Department: Computer Science and Engineering (Cyber Security)

Vision of the Department

"To ignite a passion for innovation in Computer Science and Cyber security, empowering students to become leaders who shape a secure and interconnected future"

Mission of the Department

- To provide an exceptional educational experience fostering critical thinking, creativity, and a deep understanding of cyber security principles.
- To equip graduates with in-demand skills and an ethical mindset to thrive in the dynamic cyber security landscape.
- To cultivate a collaborative learning environment connecting students with industry experts, cutting-edge research, and real-world challenges.
- To inspire a lifelong commitment to learning and dedication to building a safer, more secure digital world

Program Educational Objectives (PEOs)

- Excel as innovative technical leaders in computer science and cyber security, developing secure and robust solutions.
- Demonstrate a strong ethical mindset and contribute positively to a safer digital world.
- Show a continuous commitment to professional growth and actively engage with industry and research.
- To work efficiently in multi-disciplinary teams to establish
- good soft skills to prove themselves at IT sector.

Program Outcomes (POs)

1. **Engineering Knowledge**: Apply knowledge of mathematics, natural science, computing, engineering fundamentals and an engineering specialization as specified in WK1 to WK4 respectively to develop to the solution of complex engineering problems.
2. **Problem Analysis**: Identify, formulate, review research literature and analyze complex engineering problems reaching substantiated conclusions with consideration for sustainable development. (WK1 to WK4)
3. **Design/Development of Solutions**: Design creative solutions for complex engineering problems and design/develop systems/components/processes to meet identified needs with consideration for the public health and safety, whole-life cost, net zero carbon, culture, society and environment as required. (WK5)
4. **Conduct Investigations of Complex Problems**: Conduct investigations of complex engineering problems using research-based knowledge including design of experiments, modelling, analysis & interpretation of data to provide valid conclusions. (WK8).
5. **Engineering Tool Usage**: Create, select and apply appropriate techniques, resources and modern engineering & IT tools, including prediction and modelling recognizing their limitations to solve complex engineering problems. (WK2 and WK6)
6. **The Engineer and The World**: Analyze and evaluate societal and environmental aspects while solving complex engineering problems for its impact on sustainability with reference to economy, health, safety, legal framework, culture and environment. (WK1, WK5, and WK7).
7. **Ethics**: Apply ethical principles and commit to professional ethics, human values, diversity and inclusion; adhere to national & international laws. (WK9)

8. **Individual and Collaborative Team work:** Function effectively as an individual, and as a member or leader in diverse/multi-disciplinary teams.
9. **Communication**: Communicate effectively and inclusively within the engineering community and society at large, such as being able to comprehend and write effective reports and design documentation, make effective presentations considering cultural, language, and learning differences
10. **Project Management and Finance**: Apply knowledge and understanding of engineering management principles and economic decision-making and apply these to one's own work, as a member and a leader in a team, and to manage projects and in multidisciplinary environments.
11. **Life-Long Learning**: Recognize the need for, and have the preparation and ability for i) independent and life-long learning ii) adaptability to new and emerging technologies and iii) critical thinking in the broadest context of technological change. (WK8)

Program Specific Outcomes (PSOs)

1. Able to apply appropriate techniques for storage of huge amount of data and ensuring its integrity.
2. Choose appropriate method for data acquisition from real world and propose suitable solutions to solve problems.

Scheme of Teaching and Examination-2022 (160 Credits Scheme, NEP)
Outcome Based Education (OBE) and Choice Based Credit System (CBCS)

V Semester B. E **Academic year: 2025-26**

Sl.No.	Course Code		Course Title	Teaching Dept.	Teaching Hrs.					Credits	Examination			
					L	T	P	S	Total		CIE Marks	SEE Marks	Total Marks	Exam Hrs
1	PC	22CY501	Big Data Analytics	CY	42	-	-	48	90	3	50	50	100	3
2	PC	22CY502	Advanced Computer Networks	CY	42	-	28	50	120	4	50	50	100	3
3	PC	22CY503	Cryptography and Network Security	CY	42	-	28	50	120	4	50	50	100	3
4	PE	22CY5PEX	Professional Elective-I	CY	42	-	-	48	90	3	50	50	100	3
5	OE	22CY5OEX	Open Elective-I	Xx	42	-	-	48	90	3	50	50	100	3
6	HS	22IE56x	Institutional Elective (561: Research Methodology, 562: Management and Entrepreneurship,563: Project Management)	CY	28	-	-	32	60	2	50	50	100	3
7	PC	22 XX 507	CY Dept. Skill Lab 3 (Ethical Hacking using Kali Linux)	CY	14	-	28	18	60	2	50	50	100	3
8	HS	22SK508	Skill Development-II	T&P	-	-	28	2	30	1	50	-	50	-
				Total	**252**	**0**	**112**	**296**	**660**	**22**	**400**	**350**	**750**	**-**

L: Lecture, T-Tutorial, P-Practical/Drawing, CIE: Continuous Internal Evaluation, SEE: Semester End Examination, S: Self Learning. XX: Branch Code

Credit Distribution: PC: Professional Core-13, PE: Professional Elective-03, OE: Open Elective-03, HS: Humanity Science-03, **Total=22 Credits.**

Department: CSE (Cyber Security)			Semester:	V
Subject: Big Data Analytics				
Subject Code:	22CY501	L – T – P - S:	42-0-0-48 (In Hrs.)	
			Credits:	3

Sl. No	Course Objectives
1	To **understand** the fundamentals of Big Data and its characteristics
2	To **learn** various Big Data storage and processing frameworks
3	To **explore** data mining techniques and algorithms for large datasets
4	To **understand** security aspects and privacy concerns in Big Data
5	To **apply** Big Data analytics in cyber security domain

Unit	Description	Hrs
I	**Introduction to Big Data Analytics:** Big Data, Scalability and Parallel Processing, Designing Data Architecture, Data Sources, Quality, Pre-Processing and Storing, Data Storage and Analysis, Big Data Analytics Applications and Case Studies. **T1:** Raj Kamal & Preeti Saxena – Ch. 1, 2, 3	8
II	**Introduction to Hadoop:** Introduction, Hadoop and its Ecosystem, Hadoop Distributed File System, MapReduce Framework and Programming Model, Hadoop Yarn, Hadoop Ecosystem Tools. **Hadoop Distributed File System Basics:** HDFS Design Features, Components, HDFS User Commands. **Essential Hadoop Tools:** Using Apache Pig, Hive, Sqoop, Flume, Oozie, HBase. **T1:** Ch. 4, 5, 6; **T2:** Douglas Edline – Ch. 1, 2, 3	8
III	**NoSQL Big Data Management, MongoDB and Cassandra:** Introduction, NoSQL Data Store, NoSQL Data Architecture Patterns, NoSQL to Manage Big Data, Shared-Nothing Architecture for Big Data Tasks, MongoDB, Databases, Cassandra Databases. **T1:** Ch. 7, 8; **Ref1:** Tom White – relevant NoSQL sections	8

IV	**MapReduce, Hive and Pig:** Introduction, MapReduce Map Tasks, Reduce Tasks and MapReduce Execution, Composing MapReduce for Calculations and Algorithms, Hive, HiveQL, Pig. **T1: Ch. 9, 10; T2: Ch. 4, 5**	**8**
V	**Machine Learning Algorithms for Big Data Analytics:** Introduction, Estimating the relationships, Outliers, Variances, Probability Distributions, and Correlations, Regression analysis, Finding Similar Items, Similarity of Sets and Collaborative Filtering, Frequent Item sets and Association Rule Mining. Text, Web Content, Link, and Social Network Analytics: Introduction, Text mining, Web Mining, Web Content and Web Usage Analytics, Page Rank, Structure of Web and analysing a Web Graph, Social Network as Graphs and Social Network Analytics: **T1:** Ch. 11, 12, 13	**8**

Course outcome	Descriptions
CO1	**Understand** fundamentals of Big Data analytics.
CO2	**Investigate** Hadoop framework and Hadoop Distributed File system.
CO3	**Illustrate** the concepts of NoSQL using MongoDB and Cassandra for Big Data.
CO4	**Demonstrate** the MapReduce programming model to process the big data along with Hadoop tools.
CO5	**Apply** machine learning and advanced analytics techniques for Big Data in various domains including cyber security.

Course Articulation Matrix

PO/PSO CO	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	1									1	
CO2	3	2	2	1								1	
CO3	3	3	2	2	1							2	
CO4	3	3	3	2	2							2	
CO5	3	3	3	3	3	2						3	3

Text Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	“Big Data Analytics Introduction to Hadoop, Spark, and Machine-Learning”, McGraw Hill Education	Raj Kamal and Preeti Saxena	2018 ISBN: 9789353164966, 9353164966
2	"Hadoop 2 Quick-Start Guide: Learn the Essentials of Big Data Computing in the Apache Hadoop 2 Ecosystem"	Douglas Eadline	1st Edition, Pearson Education, 2016. ISBN13: 978-9332570351

Reference Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	"Hadoop: The Definitive Guide"	Tom White,	4th Edition, O"Reilly Media, 2015.ISBN-13: 978- 9352130672
2	"Professional Hadoop Solutions"	Boris Lublinsky, Kevin T Smith, Alexey Yakubovich	1st Edition, Wrox Press, 2014ISBN-13: 978-8126551071
3	"Hadoop Operations: A Guide for Developers and Administrators"	Eric Sammer	1st Edition, O'Reilly Media, 2012.ISBN-13: 978-9350239261

Course Assessment and Evaluation: Regular Theory Courses

Continuous Internal Evaluation (CIE): 50 Marks

Sl. No	Components		Duration (min)	Marks Conducted for	Marks reduced to	40% Min Marks in each component to write SEE
1	Theory- Internal Assessment	IA-1	90	50	20	16
		IA-2	90	50	20	
2	Activity Based Learning	ABL1	-	25	5	4
		ABL2	-	25	5	
Total CIE				150	50	20

IA-1 Syllabus: 2½ Module , IA-2 Syllabus: 2½ Module
Activity Based Learning (ABL): Online course with certification, Hobby project, Simulations, Industrial Visits, Community-Based Learning, Case-study, Problem-Based Learning, Peer Teaching, web page design, student publications, Hackathons, Quiz (Leetcode, GitHub, Hackaranks and company specific quiz), Student Development program (1 week/online or offline), ……Etc

Semester End Examination (SEE): Max 100 Marks, Duration: 3 Hrs
The question paper shall contain 10 full questions (20 marks each)**,** with **2** questions from each of the 5 Modules**,** ensuring 100% syllabus coverage**.** Students shall answer any 5 full questions with 1:1 choice. Each question may have a maximum of 4 sub-divisions.
Minimum passing Marks: 40% of Max Marks

Department: CSE (Cyber Security)			Semester:	V
Subject: Advanced Computer Networks				
Subject Code:	22CY502	L – T – P - S:	42-0-28-50 (In Hrs.)	
			Credits:	4

Sl. No	Course Objectives
1	**Understand** modern network topologies, protocols, and architectures.
2	**Apply** security principles to design robust network infrastructures.
3	**Analyze** network performance metrics, identify bottle necks, and implement Quality of Service (QoS).
4	**Assess** the impact and implementation of cutting-edge technologies.

Unit	Description	Hrs
I	**Module 1: Advanced Network Architectures and Modern Paradigms** Network Evolution and Contemporary Architectures, Software-Defined Networking (SDN) fundamentals and OpenFlow protocol, Network Function Virtualization (NFV) and service chaining, Intent-Based Networking (IBN) concepts, Cloud and Hybrid Network Architectures, Data Center Networking and fabric technologies, Network as a Service (NaaS) models, Advanced routing protocols (BGP, OSPF extensions), Multi-Protocol Label Switching (MPLS) and traffic engineering. **T1:** Ch. 1, 4, 5, 6, 8; **R1:** Ch. 4, 5, 6; **R2:** Ch. 7–10	7
II	**Module 2: Network Security and Cyber Defense Mechanisms:** Network threat landscape and contemporary attack vectors, Advanced firewall technologies and next-generation firewalls, Intrusion Detection and Prevention Systems (IDS/IPS) deployment, Network Access Control (NAC) and Zero Trust Architecture, Virtual Private Networks (VPN) and secure tunneling protocols, Network	8

	security monitoring and Security Information Event Management (SIEM), DDoS protection mechanisms and mitigation strategies, Network forensics and incident response procedures, Wireless network security and enterprise Wi-Fi protection, Network vulnerability assessment and penetration testing. **T2**: Ch. 1–6; **T1**: Ch. 8.5 (Security); **R1**: Ch. 8 (Security in networks)	
III	**Module 3: Quality of Service and Network Performance Management** QoS fundamentals and service differentiation models, Traffic classification, marking, and policing mechanisms, Queuing algorithms and scheduling techniques (FIFO, WFQ, CBWFQ), Bandwidth management and traffic shaping strategies, Network performance monitoring and analysis tools, Service Level Agreements (SLA) management and enforcement, Network capacity planning and scalability considerations, Congestion control mechanisms and optimization techniques, Network troubleshooting methodologies and best practices **T1**: Ch. 5, 6, 7; **R1**: Ch. 5, 6; **R2**: Ch. 15–17	**8**
IV	**Module 4: Emerging Technologies and Future Network Paradigms:** 5G networks architecture and security implications, Internet of Things (IoT) networking protocols and frameworks, Edge computing and fog networking architectures, Network slicing and virtualization technologies, Artificial Intelligence and Machine Learning in network management, Blockchain applications in networking and distributed systems, Green networking initiatives and energy-efficient protocols, Network automation and orchestration platforms, Microservices architecture and container networking **T1**: Ch. 9 (Multimedia & wireless), Ch. 10 (Future directions); R1: Ch. 9 (Mobile & wireless networks)	**9**

V	**Module 5: Network Management and Operational Excellence:** Network Management protocols (SNMP, NETCONF, RESTCONF), Network monitoring, analytics, and observability, Configuration management and Infrastructure as Code (IaC), DevOps practices in networking (NetDevOps) and CI/CD pipelines, Network service orchestration and automation frameworks, Software-defined WAN (SD-WAN) implementation and management, Network disaster recovery and business continuity planning, Network documentation, change management, and compliance, Cost optimization and resource management strategies, Future trends and career pathways in network engineering **T1:** Ch. 9.4, Ch. 10; **T2:** Ch. 7; **R2:** Ch. 20–23	**8**

Lab Content :

Sl. No	Experiment Description
1	**SDN Implementation:** Configure OpenFlow controllers and switches using Mininet
2	**Network Security Assessment:** Deploy and configure IDS/IPS using Snort and Suricata
3	**VPN Configuration:** Implement site-to-site and remote access VPN solutions
4	**QoS Implementation:** Configure traffic shaping, bandwidth management, and prioritization.
5	**Network Simulation:** Design complex topologies using GNS3 and Packet Tracer **IoT Network Design:** Create and secure IoT network architectures
6	**Network Monitoring:** Deploy comprehensive monitoring solutions (Nagios, PRTG, SolarWinds)
7	**Vulnerability Assessment:** Conduct network security assessments using Nmap, Nessus, and OpenV.

