MITS Kochi
Muthoot Institute of Technology and Science
(Autonomous)

M. TECH
CYBER SECURITY

CURRICULUM & SYLLABUS

2026
REGULATION

MITS Kochi
Muthoot Institute of Technology and Science
(Autonomous)

M.Tech

CYBER SECURITY

2026 REGULATION

CURRICULUM & SYLLABUS

CURRICULUM

SEM	SLOT	COURSE CATEGORY	COURSE CODE	COURSE NAME	LECTURE	TUTORIAL	PROJECT	LAB	SELF STUDY	CREDIT	CREDIT / SEM
I	A	PC	M260102/CY100A	Applied Cryptography	3	0	0	0	3	3	22
	B	PC	M260902/CN100B	Advanced Data Structures and Algorithms	4	0	0	0	4	4	
	C	PC	M260102/CY100C	Information Assurance and Security	4	0	0	0	4	4	
	D	PC	M260102/CY100D	Network and System Security	4	0	0	0	4	4	
	E	PCE	M260102/CY110E	Cyber Security & Secure Coding	3	0	0	2	5	5	
	K		M260904/CN100K	Research Methodology and IPR	3	0	0	0	1	2	
	L		M260904/CN17*L	Audit Course	0	0	0	0	2	0	
II	A	PC	M260102/CY200A	Decentralized Systems Security	0	0	0	2	6	4	24
	B	PC	M260102/CY200B	Secure Cloud and IoT	3	0	0	0	5	4	
	C	PCE	M260102/CY210C	Digital Forensics & Malware Analysis	3	0	0	0	7	5	
	D	PE	M260102/CY21*D	Program Elective I	3	0	0	0	3	3	
	E	PE	M260102/CY22*E	Program Elective II	3	0	0	0	3	3	
	F	PE	M260102/CY23*F	Program Elective III	3					3	
	K	Research Seminar	M260102/CY200K	Research Seminar / Mini Project	3	0	0	0	1	2	
III	A	PE	M260102/CY34*A	Program Elective IV	3	0	0	0	3	3	12
	M	Interdisciplinary Elective	M260102/CY35*M	Interdisciplinary Elective/MOOC	0	0	0	2	4	3	
	N	Internship	M260102/CY340N	Internship	0	0	0	0	4	2	
	K	Dissertation / Project Phase I	M260102/CY300K	Dissertation / Project Phase I	0	0	0	0	8	4	
IV	K	Dissertation / Project Phase II	M260102/CY400K	Dissertation / Project Phase II	2	0	0	0	22	12	12

SEMESTER I

COURSE DESCRIPTION							
Regulation	**2026**	**L-T-J-P-S**	**3-0-0-0-3**	**Version**	**26/0**	**Credits**	**3**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)							

Course Code	Course Name	Course Category
M260102/CY100A	**APPLIED CRYPTOGRAPHY**	**Program Specific Mathematics**

COURSE OBJECTIVES	
1	Understand mathematical foundations used in cryptography.
2	Apply encryption and hashing techniques for secure communication.
3	Analyze cryptographic protocols and authentication methods.
4	Study modern public key cryptographic systems.
5	Develop knowledge in practical cryptographic applications.

COMPETENCY STATEMENTS	
CC1	Apply Mathematical Foundations in Cryptography – Demonstrate the ability to use number theory, finite fields and mathematical techniques for designing secure cryptographic systems
CC2	Implement Secure Cryptographic Techniques – Demonstrate the ability to apply encryption, hashing and authentication mechanisms for secure data communication and protection..
CC3	Analyze Cryptographic Protocols and Security Mechanisms – Demonstrate the ability to evaluate cryptographic protocols, key exchange methods and secure communication systems against security threats and attacks.

COURSE OUTCOMES

Course Outcomes (CO): At the end of this course, learners will be able to:

CO	CO Statement	Competency Mapping	Cognitive (C)	Psychomotor (P)	Affective (A)
CO1	Explain the mathematical foundations used in cryptographic systems.	CC1	U	M	Rs
CO2	Apply symmetric and asymmetric encryption techniques for secure communication.	CC2	A	P	V
CO3	Analyze hashing and authentication mechanisms in information security	CC3	An	P	V
CO4	Evaluate cryptographic protocols and key exchange techniques.	CC3	E	Ar	O
CO5	Design secure cryptographic solutions for practical applications.	CC3	E	N	O

Cognitive (Revised blooms Level): *- **R**: Remember; **U**: Understand; **A**: Apply; **An**: Analyse; **E**: Evaluate; **C**: Create*
Psychomotor Domain (Dave's): *- **I**-Imitation, **M**-Manipulation, **P**-Precision, **Ar**-Articulation, **N**-Naturalisation*
***Affective (Krathwohl)**: - **Re**-Receiving, **Rs**-Responding, **V**-Valuing, **O**-Organization, **Ch**-Characterization*

CO	PROGRAM OUTCOMES (PO) CORRELATION MATRIX						
	PO						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1	2	1	3	1	2	1	1
2	2	1	3	3	3	1	1
3	2	1	3	2	3	1	1
4	3	2	3	2	3	2	1
5	3	2	3	3	3	2	2

Correlation levels: 1 - Low; 2 - Medium; 3 - High; No Correlation - "-"

TEACHING AND ASSESSMENT SCHEME													
Teaching Scheme / Week				**Self-Learning (S) / Semester**	**Total Hours / Semester**	**Credits C**	**Examination Scheme**						
L	**T**	**J**	**P**				**Theory**			**Practical**			**Total**
							CIA	**ESE**	**Total**	**CIA**	**ESE**	**Total**	
2	0	0	0	45	90	2	40	60	100				100

***L**: Lecture (One unit is of one-hour duration), **T**: Tutorial (One unit is of one-hour duration), **P**: Practical (One unit is of one-hour duration), **J**: Project (One unit is of one-hour duration), **S**: Self-Learning & Team Work (One unit is of one-hour duration), **CIA**: Continuous Internal Assessment, **ESE**: End Semester Examination*

SYLLABUS (Major Topics)			
Module	Title	Major Topics	Contact Hours
1	Finite Fields and Number Theory	Modular Arithmetic, Prime Numbers & finite field, Galois Fields, Euclidean Algorithm	11
2	Encryption Techniques	Symmetric Encryption, Asymmetric Encryption, RSA, ECC	12
3	Hashing and Authentication	Hash Functions, Digital Signatures, Message Authentication, PKI	9
4	Cryptographic Protocols	Key Exchange Protocols, Secure Communication, SSL/TLS Basics, Cryptographic Applications	13

