	3	3	3	2	3	2	2	3	3	3	3	3	3

Semester VI

Programme	B.Tech CSE Cyber Security	Programme Code	BTCY
Course Code	25BTCY161	Number of Hours/Week	3
Semester	VI	Max. Marks	100
Year	III	Credits	3

Course				
Course Title	NATURAL LANGUAGE PROCESSING	L	T	P
		3	0	0

COURSE OBJECTIVES:

The main learning objective of this course is to prepare the students for:

- Understand the Fundamentals of Lexical Analysis
- Explore Speech Processing Techniques
- Learn Parsing Techniques and Algorithms
- Develop Knowledge of Lexical Networks and Word Sense Disambiguation
- Apply Natural Language Processing in Real-world Applications

UNIT	TOPICS	HOURS
I	**Lexical Analysis** Lexical Analysis - Regular expression and Automata for string matching - Words and Word Forms - Morphology fundamentals - Morphological Diversity of Indian Languages - Morphology Paradigms - Finite State Machine / Transducers Based Morphology - Automatic Morphology Learning - Parts of Speech - N-gram Models - Hidden Markov Models.	9
II	**Speech Processing** Biology of Speech Processing - Place and Manner of Articulation - Word Boundary Detection - Argmax based computations - HMM and Speech Recognition - Text to Speech Synthesis - Rule Based- Concatenative based approach.	9
III	**Parsing** Theories of Parsing - Parsing Algorithms – Earley Parser - CYK Parser - Probabilistic Parsing - CYK - Resolving attachment and structural ambiguity - Shallow Parsing - Dependency Parsing - Named Entity Recognition - Maximum Entropy Models - Conditional Random Fields.	9
IV	**Lexical Knowledge Networks** Meaning: Lexical Knowledge Networks - Wordnet Theory - Indian Language Wordnets and Multilingual Dictionaries - Semantic Roles - Word Sense Disambiguation - WSD and Multilingualism - Metaphors - Coreference and Anaphora Resolution.	9
V	**UNIT V Applications** Applications: Sentiment Analysis - Text Entailment - Machine Translation - Question Answering System - Information Retrieval - Information Extraction - Cross Lingual Information Retrieval (CLIR).	9

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1 : Ability to Analyze Lexical Structures

CO2 : Competence in Speech Processing Techniques

CO3 : Proficiency in Parsing Algorithms

CO4 : Understanding and Application of Lexical Knowledge Networks

CO5 : Application of NLP Techniques in Various Domains

Text Books:

1. Jurafsky Daniel, Martin James, "Speech and Language Processing", Second Edition, Tenth Impression, Pearson Education, 2018.
2. Christopher Manning, Schutze Heinrich, "Foundations of Statistical Natural Language Processing", MIT Press, 1999. Operating System Concepts, Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, Wiley publishers, Nineth edition, 2013.

Reference Books:

1. Allen James, "Natural Language Understanding", Second Edition, Benjamin Cumming, 1995.
2. Charniack Eugene, "Statistical Language Learning", MIT Press, 1993.
3. Foundations of Statistical Natural Language Processing, The MIT Press Cambridge, Massachusetts London, England,1999.

Articulation Matrix

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO 1	1	1	0	0	0	0	1	0	0	0	1	0	1	0	1
CO 2	2	2	0	0	0	0	0	0	0	0	0	0	2	1	3
CO 3	1	2	1	0	0	0	1	0	0	0	2	3	1	2	1
CO 4	2	2	2	0	1	0	0	0	0	0	0	0	1	1	0
CO 5	3	3	1	0	0	0	0	2	0	0	0	1	2	2	0

Programme	B. Tech CSE Cyber Security	Programme Code	BTCY		
Course Code	25BTCY162	Number of Hours/Week	3		
Semester	VI	Max. Marks	100		
Year	III	Credits	3		
Course					
Course Title	COMPILER DESIGN		L	T	P
			3	0	0

COURSE OBJECTIVES:

The main learning objective of this course is to prepare the students for:

- To learn the various phases of compiler parsing techniques.
- To understand intermediate code generation and run-time environment.
- To learn to implement the front-end of the compiler.
- To learn to implement code generator.
- To learn to implement code optimization**.**

UNIT	TOPICS	HOURS
I	**Introduction To Compilers & Lexical Analysis** Introduction- Translators- Compilation and Interpretation- Language processors -The Phases of Compiler – Lexical Analysis – Role of Lexical Analyzer – Input Buffering – Specification of Tokens – Recognition of Tokens – Finite Automata – Regular Expressions to Automata NFA, DFA – Minimizing DFA – Language for Specifying Lexical Analyzers – Lex tool.	8
II	**Syntax Analysis:** Role of Parser – Grammars – Context-free grammars – Writing a grammar Top Down Parsing General Strategies – Recursive Descent Parser Predictive Parser-LL(1) – Parser-Shift Reduce Parser-LR Parser-LR (0)Item Construction of SLR Parsing Table – Introduction to LALR Parser Error Handling and Recovery in Syntax Analyzer-YACC tool – Design of a syntax Analyzer for a Sample Language	8
III	**Syntax Directed Translation & Intermediate Code Generation:** Syntax directed Definitions-Construction of Syntax Tree-Bottom-up Evaluation of S-Attribute Definitions- Design of predictive translator – Type Systems-Specification of a simple type Checker Equivalence of Type Expressions-Type Conversions. Intermediate Languages: Syntax Tree, Three Address Code, Types and Declarations, Translation of Expressions, Type Checking, Back patching.	8

IV	**Run-Time Environment And Code Generation:** Runtime Environments – source language issues – Storage organization – Storage Allocation Strategies: Static, Stack, and Heap allocation – Parameter Passing-Symbol Tables – Dynamic Storage Allocation – Issues in the Design of a code generator – Basic Blocks and Flow graphs Design of a simple Code Generator – Optimal Code Generation for Expressions– Dynamic Programming Code Generation.	**8**
V	**Code Optimization:** Classification of optimization, Principle sources of optimization, Optimization of basic blocks, Peephole Optimization, Loops in flow graphs, Local optimization, Global optimization, Data flow analysis of flow graph.	**8**

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1 : Learn Compiler phases, passes, and language translation mechanisms.

CO2 : Understand the concept of token generation, parsing techniques, symbol table and intermediate code generation.

CO3 : Apply syntax-directed translation to generate intermediate code representations, such as syntax trees and three-address code, and perform type checking.

CO4 : Understand various types of errors and error handling techniques.

CO5 : Apply the code optimization algorithms.

Text Book:

1. **Alfred V. Aho, Monica S. Lam, Ravi Sethi, Jeffrey D. Ullman, "Compilers: Principles, Techniques and Tools", Second Edition, Pearson Education, 2009.**

Reference Books:

1. **Randy Allen, Ken Kennedy, Optimizing Compilers for Modern Architectures: A Dependence based Approach, Morgan Kaufmann Publishers, 2002.**
2. **Steven S. Muchnick, Advanced Compiler Design and Implementation‖, Morgan Kaufmann Publishers – Elsevier Science, India, Indian Reprint 2003.**
3. **Keith D Cooper and Linda Torczon, Engineering a Compiler‖, Morgan Kaufmann Publishers Elsevier Science, 2004.**
4. **V. Raghavan, Principles of Compiler Design‖, Tata McGraw Hill Education Publishers, 2010.**
5. **Allen I. Holub, Compiler Design in C‖, Prentice-Hall Software Series, 1993.**

CO-PO-PSO Mapping Table :(B. Tech):

CO/PO /PSO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO3
CO1	3	2	1	1	2	2	1	1	3	2	2	1	3	2	1
CO2	2	3	2	1	3	2	3	1	2	3	1	2	2	3	2
CO3	3	2	3	2	2	3	1	1	2	2	3	2	3	2	2
CO4	2	3	2	3	2	1	2	2	3	3	2	3	2	1	3
C05	1	1	2	3	1	2	3	3	1	1	3	2	1	2	3

Programme	**B. Tech CSE Cyber Security**	**Programme Code**	**BTCY**		
Course Code	25BTCY163	**Number of Hours/Week**	**3**		
Semester	**VII**	**Max. Marks**	**100**		
Year	**III**	**Credits**	**3**		
Course					
Course Title	**WEB TECHNOLOGY**		**L**	**T**	**P**
			3	**0**	**0**

COURSE OBJECTIVES:

The main learning objectives of this course are to prepare students to:

1. **Understand Web Basics and Frontend Development:** Learn the fundamentals of web technologies, including HTML5, CSS3, and Bootstrap, for creating interactive and responsive web designs.
2. **Develop Client-side Programming Skills:** Gain proficiency in JavaScript, including DOM manipulation, event handling, and JSON, to create dynamic web content.
3. **Master Server-side Programming:** Understand Java Servlets, their life cycle, session management, cookies, and database connectivity using JDBC for backend development.
4. **Explore PHP and XML for Web Development:** Learn PHP programming for server-side scripting and understand XML for data representation, validation, and transformations.
5. **Introduce Modern Web Frameworks and Tools:** Gain insights into AngularJS, MVC architecture, and modern web frameworks like React, Node.js, and Django, along with tools like Firebase and Docker for building scalable web applications.

UNIT	TOPICS	HOURS
I	**WEBSITE BASICS, HTML 5, CSS 3, WEB 2.0** Web Essentials: Clients, Servers and Communication – The Internet – World wide web – HTTP.Request Message – HTTP Response Message – Web Clients – Web Servers – HTML5 – Tables.– Lists – Image – HTML5 control elements – Drag and Drop – Audio – Video controls - CSS3.– Inline, embedded and external style sheets – Rule cascading – Inheritance – Backgrounds –Border Images – Colours – Shadows – Text – Transformations – Transitions – Animations.Bootstrap Framework.	**9**
II	**CLIENT SIDE PROGRAMMING** **Java Script**: An introduction to JavaScript–JavaScript DOM Model-Exception Handling Validation- Built-in objects-Event Handling- DHTML with JavaScript- JSON introduction –Syntax – Function Files.	**9**
III	**SERVER SIDE PROGRAMMING** Servlets: Java Servlet Architecture- Servlet Life Cycle- Form GET and POST actions- Session.Handling- Understanding Cookies- DATABASE ,NNECTIVITY: JDBC. 121	**9**
IV	**PHP and XML** An introduction to PHP: PHP- Using PHP- Variables- Program control- Built-in functions Form Validation. XML: Basic XML- Document Type Definition- XML Schema, XML,Parsers and Validation, XSL ,	**9**
V	**INTRODUCTION TO ANGULAR and WEB APPLICATIONS FRAMEWORKS** Introduction to AngularJS, MVC Architecture, Understanding ng attributes, Expressions and,data binding, Conditional Directives, Style Directives, Controllers, Filters, Forms, Routers,Modules, Services; Web Applications Frameworks and Tools – Firebase- Docker- Node JSReact- Django- UI & UX.	**9**

Course Outcomes

On successful completion of this course, the student will be able to:

CO1: Understand the fundamentals of web technologies, including HTML5, CSS3, and Web 2.0 concepts
CO2: Develop interactive client-side applications using JavaScript, DOM manipulation, and JSON.
CO3: Implement server-side programming with Servlets, session handling, cookies, and database connectivity using JDBC.
CO4: Design dynamic web applications using PHP and XML with validation, schemas, and XSL transformations
CO5: Explore modern web frameworks like AngularJS, Firebase, Node.js, React, and Django for building scalable applications.

Text Books:

1. Anil Mahesh Wari, "Data Analytics made accessible," Amazon Digital Publication, 2014.
2. James R. Evans, "Business Analytics: Methods, Models, and Decisions", Pearson 2012.
3. Song, Peter X. K, "Correlated Data Analysis: Modeling, Analytics, and Applications", Springer- Verlag New York 2007.

Reference Books:

1. Glenn J. Myatt, Wayne P. Johnson, "Making Sense of Data I: A Practical Guide to Exploratory Data Analysis and Data Mining", Wiley 2009.
2. Thomas H. Davenport, Jeanne G. Harris and Robert Morison, "Analytics at Work: Smarter Decisions, Better Results", Harvard Business Press, 2010.

Mapping Table COs with POs

CO-PO-PSO Mapping Table:(**B. tech Cybersecurity)**

CO	**PO 1**	**PO 2**	**PO 3**	**PO 4**	**PO 5**	**PO 6**	**PO 7**	**PO 8**	**PO 9**	**PO 10**	**PO 11**	**PO 12**	**PSO 1**	**PSO 2**	**PSO3**
CO1	3	2	1	2	2	1	2	2	2	2	1	1	2	1	1
CO2	3	3	2	2	3	2	3	2	2	3	2	2	2	2	1
CO3	3	3	3	2	3	3	2	2	3	3	3	3	2	3	2
CO4	3	2	2	3	3	2	3	3	2	3	3	3	2	2	3
C05	3	3	3	3	3	3	3	3	3	3	3	3	2	3	3

3 – high, 2 – Average, 1 - Low , 0-Null

Discipline Specific Elective - V

Programme	B. Tech-CSE(Cyber Security)	Programme Code	BTCY		
Course Code	25BTCY361	Number of Hours/Week	3		
Semester	VI	Max. Marks	100		
Year	III	Credits	3		
Course					
Course Title	CYBER CRIMINOLOGY AND CYBER CRIMES		L	T	P
			3	0	0

COURSE OBJECTIVES:

- Explore security challenges in mobile/wireless devices and common cybercrime techniques.
- Introduce computer forensics principles, including evidence handling and investigation.
- Understand the role of security policies and cyber laws in protecting digital assets

UNIT	TOPICS	HOURS
I	**Introduction to Cyber Crime:** Cybercrime- Definition and Origins of the word Cybercrime and Information Security, who are Cybercriminals? Classifications of Cybercrimes, A Global Perspective on Cybercrimes, Cybercrime Era: Survival Mantra for the Netizens. Cyber offenses: How Criminals Plan the Attacks, Social Engineering, Cyber stalking, Cybercafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Attack Vector	9
II	**Cyber Crime:** Mobile and Wireless Devices-Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication Service Security, Attacks on Mobile/Cell Phones, Mobile Devices: Security Implications for organizations, Organizational Measures for Handling Mobile, Organizational Security Policies and Measures in Mobile Computing Era	9
III	**Tools and Methos used in Cyber Crime:** Introduction, Proxy Servers and Anonymizers, Phishing, Password Cracking, Keyloggers and Spywares, Virus and Worms, Trojan-horses and Backdoors, Steganography, DoS and DDoS At-tacks, SQL Injection, Buffer Overflow, Attacks on Wireless Networks. Phishing and Identity Theft: Introduction to Phishing, Identity Theft (ID Theft)	9
IV	**Understanding Computer Forensics:** Introduction, Digital Forensics Science, The Need for Computer Forensics, Cyber forensics and Digital Evidence, Forensics Analysis of E-Mail, Digital Forensics Life Cycle, Chain of Custody Concept, Network Forensics, Approaching a Computer Forensics Investigation. Forensics and Social Networking Sites: The Security/Privacy Threats, Challenges in Computer Forensics.	9
V	**Introduction to Security Policies and Cyber Laws:** Downloaders, Backdoors, Credential Stealers, Persistence Mechanisms, Privilege Escalation, Covert malware launching, Launchers, Process Injection, Process Replacement, Hook Injection, Detours, APC injection,	9

	Signature-based techniques: malware signatures, packed malware signature, metamorphic and polymorphic malware signature, non-signature-based techniques: similarity-based techniques, machine-learning methods, invariant inferences	

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1: Understand the fundamentals of cyber-crime, its types, and global impact.

CO2 : Identify various cyber offenses, attack methods, and social engineering techniques.

CO3: Analyze security challenges in mobile and wireless environments.

CO4: Apply forensic techniques to investigate cybercrimes and handle digital evidence.

CO5: Interpret cybersecurity policies and cyber laws, including the IT Act 2000 and DPDP Act 2023.

Text Book

1. Sunit Belapure and Nina Godbole, "Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiley India Pvt Ltd, ISBN: 978-81- 265-21791, Publish Date 2013.