Course Outcomes:

Course outcome	Descriptions
CO1	**Analyze** and evaluate advanced network architectures.
CO2	**Design** and implement comprehensive network security solutions to protect against cyber threats and vulnerabilities
CO3	**Apply** QoS mechanisms and performance optimization techniques to ensure efficient network operations
CO4	**Assess** emerging network technologies and their integration into existing infrastructure for future-ready solutions
CO5	**Implement** network management, automation, and operational excellence practices.

Course Articulation Matrix

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

Text Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	" Computer Networks: A Top-Down Approach"	James F. Kurose and Keith W. Ross	8th Edition, Pearson, 2021
2	" Network Security Essentials: Applications and Standards	William Stallings	6th Edition, Pearson, 2017

Reference Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	Computer Networks	Andrew S. Tanenbaum and David J. Wetherall	5th Edition, Pearson, 2013
2	Network Warrior	Gary A. Donahue	2nd Edition, O'Reilly Media, 2011

Course Assessment and Evaluation: Integrated Courses

Continuous Internal Evaluation (CIE): 50 Marks						
Sl. No	**Components**		**Duration (min)**	**Marks Conducted for**	**Marks reduced to**	**40% Min Marks in each component to write SEE**
1	Theory-Internal Assessment	IA-1	90	50	15	12
		IA-2	90	50	15	
2	Periodic Lab Assessment		-	30	10	4
3	Lab CIE		-	20	5	4
4	One Open Ended Experiment /Project		-	10	5	2
	Total CIE			**150**	**50**	**20**

IA-1 Syllabus: 2½ Module , IA-2 Syllabus: 2½ Module
Rubrics for Periodic Lab Assessment: Attendance (5M), Lab record (10 M), Conduction of Experiments(10M) and Viva(5M)-**Total 30M**
Lab CIE: Write-up(5M), Conduction/Execution/Demonstration(10M) and Viva(5M)-**Total 20M**
One Open Ended Experiment /Project: Experimental/project Design (4 marks), Execution/demonstration (3 marks) and Analysis/Viva (3marks) – **Total 10M**

Semester End Examination (SEE): Max 100 Marks, Duration: 3 Hrs
The question paper shall contain 10 full questions (20 marks each)**,** with 2 questions from each of the 5 Modules, ensuring 100% syllabus coverage. Students shall answer any 5 full questions with 1:1 choice**.** Each question may have a maximum of 4 sub-divisions**.**
Minimum passing Marks: 40% of Max Marks

Department: CSE (Cyber Security)			**Semester:**	**V**
Subject: Cryptography and Network Security				
Subject Code:	**22CY503**	**L – T – P - S:**	**42-0-28-50 (In Hrs.)**	
			Credits:	**4**

Sl. No	**Course Objectives**
1	**Understand** security mechanism with encryption and decryption ciphers.
2	**Illustrate** various security algorithms.
3	To **understand** key management and internet security techniques.
4	**Learn** Application-level security mechanisms.
5	**Implement** network and application-layer security protocols to protect data integrity

Unit	**Description**	**Hrs**
I	**Information and Network Security Concepts:** Cyber security, Information security, and Network security, OSI Security architecture, Security attacks, Security services, Security mechanisms, Cryptography, Network Security, **Classical Encryption Techniques:** Symmetric Cipher Model, Substitution Techniques, Transposition Techniques, Steganography. **T1:** Ch. 1, 2, 3; **R1:** Ch. 1, 2	**8**
II	**Block Cipher and the Data Encryption Standard:** Traditional Block cipher structure, The Data Encryption Standard, The Strength of DES, Block cipher design principles, **Block Cipher Operation:** Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback Mode, Output Feedback Mode. **T1:** Ch. 4, 6; **R1:** Ch. 3	**8**
III	**Number Theory and Public Key Cryptosystem: Number Theory:** Prime Numbers, Fermat's and Euler's Theorems, Testing for Primality. **Public-Key Cryptography and RSA:** Principles of Public- Key Cryptosystems, The RSA Algorithm. **Other Public Key Cryptosystem:** Diffie-Hellman Key Exchange, Elgamal Cryptographic System. **Cryptographic Hash Functions:** Applications of Cryptographic Hash functions, Two simple hash	**8**

	Functions, Secure Hash Algorithm (SHA). **T1:** Ch. 7, 8, 9, 11; **R1:** Ch. 4, 6	
IV	**Message Authentication Codes:** Message Authentication Functions**. Digital Signatures:** Digital Signatures, NIST Digital Signature Algorithm. **Cryptographic Key Management and Distribution:** Distribution of public keys, X.509 Certificates, **User Authentication:** Kerberos**. Transport level security:** Web Security considerations, Transport Layer Security. **T1: Ch. 12, 13, 14, 15; R2: Ch. 7**	**8**
V	**Electronic Mail Security:** Internet Mail Architecture, Email threats and Comprehensive Email Security**. IP Security:** IP Security Overview, IP Security Policy. **Network Endpoint Security:** Firewalls, Intrusion Detection Systems, Malicious Software, Distributed Denial of Service Attacks. **T1:** Ch. 18, 19, 20; **R2:** Ch. 8, 9	**8**

LAB CONTENT:

Sl. No	Experiment Description
1	Program to illustrate Caesar Cipher.
2	Program to illustrate Playfair Cipher.
3	Program to illustrate Hill Cipher.
4	Program to illustrate Vigenère Cipher.
5	Implement the following TRANSPOSITION TECHNIQUES concepts: Rail fence – row & Column Transformation.
6	Implement the DES algorithm.
7	Implement the SHA-1 algorithm.
8	Implement MD5 algorithm.
9	Implement the Signature Scheme - Digital Signature Standard.
10	Implement Fermat's Theorem, Eulers totient function to check primality of a given number.
11	Implement RSA algorithm.
12	Implement Diffie Hellman algorithm.
13	Implement Elgamal cryptosystem.

Course Outcomes:

Course outcome	Descriptions
CO1	**Understand** various encryption and decryption techniques.
CO2	**Apply** public key cryptography algorithms.
CO3	**Identify** cryptographic techniques to achieve confidentiality, authentication.
CO4	Able to **understand** and apply application-level security techniques.
CO5	**Implement** network and application-layer security protocols to protect data integrity, confidentiality, and availability in real-world communication systems.

Course Articulation Matrix:

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

Text Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	Cryptography and Network Security	William Stallings	Eighth Edition, Prentice Hall of India, 2023. ISBN-13 978-9357059718

Reference Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	Cryptography and Network Security	Atul Kahate	Tata McGrawHill, 4th Edition 2019 ISBN-13 978-9353163303
2	Network Security: Private Communication in a Public World	Charlie Kaufman, Radia Perlman, Mike Speciner	Third Edition, 2024 Pearson, Education Asia. ISBN-13 978-8196874339

Course Assessment and Evaluation: Integrated Courses

Continuous Internal Evaluation (CIE): 50 Marks						
Sl.No	**Components**		**Duration(min)**	**Marks Conducted for**	**Marks reduced to**	**40% Min Marks in each component to write SEE**
1	Theory-Internal Assessment	IA-1	90	50	15	12
		IA-2	90	50	15	
2	Periodic Lab Assessment		-	30	10	4
3	Lab CIE		-	20	5	4
4	One Open Ended Experiment /Project		-	10	5	2
	Total CIE			**150**	**50**	**20**

IA-1 Syllabus: 2½ Module , IA-2 Syllabus: 2½ Module
Rubrics for Periodic Lab Assessment: Attendance (5M), Lab record (10 M), Conduction of Experiments(10M) and Viva(5M)-**Total 30M**
Lab CIE: Write-up(5M), Conduction/Execution/Demonstration(10M) and Viva(5M)-**Total 20M**
One Open Ended Experiment /Project: Experimental/project Design (4 marks), Execution/demonstration (3 marks) and Analysis/Viva (3marks) – **Total 10M**

Semester End Examination (SEE): Max 100 Marks, Duration: 3 Hrs
The question paper shall contain 10 full questions (20 marks each)**,** with 2 questions from each of the 5 Modules, ensuring 100% syllabus coverage. Students shall answer any 5 full questions with 1:1 choice**.** Each question may have a maximum of 4 sub-divisions**.**
Minimum passing Marks: 40% of Max Marks

Department: CSE (Cyber Security)			Semester:	V
Subject: Artificial Intelligence in Cyber Security				
Subject Code:	**22CYPE541**	**L – T – P - S:**	**42-0-0-48 (In Hrs.)**	
			Credits:	**3**

Sl. No	Course Objectives
1	To **understand** the application of Artificial Intelligence (AI) in cyber security.
2	To **explore** AI-based threat detection and prediction models.
3	To **apply** Machine Learning (ML) and Deep Learning (DL) techniques in cyber threat analysis.
4	To **design** AI-driven cyber defense mechanisms.
5	To **study** real-world AI applications in malware analysis, intrusion detection, and phishing detection.

Unit	Description	Hrs
I	**Module 1: Introduction to AI in Cyber Security** • Role of AI in Cyber Security • Overview of Threat Landscape • AI vs Traditional Security Approaches • AI Algorithms Overview: Supervised, Unsupervised, Reinforcement Learning • Tools & Frameworks (TensorFlow, Scikit-learn, Keras) **T1:** Ch. 1–2; **T2:** Ch. 1–3	**8**
II	**Module 2: Machine Learning Techniques for Threat Detection** • Classification Algorithms: Decision Trees, Random Forests, SVM • Anomaly Detection using Clustering (K-Means, DBSCAN) • Feature Engineering for Threat Data • Case Study: ML in Intrusion Detection System (IDS) **T2:** Ch. 4–7; **R3:** Sections 2–4	**8**
III	**Module 3: Deep Learning for Cyber Security**	**8**

	• Neural Networks and Deep Learning Basics • Convolutional Neural Networks (CNN) for Malware Classification • Recurrent Neural Networks (RNN) for Log Analysis • Autoencoders for Anomaly Detection • Case Study: Deep Learning for Phishing URL Detection **T1:** Ch. 5–7; **R1:** Ch. 3–4	
IV	**Module 4: AI in Network Security and Malware Analysis** • Network Traffic Analysis using AI • Malware Behaviour Analysis • Botnet Detection using AI • Use of Graph Neural Networks in Cyber Security **T1: Ch. 8–9; R2: Ch. 7–8**	**8**
V	**Module 5: AI for Cyber Threat Intelligence and Ethical Considerations** • AI for Threat Intelligence Automation • Natural Language Processing (NLP) in Threat Intelligence • AI in Incident Response and Threat Hunting • Ethical AI Use and Adversarial ML in Cyber Security **T1:** Ch. 10–11; **R1:** Ch. 6; **R3:** Section 5	**8**

Course Outcomes:

Course outcome	Descriptions
CO1	**Understand** the fundamentals and role of AI in Cyber Security
CO2	**Apply** ML techniques to detect and classify cyber threats
CO3	**Analyse** cyber threats using Deep Learning models
CO4	**Evaluate** AI-driven threat intelligence systems and ethical challenges in AI-based security
CO5	**Design** AI-based cyber defense mechanisms integrating ML, DL, and NLP techniques to proactively mitigate evolving cyber threats.

Course Articulation Matrix

PO/PSO CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3												
CO2	3	2	2	2			2	2						
CO3	3	2	3	3	2	2	2	2						
CO4	3	2	3	2	2	2	3	2	2	2	2	2		
CO5	3	3	3	3	2	3	3	2	2			2		

Text Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	"Cyber Security Using Modern Technologies: Artificial Intelligence and the Internet of Things"	Srinivas Mukkamala & Andrew S. Prowell	Springer, 2021
2	"Introduction to Machine Learning with Applications in Information Security"	Mark Stamp	CRC Press, 2018

Reference Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	"Anomaly Detection: A Survey"	Chandola V., Banerjee A., & Kumar V	ACM Computing Surveys.
2	"Guide to Computer Network Security"	Joseph Migga Kizza	Springer.
3	"Artificial Intelligence for Cybersecurity: Techniques, Tools, and Applications"	James Ma Weiming	Wiley, 2020.

Course Assessment and Evaluation: Regular Theory Courses

Continuous Internal Evaluation (CIE): 50 Marks						
Sl.No	**Components**		**Duration (min)**	**Marks Conducted for**	**Marks reduced to**	**40% Min Marks in each component to write SEE**
1	Theory-Internal Assessment	IA-1	90	50	20	16
		IA-2	90	50	20	
2	Activity Based Learning	ABL 1	-	25	5	4
		ABL 2	-	25	5	
Total CIE				150	50	20

IA-1 Syllabus: 2½ Module , IA-2 Syllabus: 2½ Module
Activity Based Learning (ABL): Online course with certification, Hobby project, Simulations, Industrial Visits, Community-Based Learning, Case-study, Problem-Based Learning, Peer Teaching, web page design, student publications, Hackathons, Quiz (Leetcode, GitHub, Hackaranks and company specific quiz), Student Development program (1 week/online or offline), ……Etc

Semester End Examination (SEE): Max 100 Marks, Duration: 3 Hrs
The question paper shall contain 10 full questions (20 marks each)**,** with **2** questions from each of the 5 Modules**,** ensuring 100% syllabus coverage**.** Students shall answer any 5 full questions with 1:1 choice. Each question may have a maximum of 4 sub-divisions.
Minimum passing Marks: 40% of Max Marks

Department: CSE (Cyber Security)			Semester:	V
Subject: Advanced Algorithms				
Subject Code:	22CYPE542	L – T – P - S:	42-0-0-48 (In Hrs.)	
			Credits:	3

Sl. No	Course Objectives
1	**Understand** and apply advanced algorithmic design techniques for complex computational problems in cybersecurity.
2	**Analyze** the efficiency and complexity of various algorithms.
3	**Design** and implement algorithms for secure communication, data integrity, and authentication.
4	**Evaluate** different algorithmic approaches and apply them to develop solutions for real-world cybersecurity challenges.