SUGGESTED LEARNING RESOURCES			
Text Book			
Sl. No.	Title of Book	Author	Publication
1	Cryptography and Network Security	William Stallings	Pearson, 8th Edition, 2023
2	Applied Cryptography	Bruce Schneier	Wiley, 20th Anniversary Edition
3	Understanding Cryptography	Christof Paar & Jan Pelzl	Springer, 2010
4	Introduction to Modern Cryptography	Jonathan Katz & Yehuda Lindell	CRC Press, 3rd Edition, 2020
5	Cryptographic Engineering	Cetin Kaya Koc	Springer, 2009
Reference			
Sl. No.	Title of Book	Author	Publication
1	Handbook of Applied Cryptography	Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone	CRC Press
2	Serious Cryptography	Jean-Philippe Aumasson	No starch
3	Network Security with OpenSSL	John Viega, Matt Messier & Pravir Chandra	O'Reilly Media
Web Resource			
1	https://nptel.ac.in/courses/106105031		
2	https://ocw.mit.edu/		
3	https://www.coursera.org/learn/crypto		

DETAILED SYLLABUS					
Module	Topic	Mode of Delivery	COs	Learning Domain Level C	Hrs
1	Introduction to Cryptography and Security Goals	Lecture	CO1	U	
	Modular Arithmetic and Euclidean Algorithm	Lecture	CO1	U	
	Prime Numbers and Finite Fields	Lecture	CO1	U	
	Mathematical Foundations for Cryptography	Lecture	CO1	A	
2	Symmetric Key Encryption Techniques	Lecture	CO2	U	
	Asymmetric Encryption and RSA Algorithm	Lecture	CO2	A	
	Elliptic Curve Cryptography Basics	Lecture	CO2	U	
	Encryption Algorithm Analysis	Lecture	CO2	An	
3	Cryptographic Hash Functions	Lecture	CO3	U	
	Digital Signatures and Authentication	Lecture	CO3	A	
	Message Authentication Codes and PKI	Lecture	CO3	An	
	Hashing and Authentication Applications	Lecture	CO3	A	
4	Key Exchange Protocols	Lecture	CO4	U	
	SSL/TLS and Secure Communication	Lecture	CO4	A	
	Cryptographic Protocol Attacks	Lecture	CO4	An	
	Security Evaluation of Cryptographic Systems	Lecture	CO4	E	

TABLE OF SPECIFICATIONS (ToS) FOR QUESTION PAPER DESIGN									
Module	Module Title	Teaching Hours	Distribution of Marks (Revised Bloom's Level)						Total Marks
			R	U	A	An	E	C	
1	Finite Fields and Number Theory			X	X				15
2	Encryption Techniques			X	X	X			15
3	Hashing and Authentication			X	X				15
4	Cryptographic Protocols			X	X	X			15
This ToS shall be treated as a general guideline for students and teachers for distribution of marks.									

ASSESSMENT PATTERN	
Assessment	**Marks**
Continuous Internal Assessment	**40**
Learning Activity	10
Internal Examination	10
Course project	20
End Semester Examination	**60**
Total	**100**

COURSE DESCRIPTION							
REGULATION	**2026**	**L-T-J-P-S**	**4-0-0-0-4**	**VERSION**	**26/0**	**CREDITS**	**4**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)							

COURSE CODE	COURSE NAME	COURSE CATEGORY
M260902/CN100B	**ADVANCED DATA STRUCTURES AND ALGORITHMS**	PC
PRE-REQUISITE		
Nil		

PREAMBLE
The course provides learners with knowledge of advanced data structures, algorithm design techniques, and computational problem-solving methods used in modern computing applications. The course focuses on efficient algorithm analysis, network flow, probabilistic and approximation algorithms, and advanced data structures to design and implement optimized software solutions for real-world problems.

RATIONALE
• The course aims to enhance learners' analytical thinking and computational problem-solving abilities through the study of advanced algorithms and efficient data structures used in modern computing environments. • It helps learners evaluate algorithmic efficiency, improve software performance, and develop scalable solutions for real-world applications in domains such as artificial intelligence, data analytics, networking, and large-scale computing systems. • The course also supports preparation for research, higher education, and industry-focused software development by focusing on the effective design and implementation of algorithms.

COMPETENCY STATEMENT/s
Demonstrate the ability to apply advanced data structures, algorithmic analysis techniques, and specialized algorithms (such as amortized, probabilistic, and network flow algorithms) to solve computational problems efficiently.
Design, develop, and implement efficient software solutions by integrating suitable advanced data structures and algorithms for real-world applications.

CO	CO Statement	Cognitive (C)	Psychomotor (P)	Affective (A)
1	Analyse the relevance of amortized analysis and applications.	A	M	Rs
2	Illustrate string matching algorithms.	A	P	Rs
3	Illustrate advanced data structures like Binomial heap, Fibonacci heap & Disjoint set	A	P	Rs
4	Illustrate network flow algorithms and applications.	A	P	Rs
5	Make use of probabilistic algorithms and approximation algorithms in computing.	A	P	Rs
6	Design, develop and implement software using advanced data structures and algorithms.	C	Ar	O

TEACHING AND ASSESSMENT SCHEME												
Teaching Scheme / Week					**Hours / Semester**	**Credit**	**Examination Scheme**					
							Theory			**Practical**			**Total**
L	**T**	**J**	**P**	**S**	**120**	**C**	**CIA**	**ESE**	**Total**	**CIA**	**ESE**	**Total**	
4	0	0	0	4		4	40	60	100				100
***L**: Lecture (One unit is of one-hour duration), **T**: Tutorial (One unit is of one-hour duration), **P**: Practical (One unit is of one-hour duration), **J**: Project (One unit is of one-hour duration), **S**: Self-Learning & Team Work (One unit is of one-hour duration), **CIA**: Continuous Internal Assessment, **ESE**: End Semester Examination*												

SYLLABUS (Major Topics)			
Module	Title	Major Topics	Hrs
1	Amortized analysis and String matching	Asymptotic Notations and Complexity Analysis, Amortized Analysis, String Matching Algorithms	16
2	Advanced data structures	Binary Heap Binomial Heap Fibonacci Heap Disjoint Set	16
3	Network flow	Residual Network & Augmenting Path,Max Flow Min-Cut Theorem, Ford–Fulkerson Algorithm ,Edmonds–Karp Algorithm	12
4	Probabilistic algorithms & Approximation algorithm	Types of Probabilistic Algorithms, Monte Carlo Algorithms, Las Vegas Algorithms Vertex Cover Problem, Travelling Salesman Problem , Set Covering Problem, Subset Sum Problem	16

Sl. No	Self-learning / Team Work Description
1	Course Project (25)
2	Case study for real-world applications of Fibonacci heap structure, Fibonacci heap operations, Maximum bipartite matching, Euler's Theorem ,Fermat's Theorem and vertex cover problem (10)
3	Implementation of Algorithms (25)

SUGGESTED LEARNING RESOURCES

Text Book			
Sl. No.	Title of Book	Author	Publication
1	Introduction to Algorithms	T. H. Cormen, C. E. Leiserson, R. L. Rivest and C. Stein	MIT Press, 3rd edition, 2009
2	Fundamentals of algorithms	Gilles Brassard and Paul Bratley	Prentice-hall of India Private Limited, 2001