2. Basta, Basta, Brown, Kumar, Cyber Security and Cyber Laws, 1st edition, Cengage Learning publication

3. Dr. Surya Prakash Tripathi, Ritendra Goyal, Praveen Kumar Shukla, KLSI. "Introduction to information security and cyber laws". Dream tech Press. ISBN: 9789351194736, 2015

Reference Books

1. Cyber Security and Date Privacy by Krishan Kumar Goyal , Amit Garg , Saurabh Singhal , HP HAMILTON LIMITED Publication, ISBN-13-978-1913936020
2. James Graham, Ryan Olson, Rick Howard, "Cyber Security Essentials", CRC Press, 15-Dec 2010

Mapping of Course Outcomes (COs) with PSOs- BTech

3 – high, 2 – Average, 1 - low, 0-null

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	2	2	2	3	2	2	3	2	2	2	2	3	2	2
CO2	3	3	2	3	3	2	2	2	3	2	2	2	3	3	3
CO3	3	3	3	3	3	3	3	2	2	3	3	3	3	3	3
CO4	3	2	3	3	3	3	2	3	3	2	2	3	3	3	3
C05	3	2	3	3	3	3	3	3	3	3	2	3	3	3	3

Programme	B.Tech CSE Cyber Security	Programme Code	BTCY
Course Code	23BTCY362	Number of Hours/ Week	3
Semester	VI	Max. Marks	100
Year	III	Credits	3

Course

Course Title	DESIGN OF INTERNET OF THINGS	L	T	P
		3	0	0

COURSE OBJECTIVES:

The main aim of this course is to prepare the students for:

- To understand the overview of Internet of Things and the design principles for the connected devices of IoT
- To understand the design principle for web and internet connectivity.
- To learn the the concepts of data acquiring, organizing and processing steps and the methods of data collection, storage and computing using cloud platform.
- To understand concepts of sensors participatory sensing RFIDs and wireless sensor networks and the methods of Prototyping Embedded Devices for IoT and M2M.
- To learn the privacy, security and Vulnerabilities solutions of IoT.

UNIT	TOPICS	HOURS
I	**Internet of Things - Overview:** Internet of Things-IoT Conceptual framework- IoT Architectural view- Technology behind IoT- Sources of IoT- M2M communication- Examples of IoT. **Design Principles for connected devices:** Introduction - IoT M2M System layers and design standardization- Communication Technologies- data Enrichment, Data consolidation and device management at gate way. Ease of designing and affordability.	9
II	**Design Principle for web connectivity:** Introduction-Web communication protocols for connected devices - Message communication protocols for connected devices- Web connectivity for connected devices -Network using gateway , SOAP, REST, HTTP, RESTful and WebSockets. **Internet Connectivity principle:** Internet connectivity-Internet based communication- Ip Addressing in the IoT- Media Access Control- Applications layer protocols - HTTP, HTTPS, FTP and Telnet and others.	9

III	**Data Acquiring, organizing, processing and Analytics:** Data acquiring and storage, Organizing the data - Transaction, business process, and enterprise systems,- Analytics- Knowledge acquiring - managing and storing processes. **Data collection, Storage, and computing using cloud platform:** Cloud computing paradigm for data collection, storing and computing Services and cloud service models -IoT Cloud based services using Xively, Nimbits, and other platforms.	**9**
IV	**Sensors participatory sensing RFIDs and wireless sensor networks** : Introduction , Sensor Technology , participatory sensing - Industrial and Automative Io T - Actuator- Sensor data communication protocols- Radio frequency identification technology - Wireless sensor network technology . **Prototyping Embedded Devices for IoT and M2M:** Embedded computing basics- Embedded platforms for prototyping- Things always connected to the internet /cloud.	**9**
V	**IoT privacy, security and Vulnerabilities solutions:** Introduction, -Vulnerabilities, Security requirements, and threat analysis- Use cases and misuse cases- IoT security tomography and layered attacker model- Identity management and establishment- Access control and secure message communication- Security models , Profiles and Protocols for IoT.	**9**

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1 : Understand the fundamental concepts, architectural framework, and technologies behind the Internet of Things (IoT), including M2M communication and IoT design principles.

CO2 : Learn the design principles of web and internet connectivity.

CO3 : Understand the methods of data acquiring, organizing, processing and analytics also the process of data collection, storage, and computing using cloud platform.

CO4 : Understand the concepts of sensors participatory sensing RFID and wireless sensors networks also the concepts of Prototyping Embedded Devices for IoT and

CO5 : Learn the the methods of IoT privacy, security and Vulnerabilities solutions:

Text Books:

1. Internet of Things, Architecture andDesign principle" Raj Kamal, Mc Graw Hill (Education India private LTD, (2017).
2. Internet of Things (IoT), Dr. Rajiv Chopra, S.K. Kataria & Sons, I st Ed. 2022, ISBN: 978-93-5014-735-1

Reference Books:

1. Raj Kamal, " INTERNET OF THINGS (IOT): Architecture and Design Principles |2nd Edition, paper back, 14 June. 2022.
2. Simone Cirani Caligoo, Gianluigi Ferrari, Marco Picone and Luca Veltri, "Internet of Things Architectures, Protocols and Standards", © 2019 John Wiley & Sons Ltd.

Mapping of Course Outcomes (CO's) with PO's & PSO's

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PS 9	**PS O1**	**PS O2**	**PS O3**
CO 1	3	2	2	3	1	1	1	1	2	2	2	1
CO 2	3	3	2	3	1	1	1	1	2	2	2	1
CO 3	3	2	3	3	1	2	1	1	2	3	2	2
CO 4	3	3	3	3	1	2	2	1	2	3	2	2
CO 5	3	3	3	3	2	2	3	1	2	3	3	2

3 – High, 2 – Average, 1 - Low , 0-Null

Programme	B.Tech CSE Cyber Security	Programme Code	BTCY
Course Code	25BTCY363	Number of Hours/Week	3
Semester	VI	Max. Marks	100
Year	III	Credits	3

Course				
Course Title	AUGMENTED INTELLIGENCE	L	T	P
		3	0	0

COURSE OBJECTIVES:

The main learning objective of this course is to prepare the students for:

- Understand the fundamental concepts and evolution of augmented intelligence and its applications in various industries.
- Analyze the enabling technologies such as machine learning, natural language processing, and computer vision for building augmented intelligence systems.
- Apply principles of human-computer interaction and collaborative systems to design user-friendly augmented intelligence solutions.
- Evaluate different architectures and methodologies for developing, deploying, and maintaining augmented intelligence systems.
- Create innovative augmented intelligence solutions by leveraging emerging technologies and addressing ethical considerations.

UNIT	TOPICS	HOURS
I	**Introduction to Augmented Intelligence** Overview and Evolution - Definition, history, and evolution of augmented intelligence - Human-Centric AI - Difference between AI and augmented intelligence; role in enhancing human decision-making. Applications: Healthcare, finance, education, customer service, and other industries - Ethics and Challenges: Ethical considerations, biases in AI, data privacy, and security issues.	8
II	**Enabling Technologies for Augmented Intelligence** Machine Learning (ML) - Supervised, unsupervised, and reinforcement learning - Natural Language Processing (NLP) - Text processing, sentiment analysis, and conversational AI - Computer Vision: Image recognition, object detection, and augmented reality - Data Analytics: Big data technologies, real-time analytics, and predictive modeling.	8
III	**Human-Machine Collaboration** Human-Computer Interaction (HCI) - Principles of HCI, user experience (UX) design, and usability - Collaborative Systems - Tools and platforms for human-machine collaboration - Cognitive Augmentation: Enhancing cognitive tasks with AI tools - Case Studies- Examples of	8

	successful human-machine collaboration in different sectors.	
IV	**Designing and Developing Augmented Intelligence System** System Architecture - Components and architecture of augmented intelligence systems - Data Collection and Integration - Data sources, data integration, and preprocessing - Model Training and Optimization: Training ML models, hyperparameter tuning, and performance evaluation -Deployment and Maintenance: Deploying AI systems, monitoring performance, and continuous improvement.	**8**
V	**Future Trends and Innovations** Emerging Technologies - Trends in AI, ML, IoT, and edge computing - Augmented Intelligence in Industry 4.0 - Role in smart manufacturing, automation, and supply chain optimization - Ethical AI - Ensuring fairness, accountability, transparency, and inclusivity - Future Directions: Research directions, potential innovations, and societal impact.	**8**

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1 : Explain the concept of augmented intelligence and its distinction from traditional AI, along with its applications and ethical challenges.

CO2 : Demonstrate the use of machine learning, natural language processing, and computer vision in the development of augmented intelligence systems.

CO3 : Design human-centric AI solutions that enhance human decision-making through effective human-machine collaboration.

CO4: Evaluate the performance of augmented intelligence systems, focusing on model optimization, data integration, and system architecture.

CO5 : Develop forward-thinking augmented intelligence solutions, incorporating emerging technologies and ethical practices to address future challenges.

Text Books:

1. Jena OP, editor. Augmented Intelligence: Deep Learning, Machine Learning, Cognitive Computing, Educational Data Mining. Bentham Science Publishers; 2022 Jul 29.

Reference Books:

1. Geroimenko V, editor. Augmented Reality and artificial intelligence: the Fusion of advanced technologies. Springer Nature; 2023 Apr 29.

Articulation Matrix

	PO 1	PO2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO 1	1	0	0	0	0	1	2	0	0	0	3	2	0	0	0
CO 2	0	0	0	0	1	2	0	0	0	2	2	3	0	1	2
CO 3	1	2	0	0	1	1	2	0	0	0	1	1	0	0	3
CO 4	2	0	0	0	1	3	0	0	0	2	1	0	2	0	1
CO 5	3	0	0	0	0	1	2	0	0	3	0	0	1	2	1

Discipline Specific Elective - VI

Programme	B.Tech Cyber Security	Programme Code	BTCY		
Course Code	23BTCY364	Number of Hours/Week	3		
Semester	VI	Max. Marks	100		
Year	III	Credits	3		
Course					
Course Title	REVERSE ENGINEERING		L	T	P
			3	0	0

COURSE OBJECTIVES:

1. To understand the fundamentals of reverse engineering and its applications in cybersecurity.
2. To analyze executable files and binary structures for vulnerability assessment.
3. To explore static and dynamic analysis techniques for malware detection and software security.
4. To study disassembly, decompilation, and debugging techniques for code analysis.

UNIT	TOPICS	HOURS
I	**Introduction to Reverse Engineering**: Overview of Reverse Engineering: Definition, Goals, and Ethical Considerations. Applications in Cybersecurity: Malware Analysis, Software Security, and Digital Forensics. Software and Hardware Reverse Engineering. Basics of Assembly Language and Machine Code Interpretation.	9
II	**Static Analysis Techniques:** Understanding Executable File Formats: PE, ELF, and Mach-O. Disassembly Techniques: Introduction to IDA Pro, Ghidra, and Radare2.String Analysis, API Calls, and Control Flow Graphs. Identifying Code Obfuscation and Packing Techniques.	9
III	**Dynamic Analysis and Debugging: Debugging Basics:** Tools (OllyDbg, WinDbg, GDB) and Techniques. Breakpoints, Stack Analysis, and Memory Inspection. Detecting and Analyzing Malware Behavior. Evasion Techniques and Anti-Debugging Mechanisms.	9
IV	**Decompilation and Code Reconstruction:** Reverse Engineering High-Level Code from Executables.Decompilers: RetDec, Hex-Rays, and Snowman. Recovering Algorithms and Identifying Code Structures. Reverse Engineering for Software Patching and Exploit Development.	9
V	**Advanced Reverse Engineering and Case Studies:** Advanced Malware Analysis Techniques. Firmware Reverse Engineering and IoT Security. Cryptographic Algorithm Analysis. Case Studies: Real-World Reverse Engineering Applications.	9

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1 : Understand the principles and ethical implications of reverse engineering.

CO2 : Analyze software binaries using static analysis techniques.

CO3 : Perform dynamic analysis and debugging for vulnerability assessment.

CO4 : Apply decompilation and code reconstruction techniques to understand software behavior.

CO5 : Conduct advanced reverse engineering using modern tools and methodologies.

Text Book

1. Eldad Eilam - 'Reversing: Secrets of Reverse Engineering', Wiley, 2005.
2. Dennis Yurichev - 'Reverse Engineering for Beginners', Self-Published, 2018.

Reference Books

1. Bruce Dang, Alexandre Gazet, Elias Bachaalany - 'Practical Reverse Engineering', Wiley, 2014.
2. Chris Eagle - 'The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler', No Starch Press, 2011.

Mapping of Course Outcomes (COs) with PSOs

	PO 1	PO 2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO 10	PO 11	PO 12	PS O1	PS O2	PS O3
CO1	3	2	0	1	2	1	1	2	0	2	1	2	3	1	3
CO2	1	2	1	0	2	2	0	1	1	0	0	0	3	0	2
CO3	2	0	3	3	3	3	0	1	1	3	0	3	2	3	2
CO4	2	3	1	3	0	3	1	0	0	0	0	0	2	0	2
C05	1	2	0	1	0	2	2	3	0	2	0	0	3	1	3

3 – high, 2 – Average, 1 - low , 0-null

Programme	B. Tech CSE Cyber Security	Programme Code	BTCY
Course Code	25BTCY365	Number of Hours/Week	3
Semester	VI	Max. Marks	100
Year	III	Credits	3

Course				
Course Title	DIGITAL FORENSICS	L	T	P
		3	0	0

COURSE OBJECTIVES:

- Equip students with foundational knowledge of computer forensics.
- Cover evidence collection and digital investigation processes.
- Explore data recovery techniques and legal considerations.
- Develop skills in forensic analysis of various digital platforms.

UNIT	TOPICS	HOURS
I	**Computer forensics fundamentals** What are computer forensics, use of computer forensics in law enforcement, Computer forensics assistance to human resource/employment proceedings, Computer forensics services, benefits of professional forensics methodology, steps taken by Computer forensics specialists, who can use Computer forensics evidence, Types of Computer forensics technology: types of military Computer forensics technology, types of law enforcement, Computer forensic technology, types of business Computer forensic technology. Types of vendor and computer forensics services: Occurrence of cybercrime, cyber detectives, computer forensics investigative services, forensics process improvement.	9
II	**Data recovery** Data recovery defined, data back-up and recovery, the role of back-up in data recovery, the data recovery solution. Evidence collection and data seizure- Why collective evidence, Collection options, obstacles, types of evidence, the rules of evidence, volatile evidence, general procedure, collection and archiving, methods of collection, artifacts, collection steps, controlling contamination: the chain of custody. Duplication and preservation of digital evidence, Preserving the digital crime scene, computer evidence processing steps, legal aspects of collecting and preserving Computer forensics evidence.	9
III	**Conducting Digital Investigations** Digital Investigation Process Models, Scaffolding for Digital Investigations, Applying the Scientific Method in Digital Investigations, Investigative Scenario: Security Breach. Handling a Digital Crime Scene-Published Guidelines for Handling Digital Crime Scenes, Fundamental Principles, Authorization, Preparing to Handle Digital Crime Scenes, Surveying the Digital Crime Scene, Preserving the Digital Crime Scene, Investigative Reconstruction with Digital Evidence: Equivocal Forensic	9

	Analysis, Victimology, Crime Scene Characteristics, Threshold Assessments.	
IV	**Violent Crime and Digital Evidence** The Role of Computers in Violent Crime, Processing the Digital Crime Scene, Investigative Reconstruction, Digital Evidence as Alibi, Investigating an Alibi, Time as Alibi, Location as Alibi. Sex Offenders on the Internet, Old Behaviours, New Medium, Legal Considerations, Identifying and Processing Digital Evidence, Investigating Online Sexual Offenders, Investigative Reconstruction, Case Example: Scott Tyree, Case Example: Peter Chapman. Computer Intrusions -How Computer Intruders Operate, Investigating Computer Intrusions, Forensic Preservation of Volatile Data, Post-Mortem Investigation of a Compromised System, Investigation of Malicious Computer Programs, Investigative Reconstruction. Cyberstalking: How Cyber stalkers Operate, Investigating Cyberstalking, Cyberstalking, Case Example.	**9**
V	**Computer Basics for Digital Investigators:** A Brief History of Computers, Basic Operation of Computers, Representation of Data, Storage Media and Data Hiding, File Systems and Location of Data, Dealing with Password Protection and Encryption Applying, Forensic Science to Computers: Preparation, Survey, Documentation, Preservation, Examination and Analysis, Reconstruction, Reporting, Digital Evidence on Windows Systems: File Systems, Data Recovery, Log Files, Registry, Internet Traces, Program Analysis. Digital Evidence on UNIX Systems - UNIX Evidence Acquisition Boot Disk, File Systems, Overview of Digital Evidence Processing Tools, Data Recovery, Log Files, File System Traces, Internet Traces, Digital Evidence on the Internet-Role of the Internet in Criminal Investigations, Internet Services: Legitimate versus Criminal Uses, Using the Internet as an Investigative Tool, Online Anonymity and Self-Protection, E-mail Forgery and Tracking, Usenet Forgery and Tracking, Searching and Tracking on IRC.	**9**

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1: Explain the fundamentals of computer forensics and its applications in law enforcement, business, and military contexts.

CO2 : Apply data recovery techniques and evidence collection procedures while ensuring legal compliance.

CO3: Conduct digital investigations, including handling and preserving digital crime scenes.

CO4: Analyze digital evidence related to cybercrimes, computer intrusions, and online offenses.

CO5: Utilize forensic tools and techniques for examining digital evidence across different platforms, including Windows, UNIX, and Internet-based systems.