Unit	Description	Hrs
I	**Foundations of Algorithm Analysis and Cryptographic Algorithms** **Review of Algorithm Analysis:** Asymptotic notations (Big-O, Omega, Theta), recurrence relations, time and space complexity. **Symmetric-Key Cryptography**: Principles of block ciphers (AES overview, modes of operation) and stream ciphers. **Cryptographic Hash Functions:** Properties and common algorithms (SHA-256). **Random Number Generation:** Pseudo-random vs. cryptographically secure random number generators. **T1:** Ch. 2–6; **T2:** Ch. 1–4; **R1:** Ch. 1–5	**9**
II	**Asymmetric Cryptography and Key Management** **Public-Key Cryptography Principles:** Concepts of public/private keys, one-way functions. **RSA Algorithm:** Key generation, encryption, decryption, and basic security considerations. **Diffie-Hellman Key Exchange:** Working principle. **Elliptic Curve Cryptography (ECC):** Overview of principles and advantages. **Digital Signatures:** Principles and common algorithms.	**9**

	Key Management and PKI: Digital Certificates, X.509 standard, Certificate Authorities (CAs). **T1:** Ch. 9–14; **R1:** Ch. 6–10	
III	**Network Security Algorithms and Protocols** **Authentication Algorithms:** Challenge-response protocols, Kerberos overview. **IPSec:** Architecture and security services (AH, ESP). **SSL/TLS:** Handshake protocol, record protocol. **Wireless Security Algorithms:** WPA2/WPA3 overview. **Intrusion Detection Algorithms:** Signature-based vs. Anomaly-based methods (conceptual). **T1:** Ch. 17–21; **R2:** Ch. 5–7	**8**
IV	**Algorithms for Cybersecurity Applications (8 Hours)** **Malware Analysis Algorithms:** Static (disassembly, control flow) and dynamic analysis (sandboxing) techniques. **Forensic Algorithms:** Hashing for integrity, data carving basics. **Access Control Algorithms:** DAC, MAC, RBAC principles. **Secure Coding & Vulnerability Detection**: Introduction to SAST/DAST algorithms. **Blockchain Fundamentals:** Hashing, Merkle trees, consensus algorithms (Proof of Work). **T1:** Ch. 22–23; **T2:** Graphs & hashing; **R2:** Ch. 8–10	**8**

Course Outcomes:

Course outcome	Descriptions
CO1	**Apply** algorithmic techniques for solve cybersecurity problems.
CO2	**Analyze** the efficiency and security cryptographic and network security algorithms.
CO3	**Design** and implement algorithms for secure communication and authentication.
CO4	**Evaluate** detection techniques and develop solutions for real-world cybersecure solutions.
CO	**Apply** emerging paradigms like homomorphic encryption, quantum cryptography, and zero-knowledge proofs.

Course Articulation Matrix:

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

Text Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	Cryptography and Network Security: Principles and Practice	William Stallings	Pearson Education latest edition
2	Introduction to Algorithms	Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein,	MIT Press. (Latest Edition)

Reference Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	Handbook of Applied Cryptography	Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone	CRC Press.
2	Software Security: Building Security In	Gary McGraw	Addison-Wesley Professional.

Course Assessment and Evaluation: Regular Theory Courses

Continuous Internal Evaluation (CIE): 50 Marks						
Sl. No	**Components**		**Duration (min)**	**Marks Conducted for**	**Marks reduced to**	**40% Min Marks in each component to write SEE**
1	Theory-Internal Assessment	IA-1	90	50	20	16
		IA-2	90	50	20	
2	Activity Based Learning	ABL 1	-	25	5	4
		ABL 2	-	25	5	
Total CIE				150	50	20

IA-1 Syllabus: 2½ Module , IA-2 Syllabus: 2½ Module
Activity Based Learning (ABL): Online course with certification, Hobby project, Simulations, Industrial Visits, Community-Based Learning, Case-study, Problem-Based Learning, Peer Teaching, web page design, student publications, Hackathons, Quiz (Leetcode, GitHub, Hackaranks and company specific quiz), Student Development program (1 week/online or offline), ……Etc

Semester End Examination (SEE): Max 100 Marks, Duration: 3 Hrs
The question paper shall contain 10 full questions (20 marks each)**,** with **2** questions from each of the 5 Modules**,** ensuring 100% syllabus coverage**.** Students shall answer any 5 full questions with 1:1 choice. Each question may have a maximum of 4 sub-divisions.
Minimum passing Marks: 40% of Max Marks

Department: CSE (Cyber Security)			Semester:	V
Subject: Identity & Access Management				
Subject Code:	22CY5PE43	L – T – P - S:	42-0-0-48 (In Hrs.)	
			Credits:	3

Sl. No	Course Objectives
1	**Identity** lifecycle, governance and compliance requirements.
2	**Authentication** and federation (SSO, SAML, OAuth2/OIDC).
3	**Implement** role-based access control, provisioning and privileged access controls.
4	**Apply** practical IAM tooling concepts.

Module	Description	Hrs
I	**Foundations & Identity Lifecycle** Overview of identity vs. access, identity types (human, machine, device), identity lifecycle (on-boarding → provisioning → entitlement → review → off-boarding), identity stores (LDAP, AD, cloud directories), identifiers and attributes, identity assurance levels. T1: Ch 1,2 T2: Ch 1,2	8
II	**Authentication & MFA**: Authentication factors, password best-practices, hashing & salting, multi-factor authentication (push, TOTP, hardware tokens, biometrics), authentication protocols (Kerberos basics, RADIUS), risk-based and adaptive authentication. T1: Ch 3,4 T2: Ch 4,5	8
III	**Authorization & Access Control Models** Access control models: DAC, MAC, RBAC, ABAC; role engineering and role mining; separation of duties (SoD); policy languages & engines (XACML basics); privilege escalation, least privilege. T1: Ch 5 T2: Ch 3,6	8

IV	**Federation, SSO & Modern Protocols** Federated identity concepts, Identity Provider (IdP) / Service Provider (SP) models; SAML 2.0 overview, OAuth 2.0 flows, OpenID Connect; JWT structure; provisioning protocols (SCIM); integrating cloud apps and SaaS. T1: Ch 6,7 T2: Ch 7	**8**
V	**IAM Governance, PAM, Auditing & Emerging Topics** IAM governance: policies, access review, certification, attestation; privileged access management (PAM) concepts; identity analytics (detecting privilege creep); IAM metrics/KPIs; compliance (ISO, NIST, privacy); trends: identity orchestration, password less, decentralized identity. T1: Ch 8,9 T2: Ch 8,9	**8**

Text Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	Identity and Access Management: Business Performance Through Connected Intelligence	Ertem Osmanoglu, Syngress / Elsevier	2013.
2	Access Control and Identity Management	Mike Chapple, Jones & Bartlett Learning	3rd Edition, 2020

Reference Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	Digital Identity: Unmasking Identity Management Architecture (IMA)	Phillip J. Windley, O'Reilly	2020
2	Microsoft Learn / SC-300 course materials	Microsoft Identity & Access Administration	CRC Press, 2020.

Course Outcomes:

Course outcome	Descriptions
CO1	**Describe** identity lifecycle, authentication, authorization models and IAM terminology.
CO2	**Design** secure authentication and federation solutions using SAML / OAuth2 / OIDC.
CO3	**Apply** RBAC/ABAC and provisioning concepts to model access for an enterprise scenario.
CO4	**Evaluate** IAM governance, compliance and risk controls (access reviews, SoD, audit trails).
CO5	**Demonstrate** basic IAM tasks using tools and produce an access-control / PAM design report

Course Articulation Matrix:

PO/PSO CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2
CO1	3	2	1	2	1	1	1	1	1	1	1		
CO2	3	3	2	2	1	1	1	1	1	2	1		
CO3	3	3	3	2	1	1	2	1	1	2	1		
CO4	2	3	2	3	2	2	1	1	2	1	1		
CO5	3	2	2	2	2	1	2	1	1	1	1		

Course Assessment and Evaluation: Regular Theory Courses

Continuous Internal Evaluation (CIE): 50 Marks						
Sl. No	**Components**		**Duration (min)**	**Marks Conducted for**	**Marks reduced to**	**40% Min Marks in each component to write SEE**
1	Theory-Internal Assessment	IA-1	90	50	20	16
		IA-2	90	50	20	
2	Activity Based Learning	ABL 1	-	25	5	4
		ABL 2	-	25	5	
Total CIE				150	50	20

IA-1 Syllabus: 2½ Module , IA-2 Syllabus: 2½ Module
Activity Based Learning (ABL): Online course with certification, Hobby project, Simulations, Industrial Visits, Community-Based Learning, Case-study, Problem-Based Learning, Peer Teaching, web page design, student publications, Hackathons, Quiz (Leetcode, GitHub, Hackaranks and company specific quiz), Student Development program (1 week/online or offline), ……Etc

Semester End Examination (SEE): Max 100 Marks, Duration: 3 Hrs
The question paper shall contain 10 full questions (20 marks each)**,** with **2** questions from each of the 5 Modules**,** ensuring 100% syllabus coverage**.** Students shall answer any 5 full questions with 1:1 choice. Each question may have a maximum of 4 sub-divisions.
Minimum passing Marks: 40% of Max Marks

Department: CSE (Cyber Security)			Semester:	V
Subject: Cyber Security Fundamentals				
Subject Code:	22CYOE551	L – T – P - S:	42-0-0-48 (In Hrs.)	
			Credits:	3

Sl. No	Course Objectives
1	**Develop** an understanding of cybersecurity fundamentals, threat landscape, and security principles.
2	**Learn** to identify, assess, and manage cybersecurity risks in using systematic methods.
3	To **provide** hands-on experience with essential cybersecurity tools and best practices to protect digital assets.
4	To **understand** the ethical, legal, and social implications of cybersecurity, including privacy responsible disclosure practices.

Unit	Description	Hrs
I	**Module 1: Cybersecurity Fundamentals and Threat Landscape:** **Introduction to Cybersecurity:** Definition, importance, and scope of cybersecurity **Information Security Triad:** Confidentiality, Integrity, and Availability (CIA) **Cybersecurity vs Information Security:** Distinctions and overlaps **Threat Landscape Overview:** Current cybersecurity statistics, trends, and predictions **Types of Cyber Threats:** Malware, phishing, social engineering, advanced persistent threats (APTs) **Cybersecurity Stakeholders:** Individuals, organizations, governments, and international bodies **Digital Footprint and Privacy:** Understanding personal digital exposure and privacy implications **Case Studies:** Major cybersecurity incidents and their impact (Equifax, SolarWinds, Colonial Pipeline) Indian cybersecurity incidents and national response	7

	Social media privacy breaches and consequences **T1: Ch. 1–3; T2: Ch. 1–2; R1: Ch. 1–2**	
II	**Module 2: Network Security and Cyber Attacks:** **Network Security Fundamentals:** TCP/IP security issues, common network vulnerabilities **Network Attack Types:** Denial of Service (DoS) and Distributed DoS (DDoS) Man-in-the-Middle (MitM) attacks Packet sniffing and network reconnaissance Wireless network attacks (Wi-Fi security issues) **Web Application Security:** OWASP Top 10 vulnerabilities SQL injection, cross-site scripting (XSS) Session hijacking and authentication bypass **Email Security:** Phishing, spear phishing, email spoofing **Mobile Security:** Mobile malware, app security, BYOD concerns **T1: Ch. 4–6; T2: Ch. 3–5; R2: Ch. 1–3**	**8**
III	**Module 3: Cryptography and Data Protection** **Cryptography Basics:** History, importance, and applications **Symmetric vs Asymmetric Cryptography:** Key differences, use cases, strengths, and weaknesses **Hashing and Digital Signatures:** Message integrity, authentication, non-repudiation **Public Key Infrastructure (PKI):** Digital certificates, certificate authorities, trust models **Data Protection Techniques:** Data classification and handling Encryption at rest and in transit Backup and recovery strategies Data loss prevention (DLP) **Privacy Technologies:** VPNs, Tor, anonymous communication **Emerging Cryptography:** Quantum cryptography basics, post-quantum cryptography **T1: Ch. 7–9; T2: Ch. 6–7**	**8**
IV	**Module 4: Cybersecurity Governance and Risk Management** **Risk Management Fundamentals:** Risk identification, assessment, mitigation, and monitoring **Cybersecurity Frameworks:** NIST Cybersecurity Framework	**8**

	ISO 27001/27002 overview Indian cybersecurity frameworks and guidelines **Compliance and Regulations:** Indian IT Act 2000 and amendments Personal Data Protection Bill implications Industry-specific regulations (banking, healthcare, etc.) **Security Policies and Procedures:** Information security policy development Acceptable use policies Incident response procedures **Business Continuity and Disaster Recovery:** Planning for cybersecurity incidents **Cybersecurity Metrics and Reporting:** KPIs, dashboards, executive reporting **T1: Ch. 10–12; T2: Ch. 8–9**	
V	**Module 5: Incident Response and Emerging Technologies:** **Incident Response Process:** Incident identification and classification Containment, eradication, and recovery, Lessons learned and process improvement **Digital Forensics Basics:** Evidence collection, chain of custody, forensic tools **Cybersecurity Awareness and Training:** Human factors in cybersecurity Security awareness program development Social engineering defence **Emerging Technologies and Security:** Cloud security fundamentals Internet of Things (IoT) security challenges Artificial Intelligence and Machine Learning in cybersecurity Blockchain security implications **Career Paths in Cybersecurity:** Roles, skills, certifications, and career development **Ethical Hacking and Responsible Disclosure:** Bug bounty programs, vulnerability disclosure T1: Ch. 13–15; T2: Ch. 10–12; R2: Ch. 5–6	**8**

Course Outcomes

Course outcome	Descriptions
CO1	**Analyze** Cybersecurity Threats and Vulnerabilities.
CO2	**Apply** Security Controls and Countermeasures.
CO3	**Evaluate** Cybersecurity Frameworks.
CO4	**Demonstrate** Ethical Cybersecurity Practices
CO5	**Investigate** emerging cybersecurity technologies and career opportunities.

Course Articulation Matrix:

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

Text Books:

Sl. No	Text Book title	Author	Volume and Year of Edition
1	Cybersecurity Essentials	Charles J. Brooks, Christopher Grow, Philip Craig, and Donald Short	Wiley, 2022
2	Introduction to Computer Security" (1st Edition)	Michael T. Goodrich and Roberto Tamassia	Pearson, 2020

Reference Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	The Art of Deception: Controlling the Human Element of Security	Kevin D. Mitnick and William L. Simon	Wiley, 2002
2	Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software	Michael Sikorski and Andrew Honig	Starch Press, 2012

Course Assessment and Evaluation: Regular Theory Courses

Continuous Internal Evaluation (CIE): 50 Marks						
Sl. No	**Components**		**Duration (min)**	**Marks Conducted for**	**Marks reduced to**	**40% Min Marks in each component to write SEE**
1	Theory-Internal Assessment	IA-1	90	50	20	16
		IA-2	90	50	20	
2	Activity Based Learning	ABL 1	-	25	5	4
		ABL 2	-	25	5	
Total CIE				150	50	20

IA-1 Syllabus: 2½ Module , IA-2 Syllabus: 2½ Module
Activity Based Learning (ABL): Online course with certification, Hobby project, Simulations, Industrial Visits, Community-Based Learning, Case-study, Problem-Based Learning, Peer Teaching, web page design, student publications, Hackathons, Quiz (Leetcode, GitHub, Hackaranks and company specific quiz), Student Development program (1 week/online or offline), ……Etc

Semester End Examination (SEE): Max 100 Marks, Duration: 3 Hrs
The question paper shall contain 10 full questions (20 marks each)**,** with **2** questions from each of the 5 Modules**,** ensuring 100% syllabus coverage**.** Students shall answer any 5 full questions with 1:1 choice. Each question may have a maximum of 4 sub-divisions.
Minimum passing Marks: 40% of Max Marks

Department: CSE (Cyber Security)			**Semester:**	**V**
Subject: Research Methodology				
Subject Code:	**22IE561**	**L – T – P - S:**	**28-0-0-32 (In Hrs.)**	
			Credits:	**2**

Sl. No	Course Objectives
1	To give an overview of the research methodology and explain the technique of defining a research problem.
2	To explain carrying out a literature search, its review and to explain various research designs and their characteristics.
3	To explain the details of sampling designs, and also different methods of data collections.
4	To develop theoretical, conceptual frameworks, writing a review, to explain the art of interpretation and the art of writing research reports.