Reference			
Sl. No.	Title of Book	Author	Publication
1	Randomized Algorithms	Rajeev Motwani, Prabhakar Raghavan	Cambridge University Press, 2000
2	The Design and Analysis of Algorithms	Dexter C. Kozen	Springer
3	Algorithm Design	Jon Kleinberg and Eva Tardos	Pearson Education, 2006

Web Resource	
1	Data Structures and Algorithms Design, Prof. Nitin Saxena, NPTEL-IIT, Madras
2	Data Structures and Algorithms, Prof. Naveen Garg, NPTEL-IIT Delhi

DETAILED SYLLABUS								
Module	**Title**	**Topic**	**Mode of Delivery**	**CO**	**Learning Domain**			**Hrs**
					C	**P**	**A**	
1	Amortized analysis and String matching	Overview of asymptotic notations	L	CO1	U			2
		Complexity analysis	L	CO1	U			2
		Amortized analysis – aggregate analysis	L	CO1	A	M	Rs	2
		Accounting method	L	CO1	A	M	Rs	2
		Potential method	L	CO1	U	M	Rs	2
		String matching – introduction	L	CO2	A			2
		Rabin-Karp algorithm	L	CO2	A	P	Rs	2
		Knuth-Morris-Pratt algorithm	L	CO2	U	P	Rs	2
2	Advanced data structures	Overview of binary heap	L	CO3	A			2
		Binary heap operations	L	CO3	A	P	Rs	2
		Binomial tree and heap	L	CO3	A	P	Rs	2

		Binomial heap operations	L	CO3	A	P	Rs	2
		Fibonacci heap structure	L	CO3	A	P	Rs	2
		Fibonacci heap operations	L	CO3	A	P	Rs	2
		Disjoint set – overview, linked list representation	L	CO3	A	P	Rs	2
		Disjoint set forests	L	CO3	A	P	Rs	2
3	Network flow	Network flow properties, examples	L	CO4	U			2
		Residual network, augmenting path, cut of network	L	CO4	A	M	Rs	2
		Maxflow-mincut theorem	L	CO4	A			2
		Ford-Fulkerson algorithm	L	CO4	A	P	Rs	2
		Edmonds-Karp algorithm	L	CO4	A	P	Rs	2
		Maximum bipartite matching	L	CO4	A	P	Rs	2
4	Probabilistic algorithms & Approximation algorithms	Introduction, types of probabilistic algorithms	L	CO5	U			2
		Monte-Carlo algorithms – Verifying matrix multiplication	L	CO5	A	P	Rs	2
		Euler's Theorem and Fermat's Theorem	L	CO5	A	P	Rs	2
		Primality testing – Miller-Rabin test	L	CO5	A	P	Rs	2
		Las Vegas algorithms – Probabilistic selection and quick sort	L	CO5	A	P	Rs	2
		Introduction to approximation algorithms	L	CO5	U			2
		Vertex-cover problem	L	CO5	A	P	Rs	2
		Traveling-salesman problem	L	CO5	A	P	Rs	2

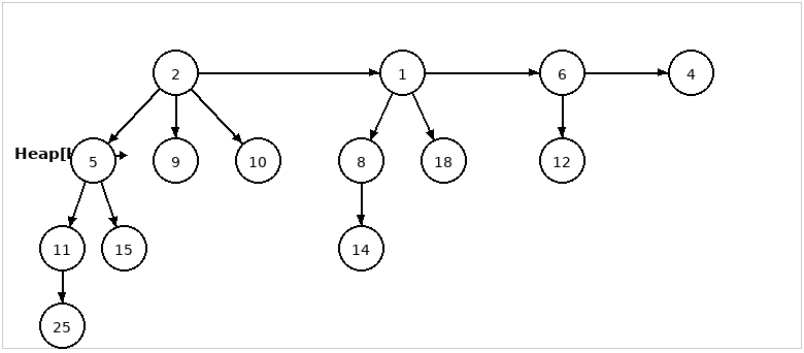
TABLE OF SPECIFICATIONS (ToS) (ESE Question Paper Design) (Use √)								
Module	Module Title	Distribution of Marks (RBL)						Total Marks
		R	U	A	An	E	C	
1	Amortized analysis and String matching		X	X				15
2	Advanced data structures		X	X				15
3	Network flow		X	X				15
4	Probabilistic algorithms & Approximation algorithms		X	X				15
This ToS shall be treated as a general guideline for students and teachers for distribution of marks.								

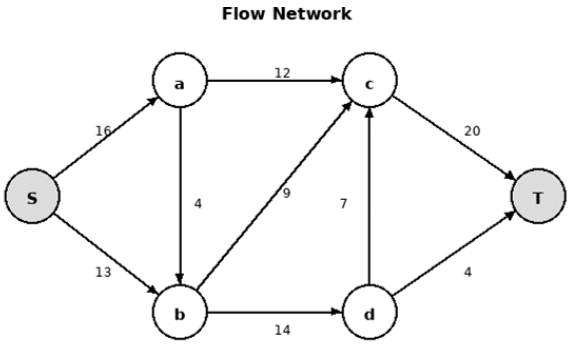
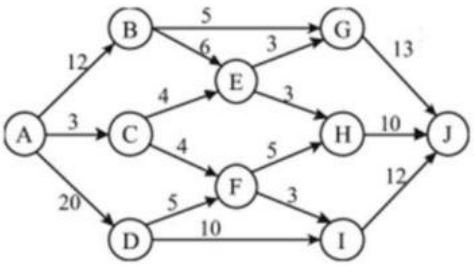
ASSESSMENT PATTERN		
Assessment		**Marks**
Continuous Internal Assessment		**40**
1	Internal Examination	10
2	Learning Activity/ Seminar	10
3	Course Project	20
End Semester Examination – Theory		**60**
Total		**100**

MITS Kochi — Muthoot Institute of Technology and Science (Autonomous)

MODEL QUESTION PAPER

FIRST SEMESTER M. TECH DEGREE END SEMESTER EXAMINATION, (2026 SCHEME)			
Course Code:	**M260902/CN100B**		
Course Name:	**ADVANCED DATA STRUCTURES AND ALGORITHMS**		
Max. Marks	**60**	**Duration**:	**2 hours 30 minutes**
Common to AD & CY			
Use of Data Book / IS codes, etc to be specified by the question paper setter			