Text Book

1. Bill Nelson, Amelia Phillips, Christopher Steuart, – Guide to Computer Forensics and Investigations‖, Cengage Learning, India Sixth Edition, 2019

2. CEH official Certified Ethical Hacking Review Guide, Wiley India Edition, Version 11, 2021.

3. Dejey, S. Murugan - Cyber Forensics, Oxford University Press, India, 2018

Reference Books

1. Computer Forensics: Computer Crime Scene Investigation, John R. Vacca, 1 ST Edition, Charles River Media, 2005

2. Digital Evidence and Computer Crime Forensic Science, Computers and the Internet, Eoghan Casey, 3rd edition, Elsevier, Academic Press, 2011

Mapping of Course Outcomes (COs) with PSOs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	1	1	2	1	0	0	0	0	0	0	0	3	2	1
CO2	3	3	2	1	0	3	0	0	0	0	0	0	3	3	2
CO3	3	3	3	1	3	3	0	0	0	0	0	0	3	3	3
CO4	3	3	3	3	3	3	0	0	0	0	0	0	3	3	3
CO5	3	3	3	3	3	3	0	0	0	0	0	0	3	3	3

3 – high, 2 – Average, 1 - low, 0-null

Programme	B. Tech CSE -Cyber Security	Programme Code	BTCY
Course Code	25BTCY366	Number of Hours/Week	3
Semester	VIII	Max. Marks	100
Year	IV	Credits	3

Course				
Course Title	CYBER THREAT INTELLIGENCE	L	T	P
		3	0	0

COURSE OBJECTIVES:

- Introduce the concept of Cyber Threat Intelligence (CTI), its need, and how it differs from traditional cybersecurity.
- Explain the various types of threat actors and their behavior, motivations, and tactics.
- Equip students with knowledge about different threat intelligence data sources, platforms, and data analysis techniques.
- Enable students to perform threat analysis and hunting using modern tools.
- Emphasize ethical considerations and the importance of information sharing frameworks in CTI.

UNIT	TOPICS	HOURS
I	**Introduction to Cyber Threat Intelligence** Definition and need for Cyber Threat Intelligence (CTI) - Types of CTI: Tactical, Operational, Strategic - Intelligence Cycle: Direction - Collection, Processing, Analysis, Dissemination, Feedback - CTI vs Traditional Cyber Security	7
II	**Threat Actors and Adversary Behavior** Types of Threat Actors: Hacktivists, Cybercriminals, APTs, Insider threats - Motivations and Objectives of Threat Actors - Adversary Tactics, Techniques, and Procedures (TTPs) - Kill Chain Model & MITRE ATT&CK Framework	7
III	**Data Collection and Threat Intelligence Platforms** Intelligence sources: Open Source Intelligence (OSINT), Dark Web, Social Media, Logs - Indicators of Compromise (IoCs), TTPs, Threat Feeds - Threat Intelligence Platforms (TIPs): MISP, Open Threat Exchange (OTX) - Data enrichment and analysis techniques	7
IV	**Threat Analysis and Hunting** Threat analysis lifecycle - Correlation and prioritization of intelligence - Threat hunting methodologies (hypothesis-based, IOC-driven) - Introduction to tools: Splunk, ELK stack, Wireshark for threat analysis	7
V	**CTI Reporting, Ethics and Information Sharing** Creating intelligence reports: tactical vs strategic - Visualization of CTI: dashboards, graphs - Legal, Ethical and Privacy Issues in CTI - Information sharing frameworks: ISACs, STIX/TAXII	7

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1: Understand CTI principles and why organizations need it
CO2 : Classify different threat actors and their behaviors
CO3: Understand CTI data sources and how to extract useful threat data
CO4: Analyze and correlate threat data
CO5: Understand CTI sharing laws, ethics, and frameworks

Text Book

Zane Pokorny, et al., *The Threat Intelligence Handbook*

Reference Books

- Dalziel, H. (2014). *Cyber threat intelligence*. Syngress. https://doi.org/10.1016/C2013-0-18052-6

- Roberts, S. J., & Brown, R. (2017). *Intelligence-driven incident response: Outwitting the adversary*. O'Reilly Media.

- Bejtlich, R. (2013). *The practice of network security monitoring: Understanding incident detection and response*. No Starch Press.

- Whaley, B. (2016). *Cyber intelligence: Using data to understand emerging threats*. Rowman & Littlefield.

- White, A. J., & Clark, B. (2017). *Blue team field manual (BTFM)*. CreateSpace Independent Publishing Platform.

Mapping of Course Outcomes (COs) with PSOs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	1	1	2	1	0	0	0	0	0	0	0	3	2	1
CO2	3	3	2	1	0	3	0	0	0	0	0	0	3	3	2
CO3	3	3	3	1	3	3	0	0	0	0	0	0	3	3	3
CO4	3	3	3	3	3	3	0	0	0	0	0	0	3	3	3
CO5	3	3	3	3	3	3	0	0	0	0	0	0	3	3	3

3 – high, 2 – Average, 1 - low, 0-null

Open Electives - II

Programme	B.Tech CSE Cyber Security	Programme Code	BTCY
Course Code	25BTCY061	Number of Hours/Week	3
Semester	VII	Max. Marks	100
Year	IV	Credits	3

Course				
Course Title	Artificial Intelligence Tools	L	T	P
		3	0	0

COURSE OBJECTIVES:

The main aim of this course is to prepare the students for:

- To provide hands-on experience with AI tools without deep programming prerequisites.
- To expose students to real-world applications of AI in their own domains.
- To foster creative thinking through experimentation with AI-powered platforms and systems.

#	Practical Title	Tool(s)	Description
1	Intro to AI Tools	ChatGPT, Google Bard	Explore AI chatbots for answering domain-specific questions (e.g., finance, biology, marketing).
2	Text Summarization	ChatGPT, Quillbot	Input long articles or reports and generate concise summaries.
3	AI in Image Captioning	Canva + GPT/Vision API	Upload an image and generate a descriptive caption using AI.
4	Create a Resume with AI	Kickresume, ChatGPT	Use AI to build a professional resume tailored to a job role.
5	Data Analysis without Coding	Google AutoML Tables / Orange	Load CSV data (e.g., survey data) and perform classification or clustering.
6	Sentiment Analysis	MonkeyLearn / ChatGPT / Google Sheets AI	Analyze feedback or product reviews to detect sentiment.
7	AI-Based Presentation Generator	Tome / Canva Docs	Generate a slide deck based on a topic using AI.
8	AI in Healthcare (Domain App)	Symptom Checker AI / Infermedica	Input symptoms and explore AI-driven diagnostics (for Life Sciences).
9	Generate Art with AI	DALL·E, Bing Image Creator, Midjourney	Create concept illustrations or visuals based on prompts.
10	Voice to Text & Transcription	Whisper by OpenAI / Otter.ai	Record voice notes and convert them into text (useful in journalism/management).
11	AI Tools for Education	Khanmigo / Socratic / Scribe AI	Explore how AI can tutor, quiz, or assist with concept explanation.
12	Create Your Own Chatbot	Dialogflow / Poe.com	Design a domain-specific chatbot (e.g., campus assistant or career advisor).

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1 :	Identify and use key AI tools for data analysis, image processing, NLP, and automation.
CO2 :	Build simple AI-driven projects or visualizations without coding (or minimal coding).
CO3 :	Apply AI concepts to solve or analyze domain-specific problems.
CO4 :	Evaluate the role and limitations of AI tools in decision-making.
CO5 :	Understand ethical aspects and responsible AI tool usage.

Tools & Platforms (Free or Freemium)

- **ChatGPT** (OpenAI)
- **Google Teachable Machine**
- **DALL·E / Bing Image Creator**
- **Canva AI**, **Tome**, **Otter.ai**
- **MonkeyLearn**, **Google Colab**
- **AutoML Tables (Google Cloud)**
- **Socratic (by Google)**
- **Poe.com**, **Quillbot**, **HuggingFace Spaces**

Mapping of Cos with POs and PSOs for_____

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6
CO1																		
CO2																		
CO3																		
CO4																		
CO5																		

3 – High, 2 – Average, 1 - low, 0 - null

Programme	B.Tech CSE Cyber Security	Programme Code	BTCY
Course Code	25BTCY062	Number of Hours/Week	3
Semester	VII	Max. Marks	100
Year	IV	Credits	3

Course				
Course Title	INTERNET OF THINGS	L	T	P
		3	0	0

COURSE OBJECTIVES:

The main aim of this course is to prepare the students for:

- To introduce the fundamentals of IoT and its architecture.
- To familiarize students with sensors, communication protocols, and real-world applications.
- To develop an understanding of how IoT transforms various domains.
- To explore the ethical, privacy, and security issues in IoT systems.
- To encourage interdisciplinary applications using IoT solutions.

UNIT	TOPICS	HOURS
I	**Introduction to IoT:** Definition and Evolution of IoT - Characteristics of IoT (Connectivity, Sensing, Intelligence, Action) - IoT vs Traditional Internet - IoT Ecosystem: Devices, Network, Cloud, Analytics - Applications in agriculture, healthcare, logistics, environment	9
II	**IoT Architecture and Devices:**Basic IoT architecture (Perception, Network, Application layers) - Microcontrollers and boards: Arduino, Raspberry Pi (overview) - Sensors: Temperature, Humidity, Proximity, Gas, Motion - Actuators and control mechanisms - Analog vs Digital sensors	9
III	**Communication Protocols in IoT:** Wired and Wireless technologies - Short-range protocols: Bluetooth, ZigBee, Wi-Fi - Long-range protocols: LoRa, NB-IoT, LTE - Internet protocols: MQTT, CoAP, HTTP - Edge vs Cloud communication	9
IV	**IoT Data and Cloud Integration:** Data collection and processing in IoT - Real-time monitoring and dashboards - Cloud platforms for IoT: Thingspeak, Blynk, AWS IoT, Azure IoT - Case Study: Smart irrigation, Wearables, Energy monitoring - Basics of data analytics for decision-making	9
V	**Security, Ethics and Emerging Trends:** IoT Security: Challenges and solutions - Privacy concerns and data protection - Role of AI and Machine Learning in IoT - Digital Twins and Industry 4.0 - Regulatory frameworks and responsible innovation	9

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1 :	Understand the basic architecture and components of IoT systems.
CO2 :	Identify applications of IoT in non-CS domains (e.g., agriculture, healthcare, smart cities).
CO3 :	Use basic sensors and microcontrollers (e.g., Arduino or ESP32) for IoT projects.
CO4 :	Analyze data flow from edge devices to cloud storage.
CO5 :	Discuss IoT security, privacy, and data ethics.

Text Book

Internet of Things – A Hands-on Approach, Arshdeep Bahga, Vijay Madisetti
***Getting Started with the Internet of Things,*:** Cuno Pfister (O'Reilly)

Mapping of Cos with POs and PSOs for_____

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6
CO1																		
CO2																		
CO3																		
CO4																		
CO5																		

3 – High, 2 – Average, 1 - low, 0 – null

Programme	**B.Tech CSE Cyber Security**	**Programme Code**	**BTCY**		
Course Code	**25BTCY063**	**Number of Hours/Week**	**3**		
Semester	**VII**	**Max. Marks**	**100**		
Year	**IV**	**Credits**	**3**		
Course Title	**MACHINE LEARNING FOR CYBER SECURITY**		**L**	**T**	**P**
			3	**0**	**0**

L-Lecture Hours T-Tutorial Hours P-Practical Hours

COURSE OBJECTIVES

The course aims to:

1. Introduce the fundamental concepts of machine learning (ML) and their applications in cybersecurity.
2. Develop the ability to preprocess and engineer features from cybersecurity datasets.
3. Apply classification, clustering, and ensemble ML techniques for detecting security threats.
4. Explore deep learning techniques, including CNNs and RNNs, for advanced threat detection.
5. Understand and address adversarial ML threats, explainability, and ethical issues in cybersecurity ML deployments.

UNIT	TOPICS	HOURS
I	**Introduction to Cybersecurity and Machine Learning** Overview of cybersecurity landscape - Introduction to machine learning (ML): supervised, unsupervised, reinforcement learning - Data types in cybersecurity (logs, flows, binaries) - Challenges in applying ML to cybersecurity - Python and scikit-learn setup for ML	9
II	**Data Preprocessing and Feature Engineering for Cybersecurity** Data sources: IDS logs, network traffic, malware datasets - Cleaning and transforming security data - Feature extraction and selection techniques - Handling imbalanced datasets (e.g., SMOTE) - Exploratory Data Analysis (EDA)	9
III	**ML Models for Cyber Threat Detection** Classification algorithms (SVM, Decision Trees, Random Forests, k-NN, Naive Bayes) - Clustering (K-means, DBSCAN) - Ensemble methods (Bagging, Boosting) - Evaluation metrics: Accuracy, Precision, Recall, F1, ROC-AUC - Hands-on: Detecting intrusions using KDD Cup 99 or UNSW-NB15 datasets	9
IV	**Deep Learning and Advanced Models for Cybersecurity** Neural Networks, CNNs, RNNs/LSTMs - Autoencoders for anomaly detection - Transfer learning and pre-trained models - Natural Language Processing (NLP) for phishing/email analysis - Frameworks: TensorFlow, Keras, PyTorch	9
V	**Adversarial ML, Explainability & Real-world Use Cases** Adversarial attacks and model robustness - Explainable AI (XAI) in cybersecurity - Case studies: SIEM integration, malware detection, phishing defense - Deployment of ML models in cybersecurity pipelines - Ethical and legal aspects of AI in security	9

45 Hours

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1: Understand ML fundamentals and their relevance to cybersecurity
CO2: Build cybersecurity datasets for ML models
CO3: Apply clustering to detect anomalies
CO4: Implement deep learning for malware and intrusion detection
CO5: Apply ML in real-world cyber defense scenarios

Text Books:

Kwon, D. (2019). *Machine learning for cybersecurity cookbook: Over 80 recipes to secure, detect, and investigate using machine learning*. Packt Publishing.

Reference Books:

- Dua, S., & Du, X. (2016). *Data mining and machine learning in cybersecurity*. CRC Press.

- Mohri, M., Rostamizadeh, A., & Talwalkar, A. (2018). *Foundations of machine learning* (2nd ed.). MIT Press.

- Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In *IEEE Symposium on Security and Privacy*, 305–316. https://doi.org/10.1109/SP.2010.25

- Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). A survey of deep learning methods for cybersecurity. *Information*, 10(4), 122. https://doi.org/10.3390/info10040122

- Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.

CO-PO-PSO MAPPING _____

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO 11	PO 12	PS O1	PS O2	PS O3
CO1															
CO2															
CO3															
CO4															
CO5															

3 – high, 2 – Average, 1 - low , 0-null

Programme	B.Tech CSE Cyber Security	Programme Code	BTCY		
Course Code	25BTCY261	Number of Hours/Week	2		
Semester	VI	Max. Marks	100		
Year	III	Credits	1		
Course					
Course Title	Natural Language Processing Lab		L	T	P
			0	0	2

COURSE OBJECTIVES:

The main learning objective of this course is to prepare the students for:

- **Understand** the fundamental concepts of Natural Language Processing (NLP) and its applications.
- **Implement** basic NLP techniques such as tokenization, stemming, lemmatization, and POS tagging.
- **Analyze** various NLP models for text classification, sentiment analysis, and named entity recognition.
- **Evaluate** the performance of different NLP algorithms using appropriate metrics.

Develop real-world NLP applications using machine learning and deep learning frameworks.

LIST OF EXPERIMENTS:

1. Tokenization and Text Preprocessing in NLP
2. Part-of-Speech (POS) Tagging using NLTK and SpaCy
3. Named Entity Recognition (NER) for Text Analysis
4. Sentiment Analysis using Machine Learning
5. Text Classification with Naïve Bayes and SVM
6. Word Embeddings: Word2Vec, GloVe, and FastText
7. Machine Translation using Seq2Seq Models
8. Text Summarization: Extractive vs. Abstractive Methods
9. Building a Chatbot using Transformer Models
10. Topic Modeling with Latent Dirichlet Allocation (LDA)

COURSE OUTCOME:

Upon successful completion of the course, students will be able to:

- **Explain** the key concepts and challenges in NLP. *(Bloom's Level: Understand)*
- **Apply** NLP preprocessing techniques to process and clean textual data. *(Bloom's Level: Apply)*
- **Demonstrate** the working of different NLP models in practical scenarios. *(Bloom's Level: Apply)*
- **Assess** the efficiency and effectiveness of NLP models using evaluation metrics. *(Bloom's Level: Evaluate)*
- **Design** and implement NLP-based solutions for real-world applications. *(Bloom's Level: Create)*

Articulation Matrix

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO 1	1	1	0	0	0	0	1	0	0	0	1	0	1	0	1
CO 2	2	2	0	0	0	0	0	0	0	0	0	0	2	1	3
CO 3	1	2	1	0	0	0	1	0	0	0	2	3	1	2	1
CO 4	2	2	2	0	1	0	0	0	0	0	0	0	1	1	0
CO 5	3	3	1	0	0	0	0	2	0	0	0	1	2	2	0

3 -High, 2 – Average, 1 - low, 0-null

Programme	**B.Tech CSE Cyber Security**	**Programme Code**	**BTCY**		
Course Code	**25BTCY262**	**Number of Hours/Week**	**2**		
Semester	**VI**	**Max. Marks**	**100**		
Year	**III**	**Credits**	**1**		
Course					
Course Title	**COMPILER DESIGN LAB**		**L**	**T**	**P**
			0	**0**	**2**

COURSE OBJECTIVES:

The main learning objective of this course is to prepare the students for:

- Master lexical analysis tools – build both manual and Lex-based scanners to identify tokens accurately.
- Design and implement parsers – convert grammars to YACC specifications, construct ASTs, and resolve syntax errors.
- Apply semantic analysis – implement symbol tables, type checking, and control/data flow analyses for semantic correctness.
- Simulate run-time behavior – experiment with storage-allocation strategies and DAG construction to support code generation.
- Introduce code optimisation techniques – perform basic-block, peephole, and global optimisations to improve compiled output efficiency.