Unit	Description	Hrs
I	**Research Methodology:** Introduction, Meaning of Research, Objectives of Research, Motivation in Research, Types of Research, Research Approaches, Significance of Research, Research Methods versus Methodology, Research and Scientific Method, Importance of Knowing How Research is Done, Research Process, Criteria of Good Research, and Problems Encountered by Researchers in India. **Defining the Research Problem:** Research Problem, Selecting the Problem, Necessity of Defining the Problem, Technique Involved in Defining a Problem, An Illustration. **T1:** Ch. 1–3	**6hrs**

II	**Reviewing the literature:** Place of the literature review in research, bringing clarity and focus to your research problem, improving research methodology, Broadening knowledge base in research area, enabling contextual findings, how to review the literature, searching the existing literature, reviewing the selected literature, developing a theoretical framework, developing a conceptual framework, Writing about the literature reviewed. **T2:** Ch. 3–4; **R2:** Ch. 1–4	**5hrs**
III	**Research Design:** Meaning of Research Design, Need for Research Design, Features of a Good Design, Important Concepts Relating to Research Design, Different Research Designs, Basic Principles of Experimental Designs, Important Experimental Designs. **Design of Sample Surveys:** Introduction, Sample Design, Sampling and Non-sampling Errors, Sample Survey versus Census Survey, Types of Sampling Designs. **T1:** Ch. 4–5	**7hrs**
IV	**Data Collection**: Experimental and Surveys, Collection of Primary and Secondary Data, Selection of Appropriate Method for Data Collection, Case Study Method. **Hypothesis-** Basic concepts, types of hypothesis, Formulation of hypothesis, testing of hypothesis, Analysis of data, **Interpretation of data-** Meaning of Interpretation, Technique of Interpretation, Precaution in Interpretation, Editing, classification and tabulation. **T1:** Ch. 6–7	**6hrs**
V	Report Writing: Significance of Report Writing, Different Steps in Writing Report, Layout. Types of Reports, Oral Presentation, Mechanics of Writing a Research Report, Precautions for Writing Research Reports. Research ethics, Citations, Similarity check. T1: Ch. 8–9; R1: Ch. 10	**4hrs**

Course outcome:

Course outcome	Descriptions
CO1	At the end of the course the student will be able to: Discuss research methodology and the technique of defining a research problem
CO2	Explain the functions of the literature review in research, carrying out a literature search
CO3	Developing theoretical and conceptual frameworks and writing a review
CO4	Explain various research designs, their characteristics. explain the art of interpretation and the art of writing research reports
CO5	Apply research ethics, proper citation practices, and plagiarism prevention techniques in preparing research reports and presentations.

Course Articulation Matrix:

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

Text Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	Research Methodology: Methods and Techniques	C.R. Kothari, GauravGarg	New Age International 4th Edition, 2018
2	Research Methodology a step- by-step guide for beginners. (For the topic Reviewing the literature under module 2	Ranjit Kumar	SAGE Publications Ltd. 3rd Edition, 2011

Reference Books:

Sl. No	Reference Book Title	Author	Volume and Year of Edition
1	Research Methods: the concise knowledge base	Trochim	Atomic Dog Publishing2005
2	Conducting Research Literature Reviews: From the Internet to Paper	Fink A	Sage Publications 2009

Course Assessment and Evaluation: Regular Theory Courses

Continuous Internal Evaluation (CIE): 50 Marks						
Sl. No	**Components**		**Duration (min)**	**Marks Conducted for**	**Marks reduced to**	**40% Min Marks in each component to write SEE**
1	Theory-Internal Assessment	IA-1	90	50	20	16
		IA-2	90	50	20	
2	Activity Based Learning	ABL 1	-	25	5	4
		ABL 2	-	25	5	
Total CIE				150	50	20

IA-1 Syllabus: 2½ Module , IA-2 Syllabus: 2½ Module
Activity Based Learning (ABL): Online course with certification, Hobby project, Simulations, Industrial Visits, Community-Based Learning, Case-study, Problem-Based Learning, Peer Teaching, web page design, student publications, Hackathons, Quiz (Leetcode, GitHub, Hackaranks and company specific quiz), Student Development program (1 week/online or offline), ……Etc

Semester End Examination (SEE): Max 100 Marks, Duration: 3 Hrs
The question paper shall contain 10 full questions (20 marks each)**,** with **2** questions from each of the 5 Modules**,** ensuring 100% syllabus coverage**.** Students shall answer any 5 full questions with 1:1 choice. Each question may have a maximum of 4 sub-divisions.
Minimum passing Marks: 40% of Max Marks

Department: CSE (Cyber Security)			Semester:	V
Subject: Management and Entrepreneurship				
Subject Code:	22IE562	L - T - P -S:	28-0-0-32 (In Hrs.)	
			Credits:	2

Sl. No	Course Objectives
1	**Explain** fundamentals of management, functions of a manager. Also explain planning, organizing, and staffing, decision making processes and explain the organizational structure.
2	**Describe** the understanding of motivation and different control systems in management, leadership process, understanding of Entrepreneurship and its development process.
3	**Illustrate** Small Scale Industries, various types of supporting agencies and financing available for an entrepreneur and summarize the preparation of project report, need significance of report. Also to explain about industrial ownership.
4	To **explain** various forms of the intellectual property, its relevance and business impact in the changing global business environment and to discuss leading International Instruments concerning Intellectual Property Rights.

Unit	Description	Hrs
I	**Introduction** - Meaning, nature and characteristics of management, scope and Functional areas of management, goals of management, levels of management, **Planning-** Nature, importance, types of plans, steps in planning, **Organizing-** nature and purpose, types of Organization, Staffing- meaning, process of recruitment and selection. **Directing and controlling**- meaning and nature of directing, leadership styles, motivation Theories, Communication- Meaning and importance, Coordination meaning and importance, Controlling- meaning, steps in controlling, methods of establishing control. **T1:** Ch. 1–6, 8–10; **R1:** Ch. 1–3	6 hrs

II	**Entrepreneur** — meaning of entrepreneur, characteristics of entrepreneurs, classification and types of entrepreneurs, various stages in entrepreneurial process, role of entrepreneurs in economic development, entrepreneurship in India and barriers to entrepreneurship. Identification of business opportunities, market feasibility study, technical feasibility study, financial feasibility study and social feasibility study. **R2:** Ch. 1–4**; T1:** Ch. 16	**5 hrs**
III	**Preparation of project and ERP (Enterprise resource planning)** - meaning of project, project identification, project selection, project report, need and significance of project report, contents, formulation, guidelines by planning commission for project report, Enterprise Resource Planning: Meaning and Importance-ERP and Functional areas of Management — Marketing / Sales-Supply Chain Management — Finance and Accounting — Human Resources — Types of reports and methods of report generation. **R2:** Ch. 5–6; **R3:** Ch. 12; **T1:** Ch. 18	**5hrs**
IV	**Micro and Small Enterprises:** Definition of micro and small enterprises, characteristics and advantages of micro and small enterprises, steps in establishing micro and small enterprises, Government of India indusial policy 2007 on micro and small enterprises, case studies in respective domains. Institutional support: MSME-DI, NSIC, SIDBI, KIADB, KSSIDC, TECSOK, KSFC, DIC and District level single window agency. **R3:** Ch. 14; **R2:** Ch. 7–8	**6hrs**
V	**Intellectual Property:** Introduction to IP: Importance of IPR, International conventions / agreements / treaties, Origin of IP law and history, laws related to IP in India: Indian Patent Act 1970, WIPO. **Patents:** Criteria for patentability, patentable and non-Patentable Matters, introduction to Prior Art Search, types of patent application: ordinary, convention, PCT, divisional and Patent of addition, filing procedure, drafting complete specification and claims. **Copyright:** Criteria, filing procedure, Copyright Infringement, rights of authorship and ownership, Fair Use, first sale doctrine, moral rights and economic rights. **Trademarks:** definition, eligibility Criteria, types of patents, filing procedure, Classification of Trademarks and well-known mark	**6hrs**

	Geographical Indications: Definitions, importance, filing procedure, GI ecosystem in India and case laws **Industrial design:** eligibility criteria, Non- Protectable Industrial Designs India, Procedure for Registration, importance of design registration. T2: Ch. 1–7	

Course Outcomes:

Course outcome	Descriptions
CO1	**Explain** management functions of a manager. Also explain planning and decision-making processes. Organizational structure, staffing and leadership processes.
CO2	**Describe** the understanding of motivation and different control systems in management and understanding of Entrepreneurships and its development process.
CO3	**Illustrate** Small Scale Industries, various types of supporting agencies and financing available for an entrepreneur. Summarize the preparation of project report, need significance of report.
CO4	Shall get an adequate knowledge on patent and copyright for their innovative research works and provides further the way for developing their idea for innovations.
CO5	**Apply** knowledge of Intellectual Property Rights (IPR) to protect innovative ideas, assess patentability, and comply with legal and ethical standards in entrepreneurship and research.

Course Articulation Matrix:

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

Text Books:

Sl.No	Text Book title	Author	Volume and Year of Edition
1	Principles of Management	P. C. Tripathi, P. N. Reddy	Tata McGraw Hill, 4th / 6th Edition, 2010.
2	Intellectual property rights - Unleashing the knowledge economy	Pmbuddha Ganguli	Tata MccrawHiU Publishing Company Ltd

Reference Books:

Sl.No	Reference Book Title	Author	Volume and Year of Edition
1	Management and Entrepreneurship	Kanishka Bedi	Oxford University Press-2017
2	Entrepreneurship Development	S S Khanka	S Chand & Co.
3	Dynamics of Entrepreneurial Development & Management -	Vasant Desai	Himalaya Publishing House

Course Assessment and Evaluation: Regular Theory Courses

Continuous Internal Evaluation (CIE): 50 Marks						
Sl. No	**Components**		**Duration (min)**	**Marks Conducted for**	**Marks reduced to**	**40% Min Marks in each component to write SEE**
1	Theory-Internal Assessment	IA-1	90	50	20	16
		IA-2	90	50	20	
2	Activity Based Learning	ABL 1	-	25	5	4
		ABL 2	-	25	5	
Total CIE				150	50	20

IA-1 Syllabus: 2½ Module , IA-2 Syllabus: 2½ Module

Activity Based Learning (ABL): Online course with certification, Hobby project, Simulations, Industrial Visits, Community-Based Learning, Case-study, Problem-Based Learning, Peer Teaching, web page design, student publications, Hackathons, Quiz (Leetcode, GitHub, Hackaranks and company specific quiz), Student Development program (1 week/online or offline), ……Etc

Semester End Examination (SEE): Max 100 Marks, Duration: 3 Hrs

The question paper shall contain 10 full questions (20 marks each)**,** with **2** questions from each of the 5 Modules**,** ensuring 100% syllabus coverage**.** Students shall answer any 5 full questions with 1:1 choice. Each question may have a maximum of 4 sub-divisions.

Minimum passing Marks: 40% of Max Marks

Department: CSE (Cyber Security)			Semester :	V
Subject: Project Management				
Subject Code:	**22IE563**	**L – T – P - S:**	**28-0-0-32 (In Hrs.)**	
			Credits:	**2**

Sl. No	Course Objectives
1	To **understand** the scope, timing and quality of the project, and to analyze the project goals, constraints, deliverables, performance criteria, control needs and resource requirement in consultation with stake holders.
2	To **implement** the process of project management, life cycle and the embodied concepts, tools and techniques in order to achieve project success.
3	To **understand** the team efforts and stakeholders in professional manner, respecting differences, to ensure a collaborative project environment.
4	To **apply** project management practices to new programs, initiatives, products, services and events relative to the needs of stakeholders.

Unit	Description	Hrs
I	**Introduction:** Project, Program, and portfolio, Operations management, Product life cycle, Project life cycle, Project management life cycle, Role of project manager and office, Ten Project Knowledge areas with their associated processes **Project Integration Management:** Develop project charter, develop project management plan, Direct & manage project work, monitor control project, Perform integrated change control, Close project / phase. **T1:** Ch.1–4 | **T2:** Ch.1–2	**6hrs**

II	**Project scope management:** Plan scope management, collect requirements, define scope, Create WBS (Work Breakdown Structure), Validate Scope, Control scope. **Project Schedule management: Plan Schedule management** Define activities, Sequence activities, Estimate activity durations, Develop schedule, and Control schedule. **T1:** Ch.5–6 | **T2:** Ch.3, 5	**5hrs**
III	**Project cost management:** Plan cost management, estimate cost, Determine budget, and Control costs. Project quality management: Plan quality management, manage quality and Control quality **Project resource management:** Plan resource management, estimate activity resources, acquire resources, develop team, Manage team and Control resources. **T1:** Ch.7–9 | **T2:** Ch.6–8	**6 hrs**
IV	**Project communication management:** Plan communication management, manage communications and Monitor communications Project risk management: Plan risk management, identify risks, perform qualitative risk analysis, perform quantitative risk analysis, Plan risk responses, Implement risk responses and Monitor risks. Project Procurement management: Plan procurement management, Conduct procurement, Control procurements. **T1:** Ch.10–12 | **T2:** Ch.9–11	**6hrs**
V	**Project stake holder management:** Identify stake holders, Plan stake holder management, Manage stake holder engagement, and Monitor stake holder engagement. A case study relevant to the domain knowledge of the department is taken up to explain the principles of the project management as brought out above. **T1:** Ch.13 | **T2:** Ch.12	**5hrs**

Course outcomes:

Course outcome	Descriptions
CO1	**Outline** the procedure for analysing a project and define the rational of work break structure
CO2	**Illustrate** the use of network techniques for successful project implementation
CO3	**Design** the procedure for overall financial analysis of the project alongside the resource's requirement and ideal quality
CO4	I**dentify** the sources and process for communication, risk management and procurement and build a comprehensive plan for the stakeholder
CO5	**Apply** integrated project management principles through domain-specific case studies to evaluate stakeholder engagement, project success factors, and continuous improvement strategies.