PART A			
(Answer all questions. Each question carries 5 marks)			
No.	***Question***	***CO***	***Marks***
1	A stack supports Push, Pop, and Multipop(k) operations where Multipop pops min(k, stack size) elements. Using the aggregate method of amortized analysis, show that the amortized cost of each operation is O(1). Also verify using the accounting method by assigning appropriate credits.	CO 1	(5)
2	Show the Binomial Heap that results after performing Delete-Min on the heap shown in the figure below. Illustrate all intermediate steps including extraction of children, reversal, and the UNION operation. State the time complexity. 	CO 3	(5)
3	Justify how Edmonds-Karp algorithm out performs Ford Fulkerson Method on a worst case instance ?	CO4	(5)
4	Apply the APPROX-VERTEX-COVER algorithm on the graph G = (V, E) where V = {a,b,c,d,e,f,g} and E = {(a,b),(b,c),(c,d),(d,e),(e,f),(f,g),(g,a),(b,e),(c,f)}. Show each step of edge selection and the final vertex cover.	CO5	(5)
PART B			
(Answer one full question from each module, each carries 10 marks.)			
No.	***Module 1***	***CO***	***Marks***
5	(a) A binary counter of k bits supports the Increment operation. Using the potential method, where the potential Φ equals the number of 1-bits in the counter, derive the amortized cost of Increment. Hence prove that n increments starting from zero cost O(n) in total.	CO1	(4)
	(b) A cybersecurity system monitors network traffic logs to detect repeated suspicious patterns. To efficiently identify patterns without rechecking characters, the system uses the Knuth-Morris-Pratt (KMP) algorithm. The system needs to detect occurrences of a suspicious signature: Pattern (P) = "AABAAB" Text (T) = "AABAABAABAAB" Construct the LPS (Longest Prefix Suffix) array for the pattern. Use the KMP algorithm to find all occurrences of P in T & Show the complete trace table.	CO2	(6)
OR			
6	(a) A dynamic array doubles its size whenever it becomes full. Using the accounting method of amortized analysis, assign an amortized cost per insertion such that the average cost remains O(1). Justify your assignment with appropriate credit and debit accounting.	CO1	(4)
	(b) A university uses an automated plagiarism detection system to check student assignments. The system scans large documents to find repeated phrases efficiently. To speed up the process, it uses the Rabin–Karp	CO2	(6)

	algorithm with rolling hash, which allows quick comparison of substrings without checking each character repeatedly. The system is configured with: Pattern (P) = "ABC" Text (T) = "ABCDABCDEABC" Prime number (q) = 101 Demonstrate how Rabin-Karp algorithm can be used to identify the plagiarism by considering the given scenario.		
	Module 2		
7	(a) Perform Extract-Min on a Fibonacci Heap whose root list contains nodes with keys {3, 7, 18, 38} (with children: 7→ {24,17,23}, 18→ {21,39,41}, 38 has no children, 3→none). Show the consolidation procedure step by step.	CO3	(6)
	(b) Explain the Disjoint Set Forest with path compression and union by rank. Trace: MakeSet(1..6), Union(1,2), Union(3,4), Union(5,6), Union(1,3), Find(6), Union(1,5). Draw the resulting forest after each union.	CO3	(4)
	OR		
8	(a) Perform the Delete-Min operation on a binomial heap containing keys {1, 6, 10, 12, 25, 8, 14, 29, 18, 11, 17, 38, 27}. Show all intermediate steps including the extraction, reversal of children, and union operation. State the time complexity.	CO3	(6)
	(b) Illustrate the structure of a Fibonacci Heap. Define the potential function used in its amortized analysis and derive the amortized cost of the Insert and Find-Minimum operations.	CO3	(4)
	Module 3		
9	A smart city manages its water distribution system using a network of pipelines. Each pipeline has a maximum capacity (in liters per minute). The goal is to efficiently transport water from the main reservoir (source S) to the city storage tank (sink T). The network is represented as a directed graph with the following capacities:  Apply the Ford–Fulkerson algorithm to compute the maximum flow from S to T, and identify physical significance of the minimum cut in this scenario.	CO4	(10)
	OR		
10	 A data communication company is designing a high-speed data transmission network between multiple routers. Each router is represented as a node, and the communication links between them have limited bandwidth capacities (as shown in the diagram). The company wants to determine the maximum amount of data (flow) that can be transmitted from the main server (source A) to the destination server (sink J). To achieve this, they decide to apply the Edmonds-Karp algorithm, which uses Breadth-First Search (BFS) to find the shortest augmenting paths in terms of edges. Identify the augmenting paths from source A to sink J & determine the maximum flow from A to J.	CO4	(10)

	Module 4		
11	(a) A cloud computing company manages a load balancer that distributes incoming tasks to servers. Each task has a priority value, and the system must sort these priorities quickly to ensure efficient scheduling. However, due to unpredictable workloads, the system uses a Probabilistic (Randomized) Quick Sort algorithm, where the pivot is chosen randomly to avoid worst-case performance. The current set of task priorities is: [16,12, 10, 8, 4, 2] With the help of the step by step procedure, demonstrate how this algorithm helps to manage unpredictable workloads. Also show how this algorithm improve the worst case performance.	CO5	(6)
	(b) Describe the Monte Carlo algorithm for verifying matrix multiplication AB = C for n×n matrices. Explain how a random vector r ∈ {0,1}^n is used, analyse the one-sided error probability, and state the time complexity advantage over the naive O(n^3) method	CO5	(4)
	OR		
12	(a) A logistics company uses delivery drones to distribute packages between 5 locations: {A, B, C, D, E} To minimize travel cost while ensuring fast computation, the system applies the APPROX-TRAVELLING-SALESMAN algorithm (MST + preorder traversal). Distances between locations: A-B=3, A-C=1, A-D=5, A-E=8, B-C=4, B-D=7, B-E=9, C-D=2, C-E=6, D-E=3. Find the approximate tour and state its cost.	CO5	(6)
	(b) A cybersecurity system is generating encryption keys and must ensure that a selected number is prime before using it in secure communication. The system applies the Miller–Rabin algorithm to test the number is prime or not. Demonstrate the step by step procedure to check a selected number 97 is prime or not	CO5	(4)

****

COURSE DESCRIPTION							
Regulation		**L-T-J-P-S**	**4-0-0-0-4**	**Version**		**Credits**	4
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)							

Course Code	**Course Name**	**Course Category**
M260102/CY100C	**Information Assurance and Security**	**PC**
Pre-requisite		
The student should have basic knowledge of software development, operating systems, and version control concepts.		

COURSE OBJECTIVES	
1	To provide a strong foundation in information assurance and security concepts, including security goals, threats, vulnerabilities, security policies, and cyber defense mechanisms.
2	To develop knowledge of security models, authentication techniques, identity and access management, and access control mechanisms for securing information systems.
3	To enable students to understand risk assessment, security governance, compliance frameworks, auditing practices, and organizational security management strategies.
4	To equip students with the principles and practices of incident response, disaster recovery, business continuity, and security operations in modern computing environments.

COMPETENCY STATEMENT (CC)	
CC1	Apply foundational concepts of information assurance, security principles, authentication, and access control mechanisms to secure information systems and digital assets.
CC2	Analyze and implement risk management, security governance, incident response, and disaster recovery practices for organizational cyber security and business continuity.