LIST OF EXPERIMENTS:

1. Implementation of Symbol Table

2. Develop a lexical analyzer to recognize a few patterns in C. (Ex. identifiers, constants, comments, operators etc.)

3. Implementation of Lexical Analyzer using Lex Tool

4. Generate YACC specification for a few syntactic categories.

a) Program to recognize a valid arithmetic expression that uses operator +, - , * and /.

b) Program to recognize a valid variable which starts with a letter followed by any number of letters or digits.

c) Implementation of Calculator using LEX and YACC

5. Convert the BNF rules into Yacc form and write code to generate Abstract Syntax Tree.

6. Implement type checking

7. Implement control flow analysis and Data flow Analysis

8. Implement any one storage allocation strategies (Heap, Stack)

9. Construction of DAG

10. Implementation of Simple Code Optimization Techniques.

COURSE OUTCOME:

Upon successful completion of the course, students will be able to:

CO1	Implement Lexical Analysis: Construct accurate tokenizers for a subset of C both manually and with Lex.
CO2	Develop Syntax Analyzers: Write YACC grammars, resolve conflicts, and generate Abstract Syntax Trees for arithmetic expressions, variables, and calculators.
CO3	Perform Semantic Checks: Build symbol tables, enforce type-checking rules, and validate programs for semantic correctness.
CO4	Analyze Program Flow & Storage: Generate control- and data-flow graphs, construct DAGs, and experiment with stack vs. heap allocation to model run-time behavior.
CO5	Optimize Intermediate Code: Apply basic-block, peephole, and global data flow optimizations to improve execution efficiency of compiled code.

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO1**	**PSO2**	**PSO3**
CO1	3	2	2	3	3	1	1	1	1	2	2	3	3	2	3
CO2	3	3	2	3	3	1	1	1	1	2	2	3	3	3	3
CO3	3	3	3	3	3	2	1	1	1	2	3	3	3	3	3
CO4	3	3	3	3	3	2	1	1	1	2	3	3	3	3	3
C05	3	3	2	3	3	2	1	1	1	3	3	3	3	3	3

3 -High, 2 – Average, 1 - low, 0-null

Semester VII

Programme	**B.Tech CSE Cyber Security**	**Programme Code**	**BTCY**		
Course Code	**25BTCY171**	**Number of Hours/Week**	**3**		
Semester	**VII**	**Max. Marks**	**100**		
Year	**IV**	**Credits**	**3**		
Course Title	**HIGH PERFORMANCE COMPUTING**		**L**	**T**	**P**
			3	**0**	**2**

L-Lecture Hours T-Tutorial Hours P-Practical Hours

COURSE OBJECTIVES:

- To understand high-performance computing (HPC) system architectures and various computational models.
- To learn the fundamentals of CUDA programming and its applications in parallel computing.
- To apply parallel execution models and methodologies for developing parallel programming and applications.
- To design and implement compute-intensive applications on HPC platforms for optimized performance.
- To explore advanced techniques and tools for improving efficiency in high-performance computing environments.

UNIT	TOPICS	HOURS
I	**Parallel Programming & Computing - Introduction** Era of Computing - Parallel Computing - Multiprocessors and Multicomputer Architectures - Scalar vs Vector Processing - Multivector and Superscalar Machines - Pipelined Processors - SIMD Computers - Conditions of parallelism - Program flow mechanisms - Types of Parallelism – ILP, PLP, LLP - Program partitioning and scheduling.	9
II	**Introduction to High Performance Computing** Era of Computing - Scalable Parallel Computer Architectures - Towards low-cost computing - Network of Workstations project by Berkeley - Cluster Computing Architecture – Components - Cluster Middleware and SSI - Need of Resource Management and Scheduling - Programming Environments	9
III	**Cluster Computing** Introduction to Cluster Computing - Basics and importance of cluster computing -	9

	Clustering Models and Architectures - Key architectures and factors affecting cluster design - Types of Clusters - High-performance, high-availability, and load- balancing clusters - Fault Detection and Handling - Heartbeats, Check Pointing, and Watchdog Timers - Failover and Recovery - Concepts of failover and failback.	
IV	**High Speed Networks & Message Passing** Introduction to High-Speed Networks, Lightweight Messaging Systems, Xpress Transport Protocol, Software RAID and Parallel File systems, Load Balancing Over Networks – Algorithms and Applications, Job Scheduling approaches and Resource Management in Cluster	9
V	**CUDA Programming** Introduction to CUDA architecture for parallel processing, CUDA Parallelism Model, Foundations of shared memory, Introduction to CUDA-C, Parallel programming in CUDA-C, Thread Cooperation and Execution Efficiency, Constants memory and events, Memory Management, CUDA C on multiple GPUs - OpenMP: Parallel Programming using OpenMP.	9

45 PERIODS

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1: Understand the foundational concepts of computer architecture and modern processors.

CO2: Grasp the fundamental principles of access optimization and parallel computers.

CO3: Explain the various parallel processing platforms utilized in high-performance computing.

CO4: Design efficient and high-performance parallel programming solutions.

CO5: Learn and implement parallel programming using the message-passing paradigm.

Text Books:

1. Laurence T.Yang, Minyi Guo – High Performance Computing Paradigm and Infrastructure, John Wiley.
2. Ahmar Abbas, Grid Computing: Practical Guide to Technology & Applications, Firewall Media, 2004.
3. Joshy Joseph and Craig Fellenstein , Grid Computing, Pearson Education, 2004.
4. Georg Hager and Gerhard Wellein, Introduction to High Performance Computing for Scientists and Engineers, CRC Press.

Reference Books:

1. Lan Foster, et al., The Open Grid Services Architecture, Version 1.5 (GFD.80). Open Grid Forum, 2006.
2. Rajkumar Buyya, High Performance Cluster Computing: Architectures and Systems. Prentice Hall India, 1999.
3. Kai Hwang, Advanced Computer Architecture: Parallelism, Scalability, Programmability, McGraw Hill International Editions

CO-PO-PSO MAPPING

B.Tech

Mapping of Course Outcomes (COs) with PSOs

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO 11	PO 12	PS O1	PS O2	PS O3
CO1	3	1	2	3	2	3	2	3	1	3	2	1	3	2	3
CO2	2	3	1	2	3	2	3	1	3	2	3	2	1	3	2
CO3	1	2	3	2	1	3	2	3	2	3	1	3	2	3	1
CO4	3	2	1	3	2	1	3	2	3	1	2	3	3	1	2
CO5	2	3	2	1	3	2	1	3	2	3	2	1	3	2	3

3 – high, 2 – Average, 1 - low , 0-null

Programme	B.Tech CSE Cyber Security	Programme Code	BTCY		
Course Code	25BTCY172	Number of Hours/Week	3		
Semester	VII	Max. Marks	100		
Year	IV	Credits	3		
Course					
Course Title	ETHICAL HACKING AND PENETRATION TESTING		L	T	P
			3	0	2

COURSE OBJECTIVES:

The main aim of this course is to prepare the students for:

- Interpret the fundamentals of Ethical Hacking
- Illustrate the concept of Reconnaissance, Footprinting, Scanning and Enumeration
- Experiment with System Hacking techniques and Malware Attacks
- Analyze the Concepts of attacks such as Sniffing, Denial of Service, Session Hijacking, SQL Injection and Buffer Overflows
- Analyze the importance of following Ethics of Ethical Hacking.

UNIT	TOPICS	HOURS
I	**Introduction to Ethical Hacking -** Introduction to Ethical Hacking : Gathering Target Information - Introduction to Ethical Hacking - Defining Ethical Hacking - Understanding the Purpose of Ethical Hacking -An Ethical Hacker's Skill Set - Ethical Hacking Terminology - The Phases of Ethical Hacking - Identifying Types of Hacking Technologies - Identifying Types of Ethical Hacks - Understanding Testing Types - **Gathering Target Information: Reconnaissance, Foot printing, and Social Engineering** -Reconnaissance - Understanding Competitive Intelligence . Information-Gathering Methodology : Foot printing - Using Google to Gather Information - Understanding DNS Enumeration - Understanding Who is and ARIN Lookups - Identifying Types of DNS Records - Using Trace route in Foot printing - Understanding Email Tracking - Understanding Web Spiders - Social Engineering - The Art of Manipulation - Types of Social Engineering-Attacks - Social-Engineering Countermeasures	9
II	**Gathering Network and Host Information** : Scanning and Enumeration : Scanning - The CEH Scanning Methodology - Ping Sweep Techniques - Nmap Command Switches - Scan Types - TCP Communication Flag Types - War-Dialing Techniques - Banner Grabbing and OS Fingerprinting Techniques - Scanning Anonymously. Enumeration : Null Sessions - SNMP Enumeration - **System Hacking: Password Cracking, Escalating Privileges, and Hiding Files** - The Simplest Way to Get a Password - Types of Passwords - Passive Online Attacks - Active Online Attacks - Offline Attacks - Non-electronic Attacks - Cracking a Password - Understanding the LAN Manager Hash - Redirecting the SMB Logon to the Attacker - SMB Relay MITM Attacks and Countermeasures - Password-Cracking Countermeasures - Understanding Key-loggers and Other Spyware Technologies - Escalating Privileges - Executing Applications - Buffer Overflows . Understanding Rootkits: Planting Rootkits on Windows 2000 and XP Machines - Rootkit Countermeasures. Hiding Files: NTFS File Streaming - NTFS Stream Countermeasures -	9

	Understanding Steganography Technologies - Covering Your Tracks and Erasing Evidence.	
III	**Trojans, Backdoors, Viruses, and Worms:** Trojans and Backdoors - Overt and Covert Channels - Types of Trojans - Trojan Construction Kit and Trojan Makers - Trojan Countermeasures - Viruses and Worms - Types of Viruses - Virus Detection Methods. **Gathering Data from Networks -** Understanding Host-to-Host Communication - How a Sniffer Works - Sniffing Countermeasures - Bypassing the Limitations of Switches - How ARP Works - ARP Spoofing and Poisoning Countermeasures - Wire shark Filters - Understanding MAC Flooding and DNS Spoofing. **Denial of Service and Session Hijacking**: .Denial of Service : How DDoS Attacks Work - How BOTs/BOTNETs Work - Smurf and SYN Flood Attacks – DoS/DDoS Countermeasures - Session Hijacking - Sequence Prediction - Dangers Posed by Session Hijacking - Preventing Session Hijacking	**9**
IV	**Website hacking:** How Web Servers Work - Types of Web Server Vulnerabilities. **Attacking Applications: SQL Injection and Buffer Overflows.** SQL Injection - Finding a SQL Injection Vulnerability - The Purpose of SQL Injection - SQL Injection Countermeasures - BufferOverflows - Types of Buffer Overflows and Methods of Detection - Buffer Overflow Countermeasures.	**9**
V	**Wireless Network Hacking**: Wi-Fi and Ethernet - Authentication and Cracking Techniques - MAC Filters and MAC Spoofing - Rogue Access Points - Evil Twin or AP Masquerading - Wireless Hacking Techniques - Securing Wireless Networks. **Physical Site Security, Bypassing Network Security & Ethics of Ethical Hacking: -** Components of Physical Security - Understanding Physical Security - Physical Site Security Countermeasures - What to Do after a Security Breach Occurs - Bypassing Network Security: Evading IDSs, Honeypots, and Firewalls	**9**

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1 : Interpret the fundamentals of Ethical Hacking
CO2 : Illustrate the concept of Reconnaissance, Footprinting, Scanning and Enumeration
CO3 : Experiment with System Hacking techniques and Malware Attacks
CO4 : Analyze the Concepts of attacks such as Sniffing, Denial of Service, Session Hijacking, SQL Injection and Buffer Overflows
CO5 : Analyze the importance of following Ethics of Ethical Hacking.

Text Book

1. Kimberly Graves ,Sybex(2010),CEH - Certified Ethical Hacker STUDY GUIDE,Wiley Publishing Incorp

Reference Books

1. Sean-Philip Oriyano ,Sybex(2016) ,CEH V9 - Certified Ethical Hacker STUDY GUIDE (version 9),Wiley Publishing Incorp

2. Patrick Engebretson (2011), The Basics of Hacking and Penetration Testing (Second Edition), Syngress/Elsevier.

Mapping of Cos with POs and PSOs for B. Tech

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6
CO1	3	2	2	3	2	2	3	2	2	3	2	2	2	2	3	1	2	2
CO2	3	3	3	2	3	2	3	3	3	2	3	2	2	2	2	1	1	3
CO3	3	3	2	3	2	2	3	3	2	3	2	2	3	3	2	3	3	2
CO4	3	2	2	3	1	2	3	2	2	3	1	2	3	3	2	1	1	3
CO5	3	2	2	2	1	2	3	2	2	2	1	2	3	3	3	1	2	1

3 – High, 2 – Average, 1 - low, 0 - null

Discipline Specific Elective - VII

Programme	**B.Tech CSE Cyber Security**	**Programme Code**	**BTCY**		
Course Code	**25BTCY371**	**Number of Hours/Week**	**3**		
Semester	**VII**	**Max. Marks**	**100**		
Year	**IV**	**Credits**	**3**		
Course Title	**SECURITY INFORMATION AND EVENT MANAGEMENT**		**L**	**T**	**P**
			3	**0**	**2**

L-Lecture Hours T-Tutorial Hours P-Practical Hours

COURSE OBJECTIVES

The course aims to:

- Introduce the concepts, components, and importance of Security Information and Event Management (SIEM).
- Familiarize students with SIEM architectures, log collection methods, and normalization standards.
- Teach event correlation techniques and alert creation to detect security incidents.
- Develop skills in incident response, forensic investigation, and integration with SOAR tools.
- Enable compliance reporting, SIEM optimization, and understanding of modern and emerging SIEM tools

UNIT	TOPICS	HOURS
I	**Introduction to SIEM and Security Monitoring** Overview of Information Security and the role of SIEM - History and evolution: SIM, SEM, SIEM - Key SIEM functionalities: log management, event correlation, real-time monitoring - Components of a SIEM architecture - SIEM use cases: compliance, threat detection, investigation	9
II	**SIEM Architecture and Data Collection** SIEM deployment models: on-premise vs cloud vs hybrid - Log sources: servers, endpoints, network devices, applications, cloud services - Log collection methods: agents, agentless, syslog, API-based - Data parsing and normalization - Security log standards (CEF, LEEF, JSON, Syslog)	9
III	**Event Correlation and Alerting** Correlation engine: rule-based and behavior-based detection - Building correlation rules - Creating alerts for threats: brute force, privilege abuse, malware, lateral movement - Tuning alerts and minimizing false positives - Threat intelligence integration	9
IV	**Incident Response and Forensics** Role of SIEM in incident response lifecycle - Log analysis for investigation - Real-time and historical data search - Case management and evidence collection - Integration with SOAR and forensic tools	9
V	**Compliance, Reporting, and Future Trends** Regulatory compliance: PCI-DSS, HIPAA, GDPR, ISO 27001 - Generating reports and dashboards - SIEM best practices for maintenance and optimization - Overview of modern tools: Splunk, IBM QRadar, Elastic, Azure Sentinel - Emerging trends: XDR, AI in SIEM, Cloud-native SIEM	9

45 Hours

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

- Understand what SIEM is and its importance
- Configure log collection and parsing
- Detect security events using SIEM tools
- Document incidents and findings effectively
- Generate audit-ready reports

Text Books:

The Essential Guide to Security Information and Event Management (SIEM)

Chuvakin, A., Schmidt, K., & Phillips, C. (2013). *Logging and log management: The authoritative guide to understanding the concepts surrounding logging and log management*. Syngress.

Reference Books:

- Beale, J., Baker, A., Esler, B., Northcutt, S., & Shackleford, D. (2007). *Snort intrusion detection and prevention toolkit*. Syngress.

- Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response (NIST SP 800-86)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-86

- Stallings, W. (2018). *Computer security: Principles and practice* (4th ed.). Pearson Education.