Course Articulation Matrix:

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

Text Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	Project Management Body of Knowledge	Book of Knowledge	6th Edition, PMI, USA
2	Project Management	Dennis Lock	Taylor & Francis 10th Edition- 2013

Reference Book

Sl No	Reference Books Title	Author	Volume and Year of Edition
1	Project Planning: Analysis, Selection, Implementation and Review,	Prasanna Chandra	MC- Graw Hill Education, 8th Edition, 2017.
2	Project Management-a system approach to planning, scheduling & controlling	Harold Kerzner	CBS publications and Distributions,2002

Course Assessment and Evaluation: Regular Theory Courses

Continuous Internal Evaluation (CIE): 50 Marks						
Sl. No	**Components**		**Duration (min)**	**Marks Conducted for**	**Marks reduced to**	**40% Min Marks in each component to write SEE**
1	Theory-Internal Assessment	IA-1	90	50	20	16
		IA-2	90	50	20	
2	Activity Based Learning	ABL 1	-	25	5	4
		ABL 2	-	25	5	
Total CIE				150	50	20

IA-1 Syllabus: 2½ Module , IA-2 Syllabus: 2½ Module
Activity Based Learning (ABL): Online course with certification, Hobby project, Simulations, Industrial Visits, Community-Based Learning, Case-study, Problem-Based Learning, Peer Teaching, web page design, student publications, Hackathons, Quiz (Leetcode, GitHub, Hackaranks and company specific quiz), Student Development program (1 week/online or offline), ……Etc

Semester End Examination (SEE): Max 100 Marks, Duration: 3 Hrs
The question paper shall contain 10 full questions (20 marks each)**,** with **2** questions from each of the 5 Modules**,** ensuring 100% syllabus coverage**.** Students shall answer any 5 full questions with 1:1 choice. Each question may have a maximum of 4 sub-divisions.
Minimum passing Marks: 40% of Max Marks

Department: CSE (Cyber Security)			Semester:	V
Subject: Department Skill Lab-3 (Ethical Hacking using Kali Linux)				
Subject Code:	22CY507	L – T – P - S:	14-0-28-18 (In Hrs.)	
			Credits:	2

Sl. No	Course Objectives
1	**Understand** the ethical hacking methodology and professional responsibilities in cybersecurity assessment.
2	**Utilize** the Kali Linux environment effectively.
3	**Perform** systematic reconnaissance and exploitation.
4	**Identify**, assess, and provide remediation strategies vulnerabilities in systems.

Lab Content

Sl. No	Experiment Description
1	Setting up Kali Linux Environment and Virtual Lab Configuration
2	Network Reconnaissance using Nmap and Advanced Scanning Techniques
3	Information Gathering using OSINT Tools and Techniques
4	DNS Enumeration and Subdomain Discovery using Multiple Tools
5	Web Application Vulnerability Scanning using OWASP ZAP and Burp Suite
6	SQL Injection Attack Implementation and Exploitation using SQL map
7	Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF)Attacks
8	Metasploit Framework for System Exploitation and Payload Generation
9	Wireless Network Security Testing using Air crack-ng Suite
10	Social Engineering Attacks using SET (Social Engineering Toolkit)
11	Password Cracking and Hash Analysis using John the Ripper and Hashcat
12	Post-Exploitation Techniques and Privilege Escalation Methods
13	Web Application File Upload Vulnerabilities and Directory Traversal

	Attacks
14	Network Traffic Analysis and Packet Capture using Wireshark
15	Comprehensive Penetration Testing Report Generation and Documentation

Course Outcomes:

Course outcome	Descriptions
CO1	**Configure** Kali Linux setup, and operation for penetration testing.
CO2	**Execute** Comprehensive security assessment including vulnerability scanning and network analysis.
CO3	**Implement** exploitation and post-exploitation techniques (SQL injection, XSS, etc.).
CO4	**Generate** Penetration testing reports with findings, risk assessments, and recommendations.
CO5	**Analyse** and document penetration testing Security reports and countermeasure recommendations to mitigate vulnerabilities.

Course Articulation Matrix

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

Text Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	The Hacker Playbook 3: Practical Guide To Penetration Testing" by	Peter Kim	Secure Planet LLC, 2018
2	Penetration Testing: A Hands-On Introduction to Hacking	Georgia Weidman	No Starch Press, 2014 .

Reference Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	Metasploit: The Penetration Tester's Guide	David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni	No Starch Press, 2011
2	The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws	Dafydd Stuttard and Marcus Pinto	Wiley, 2nd Edition, 2011 .

Course Assessment and Evaluation: Lab (Professional / Programme Core Lab)

Continuous Internal Evaluation (CIE): 50 Marks			
Sl. No	**Components**	**Marks Conducted for**	**40% Min Marks in each component to write SEE**
1	Periodic Lab Assessment	30	12
2	Lab CIE	20	8
	Total CIE	50	20
Rubrics for Periodic Lab Assessment: Attendance (5M), Lab record (10M), Conduction of Experiments(10M) and Viva((5M)-**Total 30M** **Lab CIE:** Write-up(5M), Conduction/Execution/Demonstration(10M) and Viva(5M**)-Total 20M**			
Semester End Examination (SEE): Max 50 Marks, Duration: 3 Hrs **Rubrics for Lab Examination:** Write-up(8M), Conduction/Execution/Demonstration(35M) and Viva(7M)-**Total 50M.** **Minimum passing Marks: 40% of Max Marks**			

Department: CSE (Cyber Security)			Semester:	V
Subject: Skill Development-II (APTITUDE SKILLS)				
Subject Code:	22SK508	L – T – P - S:	14-0-0-16 (In Hrs.)	
			Credits:	1

Sl. No	Course Objectives
1	To **equip** students with quantitative aptitude skills required for competitive exams and placement tests.
2	To **develop** the ability to interpret, analyze, and solve data-driven problems using arithmetic and visual methods.
3	To **enhance** problem-solving strategies in areas such as probability, permutations, combinations, and data sufficiency.
4	To **apply** mathematical and logical concepts in real-world problem-solving scenarios like time, work, and distance.

Module	Description	Hrs
I	**Logical Aptitude** - Syllogism, Venn-diagram method, three statement syllogism, Deductive and inductive reasoning. Introduction to puzzle and games organizing information, parts of an argument, common flaws, arguments and assumptions. **Linear Seating Arrangement** Single or Double rows facing each other or away from each other in the same direction. **Circular Seating Arrangement** · Uni- & Bi-directional problems on · Circular, Square, Rectangular, Hexagonal tables **Coding Decoding:** Letter Coding, Number Coding, symbol coding **Crypt arithmetic:** Basic concepts, addition, subtraction, multiplication of coded alphabets, Types of cryptarithm, Clocks and Calendar **Reasoning** – a. Verbal - Blood Relation, Sense of Direction, Arithmetic & Alphabet.	6

	Non- Verbal reasoning - Visual Sequence, Visual analogy and classification. Analytical Reasoning - Single & Multiple comparisons, Linear Sequencing.	
II	**Permutation and Combination:** Understanding the difference between the permutation and combination, Rules of Counting-rule of addition, rule of multiplication, factorial function, Concept of step arrangement, Permutation of things when some of them are identical, Concept of 2n, Arrangement in a circle. **Probability:** Single event probability, multi event probability, independent events and dependent events, mutually exclusive events, non-mutually exclusive events, combination method for finding the outcomes.	6
III	**Number System** Divisibility & Remainder, · Multiples & Factors, · Integers, · LCM & HCF, · Complete a number Series, · Find the Missing Term and Wrong Term **Simplification** · BODMAS Rule, · Approximation, · Decimals, · Fractions, · Surds & Indices **Percentage** Calculation-oriented basic percentage, Profit and Loss, Successive Selling type, Discount & MP, Dishonest Dealings, Partnerships Interest: Simple Interest, Compound Interest, Mixed Interest, Instalments. **Data Interpretation**: Approach to interpretation - simple arithmetic, rules for comparing fractions, calculating (approximation) fractions, short cut ways to find the percentages, Classification of data– Tables, Bar graph, line graph, Cumulative bar graph, Pie graph, Combination of graphs. Combination of table and graphs	6
IV	**Averages and Allegations mixtures**: Average: relevance of average, meaning of average, properties of average, deviation method, concept of weighted average. Allegation method: a situation where allegation technique, general representation of allegations, the straight-line approach, application of weighted average and allegation method in problems involving mixtures. Application of allegation on situations other than mixtures problems. **Data Sufficiency**: Questions based on > Quantitative aptitude, > Reasoning aptitude> Puzzles	4

V	**Ratio and Proportion** · Simple Ratios, · Compound Ratios, · Comprehend and Dividend · Direct & Indirect Proportions, · Problems on ages, · Mixtures & Allegation **Speed, Time and Distance** · Relative Speed, · Average Speed, · Problems on Train, · Boat & Stream. **Time and Work** Work Efficiency, · Work & Wages, Pipes & Cisterns	6

Note: Mention text book referred along with sections for more clarity in each unit (e.g, Text 1: 2.1,2.5,…Text2: 1.2,2.3)

Text Books:

Sl. No	Text Book title	Author	Volume and Year of Edition
1	How to Prepare for Logical Reasoning for CAT" by Arun Sharma	Arun Sharma	ISBN-10: 9352602280 ISBN-13: 9789352602287
2	A Modern Approach to Verbal & Non-Verbal Reasoning" by R.S. Aggarwal	R.S. Aggarwal	ISBN-10: 8121924987 ISBN-13: 978-8121924986

Reference Books:

Sl. No	Text Book title	Author	Volume and Year of
1	Quantitative Aptitude for Competitive Examinations" by R.S. Aggarwal	R.S. Aggarwal	ISBN-10: 9352534026 ISBN-13: 978-9352534021
2	Logical Reasoning and Data Interpretation for the CAT" by Nishit K. Sinha	Nishit K. Sinha	ISBN-10: 933922269X ISBN-13: 978-9339222694

Course Outcomes:

Course outcome	At the end of the course students will be able to
CO1	**Apply** logical reasoning techniques to solve syllogisms, puzzles, seating arrangements, and coding-decoding problems. (Apply)
CO2	**Solve** permutation, combination, and probability problems using appropriate mathematical principles. (Apply/Analyze)
CO3	**Demonstrate** proficiency in number systems, percentages, interests, profit & loss, and data interpretation. (Apply)
CO4	**Analyze** problems involving averages, mixtures, allegations, and data sufficiency using logical and quantitative methods. (Analyze)
CO5	**Apply** concepts of ratio, proportion, time, speed, distance, and work to solve complex real-life aptitude problems. (Apply/Analyze)

Course Articulation Matrix

PO/PSO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO 1	PO 1	PO 1	PS O	PS O
CO1	3	2				2		3	2					
CO2	3	3	2			2		3	3	2				
CO3	3	2				2		3	2					
CO4	3	3	2			2		3	3	2				
CO5	3	3	2			2		3	3	2				

Course Assessment and Evaluation: Humanities and Social Science Courses (CIP, UHV, Environmental Science, Communicative English, Skill Development)

Sl. No	Components		Duration(min)	Marks Conducted for	Min Marks To pass the Course
1	Theory- Internal Assessment	IA-1	90	50	40
		IA-2	90	50	
	Total CIE			100	40

Scheme of Teaching and Examination-2022 (160 Credits Scheme, NEP)
Outcome Based Education (OBE) and Choice Based Credit System (CBCS)

VI Semester B. E **Academic year: 2025-26**

Sl. No.	Course Code		Course Title	Teaching Dept.	Teaching Hrs.					Credits	Examination			
					L	T	P	S	Total		CIE Marks	SEE Marks	Total Marks	Exam Hrs
1	PC	22CY601	Software Engineering	CY	42	-	-	48	90	3	50	50	100	3
2	PC	22CY602	Cyber Attacks and Defense Strategies	CY	42	-	28	50	120	4	50	50	100	3
3	PC	22CY603	Web Technology and Security	CY	42	-	28	50	120	4	50	50	100	3
4	PE	22 XX 6PE4X	Professional Elective-II	CY	42	-	-	48	90	3	50	50	100	3
5	OE	22 XX6OE5X	Open Elective-II	HS	42	-	-	48	90	3	50	50	100	3
6	PC	22CY66X	Online-Course: NPTEL/MOOC/SWAYAM 22NP661-NPTEL 22MC662-MOOC 22SW663-SWAYAM	CY	-	-	-	60	60	2	-	-	100	-
7	PW	22CYMP607	Mini-project	CY	-	-	42	18	60	2	50	50	100	3
8	HS	22SK608	Preplacement Training	T&P	-	-	28	2	30	1	50	-	50	-
				Total	**210**		**126**	**324**	**660**	**22**	**350**	**300**	**750**	**-**

L: Lecture, T-Tutorial, P-Practical/Drawing, CIE: Continuous Internal Evaluation, SEE: Semester End Examination, S: Self Learning. XX: Branch Code

Credit Distribution: PC: Professional Core-13, PE: Professional Elective-03, OE: Open Elective-03, PW: Project Work-02, HS: Humanity Science-01, **Total=22 Credits**

Department: CSE (Cyber Security)			**Semester:**	**VI**
Subject: Software Engineering				
Subject Code:	**22CY601**	**L – T – P - S:**	**42-0-0-48 (In Hrs.)**	
			Credits:	**3**

Sl. No	**Course Objectives**
1	**To provide a working knowledge of the techniques** used for the estimation, design, testing, and quality management of large-scale software development projects.
2	**To introduce foundational and advanced concepts,** including software process models, requirements engineering, architectural design, testing methodologies, risk and quality management, and UML modeling diagrams.
3	**To provide an understanding of the working knowledge** of the techniques for estimation, design, testing, and quality management of large software development projects.
4	**To cover foundational and advanced topics** including process models, software requirements, software design, software testing, software process/product metrics, risk management, quality management, and UML diagrams.