COURSE OUTCOMES (CO)

Course Outcomes (CO): At the end of this course, learners will be able to:

CO	**CO Statement**	**CC Mapping**	**Cognitive (C)**	**Psychomotor (P)**	**Affective (A)**
CO1	Explain the fundamental concepts of information assurance, security principles, threats, vulnerabilities, and the CIA triad.	CC1	A		Rs
CO2	Analyse security models, authentication techniques, and access control mechanisms used in secure systems.	CC1	A	M	Rs
CO3	Apply risk assessment, security governance, compliance standards, and security auditing techniques in organizational environments.	CC2	A	P	Val
CO4	Demonstrate knowledge of incident response, disaster recovery, business continuity, and cyber defense practices.	CC2	Ap	M	Val
C05	Implement appropriate security controls and identity management strategies for protecting organizational information assets.	CC1	Ap	P	Val

Cognitive (Revised blooms Level): *- **R**: Remember; **U**: Understand; **A**: Apply; **An**: Analyse; **E**: Evaluate; **C**: Create*
Psychomotor Domain (Dave's): *- **I**-Imitation, **M**-Manipulation, **P**-Precision, **Ar**-Articulation, **N**-Naturalisation*
***Affective (Krathwohl)**: - **Re**-Receiving, **Rs**-Responding, **V**-Valuing, **O**-Organization, **Ch**-Characterization*

CO	**Program Outcomes (PO) & Program Specific Outcomes (PSO) Correlation Matrix**													
	PO											**PSO**		
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**1**	**2**	**3**
1	3	2	–	–	1	–	–	1	–	1	–	2	1	–
2	3	3	2	1	2	–	–	1	–	1	–	3	2	1
3	2	3	2	2	2	1	–	2	1	1	1	3	2	1

4	2	2	2	2	2	1	1	2	1	1	1	2	3	2
5	2	3	3	2	3	1	-	2	1	1	-	3	3	2
Correlation [3 – High, 2 -Medium, 1 – Low]														

TEACHING AND ASSESSMENT SCHEME									
Teaching Scheme / Week					**Credit**	**Hours / Semester**	**Examination Scheme**		
							Theory		
L	**T**	**J**	**P**	**S**	**C**		**CIA**	**ESE**	**Total**
4	0	0	0	4	4	120	40	60	100
***L**: Lecture (One unit is of one-hour duration), **T**: Tutorial (One unit is of one-hour duration), **P**: Practical (One unit is of one-hour duration), **J**: Project (One unit is of one-hour duration), **S**: Self-Learning & Team Work (One unit is of one-hour duration), **CIA**: Continuous Internal Assessment, **ESE**: End Semester Examination*									

SYLLABUS (Major Topics)			
Module	Title	Major Topics	Hrs
1	Introduction to Information Assurance and Security	Introduction to Information Assurance and Security: Fundamentals of information security, Need for security, Security goals and services, CIA Triad (Confidentiality, Integrity and Availability), Security attacks and vulnerabilities, Threat landscape, Principles of information assurance, Security policies and procedures, Basic cryptographic concepts, Security governance and standards, Overview of cyber defense mechanisms. **(Text 1 – Relevant topics from Chapters 1–3, Text 2 – Relevant topics from Chapters 1–2)**	10
2	Security Models, Authentication and Access Control	Security models and principles: Bell-LaPadula model, Biba model, Clark-Wilson model, Authentication mechanisms and authorization, Multi-factor authentication, Biometrics, Identity and Access Management (IAM), Access control models – DAC, MAC and RBAC, Password management, Network security basics, Firewalls, VPNs, Secure communication principles, Security architecture and assurance fundamentals. **(Text 2 – Relevant topics from Chapters 3–6, Text 5 – Relevant topics from Chapters 1–3)**	10
3	Risk Management, Governance and Compliance	Risk assessment and security governance: Risk identification and analysis, Vulnerability assessment, Threat modeling, Risk mitigation strategies, Security auditing and monitoring, Compliance standards and frameworks, Business continuity planning, Enterprise security management, Legal and ethical aspects of information security, Governance policies, Security awareness and training, Cyber security best practices. **(Text 1 – Relevant topics from Chapters 4–6, Text 3 – Relevant topics from Chapters 2–5)**	20
4	Incident Response and Disaster Recovery	Incident response and disaster recovery: Incident handling process, Security operations and monitoring, Intrusion detection and prevention concepts, Digital forensics basics, Disaster recovery planning, Backup and recovery mechanisms, Business continuity management, Cyber incident reporting, Security operations center (SOC) overview, Enterprise security operations, Emerging trends in information assurance and cyber defense. **(Text 3 – Relevant topics from Chapters 6–8, Text 4 – Relevant topics from Chapters 7–10)**	20

SELF-LEARNING / TEAM WORK		
Sl. No	Self-learning / Team Work Description	Hrs
1	Study and present recent cyber security incidents/data breaches and analyze their impact on information assurance principles.	2
2	Self-learning assignment on current security standards/frameworks (ISO 27001, NIST, GDPR, etc.) and prepare a brief report.	2

3	Group case study on risk assessment and incident response planning for an organizational scenario.	2
4	Explore emerging trends in cyber security and information assurance (Zero Trust, AI-based security, cloud security) and prepare a presentation.	2
5	Team activity: Compare different authentication and access control mechanisms (MFA, Biometrics, RBAC, MAC, DAC) and present findings.	2

SUGGESTED LEARNING RESOURCES

Text Book			
Sl. No.	Title of Book	Author	Publication
1	*Information Security: Principles and Practice* (2nd ed.)	Mark Stamp	Wiley

Reference			
Sl. No.	Title of Book	Author	Publication
2	*Computer Security: Principles and Practice* (4th ed.)	William Stallings & Lawrie Brown	Pearson
3	*Information Assurance Fundamentals for IT Professionals*	Corey Schou & Steven Hernandez	McGraw-Hill Education
4	*Security in Computing* (5th ed.)	Charles P. Pfleeger & Shari Lawrence Pfleeger	Pearson
5	*Network Security Essentials: Applications and Standards* (6th ed.)	William Stallings	Pearson

Web Resource	
1	https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content
2	https://www.netacad.com/courses/cybersecurity/introduction-cybersecurity
3	https://www.ibm.com/training/security
4	https://www.isc2.org/training/certified-in-cybersecurity
5	https://portswigger.net/web-security

DETAILED SYLLABUS *(Self-learning if any to be marked)*

Module	Topic	Mode of Delivery	CO	Learning Domain			Hrs
				C	P	A	
1	Fundamentals of Information Security and Need for Security	Lecture	CO1	A	–	Rs	1
	Security goals and services	Lecture	CO1	A	–	Rs	1
	CIA Triad (Confidentiality, Integrity, Availability)	Lecture + Discussion	CO1	A	–	Rs	1
	Security threats, attacks and vulnerabilities	Lecture	CO1	A	–	Rs	1
	Threat landscape and cyber risks	Lecture + Case Study	CO1	A	–	Val	1
	Principles of Information Assurance	Lecture	CO1	A	–	Rs	1
	Security policies and procedures	Lecture	CO1	A	M	Rs	1
	Basic cryptographic concepts	Lecture+ Demonstration	CO1	A	M	Rs	1
	Security governance and standards	Lecture	CO1	A	–	Val	1
	Overview of cyber defense mechanisms	Lecture	CO1	A	–	Val	1