- Sanders, C. (2010). *Practical packet analysis: Using Wireshark to solve real-world network problems* (2nd ed.). No Starch Press.

- Scarfone, K., & Mell, P. (2007). *Guide to intrusion detection and prevention systems (IDPS)* (NIST SP 800-94). National Institute of Standards and Technology.

CO-PO-PSO MAPPING

B.Tech

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO 11	PO 12	PS O1	PS O2	PS O3
CO1	3	1	2	3	2	3	2	3	1	3	2	1	3	2	3
CO2	2	3	1	2	3	2	3	1	3	2	3	2	1	3	2
CO3	1	2	3	2	1	3	2	3	2	3	1	3	2	3	1
CO4	3	2	1	3	2	1	3	2	3	1	2	3	3	1	2
CO5	2	3	2	1	3	2	1	3	2	3	2	1	3	2	3

3 – high, 2 – Average, 1 - low , 0-null

Programme	B.Tech CSE Cyber Security	Programme Code	BTCY		
Course Code	25BTCY372	Number of Hours/Week	3		
Semester	VII	Max. Marks	100		
Year	IV	Credits	3		
Course Title	SECURE SOFTWARE DEVELOPMENT		L	T	P
			3	0	0

L-Lecture Hours T-Tutorial Hours P-Practical Hours

COURSE OBJECTIVES

The course aims to:

- Introduce the principles of secure software development and common software vulnerabilities.
- Emphasize the importance of secure design, threat modeling, and architectural best practices.
- Enable the application of secure coding standards across various programming languages.
- Familiarize students with security testing tools, code reviews, and vulnerability detection techniques.
- Explore secure deployment strategies and DevSecOps for maintaining software integrity throughout its lifecycle.

UNIT	TOPICS	HOURS
I	**Foundations of Secure Software Development** Introduction to software security - Common software vulnerabilities (OWASP Top 10) - Secure development lifecycle (SDL/SSDLC) - CIA triad (Confidentiality, Integrity, Availability) - Security policies and principles (least privilege, defense in depth)	9
II	**Secure Design Principles** Threat modeling and risk assessment - Secure design principles (e.g., fail-safe defaults, secure by design) - Design patterns for security - STRIDE model and attack surface analysis - Security architecture for web and mobile applications	9
III	**Secure Coding Practices** Input validation and output encoding - Authentication and authorization best practices - Secure session management -Error handling and logging - Language-specific secure coding (C/C++, Java, Python, etc.)	9
IV	**Secure Testing and Code Review** Static and dynamic code analysis - Secure unit and integration testing -Fuzz testing and penetration testing - Vulnerability scanning tools (SonarQube, Snyk, etc.) - Secure code review checklist	9
V	**Secure Deployment and Maintenance** Secure DevOps (DevSecOps) practices - Patch management and update mechanisms - Secure configuration and containerization - Application logging and monitoring - Incident response and secure retirement of software	9

45 Hours

COURSE OUTCOMES:

On successful completion of this course, the student will be able to
CO1: Understand the core concepts of software security
CO2: Apply threat modeling in early SDLC stages
CO3: Implement secure authentication and access control
CO4: Use tools to detect and fix vulnerabilities
CO5: Deploy and maintain software with ongoing security

Text Books:

Viega, J., & McGraw, G. (2001). *Building secure software: How to avoid security problems the right way*. Addison-Wesley.

Reference Books:

- Howard, M., & LeBlanc, D. (2002). *Writing secure code* (2nd ed.). Microsoft Press.

- Chess, B., & West, J. (2007). *Secure programming with static analysis*. Addison-Wesley Professional.

- OWASP Foundation. (2021). *OWASP Top 10 – 2021: The ten most critical web application security risks*. https://owasp.org/Top10/

- Wheeler, D. A. (2011). *Secure programming for Linux and Unix HOWTO*. Linux Documentation Project.

- Rouse, M., & Barrett, B. (2018). *DevSecOps: Integrating security into DevOps*. TechTarget. *(Available online or in DevSecOps practice guides)*

CO-PO-PSO MAPPING

B.Tech

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO 11	PO 12	PS O1	PS O2	PS O3
CO1	3	1	2	3	2	3	2	3	1	3	2	1	3	2	3
CO2	2	3	1	2	3	2	3	1	3	2	3	2	1	3	2
CO3	1	2	3	2	1	3	2	3	2	3	1	3	2	3	1
CO4	3	2	1	3	2	1	3	2	3	1	2	3	3	1	2
CO5	2	3	2	1	3	2	1	3	2	3	2	1	3	2	3

3 – high, 2 – Average, 1 - low , 0-null

Programme	B. Tech CSE Cyber Security	Programme Code	BTCY
Course Code	25BTCY373	Number of Hours/Week	3
Semester	VII	Max. Marks	100
Year	IV	Credits	3

Course

Course Title	NATURE INSPIRED COMPUTING	L	T	P
		3	0	0

COURSE OBJECTIVES:

The main learning objective of this course is to prepare the students for:

- Understand the Fundamentals of Bio-Inspired Computing.
- Learn Evolutionary Models, Optimization Techniques and Explore Genetic Algorithms.
- Investigate the biological basis of ant colonies and how this inspires optimization algorithms.
- Explore variable-length PSO and its applications in optimization problems.
- Application-Oriented Learning and Explore Advanced Nature-Inspired Algorithms .

UNIT	TOPICS	HOURS
I	**INTRODUCTION:** From Nature-to-Nature Computing, – Fundamentals of bio-inspired models and bio-inspired computing. Evolutionary models and techniques- Optimisation Problems- Single and multi-objective optimisation, heuristic, meta-heuristic and hyper heuristic functions.	8
II	**Genetic Algorithms:** Genetic algorithms: Mathematical foundation, Genetic problem solving, crossover and mutation. Genetic algorithms and Markov process, applications of genetic algorithms.	8
III	**Optimization Algorithms:** Ant Colonies, hybrid ant system, Ant Foraging Behavior, Ant Colony Optimization, SACO and scope of ACO algorithms, Ant Colony Algorithm (ACA), Variations of ACO.	8
IV	**Swarm Algorithms:** Particle Swarm algorithms - particles moves, particle swarm optimization, variable length PSO, applications of PSO. Artificial Bee Colony algorithms - ABC basics, ABC in optimization, multi-dimensional bee colony algorithms, applications of bee algorithms.	8
V	**Applications:** Selected nature inspired techniques - Bat algorithm- Cuckoo search algorithm. Deep Learning-Pattern recognition -Cybersecurity and its applications -Complex Network.	8

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1 : Apply nature-inspired computational techniques to solve real-world optimization and problem-solving tasks.

CO2 : Demonstrate the ability to Implement Genetic Algorithms for Optimization and apply them to practical scenarios.

CO3 : Utilize Ant Colony Optimization Techniques and evaluate the effectiveness of ACO algorithms in comparison to other optimization techniques.

CO4 : Apply Swarm Intelligence Algorithms and analyse their applicability in real-world optimization problems.

CO5 : Encourage creative and innovative problem-solving approaches by applying nature-inspired algorithms in emerging fields such as artificial intelligence, machine learning, and data science.

Text Book:

1. Fundamentals of Natural Computing: Basic Concepts, Algorithms, and applications, L. N. de Castro (2006).

2. Leandro Nunes de Castro, “Fundamentals of Natural Computing, Basic Concepts, Algorithms and Applications", Chapman & Hall/ CRC, Taylor and Francis Group, 2007

3. Evolutionary Optimization Algorithms, D. Simon (2013), Wiley

Reference Books:

1. Floreano D. and Mattiussi C., "Bio-Inspired Artificial Intelligence: Theories, Methods, and Technologies", MIT Press, Cambridge, MA, 2008.

2. Albert Y.Zomaya, "Handbook of Nature-Inspired and Innovative Computing", Springer, 2006.

3. Marco Dorrigo, Thomas Stutzle,” Ant Colony Optimization”, PHI, 2005.

CO-PO-PSO Mapping Table :(B. Tech)

CO/PO /PSO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO3
CO1	3	2	1	2	1	2	1	2	1	2	1	2	3	2	2
CO2	3	3	3	3	3	2	1	2	1	3	2	3	3	2	2
CO3	2	3	3	3	2	2	1	3	2	3	2	2	3	2	2
CO4	3	2	3	2	3	3	1	2	2	3	2	3	3	2	3
C05	3	3	3	3	3	3	2	2	3	3	2	3	3	3	3

Discipline Specific Elective - VIII

Programme	**B.Tech CSE Cyber Security**	**Programme Code**	**BTCY**		
Course Code	**25BTCY374**	**Number of Hours/Week**	**3**		
Semester	**VII**	**Max. Marks**	**100**		
Year	**IV**	**Credits**	**3**		
Course Title	**MACHINE LEARNING FOR CYBER SECURITY**		**L**	**T**	**P**
			3	**0**	**0**

L-Lecture Hours T-Tutorial Hours P-Practical Hours

COURSE OBJECTIVES

The course aims to:

1. Introduce the fundamental concepts of machine learning (ML) and their applications in cybersecurity.
2. Develop the ability to preprocess and engineer features from cybersecurity datasets.
3. Apply classification, clustering, and ensemble ML techniques for detecting security threats.
4. Explore deep learning techniques, including CNNs and RNNs, for advanced threat detection.
5. Understand and address adversarial ML threats, explainability, and ethical issues in cybersecurity ML deployments.

UNIT	TOPICS	HOURS
I	**Introduction to Cybersecurity and Machine Learning** Overview of cybersecurity landscape - Introduction to machine learning (ML): supervised, unsupervised, reinforcement learning - Data types in cybersecurity (logs, flows, binaries) - Challenges in applying ML to cybersecurity - Python and scikit-learn setup for ML	9
II	**Data Preprocessing and Feature Engineering for Cybersecurity** Data sources: IDS logs, network traffic, malware datasets - Cleaning and transforming security data - Feature extraction and selection techniques - Handling imbalanced datasets (e.g., SMOTE) - Exploratory Data Analysis (EDA)	9
III	**ML Models for Cyber Threat Detection** Classification algorithms (SVM, Decision Trees, Random Forests, k-NN, Naive Bayes) - Clustering (K-means, DBSCAN) - Ensemble methods (Bagging, Boosting) - Evaluation metrics: Accuracy, Precision, Recall, F1, ROC-AUC - Hands-on: Detecting intrusions using KDD Cup 99 or UNSW-NB15 datasets	9
IV	**Deep Learning and Advanced Models for Cybersecurity** Neural Networks, CNNs, RNNs/LSTMs - Autoencoders for anomaly detection - Transfer learning and pre-trained models - Natural Language Processing (NLP) for phishing/email analysis - Frameworks: TensorFlow, Keras, PyTorch	9
V	**Adversarial ML, Explainability & Real-world Use Cases** Adversarial attacks and model robustness - Explainable AI (XAI) in cybersecurity - Case studies: SIEM integration, malware detection, phishing defense - Deployment of ML models in cybersecurity pipelines - Ethical and legal aspects of AI in security	9

45 Hours

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1: Understand ML fundamentals and their relevance to cybersecurity
CO2: Build cybersecurity datasets for ML models
CO3: Apply clustering to detect anomalies
CO4: Implement deep learning for malware and intrusion detection
CO5: Apply ML in real-world cyber defense scenarios

Text Books:

Kwon, D. (2019). *Machine learning for cybersecurity cookbook: Over 80 recipes to secure, detect, and investigate using machine learning*. Packt Publishing.

Reference Books:

- Dua, S., & Du, X. (2016). *Data mining and machine learning in cybersecurity*. CRC Press.

- Mohri, M., Rostamizadeh, A., & Talwalkar, A. (2018). *Foundations of machine learning* (2nd ed.). MIT Press.

- Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In *IEEE Symposium on Security and Privacy*, 305–316. https://doi.org/10.1109/SP.2010.25

- Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). A survey of deep learning methods for cybersecurity. *Information*, 10(4), 122. https://doi.org/10.3390/info10040122

- Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.

CO-PO-PSO MAPPING

B.Tech

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO 11	PO 12	PS O1	PS O2	PS O3
CO1	3	1	2	3	2	3	2	3	1	3	2	1	3	2	3
CO2	2	3	1	2	3	2	3	1	3	2	3	2	1	3	2
CO3	1	2	3	2	1	3	2	3	2	3	1	3	2	3	1
CO4	3	2	1	3	2	1	3	2	3	1	2	3	3	1	2
CO5	2	3	2	1	3	2	1	3	2	3	2	1	3	2	3

3 – high, 2 – Average, 1 - low , 0-null

Programme	**B.Tech CSE Cyber Security**	**Programme Code**	**BTCY**		
Course Code	**25BTCY375**	**Number of Hours/Week**	**3**		
Semester	**VII**	**Max. Marks**	**100**		
Year	**IV**	**Credits**	**3**		
Course Title	**NATURAL LANGUAGE PROCESSING FOR SECURITY**		**L**	**T**	**P**
			3	**0**	**0**

L-Lecture Hours T-Tutorial Hours P-Practical Hours

COURSE OBJECTIVES:

- To introduce techniques and tools of NLP
- Apply them to solve security-related problems such as phishing detection, malware classification, spam analysis, and threat intelligence.

UNIT	TOPICS	HOURS
I	**Introduction to NLP and Security** Overview of NLP and cybersecurity - Text as a data source in security (emails, logs, URLs, chats) - Applications: phishing detection, spam classification, sentiment in threat reports - Basics of NLP: tokenization, stemming, lemmatization - Introduction to Python NLP tools (NLTK, spaCy)	9
II	**Feature Engineering and Representation** Bag of Words, TF-IDF, and n-grams - Word embeddings: Word2Vec, GloVe, fastText - Sentence embeddings: Sentence-BERT, Universal Sentence Encoder - Dimensionality reduction for text (PCA, t-SNE) - Handling noisy, unstructured security texts (logs, alerts)	9
III	**Text Classification for Security Threats** Classification algorithms (Naive Bayes, SVM, Logistic Regression, Random Forest) - Neural networks (RNNs, LSTMs, Transformers) - Spam and phishing detection in email and SMS - Malicious URL and domain detection using NLP - Dataset examples: Enron spam, PhishTank, URLNet	9
IV	**NLP in Threat Intelligence and Log Analysis** Named Entity Recognition (NER) for extracting IOCs (Indicators of Compromise) - Topic modeling (LDA, NMF) for security news and reports - Log parsing and anomaly detection using NLP - Chatbot logs and abuse pattern analysis - Sentiment analysis for hacker forums and dark web discussions	9
V	**Advanced Topics and Real-world Applications** Transformer-based models (BERT, RoBERTa, GPT) for security tasks - Explainable NLP models (LIME, SHAP) - Adversarial NLP attacks and robustness in security - Deploying NLP pipelines in security tools (SIEM, SOAR) - Case studies: phishing detection, fake news, hate speech, abuse detection	9

45 Hours

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1: Understand how NLP applies to security domains
CO2: Visualize and explore text datasets
CO3: Build classifiers for threat detection using textual data
CO4: Apply NLP to extract meaningful intelligence from threat reports and logs
CO5: Implement transformer models for classification and threat detection

Text Books:

Steven Bird, Ewan Klein, Edward Loper, *Natural Language Processing with Python – Analyzing Text with the Natural Language Toolkit*

Reference Books:

- Jurafsky, D., & Martin, J. H. (2021). *Speech and language processing* (3rd ed., draft). Stanford University.
(Available online: https://web.stanford.edu/~jurafsky/slp3/)

- Goldberg, Y. (2017). *Neural network methods for natural language processing*. Morgan & Claypool Publishers.

- Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., ... & Polosukhin, I. (2017). Attention is all you need. *Advances in Neural Information Processing Systems, 30,* 5998–6008.
https://papers.nips.cc/paper_files/paper/2017/hash/3f5ee243547dee91fbd053c1c4a845aa-Abstract.html

- Zhang, Y., & Wallace, B. (2017). A sensitivity analysis of (and practitioners' guide to) convolutional neural networks for sentence classification. In *Proceedings of the 8th International Joint Conference on Natural Language Processing* (pp. 253–263).
https://doi.org/10.18653/v1/I17-1042

- Chakraborty, S., Alam, M., & Bhowmick, S. (2022). *Applied natural language processing for cybersecurity*. Springer.

CO-PO-PSO MAPPING

B.Tech

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO 11	PO 12	PS O1	PS O2	PS O3
CO1	3	1	2	3	2	3	2	3	1	3	2	1	3	2	3
CO2	2	3	1	2	3	2	3	1	3	2	3	2	1	3	2
CO3	1	2	3	2	1	3	2	3	2	3	1	3	2	3	1
CO4	3	2	1	3	2	1	3	2	3	1	2	3	3	1	2
CO5	2	3	2	1	3	2	1	3	2	3	2	1	3	2	3

3 – high, 2 – Average, 1 - low , 0-null

Programme	B.Tech-CSE(Cyber Security)	Programme Code	BTCY		
Course Code	23BTCY376	Number of Hours/Week	3		
Semester	VII	Max. Marks	100		
Year	IV	Credits	3		
Course					
Course Title	CLOUD SECURITY AND GOVERNANCE		L	T	P
			3	0	0

COURSE OBJECTIVES:

- Understand the architecture, models, and benefits of cloud computing
- Learn about compliance, auditing, and risk management in cloud security
- Explore data security measures, including encryption and key management
- Gain knowledge of identity management, virtualization, and secure cloud operations.