Module	**Description**	**Hrs**
I	**Introduction to Software Engineering:** The evolving role of software, changing nature of software, software myths. **A Generic view of process:** Software engineering- a layered technology, a process framework, the capability maturity model integration (CMMI), process patterns, process assessment, personal and team process models. Process models: The waterfall model, incremental process models, evolutionary process models, the unified process. **Agile Software Development:** Agile methods, Agile development techniques, Agile project management.	**9**
II	**Software Requirements:** Functional and non-functional	

	requirements, user requirements, system requirements, interface specification, the software requirements document. Requirements engineering process: Feasibility studies, requirements elicitation and analysis, requirements validation, requirements management. System models: Context models, behavioral models, data models, object models, structured methods	**8**
III	**Design Engineering:** Design process and design quality, design concepts, the design model. **Creating an architectural design:** software architecture, data design, architectural styles and patterns, architectural design, conceptual model of UML, basic structural modeling, class diagrams, sequence diagrams, collaboration diagrams, use case diagrams, component diagrams.	**7**
IV	**Testing Strategies:** A strategic approach to software testing, test strategies for conventional software, black-box and white-box testing, validation testing, system testing, the art of debugging. **Product metrics:** Software quality, metrics for analysis model, metrics for design model, metrics for source code, metrics for testing, metrics for maintenance.	**8**
V	**Metrics for Process and Products:** Software measurement, metrics for software quality. **Risk management:** Reactive Vs proactive risk strategies, software risks, risk identification, risk projection, risk refinement, RMMM, RMMM plan. **Quality Management:** Quality concepts, software quality assurance, software reviews, formal technical reviews, statistical software quality assurance, software reliability, the ISO 9000 quality standards	**8**

LAB CONTENT

Sl. No	Experiment Description
1	Development of problem statement
2	Preparation of Software Requirement Specification Document, Design Documents and Testing Phase related documents
3	Preparation of Software Configuration Management and Risk Management related documents.
4	Study and usage of any Design phase CASE tool
5	Performing the Design by using any Design phase CASE tools.
6	Develop test cases for unit testing and integration testing
7	Develop test cases for various white box and black box testing techniques.
	Sample Projects 1. Passport automation System 2. Book Bank 3. Online Exam Registration 4. Stock Maintenance System 5. Online course reservation system 6. E-ticketing 7. Software Personnel Management System 8. Credit Card Processing 9. E-book management System. 10. Recruitment system

Text Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	Software Engineering, A practitioner's Approach	Roger S. Pressman, Bruce R. Maxim	Mc Graw Hill International Edition, 9th edition, 2020 / 2021
2	Software Engineering	Ian Sommerville	Pearson Education Global Edition, 10th edition, 2016

Reference Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	Software Engineering, an Engineering approach	James F. Peters, Witold Pedrycz	Wiley Student Edition, 1st Edition, 1999 / 2000
2	Software Engineering principles and practice	Waman S Jawadekar	Mc Graw-Hill Education, 1st Edition, 2004
3	Fundamentals of object-oriented design using UML Meiler page-Jones:	Meilir Page-Jones	Pearson Education / Addison-Wesley, 1st Edition, 2000

Course Outcomes:

Course outcome	Descriptions
CO1	Ability to translate end-user requirements into system and software requirements, using e.g.UML, and structure the requirements in a Software Requirements Document (SRD).
CO2	Identify and apply appropriate software architectures and patterns to carry out high level design of a system and be able to critically compare alternative choices.
CO3	Gain hands-on experience and awareness of testing problems and develop a comprehensive software testing report.
CO4	Understand and apply software process and product metrics, risk management strategies (RMMM), and quality assurance standards like ISO 9000 to engineering life cycles.

Course Articulation Matrix

PO/PSO CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	3	2	2	1				2	3	1	2	3	2
CO2	3	3	3	2	2				2	2	1	2	3	2
CO3	2	2	2	3	3			1	3	2	1	2	2	3
CO4	2	2	1	2	1	1	1	2	2	2	3	2	2	2

Course Assessment and Evaluation: Regular Theory Courses

Continuous Internal Evaluation (CIE): 50 Marks						
Sl.No	**Components**		**Duration(min)**	**Marks Conducted for**	**Marks reduced to**	**40% Min Marks in each component to write SEE**
1	Theory-Internal Assessment	IA-1	90	50	20	16
		IA-2	90	50	20	
2	Activity Based Learning	ABL 1	-	25	5	4
		ABL 2	-	25	5	
Total CIE				150	50	20

IA-1 Syllabus: 2½ Module , IA-2 Syllabus: 2½ Module
Activity Based Learning (ABL): Online course with certification, Hobby project, Simulations, Industrial Visits, Community-Based Learning, Case-study, Problem-Based Learning, Peer Teaching, web page design, student publications, Hackathons, Quiz (Leetcode, GitHub, Hackaranks and company specific quiz), Student Development program (1 week/online or offline), ……Etc

Semester End Examination (SEE): Max 100 Marks, Duration: 3 Hrs
The question paper shall contain 10 full questions (20 marks each)**,** with **2** questions from each of the 5 Modules**,** ensuring 100% syllabus coverage**.** Students shall answer any 5 full questions with 1:1 choice. Each question may have a maximum of 4 sub-divisions.
Minimum passing Marks: 40% of Max Marks

Department: CSE (Cyber Security)			**Semester:**	**VI**
Subject: Cyber Attacks and Defense Strategies				
Subject Code:	**22CY602**	**L – T – P - S:**	**42-0-28-50 (In Hrs)**	
			Credits	**4**

Sl. No	**Course Objectives**
1	**Identify** and describe various cyber-attack methodologies and their implications.
2	**Apply** vulnerability assessment and penetration testing techniques using appropriate tools.
3	**Analyze** and implement defense mechanisms against different types of cyber threats.
4	**Develop** and enforce security policies in compliance with legal and ethical standards.

Module	**Description**	**Hrs**
I	**Module 1: Introduction to Cyber Security and Threat Landscape** • Overview of cyber security: definitions, importance, and challenges. • Types of cyber threats: malware, phishing, DoS/DDoS attacks, social engineering. • Cyber-attack lifecycle: reconnaissance, weaponization, delivery, exploitation, installation, command and control, actions on objectives. • Case studies of notable cyber-attacks. **Textbook 1 –** Related introductory chapters	**8**
II	. **Module 2: Network Reconnaissance and Vulnerability Scanning** • Network mapping techniques: ICMP queries, TCP pings, port scanning. • Vulnerability scanning tools and methodologies. • Penetration testing: black-box, white-box approaches.	**8**

	• System and network penetration strategies. **Textbook 1** – Scanning & Recon chapters	
III	**Module 3: Protocol Attacks and Défense Mechanisms** • Attacks on network layer protocols: IP spoofing, ARP poisoning. • Transport layer attacks: TCP SYN flooding, UDP flooding. • Application layer vulnerabilities: HTTP attacks, DNS spoofing. • Defense mechanisms: firewalls, intrusion detection/prevention systems, protocol hardening. **Textbook 1 & 2** – Network/Transport/Application layer security	**8**
IV	**Module 4: Malware Analysis and Defense Strategies** • Types of malwares: viruses, worms, trojans, ransomware, spyware. • Malware propagation techniques and payload delivery. • Detection and analysis of malware behavior. • Anti-malware tools and sandboxing techniques. **Textbook 1** – Malware chapters	**8**
V	**Module 5: Security Policies, Auditing, and Legal Frameworks** • Security policy development and implementation. • Security auditing: processes, tools, and compliance standards. • Cyber laws and regulations: IT Act 2000/2008, data protection laws. • Ethical hacking and professional ethics in cyber security. **Textbook 2** – IT Act, policies	**8**

LAB CONTENT

Sl. No	Experiment Description
1	Scan open TCP ports on a given host using Python
2	Extract email addresses from a given web page
3	Banner Grabbing using Python
4	Automate Nmap Scan using Bash
5	Demonstrate ARP spoofing on a local network
6	Encrypt files in a directory using symmetric key using Python
7	Detect repeated 404 errors and flag Ips
8	File Integrity Monitor using inotifywait (Bash)

Text Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	Network Security Essentials: Applications and Standards	William Stallings,	6th edition, 2016, Pearson Education.
2	Cryptography and Network Security	Atul Kahate	3rd edition, 2013, Tata McGraw-Hill.

Reference Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	Computer Security: Art and Science	Matt Bishop	2nd edition, 2003, Pearson Education.
2	Introduction to Computer Security	Michael T. Goodrich and Roberto Tamassia	1st edition, 2014, Pearson Education.

Course Outcomes:

Course outcome	Descriptions
CO1	**Develop** Python and Bash scripts to automate tasks related to reconnaissance, scanning, and foot printing.
CO2	**Implement** common network attacks using scripting tools in a test environment.
CO3	**Simulate** basic malware behavior and understand its impact.
CO4	**Analyze** system and network logs to identify suspicious activities using automated log parsers.
CO5	**Apply** automated log parsing techniques to detect anomalies and generate incident reports.

Course Articulation Matrix

PO/PSO CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2
CO1	3	3	2		2	3	3	2		2	3	3	
CO2	3	2	3	2	2	3	2	3	2	2	3	2	
CO3	3	2	2	2	2	-	3	2	2	2	2		
CO4	3	3	2	3	2	3	3	2	3	2	3		
CO5	3	3	3	3	2	3	2	3	2	3			

Course Assessment and Evaluation: Integrated Courses

Continuous Internal Evaluation (CIE): 50 Mark						
Sl.No	**Components**		**Duration (min)**	**Marks Conducted for**	**Marks reduced to**	**40% Min Marks in each component to write SEE**
1	Theory-Internal Assessment	IA-1	90	50	15	12
		IA-2	90	50	15	
2	Periodic Lab Assessment		-	30	10	4
3	Lab CIE		-	20	5	4
4	One Open Ended Experiment /Project		-	10	5	2
	Total CIE			**150**	**50**	**20**

IA-1 Syllabus: 2½ Module , IA-2 Syllabus: 2½ Module
Rubrics for Periodic Lab Assessment: Attendance (5M), Lab record (10 M), Conduction of Experiments(10M) and Viva(5M)-**Total 30M**
Lab CIE: Write-up(5M), Conduction/Execution/Demonstration(10M) and Viva(5M)-**Total 20M**
One Open Ended Experiment /Project: Experimental/project Design (4 marks), Execution/demonstration (3 marks) and Analysis/Viva (3marks) – **Total 10M**

Semester End Examination (SEE): Max 100 Marks, Duration: 3 Hrs
The question paper shall contain 10 full questions (20 marks each)**,** with 2 questions from each of the 5 Modules, ensuring 100% syllabus coverage. Students shall answer any 5 full questions with 1:1 choice**.** Each question may have a maximum of 4 sub-divisions**.**
Minimum passing Marks: 40% of Max Marks

Department: CSE (Cyber Security)	**Semester:**	**VI**

Subject: Web Technology and Security				
Subject Code:	**22CY603**	**L – T – P - S:**	**42-0-28-50 (In Hrs)**	
			Credits	**4**

Sl. No	**Course Objectives**
1	**Understand** the fundamentals of web technologies and their applications.
2	**Learn** about web security principles and practices.
3	**Develop** secure web applications using modern technologies.
4	**Identify** and mitigate common web vulnerabilities.

Module	**Description**	**Hrs**
I	**Introduction to Web Technologies** • Overview of web architecture • Client-server model • HTTP/HTTPS protocols • Web browsers and servers **Textbook 1** – HTML/HTTP intro chapters	**8**
II	**Front-End Development** • HTML5: Structure and semantics • CSS3: Styling and layouts • JavaScript: DOM manipulation and event handling • Responsive design principles **Textbook 1** – Front-end dev chapters	**8**
III	**Back-End Development** • Server-side scripting with PHP/Node.js • Database connectivity using MySQL/MongoDB • Session management and cookies • RESTful API development	**8**

	Textbook 1 – PHP/Node.js, DB integration	
IV	**Web Security Fundamentals** • Authentication and authorization mechanisms • Secure communication using SSL/TLS • Input validation and sanitization • Error handling and logging **Textbook 2** – SSL/TLS, Input validation	**8**
V	**Common Web Vulnerabilities** • Cross-Site Scripting (XSS) • Cross-Site Request Forgery (CSRF) • SQL Injection • Security tools and best practices **Textbook 2** – XSS, CSRF, SQL Injection	**8**

LAB CONTENT

Sl. No	Experiment Description
1	Design a static website using HTML and CSS.
2	Implement form validation using JavaScript.
3	Develop a dynamic web application using PHP/Node.js.
4	Connect a web application to a database and perform CRUD operations.
5	Implement user authentication and session management.
6	Demonstrate SQL injection and implement prevention techniques.
7	Demonstrate XSS and CSRF attacks and implement mitigation strategies.
8	Configure HTTPS for secure communication.

Text Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	Web Technologies: HTML, JavaScript, PHP, Java, JSP, ASP.NET, XML and Ajax, Black Book	Kogent Learning Solutions Inc.	Dreamtech Press, 1st Edition Publication Year: 2009 ISBN: 9788177229974
2	Cryptography, Network Security, and Cyber Laws	Bernard L. Menezes & Ravinder Kumar	Cengage Learning India 1st Edition, 2018 ISBN: 9789386858948

Reference Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	Cryptography and Network Security	Behrouz A. Forouzan & Debdeep Mukhopadhyay	Tata McGraw-Hill, 2nd Edition, 2010
2	Cryptography and Network Security: Principles and Practice	William Stallings	Pearson Education, 8th Edition, 2020
3	Cyber Security and Cyber Laws	Alfred Basta, Nadine Basta, Mary Brown & Ravinder Kumar	Cengage Learning India, 1st Edition, 2018

Course Outcomes:

Course outcome	Descriptions
CO1	**Explain** the fundamentals of web technologies, protocols, and architectures.
CO2	**Apply** web development technologies to design and build interactive web applications.
CO3	**Demonstrate** knowledge of web security principles, authentication, and secure communication.
CO4	**Develop** secure and efficient web-based solutions using modern frameworks and tools.
CO5	**Evaluate** the security posture of web applications and recommend best practices for protection.

Course Articulation Matrix

PO/PSO CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2
CO1	3	2	2		1				3	2	2	3	
CO2	2	2	3	1	3				2	2	3	2	
CO3	2	2	3	2	3				2	2	3		
CO4	2	2	2	1	2	2	1	2	2	2	2		
CO5	2	1	2	1	2	2		2			2		

Course Assessment and Evaluation: Integrated Courses

Continuous Internal Evaluation (CIE): 50 Marks

Sl. No	Components		Duration(min)	Marks Conducted for	Marks reduced to	40% Min Marks in each component to write SEE
1	Theory-Internal Assessment	IA-1	90	50	15	12
		IA-2	90	50	15	
2	Periodic Lab Assessment		-	30	10	4
3	Lab CIE		-	20	5	4
4	One Open Ended Experiment /Project		-	10	5	2
	Total CIE			**150**	**50**	**20**

IA-1 Syllabus: 2½ Module , IA-2 Syllabus: 2½ Module
Rubrics for Periodic Lab Assessment: Attendance (5M), Lab record (10 M), Conduction of Experiments(10M) and Viva(5M)-**Total 30M**
Lab CIE: Write-up(5M), Conduction/Execution/Demonstration(10M) and Viva(5M)-**Total 20M**
One Open Ended Experiment /Project: Experimental/project Design (4 marks), Execution/demonstration (3 marks) and Analysis/Viva (3marks) – **Total 10M**

Semester End Examination (SEE): Max 100 Marks, Duration: 3 Hrs
The question paper shall contain 10 full questions (20 marks each)**,** with 2 questions from each of the 5 Modules, ensuring 100% syllabus coverage. Students shall answer any 5 full questions with 1:1 choice**.** Each question may have a maximum of 4 sub-divisions**.**
Minimum passing Marks: 40% of Max Marks

Department: CSE (Cyber Security)			**Semester:**	**VI**
Subject: Data Science in Cyber Security				
Subject Code:	**22CY6PE41**	**L – T – P - S:**	**42-0-0-48 (In Hrs.)**	
			Credits:	**3**

Sl. No	Course Objectives
1	To **introduce** the fundamental concepts of data science and their relevance to cybersecurity applications.
2	To **enable** students to acquire and preprocess cybersecurity data for meaningful analysis.
3	To **develop** skills in applying statistical, analytical, and machine learning techniques to detect and prevent cyber threats.
4	To **equip** students with visualization tools for interpreting and communicating insights from security data.