	Security models and principles	Lecture	CO2	A	–	Rs	1
	Bell-LaPadula model	Lecture	CO2	A	–	Rs	1
	Biba model and Clark-Wilson model	Lecture	CO2	A	–	Rs	1
	Authentication and authorization mechanisms	Lecture	CO2	A	M	Rs	1
2	Multi-factor authentication	Lecture + Demonstration	CO2	A	M	Val	1
	Biometrics and Identity Management	Lecture	CO2	A	M	Val	1
	Authentication and authorization mechanisms	Lecture	CO2	A	M	Rs	1
	Multi-factor authentication	Lecture + Demonstration	CO2	A	M	Val	1
	Risk identification and analysis	Lecture	CO3	Ap	M	Val	1
	Vulnerability assessment concepts	Lecture + Demonstration	CO3	Ap	P	Val	1
	Threat modelling techniques	Lecture	CO3	Ap	P	Val	1
	Risk mitigation strategies	Lecture	CO3	Ap	M	Val	1
3	Security auditing concepts	Lecture	CO3	Ap	M	Val	1
	Compliance standards and frameworks	Lecture	CO3	Ap	–	Val	1
	Business continuity planning	Lecture	CO3	Ap	M	Val	1
	Enterprise security management	Lecture	CO3	Ap	M	Val	1
	Legal and ethical aspects of information security	Discussion	CO3	Ap	–	Val	1
	Study a recent cybersecurity compliance framework and prepare a report	Self-learning	CO3	Ap	P	Val	1
	Incident handling process	Lecture	CO4	Ap	M	Val	1
	Security operations and monitoring	Lecture	CO4	Ap	M	Val	1
	Intrusion detection and prevention concepts	Lecture+ Demonstration	CO4	Ap	P	Val	1
	Digital forensics basics	Lecture	CO4	Ap	M	Val	1
	Disaster recovery planning	Lecture	CO4	Ap	M	Val	1
4	Backup and recovery mechanisms	Lecture	CO4	Ap	P	Val	1
	Business continuity management	Lecture	CO4	Ap	M	Val	1
	Cyber incident reporting	Discussion	CO4	Ap	M	Val	1
	Security Operations Center (SOC) overview	Lecture	CO4	Ap	–	Val	1
	Analyze a recent cyber incident and propose a response strategy	Self-learning / Team Activity	CO4	E	Ar	Val	1

TABLE OF SPECIFICATIONS (ToS) (ESE Question Paper Design)								
	Module Title	Distribution of Marks (RBL)						Total Marks
		R	U	A	An	E	C	
1	Introduction to information assurance and security		X	X				15
2	Security models, authentication and Access control		X	X	X			15
3	Risk management, governance and compliance		X	X	X			15
4	Incidence response and disaster recovery		X	X	X			15
Module								

ASSESSMENT PATTERN		
Assessment		**Marks**
Continuous Internal Assessment		**40**
1	Internal Examination	10
2	Learning Activity	10
3	Course Project	20
End Semester Examination – Theory		**60**
Total		**100**

COURSE DESCRIPTION							
Regulation	**2026**	**L-T-J-P-S**	**4-0-0-0-4**	**Version**	**26/0**	**Credits**	**4**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)							

Course Code	Course Name	Course Category
M260102/CY100D	**NETWORK AND SYSTEM SECURITY**	PC

COURSE OBJECTIVES	
1	Understand computer network and operating system security concepts.
2	Analyze network attacks, vulnerabilities and defense mechanisms.
3	Apply firewall, IDS and access control techniques for secure systems.
4	Understand secure communication protocols and protection methods.
5	Develop knowledge in attack detection and system hardening.

COMPETENCY STATEMENTS	
CC1	Demonstrate the ability to analyze network protocols, threats and secure communication mechanisms.
CC2	Demonstrate the ability to apply operating system security, firewalls and intrusion detection techniques.
CC3	Demonstrate the ability to identify attacks, vulnerabilities and suitable defense mechanisms in networked systems.

COURSE OUTCOMES

Course Outcomes (CO): At the end of this course, learners will be able to:

CO	CO Statement	CC Mapping	Cognitive (C)	Psychomotor (P)	Affective (A)
CO1	Explain network and system security fundamentals.	1	U	I	Re
CO2	Apply firewall and intrusion detection mechanisms.	2	A	M	Rs
CO3	Analyze operating system vulnerabilities and attacks.	3	An	P	V
CO4	Evaluate secure communication protocols and defense methods.	1, 3	E	Ar	O
CO5	Design basic protection mechanisms for secure systems.	2, 3	C	N	Ch

Cognitive (Revised blooms Level): *- **R**: Remember; **U**: Understand; **A**: Apply; **An**: Analyse; **E**: Evaluate; **C**: Create*

Psychomotor Domain (Dave's): *- **I**-Imitation, **M**-Manipulation, **P**-Precision, **Ar**-Articulation, **N**-Naturalisation*

***Affective (Krathwohl)**: - **Re**-Receiving, **Rs**-Responding, **V**-Valuing, **O**-Organization, **Ch**-Characterization*

TEACHING AND ASSESSMENT SCHEME

Teaching Scheme / Week				Self-Learning (S) / Semester	Total Hours / Semester	Credits C	Examination Scheme						
L	T	J	P				Theory			Practical			Total
							CIA	ESE	Total	CIA	ESE	Total	
4	0	0	0	4	120	4	40	60	100				100

***L**: Lecture (One unit is of one-hour duration), **T**: Tutorial (One unit is of one-hour duration), **P**: Practical (One unit is of one-hour duration), **J**: Project (One unit is of one-hour duration), **S**: Self-Learning & Team Work (One unit is of one-hour duration), **CIA**: Continuous Internal Assessment, **ESE**: End Semester Examination*

SYLLABUS (Major Topics)			
Module	Title	Major Topics	Contact Hours
1	Network Security Fundamentals	OSI Security Architecture, TCP/IP Security, Network Attacks, Secure Network Design	15
2	Firewalls and Intrusion Detection	Firewall Technologies, IDS/IPS, VPN, Secure Communication Protocols	15
3	Operating System Security	Authentication, Access Control, System Hardening, OS Vulnerabilities	15
4	Attack Defense Mechanisms	Malware Attacks, DoS/DDoS Defense, Security Monitoring, Incident Response	15