UNIT	TOPICS	HOURS
I	**Cloud Computing Architecture and Security Framework** Cloud Computing Architectural Framework: Cloud Benefits, Business scenarios, Cloud Computing Evolution, cloud vocabulary, Essential Characteristics of Cloud Computing, Cloud deployment models, Cloud Service Models, Multi- Tenancy, Approaches to create a barrier between the Tenants, cloud computing vendors, Cloud Computing threats, Cloud Reference Model, The Cloud Cube Model, Security for Cloud Computing, How Security Gets Integrated.	9
II	**Cloud Computing: Compliance, Audit, Portability, and Interoperability** Compliance and Audit: Cloud customer responsibilities, Compliance and Audit Security Recommendations. Portability and Interoperability: Changing providers reasons, Changing providers expectations, Recommendations all cloud solutions, IaaS Cloud Solutions, PaaS Cloud Solutions, SaaS Cloud Solutions.	9
III	**Cloud Security and Risk Management** Traditional Security, Business Continuity, Disaster Recovery, Risk of insider abuse, Security baseline, Customers actions, Contract, Documentation, Recovery Time Objectives (RTOs), Customers responsibility, Vendor Security Process (VSP).	9
IV	**Cloud Computing Security:** Data Center Operations, Security challenge, Implement Five Principal Characteristics of Cloud Computing, Data center Security Recommendations. Encryption and Key Management: Encryption for Confidentiality and Integrity, Encrypting data at rest, Key Management Lifecycle, Cloud Encryption Standards, Recommendations.	9
V	**Cloud Security Framework** Identity and Access Management in the cloud, Identity and Access Management functions, Identity and Access Management (IAM) Model, Identity Federation, Identity Provisioning Recommendations, Authentication for SaaS and Paas customers, Authentication for IaaS customers, Introducing Identity Services, Enterprise Architecture with IDaaS, IDaaS Security Recommendations. Virtualization: Hardware Virtualization, Software Virtualization,	9

	Memory Virtualization, Storage Virtualization, Data Virtualization, Network Virtualization, Virtualization Security Recommendations.	

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1: Understand the fundamental architecture of cloud computing, including cloud deployment models, service models, and essential characteristics

CO2 : Analyze cloud security challenges and integrate security measures into the cloud computing framework

CO3: Examine the importance of compliance, audit, portability, and interoperability in cloud environments.

CO4: Explore risk management practices, business continuity, and disaster recovery strategies within cloud computing.

CO5: Learn encryption techniques, key management lifecycle, and security standards to ensure data confidentiality and integrity in the cloud.

Text Book

1. Dhillon, V., Metcalf, D., and Hooper, M, Blockchain enabled applications, 2017, 1st Proceedings of the 65th Academic Council (17.03.2022) 1042 Edition, CA: Apress, Berkeley.

2. Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions" by Joseph J. Bambara, Paul R. Allen, Kedar Iyer, Rene Madsen, Solomon Lederer, and Michael Wuehler

3. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder, Agenda Item 65/39 - Annexure - 35 Proceedings of the 65th Academic Council (17.03.2022) 1047 Bitcoin and cryptocurrency technologies: a comprehensive introduction, 2016, Princeton University Press

Reference Books

1. Diedrich, H., “Ethereum: Blockchains, digital assets, smart contracts, decentralized autonomous organizations”, 2016, 1st Edition, Wildfire publishing, Sydney

2. Cryptography and Network Security: Principles and Practices, William Stallings, 7th edition, 2017

3. Bashir, I., "Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained", 2nd Edition, Packt Publishing Ltd, March 30, 2018.

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	2	2	2	3	2	2	2	1	2	2	3	3	2	2
CO2	3	3	2	3	3	2	2	2	2	2	3	3	3	3	2
CO3	3	3	3	3	3	3	2	2	2	2	3	3	3	3	3
CO4	3	2	3	3	3	3	3	2	3	3	3	3	3	3	3
C05	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3

Mapping of Course Outcomes (COs) with PSOs

3 – high, 2 – Average, 1 - low , 0-null

Programme	**B.Tech CSE Cyber Security**	**Programme Code**	**BTCY**		
Course Code	**25BTCY471**	**Number of Hours/Week**	**3**		
Semester	**VIII**	**Max. Marks**	**100**		
Year	**IV**	**Credits**	**02**		
Course Title	**INDUSTRIAL INTERNSHIP**		**L**	**T**	**P**
			0	**0**	**30**

L-Lecture Hours T-Tutorial Hours P-Practical Hours

COURSE OBJECTIVES:

- Provide real-world exposure to cybersecurity practices, tools, and environments.
- Bridge the gap between academic knowledge and industry application.
- Build practical skills in areas such as network security, ethical hacking, cloud security, secure coding, and risk management.
- Encourage professional behavior, communication, and teamwork in cybersecurity projects.

	TOPICS	
	Internship Duration and Credit • **Duration**: Minimum **4 to 6 weeks** (Full-time) or equivalent part-time. • **Credits**: 02 • **Time Frame**: Ideally between the **6th and 7th semesters** or during summer break.	
	Roles and Responsibilities *Student* • Approach companies and secure internship offers (with coordinator guidance). • Maintain professionalism, punctuality, and confidentiality. • Submit reports, logbooks, and final presentation on time. *Faculty / Internship Coordinator* • Guide students on choosing companies and areas. • Review weekly progress and provide feedback. • Evaluate and grade the internship. *Industry Mentor* • Assign relevant tasks and provide regular feedback. • Evaluate student's performance and confirm completion.	
	Required Submissions Students must prepare the following:	

	1. **Internship Offer Letter** (before starting). 2. **Weekly Logbook / Timesheet** – signed by the industry mentor. 3. **Final Internship Report** (20–30 pages) – should include: o Company profile o Internship objectives o Tools & technologies used o Tasks performed o Outcomes/learning o Screenshots (if permitted) o Reflections & challenges 4. **Presentation / Viva Voce** – at the end of the internship.	
	Evaluation Criteria **Component** **Marks** Report quality 30% Technical contribution 30% Presentation/Viva 20% Logbook & discipline 10% Industry feedback 10% **Total** 100%	

45 Hours

COURSE OUTCOMES:

On successful completion of this course, the student will be able to
CO1: Apply theoretical cybersecurity knowledge to solve real-world industrial problems.
CO2: Demonstrate proficiency in using professional tools and technologies relevant to cybersecurity practices (e.g., SIEM, IDS/IPS, firewalls, vulnerability scanners).
CO3: Work effectively in a team environment, adhering to professional and ethical standards in the workplace.
CO4: Analyze security requirements and implement appropriate technical solutions in domains such as network security, application security, or incident response.
CO5: Document the internship experience, reflect on learning outcomes, and communicate findings effectively through technical reports and presentations.

CO-PO-PSO MAPPING
B.Tech

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO 11	PO 12	PS O1	PS O2	PS O3
CO1	3	1	2	3	2	3	2	3	1	3	2	1	3	2	3
CO2	2	3	1	2	3	2	3	1	3	2	3	2	1	3	2
CO3	1	2	3	2	1	3	2	3	2	3	1	3	2	3	1
CO4	3	2	1	3	2	1	3	2	3	1	2	3	3	1	2
CO5	2	3	2	1	3	2	1	3	2	3	2	1	3	2	3

3 – high, 2 – Average, 1 - low , 0-null

Open Electives

Programme	B.Tech CSE Cyber Security	Programme Code	BTCY		
Course Code	25BTCY871	Number of Hours/Week	3		
Semester	VIII	Max. Marks	100		
Year	IV	Credits	3		
Course Title	ADVANCED PYTHON PROGRAMMING		L	T	P
			3	0	0

L-Lecture Hours T-Tutorial Hours P-Practical Hours

Course Objectives

- To enhance Python programming skills with practical, high-level applications.
- To enable students from non-CSE domains to automate workflows, analyze data, and interact with APIs.
- To introduce libraries and tools relevant to scientific computing, business, engineering, and research.
- To provide hands-on experience with real-world problems in their respective domains.

UNIT	TOPICS	HOURS
I	**Advanced Python Concepts** Review of Python basics (functions, loops, lists, dictionaries) - Object-Oriented Programming (OOP): Classes, Objects, Inheritance - Error Handling and Exceptions - File I/O operations and automation (batch renaming, backups) - Introduction to decorators, generators, and comprehensions	9
II	**Working with Data and Files** Reading and writing CSV, Excel, JSON files - Using libraries: `pandas`, `openpyxl`, `csv`, `json` - Data cleaning and transformation techniques - Regular expressions for text/data extraction - Example: Automate report generation from Excel files	9
III	**Visualization and Scientific Computing** Plotting using `matplotlib` and `seaborn` - Numpy arrays and mathematical operations - Simple simulations and computations (e.g., finance, biology, physics) - Domain projects: Civil: Plot rainfall over time - Bio: Analyze gene expression data - MBA: Sales trend visualization	9
IV	**Web, APIs and Automation** Web scraping using `requests` and `BeautifulSoup` - Consuming REST APIs (OpenWeatherMap, Financial APIs) - Automation using `selenium` (e.g., filling forms, sending emails) - Real-time data integration - Mini-project: Weather notifier, live stock dashboard, attendance auto-filler	9
V	**Intro to AI/ML & Domain Applications** Basics of `scikit-learn`: Data splitting, training, prediction - Linear regression, classification (e.g., predict student performance) - Using `Streamlit` for building simple data apps - Application case studies: Medical: Predict disease probability - Business: Customer churn analysis - Mechanical: Fault prediction from sensor data	9

45 Hours

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1: Apply object-oriented and modular programming techniques in Python.
CO2: Automate routine tasks using file handling and libraries like `os`, `shutil`, and `datetime`.
CO3: Use Python libraries for data analysis, visualization, and basic ML.
CO4: Interface with APIs and process real-time data (e.g., weather, finance, IoT).
CO5: Build small domain-specific applications using Python.

Text Books:

Charles Severance, *Python for Everybody*

Al Sweigart, *Automate the Boring Stuff with Python*

Reference Books:

Jake Vander, Plas *Python Data Science Handbook*

- https://www.py4e.com/book
- https://automatetheboringstuff.com

CO-PO-PSO MAPPING

B.Tech

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO 11	PO 12	PS O1	PS O2	PS O3
CO1	3	1	2	3	2	3	2	3	1	3	2	1	3	2	3
CO2	2	3	1	2	3	2	3	1	3	2	3	2	1	3	2
CO3	1	2	3	2	1	3	2	3	2	3	1	3	2	3	1
CO4	3	2	1	3	2	1	3	2	3	1	2	3	3	1	2
CO5	2	3	2	1	3	2	1	3	2	3	2	1	3	2	3

3 – high, 2 – Average, 1 - low , 0-null

Programme	**B.Tech CSE Cyber Security**	**Programme Code**	**BTCY**		
Course Code	**25BTCY372**	**Number of Hours/Week**	**3**		
Semester	**VII**	**Max. Marks**	**100**		
Year	**IV**	**Credits**	**3**		
Course Title	**OPTIMISATION ALGORITHMS**		**L**	**T**	**P**
			3	**0**	**2**

L-Lecture Hours T-Tutorial Hours P-Practical Hours

COURSE OBJECTIVES:

- To introduce fundamental concepts of optimization and its relevance across disciplines.
- To equip students with problem-solving techniques involving linear, nonlinear, and discrete optimization.
- To expose students to metaheuristic algorithms like Genetic Algorithm and Particle Swarm Optimization.
- To enable application of optimization in engineering, business, and science problems.
- To foster critical thinking and model formulation in decision-making scenarios.

UNIT	TOPICS	HOURS
I	**Introduction to Optimization** Definition and importance of optimization - Types of optimization problems: linear, nonlinear, integer, combinatorial - Optimization in real life: engineering design, scheduling, economics, business, biology - Introduction to modeling with objective function and constraints - Feasible and optimal solutions	9
II	**Linear Programming and Applications** Formulating linear programming (LP) problems - Graphical solution method - Simplex method (conceptual overview) - Applications: resource allocation, blending, transportation - Use of Excel Solver / online solvers for LP	9
III	**Nonlinear and Constrained Optimization** Concept of convex and non-convex functions - Unconstrained vs constrained optimization - Lagrange multipliers (intuitive understanding) - One-variable optimization (Golden section search, Fibonacci method) - Applications: process optimization, engineering design	9
IV	**Metaheuristic and Evolutionary Algorithms** Need for metaheuristics in complex problems - Genetic Algorithm (GA): representation, selection, crossover, mutation - Particle Swarm Optimization (PSO): swarm behavior, velocity updates - Case studies: optimal routing, load balancing, parameter tuning - Introduction to simulation-based optimization	9
V	**Domain Applications and Tools** Optimization in: Engineering (design, energy systems, structural optimization) - Management (inventory, portfolio, marketing optimization) - Life sciences (drug formulation, resource planning) - Introduction to tools: Excel Solver, MATLAB, SciPy (`optimize`), PyGAD - Mini-project discussion: Optimization of a simple real-world process or decision	9

45 Hours

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1: Formulate real-world problems into mathematical optimization models.

CO2: Solve basic linear and nonlinear optimization problems using standard techniques.

CO3: Understand and apply metaheuristic algorithms such as Genetic Algorithm and PSO.

CO4: Use tools (Excel Solver / MATLAB / Python) for solving optimization problems.

CO5: Apply optimization in their respective domains effectively (e.g., scheduling, design, logistics)

Text Books:

Taha H.A., ***Introduction to Operations Research***

S.S. Rao, ***Engineering Optimization: Theory and Practice***

Reference Books:

Practical Optimization with Python **(Free resource)**

CO-PO-PSO MAPPING

B.Tech

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO 11	PO 12	PS O1	PS O2	PS O3
CO1	3	1	2	3	2	3	2	3	1	3	2	1	3	2	3
CO2	2	3	1	2	3	2	3	1	3	2	3	2	1	3	2
CO3	1	2	3	2	1	3	2	3	2	3	1	3	2	3	1
CO4	3	2	1	3	2	1	3	2	3	1	2	3	3	1	2
CO5	2	3	2	1	3	2	1	3	2	3	2	1	3	2	3

3 – high, 2 – Average, 1 - low , 0-null

Programme	**B.Tech CSE Cyber Security**	**Programme Code**	**BTCY**		
Course Code	**25BTCY873**	**Number of Hours/Week**	**3**		
Semester	**VII**	**Max. Marks**	**100**		
Year	**IV**	**Credits**	**3**		
Course Title	**COMPUTING LATEST**		**L**	**T**	**P**
			3	**0**	**0**

L-Lecture Hours T-Tutorial Hours P-Practical Hours

COURSE OBJECTIVES:

- To introduce foundational computing concepts to non-CS students.
- To provide digital skills and awareness of computing trends across domains.
- To develop familiarity with software tools, basic programming logic, and internet technologies.
- To discuss the societal impact, security, and ethics in computing.
- To enable students to apply computing knowledge in their academic and professional fields.

UNIT	TOPICS	HOURS
I	**Introduction to Computing & Digital Devices (7 Hours)** Basics of computers: hardware, software, I/O devices - Types of computers: desktops, laptops, tablets, embedded systems - Number systems and data representation (binary, ASCII) - Operating systems overview: Windows, Linux, Android - Role of computing in non-IT domains: engineering, biology, commerce, arts	9
II	**Office Productivity Tools & Cloud Computing** MS Word: formatting, citations, templates - MS Excel: formulas, charts, sorting, data analysis - MS PowerPoint: smart presentations - Google Workspace / Microsoft 365 tools - Basics of cloud computing: Google Drive, OneDrive, AWS overview	9
III	**Internet Technologies & Digital Communication** Understanding the Internet, WWW, URLs, ISPs - Search engines, Boolean search, plagiarism tools - Email etiquette, Zoom/Meet, collaboration platforms - Cyber hygiene: privacy, cookies, phishing, password management - Introduction to cybersecurity and digital footprint	9
IV	**Introduction to Logic, Programming & Algorithms** What is a program? What is an algorithm? - Flowcharts and pseudocode - Basic logic building: variables, conditions, loops - Introduction to Scratch / Python (no coding background required) - Applications: automate tasks, small scripts, form validation	9
V	**Emerging Technologies in Computing** Overview of AI, Machine Learning, and their non-CS applications - Basics of the Internet of Things (IoT): smart devices and automation - Cloud computing & virtualization (AWS, Azure basics) - Blockchain, Digital currency, and Web 3.0 - Green computing and ethical issues in technology	9

45 Hours

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1: Understand core computing concepts and IT terminology.