Module	Description	Hrs
I	**Module 1: Introduction to Data Science and Cyber Security** • Overview of Data Science and Cyber Security. • Types of Cybersecurity Data (logs, network traffic, malware signatures). • Role of Data Science in Security: Anomaly detection, threat intelligence, and incident response. • Data collection and preprocessing in cybersecurity context **Textbook 2** – Intro & data chapters	**8**
II	**Module 2: Data Analysis and Visualization for Cybersecurity** • Exploratory Data Analysis (EDA): Summary statistics, trends, and outlier detection. • Visualization tools: matplotlib, seaborn, plotly. • Case study: Visual analysis of firewall logs and SIEM data. • Feature extraction and engineering from cybersecurity datasets. **Textbook 2** – Visualization & analysis	**8**
III	**Module 3: Machine Learning in Cyber Security** • Supervised vs. Unsupervised Learning.	**8**

	• Classification: SVM, Decision Trees, Random Forest for malware detection. • Clustering: K-means, DBSCAN for anomaly detection. • Model evaluation: Confusion matrix, precision, recall, ROC-AUC. **Textbook 1** – Classification & clustering	
IV	**Module 4: Threat Detection and Incident Response Using Data Science** • Intrusion Detection Systems (IDS) using ML. • Phishing detection, spam filtering using NLP techniques. • Real-time threat intelligence from open sources. • Use of SOC and SIEM tools in analytics. **Textbook 1 –** IDS, phishing detection	**8**
V	**Module 5: Advanced Topics and Case Studies** • Deep Learning in cybersecurity (CNN, RNN, LSTM). • Use of big data platforms (Hadoop, Spark) in threat detection. • Case studies: Netflix's security data pipeline, Microsoft's threat hunting. • Ethical and legal considerations in security data analytics **Textbook 1** – DL, big data in security	**8**

Text Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	Machine Learning and Security: Protecting Systems with Data Science	Clarence Chio, David Freeman	O'Reilly Media, 2018, 1st Edition
2	Data Science for Business	Foster Provost, Tom Fawcett	O'Reilly Media, 2013, 1st Edition

Reference Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	Data Science for Cyber Security	Vandana Rathi	BPB Publications,2020, 1st edition
2	Machine Learning for Cybersecurity Cookbook	Emmanuel Tsukerman	Packet Publishing, 2019, 1st edition
3	Artificial Intelligence and Cybersecurity: Advances and Innovations	Zubair Baig et al.	Springer, 2020, 1st edition

Course outcomes:

Course outcome	Descriptions
CO1	**Analyze** cybersecurity datasets using data analysis tools.
CO2	**Apply** ML algorithms for classification and anomaly detection in security contexts.
CO3	**Use** visualization and analytics for threat intelligence.
CO4	**Evaluate** and present security data insights through real-world case studies.
CO5	**Implement** defensive measures and counter measures to mitigate cybersecurity risks.

Course Articulation Matrix:

PO/PSO CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2
CO1	3	3	2										
CO2	3	3	2	2	2	3	3	2	2	2			
CO3	3	3	2	2	2	3	3	2	2	3			
CO4	2	3	2	2	2	2	3	2	2			1	
CO5	2	2	2	2	2	3	2	2	3			1	

Course Assessment and Evaluation: Regular Theory Courses

Continuous Internal Evaluation (CIE): 50 Marks						
Sl.No	**Components**		**Duration (min)**	**Marks Conducted for**	**Marks reduced to**	**40% Min Marks in each component to write SEE**
1	Theory-Internal Assessment	IA-1	90	50	20	16
		IA-2	90	50	20	
2	Activity Based Learning	ABL 1	-	25	5	4
		ABL 2	-	25	5	
Total CIE				150	50	20

IA-1 Syllabus: 2½ Module , IA-2 Syllabus: 2½ Module

Activity Based Learning (ABL): Online course with certification, Hobby project, Simulations, Industrial Visits, Community-Based Learning, Case-study, Problem-Based Learning, Peer Teaching, web page design, student publications, Hackathons, Quiz (Leetcode, GitHub, Hackaranks and company specific quiz), Student Development program (1 week/online or offline), ……Etc

Semester End Examination (SEE): Max 100 Marks, Duration: 3 Hrs

The question paper shall contain 10 full questions (20 marks each)**,** with **2** questions from each of the 5 Modules**,** ensuring 100% syllabus coverage**.** Students shall answer any 5 full questions with 1:1 choice. Each question may have a maximum of 4 sub-divisions.

Minimum passing Marks: 40% of Max Marks

Department: CSE (Cyber Security)			**Semester:**	**VI**
Subject: Cyber Security in Health Care				
Subject Code:	**22CYPE642**	**L – T – P - S:**	**42-0-0-48 (In Hrs.)**	
			Credits:	**3**

Sl. No	Course Objectives
1	**Understand** the unique cybersecurity landscape of the healthcare sector
2	**Analyze** and evaluate the security vulnerabilities and risks associated with healthcare information systems.
3	**Apply** appropriate cybersecurity principles, technologies, and best practices to protect healthcare systems.
4	**Develop** strategies for incident response, disaster recovery, and compliance.

Module	Description	Hrs
I	**Healthcare Cyber Landscape & Fundamentals** **Healthcare Ecosystem:** Overview of organizations, services, and Protected Health Information (PHI). **Cyber Threats:** Common attacks like ransomware, phishing, data breaches, and their impact on patient safety. **Security Principles:** Confidentiality, Integrity, Availability (CIA) in healthcare context. **Unique Challenges:** Legacy systems, interoperability, insider threats. **Textbook 2 – Intro chapters**	**8**

II	**Healthcare Data Regulations & Compliance (8 Hours)**
	• **Indian Regulations:**
	  ○ **Digital Personal Data Protection (DPDP) Act 2023:** Key health data provisions, consent.
	  ○ **Information Technology (IT) Act, 2000 & SPDI Rules, 2011:** Relevant aspects for health data.
	• **Global Context (Brief):** Mention of **HIPAA (USA) and GDPR (EU)** as benchmarks.
	• **Ethical Considerations:** Data privacy, patient rights, ethical use of health data.
		8

	Textbook 2 – DPDP, IT Act, HIPAA, GDPR	
III	**Securing Healthcare IT Systems** • **EHR/EMR Security:** Access control, audit trails, and integrity for **Electronic Health Records.** • **Hospital IT Infrastructure:** Securing **Hospital Information Systems (HIS)** and network components. • **Cloud & Telemedicine Security:** Risks and security for **cloud-based health data** and **virtual care platforms**. • **Data Protection Techniques: Encryption for PHI** (at rest/in transit), **Identity & Access Management (IAM)** (e.g., MFA, RBAC). **Textbook 2** – HIS/EHR/Cloud	**8**
IV	**Medical Device & Operational Technology (OT) Security** • **Medical Devices & IoMT:** Types of medical devices, Internet of Medical Things (IoMT) challenges. • **Device Vulnerabilities:** Common weaknesses and attack vectors. • **IoMT Security:** Authentication, secure communication, network segmentation. • **Operational Technology (OT):** Securing hospital building management systems (BMS) and critical infrastructure. • **Relevant Standards:** Overview of medical device cybersecurity guidelines (e.g., FDA, IEC 81001-5-1). **Textbook 1** – IoMT & standards	**8**
V	**Risk Management, Incident Response & Future Trends** • **Risk Management:** Identifying, assessing, and **mitigating cybersecurity risks** in healthcare environments. • **Incident Response:** Planning and steps for **recovery from healthcare cyber incidents** (e.g., ransomware, data breaches). • **Business Continuity & Disaster Recovery (BCDR):** Ensuring **resilience of critical healthcare services**. • **Security Awareness:** Importance of **training for healthcare staff.**	**8**

	• **Emerging Technologies:** Brief overview of **AI/ML, Blockchain, and Quantum Computing** implications in healthcare cybersecurity. **Textbook 1 & 2** – Risk & recovery	

Text Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	Medical Device Cybersecurity: A Guide for Regulators, Researchers, and Manufacturers	Kevin Fu (Editor)	Medical Device Cybersecurity: A Guide for Regulators, Researchers, and Manufacturers
2	Healthcare Information Security and Privacy	John P. Campbell	Healthcare Information Security and Privacy

Reference Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	Cybersecurity in Emerging Healthcare Systems	Agbotiname Lucky Imoize	Published by the Institution of Engineering and Technology (IET), 2024.
2	Latest versions of relevant Indian government guidelines (e.g., MeitY, NHA) and international frameworks	Emmanuel Tsukerman	Publication 800-66 (HIPAA Security Rule).

Course Outcomes:

Course outcome	Descriptions
CO1	**Understand** the unique cybersecurity landscape of the healthcare sector.
CO2	**Analyze** security vulnerabilities and risks in healthcare information systems.
CO3	**Apply** cybersecurity principles and best practices to protect healthcare infrastructure.
CO4	**Outline** strategies for incident response, disaster recovery, and regulatory compliance.
CO5	**Formulate** and evaluate strategies for maintaining regulatory compliance and ethical considerations in healthcare.

Course Articulation Matrix:

PO/PSO CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2
CO1	2	2		1									
CO2	3	3	2	3	2								
CO3	2	2	3	2	3								
CO4	2	3	3	3	3	2							
CO5	2	2	2	2	2								

Course Assessment and Evaluation: Regular Theory Courses

Continuous Internal Evaluation (CIE): 50 Marks						
Sl.No	**Components**		**Duration (min)**	**Marks Conducted for**	**Marks reduced to**	**40% Min Marks in each component to write SEE**
1	Theory-Internal Assessment	IA-1	90	50	20	16
		IA-2	90	50	20	
2	Activity Based Learning	ABL 1	-	25	5	4
		ABL 2	-	25	5	
Total CIE				150	50	20

IA-1 Syllabus: 2½ Module , IA-2 Syllabus: 2½ Module

Activity Based Learning (ABL): Online course with certification, Hobby project, Simulations, Industrial Visits, Community-Based Learning, Case-study, Problem-Based Learning, Peer Teaching, web page design, student publications, Hackathons, Quiz (Leetcode, GitHub, Hackaranks and company specific quiz), Student Development program (1 week/online or offline), ……Etc

Semester End Examination (SEE): Max 100 Marks, Duration: 3 Hrs

The question paper shall contain 10 full questions (20 marks each)**,** with **2** questions from each of the 5 Modules**,** ensuring 100% syllabus coverage**.** Students shall answer any 5 full questions with 1:1 choice. Each question may have a maximum of 4 sub-divisions.

Minimum passing Marks: 40% of Max Marks

Department: CSE (Cyber Security)			**Semester:**	**VI**
Subject: Cyber Security for IoT				
Subject Code:	**22CYPE643**	**L – T – P - S:**	**42-0-0-48(In Hrs.)**	
			Credits:	**3**

Sl. No	Course Objectives
1	**Understand** the fundamental concepts of IoT architecture, components, and security challenges in interconnected device ecosystems.
2	**Analyze** various security threats, vulnerabilities, and attack vectors specific to IoT.
3	**Design** and implement security mechanisms for protecting IoT infrastructure.
4	**Evaluate** emerging security technologies and develop strategies for secure IoT deployment in real-world scenarios.

Module	Description	Hrs
I	**IoT Fundamentals and Security Landscape:** **Introduction to Internet of Things (IoT), IoT architecture:** Device, connectivity, data processing, and application layers, IoT ecosystem components: sensors, actuators, gateways, cloud platforms, Communication protocols: MQTT, CoAP, HTTP/HTTPS, WebSocket, Security challenges in IoT environments, Threat landscape and attack surface analysis, Case studies: Smart homes, industrial IoT, healthcare IoT. **Textbook 1** – IoT basics	**8**
II	**IoT Device Security and Embedded Systems Protection:** Hardware security in IoT devices, Secure boot processes and trusted execution environments, Firmware security and secure update mechanisms, Cryptographic implementations in resource-constrained devices, Physical security and tamper resistance, Side-channel attacks and countermeasures Secure key management for IoT devices, Device identity and authentication mechanisms. **Textbook 1** – Device security	**8**

III	**IoT Network Security and Communication Protection** Network security protocols for IoT: TLS/DTLS, IPSec, Wireless security: WiFi, Bluetooth, Zigbee, LoRaWAN, Gateway security and edge computing protection, Network segmentation and isolation strategies, Intrusion detection systems for IoT networks, DDoS attacks and mitigation in IoT environments Blockchain integration for IoT security, Software-defined networking (SDN) for IoT security. **Textbook 2** – Protocol & network protection	**8**
IV	**IoT Data Security and Privacy Protection** Data encryption and key management, Privacy-preserving techniques in IoT Data integrity and authentication, Secure data aggregation and processing Cloud security for IoT data, Edge computing security considerations, Compliance frameworks: GDPR, HIPAA for IoT, Anonymization and pseudonymization techniques, Homomorphic encryption for IoT data processing **Textbook 2 – Data protection frameworks**	**8**
V	**Advanced IoT Security and Emerging Technologies:** AI/ML-based security solutions for IoT, Anomaly detection and behavioral analysis, Security orchestration and automated response, Digital twins and security modelling, Quantum-resistant cryptography for IoT, 5G and IoT security integration, Industrial IoT (IIoT) security frameworks, Security testing and penetration testing for IoT, Future trends and research directions **Textbook 1 & 2** – AI/ML, penetration testing	**8**

Text Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	"Internet of Things Security: Fundamentals, Techniques and Applications"	Raghav Rao and Hrishikesh Venkataraman,	Institution of Engineering and Technology (IET), 2021.
2	"IoT Security Paradigms and Applications: Research and Practices"	Sudhir Kumar Sharma and Bharat Bhushan	CRC Press, 2021.

Reference Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations	Fadi Al-Turjman	CRC Press, 2020.
2	Cyber Security for Industrial Control Systems: From the Viewpoint of Close-Loop	Peng Cheng, Hao Zhang, and Jiming Chen	CRC Press, 2020.

Course Outcomes:

Course outcome	Descriptions
CO1	**Explain** the architecture and working principles of IOT system.
CO2	**Examine** different ways hackers can attack IoT devices and networks
CO3	**Create** and build secured IoT systems
CO4	**Access** new security technologies and architect safe and secure IoT systems.
CO5	**Propose** and implement solutions to address emerging threats and vulnerabilities in complex IOT ecosystems.