SUGGESTED LEARNING RESOURCES			
Text Book			
Sl. No.	Title of Book	Author	Publication
1	Network Security Essentials: Applications and Standards	William Stallings	Pearson Education, 6th Edition
3	Computer Security: Principles and Practice	William Stallings & Lawrie Brown	Pearson Education, 4th Edition
3	Modern Operating Systems	Andrew S. Tanenbaum & Herbert Bos	Pearson Education, 4th Edition
Reference			
Sl. No.	Title of Book	Author	Publication
1	Security Engineering: A Guide to Building Dependable Distributed Systems	Ross Anderson	Wiley, 3rd Edition
2	Operating System Security	Trent Jaeger	Morgan Kaufmann Publications
Web Resource			
1	https://nptel.ac.in/courses/106105031		
2	https://ocw.mit.edu/		
3	https://attack.mitre.org/		

DETAILED SYLLABUS							
Module	Topic	Mode of Delivery	COs	Learning Domain			Hrs
				C	P	A	
1	Introduction to Network Security, OSI Security Architecture	L	CO1	U	I	Re	3
	TCP/IP Protocol Stack Security	L	CO1	U	I	Re	3
	IPv4 and IPv6 Security	L	CO1	A	M	Rs	3
	Common Network Attacks – Spoofing, Sniffing, Session	L	CO1	A	M	Rs	3
	Hijacking, DNS Attacks	L					3
	Secure Network Design Principles	L	CO1	U	I	Re	3

2	Firewall Architecture and Types	L	CO2	U	I	Re	3
	Packet Filtering and Proxy Firewalls	L	CO2	A	M	Rs	3
	Intrusion Detection and Prevention Systems (IDS/IPS)	L	CO2	A	M	Rs	3
	VPN and Secure Tunneling	L	CO2	A	M	Rs	3
	Secure Communication Protocols – SSH, TLS, IPSec	L	CO2	A	M	Rs	3
3	Operating System Security Concepts,	L	CO3	U	I	Re	3
	Authentication and Authorization	L	CO3	A	M	Rs	3
	Access Control Models	L	CO3	A	M	Rs	3
	Password Security	L	CO3	A	M	Rs	3
	System Hardening Techniques	L	CO3	A	M	Rs	3
	Linux and Windows Security Basics	L	CO3	A	M	Rs	3
	Privilege Escalation and Vulnerability Concepts	L	CO3	A	M	Rs	3
4	Malware and Ransomware Attacks	L	CO4	U	I	Re	3
	DoS and DDoS Defense Mechanisms	L	CO4	A	M	Rs	3
	Security Monitoring and Logging	L	CO4	A	M	Rs	3
	Incident Detection and Response	L	CO4	A	M	Rs	3
	Security Auditing	L	CO4	An	P	V	3
	Basic Digital Forensics and Defense Strategies	L	CO4	An	P	V	3

Module	Module Title	Distribution of Marks (Revised Bloom's Level)						Total Marks
		R	U	A	An	E	C	
1	Network security fundamentals		x	x				
2	Firewalls and Intrusion detection		x	x	x			
3	Operating system security		x	x	x			
4	Attack Defense mechanisms		x	x	x			

ASSESSMENT PATTERN	
Assessment	**Marks**
Continuous Internal Assessment	**40**
Learning Activity	10
Internal Examination	10
Course project	20
End Semester Examination	**60**
Total	**100**

MODEL QUESTION PAPER

FIRST SEMESTER M.TECH DEGREE END SEMESTER EXAMINATION, (2026 SCHEME)			
Course Code:	**M260102/CY100D**		
Course Name:	**NETWORK AND SYSTEM SECURITY**		
Max. Marks	**60**	**Duration:**	**2 hours 30 minutes**

For CY Only

Use of Data Book / IS codes, etc to be specified by the question paper setter

PART A

(Answer all questions. Each question carries 5 marks)

No.	*Question*	*CO*	*Marks*
1	A corporate network administrator notices unusual ARP replies flooding the local segment. Identify the specific network attack being described. Explain how this attack disrupts communication and propose two countermeasures at the protocol and network design level to prevent it.	CO1	(5)
2	An organisation's firewall is configured to allow all outbound traffic but block unsolicited inbound connections. An attacker succeeds in establishing a reverse shell from an internal host to an external server. Identify why the firewall failed to prevent this and explain how an IDS/IPS deployed at the network perimeter can detect and block such traffic.	CO2	(5)
3	A Windows domain controller is found to have stored NTLM password hashes accessible to a low-privileged user. Identify the vulnerability, explain how a Pass-the-Hash attack can be executed, and describe three OS-level hardening steps that would have prevented this compromise.	CO3	(5)
4	A university web server experienced a volumetric DDoS attack that saturated its upstream bandwidth. Describe the attack mechanism, identify the DDoS type (volumetric, protocol or application layer), and propose a layered defence strategy involving ISP-level filtering, rate limiting and incident response procedures.	CO4	(5)

PART B

(Answer one full question from each module, each carries 10 marks.)

No.	*Module 1*	*CO*	*Marks*
5	(a) A network security analyst reviewing traffic logs discovers three simultaneous anomalies: (i) TCP SYN packets sent to sequential ports from a single source (ii) ICMP echo requests with oversized payloads (iii) DNS queries returning unusually large responses. For each anomaly, identify the specific attack, explain the exploit mechanism referencing the TCP/IP protocol stack layer involved and recommend a countermeasure at the appropriate OSI layer.	CO1	(6)
	(b)Compare the security features of IPv4 and IPv6 with respect to: (i) IPSec support and implementation (ii) address spoofing susceptibility (iii) multicast security. Explain two secure network design principles (X.800) that address the weaknesses identified.	CO1	(4)
	OR		
6	(a) An attacker on a shared network segment launches a session hijacking attack against an active Telnet session. Using knowledge of TCP/IP sequence number prediction and ARP spoofing, trace the full attack sequence step by step. Identify the protocol-level weaknesses exploited and explain how replacing Telnet with SSH eliminates each weakness.	CO1	(6)