CO2: Use office productivity tools and cloud services effectively.

CO3: Understand the basics of data processing, logic, and programming.

CO4: Appreciate the relevance of AI, IoT, and cloud computing in their domains.

CO5: Demonstrate safe and ethical use of digital technologies.

Text Books:

Faithe Wempen, *Computing Fundamentals*

***Introduction to Computer Science,* ITL Education Solutions**

Reference Books:

- **Google Digital Garage**: https://learndigital.withgoogle.com
- **CS50's Introduction to Computer Science** (Harvard – simplified): https://cs50.harvard.edu
- **NPTEL Course**: Basics of Computing & Internet

CO-PO-PSO MAPPING

B.Tech

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO 11	PO 12	PS O1	PS O2	PS O3
CO1	3	1	2	3	2	3	2	3	1	3	2	1	3	2	3
CO2	2	3	1	2	3	2	3	1	3	2	3	2	1	3	2
CO3	1	2	3	2	1	3	2	3	2	3	1	3	2	3	1
CO4	3	2	1	3	2	1	3	2	3	1	2	3	3	1	2
CO5	2	3	2	1	3	2	1	3	2	3	2	1	3	2	3

3 – high, 2 – Average, 1 - low , 0-null

Programme	B.Tech CSE Cyber Security	Programme Code	BTCY		
Course Code	25BTCY271	Number of Hours/Week	2		
Semester	VII	Max. Marks	100		
Year	IV	Credits	1		
Course Title	HIGH PERFORMANCE COMPUTING LAB		L	T	P
			0	0	2

Course Objectives:

- To provide an understanding of the fundamental concepts of parallel programming and computing architectures.
- To explore the principles and techniques of high-performance computing and cluster architectures.
- To enable students to work with high-speed networks and efficient resource management systems in cluster environments.
- To introduce CUDA programming for parallel processing and develop skills in shared memory and multi-GPU programming.
- To familiarize students with parallel programming tools like OpenMP for efficient parallel execution.

List of Experiments:

1. Implementation of matrix vector multiplication using OPENMP.
2. Development of parallel matrix addition using MPI.
3. Configuration of cluster setup and testing communication.
4. Implementation of fault detection using heartbeat mechanisms and develop failover and recovery strategies in a cluster.
5. Simulation of resource management in cluster environments.
6. Development of CUDA program for vector addition.
7. Development of CUDA program with shared memory.
8. Implementation of load balancing algorithms.
9. Parallelization of numerical integration using OPENMP.
10. Implementation and testing of different network topologies.

Course Outcomes:

By learning High Performance Computing, students will be able to

CO1: Demonstrate knowledge of parallel computing, architectures, and processing techniques like SIMD and pipelined processors.

CO2: Analyze the architecture and components of scalable parallel and cluster computing systems.

CO3: Implement resource management, job scheduling, and fault-tolerant mechanisms in high-speed cluster networks.

CO4: Develop CUDA-based parallel programs utilizing shared memory, thread cooperation, and multi-GPU support.

CO5: Apply OpenMP and other parallel programming models to create efficient and scalable solutions for computational problems.

CO-PO-PSO MAPPING

B.Tech

Mapping of Course Outcomes (COs) with PSOs

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO 11	PO 12	PS O1	PS O2	PS O3
CO1	3	1	2	3	2	3	2	3	1	3	2	1	3	2	3
CO2	2	3	1	2	3	2	3	1	3	2	3	2	1	3	2
CO3	1	2	3	2	1	3	2	3	2	3	1	3	2	3	1
CO4	3	2	1	3	2	1	3	2	3	1	2	3	3	1	2
CO5	2	3	2	1	3	2	1	3	2	3	2	1	3	2	3

3 – high, 2 – Average, 1 - low , 0-null

Programme	BTech. CSE Cybersecurity	Programme Code	BTCY		
Course Code	24BTCY243	Number of Hours/WK	2		
Semester	IV	Max. Marks	100		
Year	II	Credits	1		
Course Title	Ethical Hacking and Penetration Testing Lab		L	T	P
			0	0	2

COURSE OBJECTIVES:

- Analyze the practical implementation of Ethical Hacking Tools
- Interpret the concept of Foot Printing and Reconnaissance
- Apply the concept of Ping, ARP, and nslookup Commands
- Analyze the concept of DOS/DDOS attack and ARP Poisoning
- Interpret the concept of Password Cracking and Network traffic Analyzer

List of Practical

1. Introduction to Kali Linux
2. Foot Printing and Reconnaissance
3. Scanning using NMAP – Live Host, Open Ports
4. Scanning – Vulnerability, Network Diagram
5. Understanding Ping, ARP, and nslookup Commands
6. SNMP Enumeration NA PPT,kali linux metasploit
7. Sniffing using Wireshark
8. DOS/ DDOS Attack
9. ARP Poisoning using Ettercap
10. TCP DUMP – Network Traffic Analyzer Working

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1 : Analyze the practical implementation of Ethical Hacking Tools **CO2 :** Interpret the concept of Foot Printing and Reconnaissance **CO3 :** Apply the concept of Ping, ARP, and nslookup Commands **CO4 :** Analyze the concept of DOS/DDOS attack and ARP Poisoning

CO5 : Interpret the concept of Password Cracking and Network traffic Analyzer

Mapping of Course Outcomes (COs) with PSOs - cybersecurity

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO1 0	PO1 1	PO 12	PS O1	PS O2	PS O3
CO1	2	2	2	2	3	1	1	2	1	1	0	2	3	2	2
CO2	3	3	3	2	3	1	1	2	1	2	1	2	3	3	2
CO3	3	3	3	2	2	1	1	2	2	2	1	3	3	3	3
CO4	3	3	3	3	3	2	2	3	2	2	2	3	2	1	3
C05	3	3	2	3	3	2	2	3	2	2	2	3	2	3	3

3 – high, 2 – Average, 1 - low , 0-null

Semester VIII

Programme	**B.Tech CSE Cyber Security**	**Programme Code**	**BTCY**		
Course Code	**25BTCY581**	**Number of Hours/Week**	**3**		
Semester	**VIII**	**Max. Marks**	**100**		
Year	**IV**	**Credits**	**15**		
Course Title	**CYBERSECURITY CAPSTONE PROJECT**		**L**	**T**	**P**
			0	**0**	**60**

L-Lecture Hours T-Tutorial Hours P-Practical Hours

COURSE OBJECTIVES:

The capstone project aims to:

- Apply theoretical cybersecurity knowledge to solve real-world problems.
- Encourage innovation in areas like ethical hacking, cryptography, secure coding, IoT/Cloud security, etc.
- Build skills in research, project design, implementation, documentation, and presentation.

	TOPICS	
	Project Phases *Phase I – Planning (Week 1–3)* • Identify the problem and domain. • Conduct a detailed literature review. • Define objectives, scope, and expected outcomes. • Prepare a project proposal and get approval. *Phase II – Design & Implementation (Week 4–10)* • Design architecture and choose tools/platforms. • Implement modules using secure coding practices. • Apply relevant cybersecurity frameworks or standards. *Phase III – Testing & Validation (Week 11–13)* • Perform security testing (e.g., penetration testing, fuzzing, code audits). • Use tools such as Wireshark, Burp Suite, Metasploit, or custom scripts. • Validate against benchmarks or datasets (e.g., CICIDS2017, NSL-KDD). *Phase IV – Documentation & Presentation (Week 14–16)* • Write a structured report with abstract, methodology, results, and references. • Prepare a demonstration video or live demo. • Present to the evaluation committee with Q&A.	
	Outcomes • **Project Proposal** (early submission) • **Mid-term Report** (design + partial implementation)	

	• **Final Report** (complete documentation) • **Presentation Slides** • **Codebase with Comments** (GitHub recommended) • **Plagiarism Report** (≤20%) • **Demo or Prototype**	
	Evaluation Criteria **Criteria** — **Weightage (%)** Problem Understanding & Research — 15% Design & Implementation — 30% Innovation & Relevance — 15% Testing & Results Analysis — 15% Documentation Quality — 15% Presentation & Viva — 10%	

45 Hours

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1: Identify and define real-world cybersecurity problems through in-depth domain analysis and research.

CO2: Design secure, scalable, and innovative solutions using appropriate tools, technologies, and methodologies.

CO3: Implement and test cybersecurity mechanisms such as encryption, authentication, intrusion detection, or risk assessment in practical environments.

CO4: Analyze and interpret experimental results or threat data to evaluate the effectiveness and limitations of the implemented solution.

CO5: Demonstrate project management, teamwork, and communication skills through technical documentation and oral presentations.

CO-PO-PSO MAPPING

B.Tech

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO 11	PO 12	PS O1	PS O2	PS O3
CO1	3	1	2	3	2	3	2	3	1	3	2	1	3	2	3
CO2	2	3	1	2	3	2	3	1	3	2	3	2	1	3	2
CO3	1	2	3	2	1	3	2	3	2	3	1	3	2	3	1
CO4	3	2	1	3	2	1	3	2	3	1	2	3	3	1	2
CO5	2	3	2	1	3	2	1	3	2	3	2	1	3	2	3

3 – high, 2 – Average, 1 - low , 0-null

Discipline Specific Elective - IX

Programme	**B.Tech CSE Cyber Security**	**Programme Code**	**BTCY**		
Course Code	**25BTCY381**	**Number of Hours/Week**	**3**		
Semester	**VIII**	**Max. Marks**	**100**		
Year	**IV**	**Credits**	**3**		
Course Title	**MOBILE AND IOT SECURITY**		**L**	**T**	**P**
			3	**0**	**2**

L-Lecture Hours T-Tutorial Hours P-Practical Hours

COURSE OBJECTIVES:

- Provide an understanding of the fundamentals of mobile and IoT ecosystems and their unique security challenges.
- Explore mobile and IoT device vulnerabilities, threat vectors, and attack surfaces.
- Study mobile and IoT architectures, protocols, and secure communication mechanisms.
- Familiarize students with mobile operating systems' security models and secure app development practices.
- Analyze risk assessment frameworks and current trends in mobile and IoT security including AI and blockchain applications.

UNIT	TOPICS	HOURS
I	**Introduction to Mobile and IoT Security** Overview of Mobile Computing and IoT - Mobile devices vs IoT devices: Capabilities and limitations - Common security threats: Malware, Man-in-the-Middle, DoS/DDoS - Importance of security in constrained environments - Attack surfaces: Device, network, data, and application layers	9
II	**Mobile Security Architecture and Threats** Mobile OS architectures (Android, iOS) - App security: Permissions, sandboxing, app signing - Mobile malware analysis and types - Device rooting and jailbreaking - Secure mobile app development practices - Case study: Pegasus spyware	9
III	**IoT Architecture and Security Challenges** IoT communication models and protocols (MQTT, CoAP, 6LoWPAN) - Security challenges in IoT: Device identity, integrity, and updates - Threats to IoT systems: Botnets (Mirai), firmware attacks - Secure boot and Trusted Execution Environment (TEE) - IoT security lifecycle and secure provisioning	9
IV	**Network and Communication Security** Mobile network security (GSM, LTE, 5G) - IoT network protocols: Zigbee, Bluetooth LE, LoRaWAN - Secure communication techniques (TLS, DTLS, VPNs) - Authentication and access control in IoT - Wireless vulnerabilities and attacks: eavesdropping, spoofing	9
V	**Security Frameworks, Risk Assessment & Emerging Trends** Threat modeling techniques: STRIDE, DREAD - IoT and mobile security frameworks: OWASP Mobile Top 10, OWASP IoT Top 10 - Regulatory and legal	9

	compliance: GDPR, HIPAA - Blockchain applications in IoT security - Artificial Intelligence in mobile threat detection - Future directions: Zero trust architecture, Post-quantum cryptography	

45 Hours

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1: Describe the differences between mobile and IoT devices and understand their common security threats and attack surfaces.

CO2: Analyze mobile security architectures and evaluate secure mobile application development practices.

CO3: Identify IoT architecture components and apply security mechanisms for device and data protection.

CO4: Evaluate network and communication security protocols used in mobile and IoT environments.

CO5: Apply risk assessment frameworks and explore emerging security technologies and regulatory requirements in mobile and IoT domains.

Text Books:

Cirani, S., Ferrari, G., Picone, M., & Veltri, L. (2019). *Internet of things: Architectures, protocols and standards* (1st ed.). John Wiley & Sons Ltd.

Reference Books:

Nikolay Elenkov , *Android Security Internals: An In-Depth Guide to Android's Security Architecture,* No Starch Press

CO-PO-PSO MAPPING

B.Tech

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO 11	PO 12	PS O1	PS O2	PS O3
CO1	3	1	2	3	2	3	2	3	1	3	2	1	3	2	3
CO2	2	3	1	2	3	2	3	1	3	2	3	2	1	3	2
CO3	1	2	3	2	1	3	2	3	2	3	1	3	2	3	1
CO4	3	2	1	3	2	1	3	2	3	1	2	3	3	1	2
CO5	2	3	2	1	3	2	1	3	2	3	2	1	3	2	3

3 – high, 2 – Average, 1 - low , 0-null

Programme	**B.Tech CSE Cyber Security**	**Programme Code**	**BTCY**		
Course Code	**25BTCY382**	**Number of Hours/Week**	**3**		
Semester	**VIII**	**Max. Marks**	**100**		
Year	**IV**	**Credits**	**3**		
Course Title	**SECURITY IN EDGE AND FOG COMPUTING**		**L**	**T**	**P**
			3	**0**	**2**

L-Lecture Hours T-Tutorial Hours P-Practical Hours

Course Objectives:

The course aims to:

- Introduce the principles and architecture of Edge and Fog Computing and their role in modern distributed systems.
- Identify and analyze security threats, attack surfaces, and vulnerabilities specific to Edge and Fog environments.
- Explain security models and mechanisms including authentication, access control, encryption, and secure computation.
- Explore secure network communication protocols and intrusion detection/prevention techniques in edge-based networks.
- Discuss privacy-preserving methods, compliance with regulations, and emerging technologies like AI and blockchain in edge security.

UNIT	TOPICS	HOURS
I	**Fundamentals of Edge and Fog Computing** Overview of Cloud, Edge, and Fog computing paradigms - Differences and use cases of Edge vs. Fog vs. Cloud - Architecture of Fog and Edge environments - Applications in IoT, smart cities, healthcare, and autonomous systems - Introduction to security concerns in distributed computing environments	9
II	**Threats and Vulnerabilities in Edge and Fog Systems** Attack surfaces in Edge and Fog computing - Threats: Eavesdropping, data leakage, physical attacks - Man-in-the-Middle (MitM), Sybil, replay, DoS/DDoS attacks - Edge node and fog node compromise - Risk assessment strategies	9
III	**Security Models and Mechanisms** Authentication and access control models (RBAC, ABAC) - Data confidentiality, integrity, and availability in fog/edge - Identity and trust management - Encryption techniques for edge/fog nodes - Secure storage and computation offloading	9
IV	**Network and Communication Security** Secure routing and communication protocols - TLS/SSL, VPNs, and DTLS for edge networks - Lightweight security protocols for constrained devices - Intrusion detection and prevention systems - Security in software-defined networking (SDN) and NFV in edge environments	9

V	**Privacy, Compliance, and Emerging Trends** Data privacy challenges in fog/edge: anonymization, differential privacy - GDPR and other data protection regulations - Blockchain and distributed ledger technologies for edge security - AI and machine learning for threat detection - Zero Trust Architecture for edge computing	9

45 Hours

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1: Describe the fundamentals of Edge and Fog Computing, and differentiate them from traditional cloud systems.

CO2: Analyze potential security threats and vulnerabilities in Edge and Fog environments and apply appropriate risk assessment techniques.

CO3: Apply security mechanisms including authentication, encryption, and trust management in edge/fog systems.

CO4: Implement secure communication protocols and detect/prevent intrusions in edge network infrastructures.

CO5: Evaluate privacy concerns, regulatory requirements, and the use of emerging technologies in enhancing edge and fog security.