Course Articulation Matrix

PO/PSO CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2
CO1	3	2	1	2			3						
CO2	2	3	2	3			2						
CO3	2	2	3	3	2	2	2						
CO4	1	2	2	3		2	1						
CO5	3	2	1	2			3						

Course Assessment and Evaluation: Regular Theory Courses

Continuous Internal Evaluation (CIE): 50 Marks						
Sl.No	**Components**		**Duration (min)**	**Marks Conducted for**	**Marks reduced to**	**40% Min Marks in each component to write SEE**
1	Theory-Internal Assessment	IA-1	90	50	20	16
		IA-2	90	50	20	
2	Activity Based Learning	ABL 1	-	25	5	4
		ABL 2	-	25	5	
Total CIE				150	50	20

IA-1 Syllabus: 2½ Module , IA-2 Syllabus: 2½ Module
Activity Based Learning (ABL): Online course with certification, Hobby project, Simulations, Industrial Visits, Community-Based Learning, Case-study, Problem-Based Learning, Peer Teaching, web page design, student publications, Hackathons, Quiz (Leetcode, GitHub, Hackaranks and company specific quiz), Student Development program (1 week/online or offline), ……Etc

Semester End Examination (SEE): Max 100 Marks, Duration: 3 Hrs
The question paper shall contain 10 full questions (20 marks each)**,** with **2** questions from each of the 5 Modules**,** ensuring 100% syllabus coverage**.** Students shall answer any 5 full questions with 1:1 choice. Each question may have a maximum of 4 sub-divisions.
Minimum passing Marks: 40% of Max Marks

Department: CSE (Cyber Security)			**Semester:**	**VI**
Subject: Ethical Hacking Fundamentals				
Subject Code:	**22CY6OE51**	**L – T – P - S:**	**42-0-0-48 (In Hrs.)**	
			Credits:	**3**

Sl. No	Course Objectives
1	**Understand** the core concepts, methodologies, and legal frameworks surrounding ethical hacking and penetration testing.
2	**Apply** various hacking techniques and tools to identify vulnerabilities in networks, systems, and applications in a controlled environment
3	**Evaluate** the security posture of an organization and recommend appropriate countermeasures to mitigate identified risks
4	**Demonstrate** ethical conduct and professionalism while performing security assessments and reporting vulnerabilities.

Module	Description	Hrs
I	**Module 1: Introduction to Ethical Hacking** • **Core Concepts:** Hacking vs. Ethical Hacking, types of hackers, the hacking process/lifecycle. • **Ethical Hacking Methodologies:** Information gathering, scanning, enumeration, exploitation, reporting. • **Legal Frameworks:** Computer Fraud and Abuse Act (CFAA), relevant Indian IT Act sections, data privacy regulations. • **Ethical Considerations:** Code of ethics for ethical hackers, responsible disclosure, maintaining confidentiality **Textbook 1** – Intro & ethics	**8**
II	**Network Scanning & Enumeration** • **Network Scanning:** Nmap, Zenmap, port scanning techniques (TCP Connect, SYN, UDP). • **Enumeration:** Banner grabbing, OS fingerprinting, service enumeration (SMTP, DNS, SNMP). • **Vulnerability Scanning:** Nessus, OpenVAS, identifying common vulnerabilities (CVEs).	**8**

	• **Wireless Network Hacking:** Wi-Fi scanning, WEP/WPA/WPA2 cracking (theory and tools). **Textbook 1** – Scanning tools	
III	**System Hacking & Exploitation** • **System Hacking:** Password cracking techniques, privilege escalation (Windows/Linux). • **Exploitation:** Metasploit Framework, exploiting known vulnerabilities. • **Web Application Hacking:** OWASP Top 10 vulnerabilities (SQL Injection, XSS, CSRF), tools like Burp Suite. • **Client-Side Exploitation:** Social engineering techniques, phishing attacks, malware analysis (basic). **Textbook 1 & 2** – Exploits & OWASP	**8**
IV	**Post-Exploitation & Reporting** • **Post-Exploitation**: Maintaining access, covering tracks, pivoting. • **Reporting:** Documenting findings, creating professional penetration testing reports. • **Remediation:** Recommending security countermeasures, mitigation strategies. • **Incident Handling:** Basic principles of incident response and handling. **Textbook 1** – Reporting	**8**
V	**Advanced Topics & Emerging Threats** • **Mobile Hacking:** Android and iOS security vulnerabilities, mobile penetration testing. • **Cloud Security:** Cloud computing concepts, security risks in cloud environments. • **IoT Hacking:** Security challenges in IoT devices, common vulnerabilities. • **Emerging Threats:** Overview of current attack trends, zero-day exploits, advanced persistent threats (APTs). **Textbook 2** – IoT, Cloud, Mobile security	**8**

Text Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	Penetration Testing: A Hands-On Introduction to Hacking	Georgia Weidman	1st edition (September 16, 2014); ISBN-10: 1593275641; ISBN-13: 978-1593275648
2	The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws	Dafydd Stuttard and Marcus Pinto	Wiley; 2nd Edition (September 2011); ISBN-10: 978-1118026472; ISBN-13: 978-1-118-02647-2

Reference Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	Ethical Hacking and Penetration Testing Guide	Rafay Baloch	1st Edition (April 19, 2017); ISBN-10: 9781498751559; ISBN-13: 978-1-4987-5155-9
2	Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers	Peter Yaworski	1st edition (December 23, 2013); ISBN-10: 1593275684; ISBN-13: 978-1593275686

Course Outcomes:

Course outcome	Descriptions
CO1	**Understand** and describe the core concepts and key words of cyber security
CO2	**Identify** vulnerabilities in networks, systems, and applications in a controlled environment.
CO3	**Evaluate** the security posture of an organization and recommend appropriate countermeasures to avoid risks.
CO4	**Demonstrate** ethical conduct and professionalism as a security architect.
CO5	**Formulate** comprehensive penetration test reports and necessary documents.

Course Articulation Matrix

PO/PSO CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2
CO1	2	2		1		2		3		2			
CO2	3	3	2	3	3	2		2	1	2			
CO3	2	3	3	3	3	2		2	2	3	1		
CO4	1	2	2	2	2	3		3	2	3	2		
CO5	1	3	2	2	3	1	2	1	1	1			

Course Assessment and Evaluation: Regular Theory Courses

Continuous Internal Evaluation (CIE): 50 Marks

Sl. No	Components		Duration (min)	Marks Conducted for	Marks reduced to	40% Min Marks in each component to write SEE
1	Theory- Internal Assessment	IA-1	90	50	20	16
		IA-2	90	50	20	
2	Activity Based Learning	ABL 1	-	25	5	4
		ABL 2	-	25	5	
Total CIE				150	50	20

IA-1 Syllabus: 2½ Module , IA-2 Syllabus: 2½ Module
Activity Based Learning (ABL): Online course with certification, Hobby project, Simulations, Industrial Visits, Community-Based Learning, Case-study, Problem-Based Learning, Peer Teaching, web page design, student publications, Hackathons, Quiz (Leetcode, GitHub, Hackaranks and company specific quiz), Student Development program (1 week/online or offline), ……Etc

Semester End Examination (SEE): Max 100 Marks, Duration: 3 Hrs
The question paper shall contain 10 full questions (20 marks each)**,** with **2** questions from each of the 5 Modules**,** ensuring 100% syllabus coverage**.** Students shall answer any 5 full questions with 1:1 choice. Each question may have a maximum of 4 sub-divisions.
Minimum passing Marks: 40% of Max Marks

Department: CSE (Cyber Security)			**Semester:**	**VI**
Subject: Mini Project				
Subject Code:	**22CYMP607**	**L – T – P - S:**	**0-0-42-18 (In Hrs.)**	
			Credits:	**2**

Sl. No	**Course Objectives**
1	It provides application knowledge and techniques learnt in various aspects for
2	Developing the software for real problems.
3	Gives an insight into the working of the real organizations/companies.
4	Gaining deeper understanding in specific functional areas.

Module	**Description**	**Hrs**
I	**Guidelines for the Mini Project**: • A group of two students are required to carry out Mini Project work under the supervision of Project Guide. • The guide shall monitor progress of the student continuously. • Each group is required to present the progress of the Mini Project work during the semester as per the schedule given by the department. • A presentation shall be made by the group as per the schedule announced by the department. • A report shall be submitted by the candidates to the department.	**8**
II	**Evaluation Scheme:** • Continuous evaluation will be assessed by respective Project Guides based on the Regularity, Technical Knowledge and Competence, Programming Skills, Communication Skills and Documentation Skills of the students. • Students are evaluated by the team of faculty members based on the Presentation, Technical Competence, Slides Preparation, Team Working Abilities and viva voce.	**8**

Course Articulation Matrix

PO/PSO CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2
CO1	1	1		1									
CO2	2	2	1		1								
CO3	3	2	3		3								
CO4	1		1		2								
CO5	1	2	1										

Mini project
CIE evaluation (50 Marks)

Evaluation Parameters	**Marks**
Synopsis evaluation by DPEC (Novelty, societal, Industry based)	10
Meeting regularity and Presentation	15
Demonstration	15
Exhibition of the work in Hackathons/ Ideathons / Createthons	5
Report writing	5
Total	**50**

Department: CSE (Cyber Security)			**Semester:**	**6**
Subject: Skill Development-III (Technical Skills) Pre-placement Training				
Subject Code:	**22SK608**	**L – T – P - S:**	**42-0-0-48**	
			Credits:	**3**

Sl. No	Course Objectives
1	To **introduce** students to Autodesk Revit Architecture and its application in architectural design and visualization.
2	To **enable** students to create, edit, and manage building components, project views, annotations, and schedules.
3	To **develop** skills in rendering, walkthroughs, and advanced features for effective building modelling and analysis.
4	To **familiarize** students with ETABS for structural modeling, analysis, and interpretation of results including structural design and MX Road software for alignment, pavement design, and road modeling

Module	Description	Hrs
I	**Introduction to Autodesk Revit Architecture:** Starting an Architectural Project: Starting a New Architectural Project, Navigation Tools, Configuring Global Settings **Creating Architectural Walls** Starting an Architectural Project: Starting a New Architectural Project, Navigation, Tools, Configuring Global Settings, Creating Architectural Walls, **Using Basic Building Components - I:** Adding Doors, Adding Windows and Wall Openings **Using the Editing Tools:** Working with Selection Sets, Editing Tools I & II, Grouping, Elements, Retrieving Information About Elements **Working with Datum Planes and Creating Standard Views:** Working with Levels, Working with Grids, Working with Reference Planes and Work Planes, Controlling, the Display of Elements. **Working with Project Views** **Using Basic Building Components – II:** Creating Floors, Roofs & Ceilings, Shape, Editing Tools, Adding Rooms	3

	Using Basic Building Components – III: Working with Components, Adding Stairs, Adding Railings and Ramps, Creating Curtain Walls	
II	**Adding Site Features:** Working With Site Features, Property Lines and Building, Pads, Adding Site Components, Using Massing Tools, Understanding Massing, Concepts, Creating Massing, Geometry in the Family Editor, Editing Massing, Geometry in the Family Editor, Massing in the Conceptual Design Environment, Creating Massing Geometry in a Project, Creating Building Elements from Massing Geometry, Creating Families. **Adding Annotations and Dimensions** Adding Tags, Room Tags, Keynotes, Adding Symbols and Dimensions, Dimensioning Terminology and Dimensioning Tools, Adding Alternate Dimension Units and Spot Dimensions. **Creating Project Details and Schedules** Project Detailing in Autodesk Revit Architecture, Crop Regions, Fills Patterns, and Detail Components, Adding Text Notes, Creating Drafting Views, Revision Clouds, Working with Schedules **Creating Drawing Sheets, and Plotting** Creating Drawing Sheets, Creating Duplicate Dependent Views, Printing in Revit Architecture **Creating 3DViews:** Three-Dimensional (3D) Views, Dynamically Viewing Models with Navigation Tools, orienting a 3DView, Generating Perspective Views, Using a Section Box	3
III	**Rendering Views and Creating Walkthroughs** Rendering in Revit Architecture, Working with Materials, Lights, Decals and Entourage, Rendering Settings, Creating a Walkthrough Autodesk 360, Rendering **Using Advanced Features** Creating Structural Components, Generating Multiple Design Options, Using Area Analysis Tools, Masking Regions, Creating Displaced Views, Color Schemes, Working with Project Phasing Tools, Work-sharing Concepts, Elements Families, Browsers, Generating Shadows, Creating Solar Studies, Working with Point Clouds, Revit Architecture Interoperability, Linking Building	3
IV	**Introduction to ETABS:**	3

	Features and Capabilities, - User Interface and Navigation, - Basic Concepts in Structural Modelling - Defining Material Properties, -Defining Section Properties (Beams, Columns, Slabs) **Modelling Structural Elements:** -Drawing Beams, Columns, and Slabs, -Defining Loads and Load Combinations -Assigning Loads to Structural Elements, -Assigning Supports and Boundary Conditions **Analysis and Results Interpretation:** -Running the Analysis, -Viewing and Interpreting Analysis Results: Deformations, Member Forces, Reactions, - Analysing a Simple Building Structure	
V	**Design of Structural Elements:** Design of Concrete Structures, Design of Steel Structures **Detailed Modelling and Design of a Multi-Story Building** **MX road software:** Introduction to Mx road software**,** User Interface and tools, Data input total station points. **Alignment and modelling:** fixing alignment line, drawing of geometric elements,3D modelling. **Pavement Design:** Input material specification, Design and Analysis	3

Note: Mention text book referred along with sections for more clarity in each units (e.g, Text 1: 2.1,2.5,Text2: 1.2,2.3)

Text Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	Autodesk Revit for Architecture Certified User Exam Preparation (Revit 2025 Edition)	Daniel John Stine AIA, IES, CSI, CDT, Well AP	Available January 22, 2025 By Intermediate
2	Etab V18 Black book	Gaurav Verma	Cadcamcae Works, 27 Feb 2020 - Architecture

Reference Books:

Sl No	Text Book title	Author	Volume and Year of Edition
1	Residential Design Using Autodesk Revit 2025	By Daniel John Stine AIA, IES, CSI, CDT, Well AP	Published June 21, 2024 Beginner
2	Autodesk Revit 2025 BIM Management	By ASCENT	Available November 12, 2024, Intermediate

Course Outcomes:

Course outcome	Descriptions
CO1	Apply Revit tools to create and modify architectural elements, views, and building components**. (Apply)**
CO2	Develop site features, annotations, schedules, and 3D views to represent architectural projects effectively. **(Apply/Analyze)**
CO3	Demonstrate proficiency in rendering, walkthroughs, and advanced features for building visualization and analysis. **(Analyze/Create)**
CO4	Use ETABS software to model, analyze, and interpret structural elements of buildings. **(Apply/Analyze)**
CO5	Design structural elements and apply MX Road software for road alignment, pavement design, and 3D modeling**. (Apply/Create)**

Course Articulation Matrix:

PO/PSO CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2
CO1	3	2	2	2	3				2		3		
CO2	3	2	2	2	3				2		3		
CO3	3	3	2	2	3				2		3		
CO4	3	3	3	3	3				2		3		
CO5	3	3	3	3	3				3	2	3		

Course Assessment and Evaluation: Humanities and Social Science Courses (CIP, UHV, Environmental Science, Communicative English, Skill Development)

Sl. No	Components		Duration(min)	Marks Conducted for	Min Marks To pass the Course
1	Theory-Internal Assessment	IA-1	90	50	40
		IA-2	90	50	
	Total CIE			100	40