Text Books:

Rajkumar Buyya, Satish Narayana Srirama, *Fog and Edge Computing: Principles and Paradigms*, Wiley

Reference Books:

1. **Buyya, R., & Srirama, S. N. (Eds.).** (2019). *Fog and edge computing: Principles and paradigms*. Wiley.
2. **Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L.** (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal, 3*(5), 637–646. https://doi.org/10.1109/JIOT.2016.2579198
3. **Roman, R., Lopez, J., & Mambo, M.** (2018). Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems, 78,* 680–698. https://doi.org/10.1016/j.future.2016.11.009
4. **Zhang, K., Mao, Y., Leng, S., He, Y., & Zhang, Y.** (2016). Mobile-edge computing for vehicular networks: A promising network paradigm with predictive off-loading. *IEEE Vehicular Technology Magazine, 12*(2), 36–44. https://doi.org/10.1109/MVT.2016.2638981
5. **Stojmenovic, I., & Wen, S.** (2014). The fog computing paradigm: Scenarios and security issues. *Proceedings of the 2014 Federated Conference on Computer Science and Information Systems*, 1–8. https://doi.org/10.15439/2014F173

CO-PO-PSO MAPPING

B.Tech

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO 11	PO 12	PS O1	PS O2	PS O3
CO1	3	1	2	3	2	3	2	3	1	3	2	1	3	2	3
CO2	2	3	1	2	3	2	3	1	3	2	3	2	1	3	2
CO3	1	2	3	2	1	3	2	3	2	3	1	3	2	3	1
CO4	3	2	1	3	2	1	3	2	3	1	2	3	3	1	2
CO5	2	3	2	1	3	2	1	3	2	3	2	1	3	2	3

3 – high, 2 – Average, 1 - low , 0-null

Programme	**B.Tech CSE Cyber Security**	**Programme Code**	**BTCY**		
Course Code	**25BTCY383**	**Number of Hours/Week**	**3**		
Semester	**VIII**	**Max. Marks**	**100**		
Year	**IV**	**Credits**	**3**		
Course Title	**SECURITY IN SOFTWARE DEFINED NETWORK**		**L**	**T**	**P**
			3	**0**	**0**

L-Lecture Hours T-Tutorial Hours P-Practical Hours

COURSE OBJECTIVES:

The course aims to:

- Introduce the architecture and components of Software Defined Networking (SDN) and compare it with traditional networks.
- Identify and analyze security threats and vulnerabilities across the SDN architecture.
- Examine key security mechanisms and protocols used in securing SDN environments.
- Explore SDN-based solutions for real-time traffic monitoring, intrusion detection, and forensic analysis.
- Evaluate SDN security frameworks, real-world applications, and future trends including AI/ML integration.

UNIT	TOPICS	HOURS
I	**Introduction to Software Defined Networks (SDN)** Overview of SDN: Definition and architecture - Traditional networks vs. SDN - SDN components: Application layer, Control layer, Data layer - OpenFlow protocol and southbound APIs - Benefits and challenges of SDN - Security implications of network programmability	9
II	**Threats and Vulnerabilities in SDN** SDN-specific attack surfaces: Controller, switches, communication links - Threats to SDN control plane: DoS, man-in-the-middle, spoofing - Flow rule modification and hijacking - Data plane vulnerabilities: Packet dropping, rule exhaustion - Northbound API security risks	9
III	**SDN Security Mechanisms** Authentication and secure communication between layers - Controller hardening and redundancy - Flow rule validation and anomaly detection - Access control and isolation techniques - Security in OpenFlow switches - Role of TLS, PKI in SDN environments	9
IV	**Network Monitoring and Intrusion Detection** Real-time traffic monitoring in SDN - SDN-based Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) - Threat intelligence integration - Dynamic policy enforcement - SDN logging and forensic techniques	9
V	**Case Studies, Frameworks, and Future Directions** OpenDaylight, ONOS, Ryu: Security features comparison - SDN in data centers, 5G networks, and enterprise environments - Security evaluation frameworks for SDN - Integration of AI/ML for automated threat response - Research trends and emerging security challenges in SDN	9

45 Hours

COURSE OUTCOMES:

On successful completion of this course, the student will be able to
CO1: Understand the foundational architecture and programmable nature of SDN and its security implications.
CO2: Identify potential threats and vulnerabilities in SDN's control, data, and application layers.
CO3: Apply secure communication protocols and hardening techniques to protect SDN environments.
CO4: Analyze and implement network monitoring and intrusion detection mechanisms in SDN.
CO5: Evaluate real-world SDN frameworks and future research directions in securing programmable networks.

Text Books:

Paul Goransson, Chuck Black, Timothy Culver **,** *Software Defined Networks: A Comprehensive Approach,* Morgan Kaufmann (Elsevier)

Reference Books:

1. Goransson, P., Black, C., & Culver, T. (2016). *Software defined networks: A comprehensive approach* (2nd ed.). Morgan Kaufmann.
2. Kreutz, D., Ramos, F. M. V., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software-defined networking: A comprehensive survey. *Proceedings of the IEEE, 103*(1), 14–76. https://doi.org/10.1109/JPROC.2014.2371999
3. Hu, F., Hao, Q., & Bao, K. (2014). A survey on software-defined network and OpenFlow: From concept to implementation. *IEEE Communications Surveys & Tutorials, 16*(4), 2181–2206. https://doi.org/10.1109/COMST.2014.2326417
4. Lara, A., Kolasani, A., & Ramamurthy, B. (2014). Network innovation using OpenFlow: A survey. *IEEE Communications Surveys & Tutorials, 16*(1), 493–512. https://doi.org/10.1109/SURV.2013.081313.00105
5. Fichera, M., Santamaria, A. F., & Sifalakis, M. (2022). *Security in software-defined networking*. Springer.

CO-PO-PSO MAPPING
B.Tech

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO 11	PO 12	PS O1	PS O2	PS O3
CO1	3	1	2	3	2	3	2	3	1	3	2	1	3	2	3
CO2	2	3	1	2	3	2	3	1	3	2	3	2	1	3	2
CO3	1	2	3	2	1	3	2	3	2	3	1	3	2	3	1
CO4	3	2	1	3	2	1	3	2	3	1	2	3	3	1	2
CO5	2	3	2	1	3	2	1	3	2	3	2	1	3	2	3

3 – high, 2 – Average, 1 - low , 0-null

Discipline Specific Elective - X

Programme	**B.Tech CSE Cyber Security**	**Programme Code**	**BTCY**		
Course Code	**25BTCY384**	**Number of Hours/Week**	**3**		
Semester	**VIII**	**Max. Marks**	**100**		
Year	**IV**	**Credits**	**3**		
Course Title	**RESEARCH METHODOLOGY IN SECURITY**		**L**	**T**	**P**
			3	**0**	**0**

L-Lecture Hours T-Tutorial Hours P-Practical Hours

COURSE OBJECTIVES:

The course aims to:

- Introduce the fundamentals of research methodology within the context of cybersecurity.
- Enable students to identify research problems and perform literature reviews using modern tools and databases.
- Familiarize students with research design methods, including experimental, empirical, and simulation-based approaches.
- Develop competency in data analysis, use of statistical and visualization tools, and cybersecurity simulation platforms.
- Guide students in structuring, writing, and publishing research papers, with emphasis on ethics and intellectual property.

UNIT	TOPICS	HOURS
I	**Foundations of Research and Cybersecurity Context** Introduction to research methodology - Research process and characteristics of scientific research - Types of research: Fundamental, applied, exploratory, descriptive - Importance of research in cybersecurity - Security domains: Network, application, IoT, cloud, AI security - Ethics in security research (vulnerabilities, disclosures, etc.)	9
II	**Problem Formulation and Literature Review** Identifying and defining a research problem in security - Framing research objectives and hypotheses - Techniques for literature review: Searching, organizing, summarizing - Use of tools: Google Scholar, IEEE Xplore, Scopus, Zotero/Mendeley - Reviewing existing frameworks, attacks, and defense mechanisms - Gap analysis and justification for new work	9
III	**Research Design and Methods** Quantitative vs qualitative research in cybersecurity - Experimental, survey, and simulation-based research - Case study and empirical research in security - Data collection methods: Logs, packet captures, repositories (e.g., CTU-13, CICIDS) - Use of datasets for security analysis - Validity, reliability, and reproducibility in experiments	9
IV	**Data Analysis, Tools, and Simulation** Data preprocessing and statistical analysis - Use of tools: SPSS, R, Python (Pandas, SciPy), MATLAB - Visualization tools: Matplotlib, Seaborn, Tableau - Simulation environments: NS3, GNS3, Mininet (for SDN), Cuckoo sandbox - Evaluation	9

	metrics: Accuracy, Precision, Recall, ROC curves, AUC - Benchmarking and comparison of algorithms or frameworks	
V	**Writing, Publishing, and Ethical Considerations** Structure of a research paper in cybersecurity - Writing abstracts, introduction, and conclusion - Selecting journals/conferences (IEEE, ACM, Elsevier, Springer) - Peer review process and plagiarism policies - Referencing styles: IEEE, APA, BibTeX - Patents, intellectual property, and responsible disclosure	9

45 Hours

COURSE OUTCOMES:

On successful completion of this course, the student will be able to

CO1: Understand the research process, types, and the relevance of research in cybersecurity domains.

CO2: Formulate research problems, review literature systematically, and identify research gaps.

CO3: Design cybersecurity experiments using appropriate methods and ensure research validity and reproducibility.

CO4: Analyze research data using statistical tools and evaluate security systems with simulation platforms and metrics.

CO5: Write and publish research papers adhering to ethical standards, referencing styles, and publication guidelines.

Text Books:

Ranjit Kumar, ***Research Methodology: A Step-by-Step Guide for Beginners,*** SAGE Publications

Reference Books:

Atilla Elçi, Miltiadis D. Lytras, *Cybersecurity Research and Practice*, SpringerOpen

CO-PO-PSO MAPPING
B.Tech

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO 11	PO 12	PS O1	PS O2	PS O3
CO1	3	1	2	3	2	3	2	3	1	3	2	1	3	2	3
CO2	2	3	1	2	3	2	3	1	3	2	3	2	1	3	2
CO3	1	2	3	2	1	3	2	3	2	3	1	3	2	3	1
CO4	3	2	1	3	2	1	3	2	3	1	2	3	3	1	2
CO5	2	3	2	1	3	2	1	3	2	3	2	1	3	2	3

3 – high, 2 – Average, 1 - low , 0-null

Programme	**B.Tech CSE Cyber Security**	**Programme Code**	**BTCY**		
Course Code	**25BTCY385**	**Number of Hours/Week**	**3**		
Semester	**VIII**	**Max. Marks**	**100**		
Year	**IV**	**Credits**	**3**		
Course Title	**CYBER LAWS AND DIGITAL EVIDENCE**		**L**	**T**	**P**
			3	**0**	**2**

L-Lecture Hours T-Tutorial Hours P-Practical Hours

COURSE OBJECTIVES:

- To provide an understanding of the legal framework governing cyber activities.
- To equip students with knowledge of national and international cyber laws.
- To explain procedures for handling, preserving, and presenting digital evidence.
- To familiarize students with cybercrime investigation and forensic principles.
- To bridge the gap between cybersecurity technology and legal compliance.

UNIT	TOPICS	HOURS
I	**Introduction to Cyber Law and Legal Framework** Cyber law: definition, evolution, and scope - Legal recognition of electronic records and signatures - IT Act 2000 (India): Overview, amendments, key sections - Jurisdictional challenges in cyberspace -International laws and conventions (Budapest Convention, UNCITRAL)	9
II	**Cybercrimes and Offenses** Categories of cybercrimes: hacking, phishing, identity theft, cyber terrorism - Cyberstalking, cyberbullying, online harassment - Social media misuse and legal liabilities - Case studies: Real-world cybercrime prosecutions - Role of CERTs and law enforcement agencies	9
III	**Digital Evidence and Investigation** Types and sources of digital evidence: logs, emails, file metadata - Principles of digital forensics and evidence collection - Chain of custody, preservation and authentication of evidence - Tools and software used in evidence gathering - Admissibility of digital evidence in courts	9
IV	**Data Protection and Privacy Laws** Data privacy principles and compliance - General Data Protection Regulation (GDPR) - Indian Personal Data Protection Bill (PDPB) - Cross-border data transfer and legal issues - Legal obligations for data breach notifications	9
V	**Cyber Law Compliance and Ethics** Corporate legal responsibilities and due diligence - IT compliance audits and frameworks (ISO 27001, PCI-DSS) - Ethical hacking and legal boundaries - Intellectual property issues in cyberspace - Future trends in cyber law and governance	9

45 Hours

COURSE OUTCOMES:

On successful completion of this course, the student will be able to
CO1: Interpret key provisions of cyber laws such as IT Act, GDPR, and HIPAA.

CO2: Identify legal issues in cybercrimes like hacking, phishing, data breaches, etc.

CO3: Demonstrate procedures for acquiring and analyzing digital evidence.

CO4: Apply legal standards for evidence admissibility in courts.

CO5: Evaluate legal responsibilities of individuals and organizations in cyberspace

Text Books:

Vivek Sood***, Cyber Law Simplified***

Reference Books:
Handbook on Cyber Law, Government of India – Ministry of Electronics and Information Technology (MeitY)

CO-PO-PSO MAPPING

B.Tech

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO 11	PO 12	PS O1	PS O2	PS O3
CO1	3	1	2	3	2	3	2	3	1	3	2	1	3	2	3
CO2	2	3	1	2	3	2	3	1	3	2	3	2	1	3	2
CO3	1	2	3	2	1	3	2	3	2	3	1	3	2	3	1
CO4	3	2	1	3	2	1	3	2	3	1	2	3	3	1	2
CO5	2	3	2	1	3	2	1	3	2	3	2	1	3	2	3

3 – high, 2 – Average, 1 - low , 0-null

Programme	**B.Tech CSE Cyber Security**	**Programme Code**	**BTCY**		
Course Code	**25BTCY386**	**Number of Hours/Week**	**3**		
Semester	**VIII**	**Max. Marks**	**100**		
Year	**IV**	**Credits**	**3**		
Course Title	**SECURITY RISK MANAGEMENT**		**L**	**T**	**P**
			3	**0**	**2**

L-Lecture Hours T-Tutorial Hours P-Practical Hours

COURSE OBJECTIVES:

- Understand the principles and practices of risk management in the context of information security.
- Identify, assess, and prioritize risks in IT and cyber systems.
- Explore risk mitigation, control mechanisms, and cost-benefit analyses.
- Gain familiarity with frameworks and standards such as ISO 27005, NIST SP 800-30, and COBIT.
- Develop capabilities for continuous risk monitoring, reporting, and communication.

UNIT	TOPICS	HOURS
I	**Introduction to Security Risk Management** Concepts of risk, threats, vulnerabilities, and impact - Types of risks: Cyber, operational, insider threats, third-party risks - Risk management process overview - Standards and frameworks: ISO/IEC 27005, NIST RMF - Security policy, governance, and compliance overview	9
II	**Risk Identification and Assessment** Risk identification methods: Asset-based, threat-based, vulnerability-based - Risk assessment types: Quantitative vs. qualitative - Tools: Risk matrices, heat maps, decision trees - Asset valuation, threat profiling, vulnerability assessment - Risk registers and documentation	9
III	**Risk Analysis and Evaluation** Likelihood and impact assessment - Risk scoring and ranking - Exposure factor, single loss expectancy (SLE), annual loss expectancy (ALE) - Risk appetite, risk tolerance - Cost-benefit analysis and risk prioritization	9
IV	**Risk Treatment and Mitigation Strategies** Risk treatment options: Avoid, transfer, reduce, accept - Security controls: Preventive, detective, corrective, compensating - Mitigation planning and implementation - Role of insurance, outsourcing, and contracts in risk transfer - Case studies of risk treatment in enterprises	9
V	**Risk Monitoring, Reporting, and Governance** Continuous risk monitoring and reassessment - KPIs, KRIs, and dashboards - Incident handling and response planning - Integration with business continuity and disaster recovery - Documentation, reporting, and audit readiness	9

45 Hours

COURSE OUTCOMES:

On successful completion of this course, the student will be able to
CO1: Apply risk management frameworks to identify and assess security risks.
CO2: Recommend appropriate mitigation strategies and controls.
CO3: Perform risk analysis using quantitative and qualitative techniques.
CO4: Design and implement a risk management plan for an organization.
CO5: Evaluate the effectiveness of security policies in reducing organizational risk

Text Books:

Calder, A. (2019). *Information security risk management for ISO 27001/ISO 27002* (2nd ed.). IT Governance Publishing.

Reference Books:

- Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk management guide for information technology systems: Recommendations of the National Institute of Standards and Technology (NIST SP 800-30)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30

- Hubbard, D. W. (2020). *The failure of risk management: Why it's broken and how to fix it* (2nd ed.). Wiley.

- Young, W., & Leveson, N. (2014). *An integrated approach to safety and security based on systems theory*. Communications of the ACM, 57(2), 31–35. https://doi.org/10.1145/2556938

- Raggad, B. G. (2010). *Information security management: Concepts and practice*. CRC Press.

- ISACA. (2012). *COBIT 5: A business framework for the governance and management of enterprise IT*. ISACA.

CO-PO-PSO MAPPING

B.Tech

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO 11	PO 12	PS O1	PS O2	PS O3
CO1	3	1	2	3	2	3	2	3	1	3	2	1	3	2	3
CO2	2	3	1	2	3	2	3	1	3	2	3	2	1	3	2
CO3	1	2	3	2	1	3	2	3	2	3	1	3	2	3	1
CO4	3	2	1	3	2	1	3	2	3	1	2	3	3	1	2
CO5	2	3	2	1	3	2	1	3	2	3	2	1	3	2	3

3 – high, 2 – Average, 1 - low , 0-null