	(b) A network architect is designing a secure network for a hospital. Apply OSI Security Architecture principles to identify the security services and mechanisms required at the network, transport and application layers. Justify your selection for each layer based on the sensitivity of hospital data.	CO1	(4)
No.	***Module 2***	***CO***	***Marks***
7	(a) A financial institution has deployed a stateful packet-filtering firewall at its perimeter. A penetration tester discovers that an attacker can bypass the firewall using: (i) IP fragmentation to split a malicious payload across multiple packets (ii) tunnelling malicious traffic over DNS. For each technique, explain the mechanism of evasion and describe how the firewall rule set must be modified to detect and block these attacks. Illustrate with a sample rule set.	CO2	(6)
	(b) An enterprise deploys a site-to-site IPSec VPN between its headquarters and a branch office. Explain the IPSec tunnel establishment process using IKE Phase 1 and Phase 2. Compare Transport Mode and Tunnel Mode and justify which mode is appropriate for this deployment.	CO2	(4)
	OR		
8	(a) A network IDS generates the following alerts over 10 minutes: 5,000 SYN packets from a single source; 200 failed SSH login attempts from multiple sources; and repeated requests to /admin/config.php returning 403. For each alert: (i) Classify the attack type (ii) Explain the IDS detection method (signature-based or anomaly-based) (iii) Describe how an inline IPS would respond (iv) Write a detection rule in Snort/Suricata syntax.	CO2	(6)
	(b) A company wants to allow remote employees to securely access internal resources. Compare SSL/TLS VPN and IPSec VPN in terms of: (i) protocol stack operation (ii)client requirements (iii)access granularity (iv)suitability for mobile devices. Recommend the appropriate solution with justification.	CO2	(4)
No.	***Module 3***	***CO***	***Marks***
9	(a) A Linux server running a web application is compromised. Post-incident forensic analysis reveals: (i) a SUID binary was exploited for local privilege escalation (ii) a cron job was modified to execute a reverse shell (iii) /etc/passwd was altered to add a backdoor root account. For each finding, identify the vulnerability class, explain the exploitation technique, and describe the system hardening measure that would have prevented it. Reference the principle of least privilege and mandatory access control.	CO3	(6)
	(b)An organisation uses Role-Based Access Control (RBAC) to manage user permissions. Explain the RBAC model and compare it with Discretionary Access Control (DAC) and Mandatory Access Control (MAC) using a scenario involving three users with different privilege levels.	CO3	(4)
	OR		
10	(a) A Windows Active Directory environment is found to be vulnerable to Kerberoasting and Golden Ticket attacks. For each attack: (i) Explain the mechanism by which the attacker obtains and abuses Kerberos tickets (ii) Describe the artefacts left in Windows Event Logs (iii) Outline the SIEM log correlation approach for detection (iv) Propose mitigation measures including password policy enforcement, SPN management and privileged account controls.	CO3	(6)
	(b) Compare the following password storage mechanisms: MD5 hashing, bcrypt and salted SHA-256. For each mechanism, explain its resistance to brute-force and rainbow table attacks and recommend the best approach for a modern	CO3	(4)

	authentication system with justification.		
No.	***Module 4***	***CO***	***Marks***
11	(a) A cloud-hosted e-commerce platform is targeted by a multi-vector DDoS attack combining: (i) a UDP flood saturating upstream bandwidth (volumetric) (ii) a SYN flood exhausting server connection tables (protocol) (iii) an HTTP GET flood targeting the product search API (application layer). For each vector, explain the attack mechanism, identify the targeted layer and design a layered defence incorporating ISP-level BGP blackholing, rate limiting using iptables/nftables and application-layer WAF rules. Describe the incident response steps to restore service availability.	CO4	(6)
	(b) A security operations team configures centralised SIEM monitoring across 50 servers. Describe how logs from firewalls, IDS, web servers and OS audit trails are aggregated and correlated to detect: (i) lateral movement (ii) data exfiltration. Specify the key log sources, correlation rules and alert thresholds for each scenario.	CO4	(4)
	OR		
12	(a) A ransomware incident is detected on a corporate network. The malware has encrypted files on three servers and is spreading laterally via SMB. Following a structured IR plan: (i) Describe the Preparation and Identification phases including IOCs to look for, (ii) Explain the Containment steps including network segmentation and host isolation (iii) Detail the Eradication and Recovery steps including safe restoration from backups (iv) Explain how digital forensics evidence is preserved using chain-of-custody procedures.	CO4	(6)
	(b) A security auditor is evaluating the security posture of a medium-sized enterprise network. Describe a structured security audit process covering: (i) scope definition and asset inventory (ii)vulnerability scanning using open-source tools (iii) log review and configuration audit (iv) reporting with risk ratings. Explain how findings are prioritised using a risk matrix.	CO4	(4)

****

COURSE DESCRIPTION							
Regulation	**2026**	**L-T-J-P-S**	**3-0-0-3-5**	**Version**	**26/0**	**Credits**	**5**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)							

COURSE CODE	COURSE NAME	COURSE CATEGORY
M260102/CY110E	**CYBER SECURITY AND SECURE CODING**	PCE
PRE-REQUISITE		
Nil		

PREAMBLE
This course introduces the principles and practices of cyber security and secure software development. It covers secure coding standards, web application vulnerabilities, malware analysis, penetration testing and Linux system hardening. Students gain hands-on experience using industry-standard open-source tools.

RATIONALE
With rising cyber threats, organizations demand professionals who can build secure systems, detect vulnerabilities and respond to incidents. This course equips students with practical skills in secure coding, web security testing, malware analysis, penetration testing and infrastructure hardening directly aligned with industry roles in application security, SOC analysis and ethical hacking.

COMPETENCY	
CC1	Apply secure software engineering principles to develop, analyse and harden vulnerability-resistant applications.
CC2	Demonstrate proficiency in cyber security tools, attack methodologies and defensive frameworks used in industry.

COURSE OUTCOMES

Course Outcomes (CO): At the end of this course, learners will be able to:

CO	CO Statement	CC Mapping	Cognitive (C)	Psychomotor (P)	Affective (A)
CO1	Apply secure coding standards, input validation, memory safety techniques and DevSecOps practices to build vulnerability-resistant software.	1	A	P	Rs
CO2	Analyse web application vulnerabilities including SQL injection, XSS, CSRF, SSRF and API flaws using open-source security testing tools.	1	An	P	Rs
CO3	Evaluate malware behaviour through static and dynamic analysis and conduct structured penetration tests following PTES and OWASP methodologies.	2	E	Ar	V
CO4	Implement Linux system hardening, secure authentication, container security, IDS/IPS and Zero Trust architecture using compliance frameworks.	2	A	P	V

Cognitive (Revised blooms Level): *- **R**: Remember; **U**: Understand; **A**: Apply; **An**: Analyse; **E**: Evaluate; **C**: Create*
Psychomotor Domain (Dave's): *- **I**-Imitation, **M**-Manipulation, **P**-Precision, **Ar**-Articulation, **N**-Naturalisation*
***Affective (Krathwohl)**: - **Re**-Receiving, **Rs**-Responding, **V**-Valuing, **O**-Organization, **Ch**-Characterization*

TEACHING AND ASSESSMENT SCHEME

Teaching Scheme / Week					Credit	Hours / Semester	Examination Scheme						
							Theory			Practical			Total
L	T	J	P	S	C		CIA	ESE	Total	CIA	ESE	Total	
3	1	0	3	5	5	120	35	40		25			100

***L**: Lecture (One unit is of one-hour duration), **T**: Tutorial (One unit is of one-hour duration), **P**: Practical (One unit is of one-hour duration), **J**: Project (One unit is of one-hour duration), **S**: Self-Learning & Team Work (One unit is of one-hour duration), **CIA**: Continuous Internal Assessment, **ESE**: End Semester Examination*

SYLLABUS (Major Topics)			
Module	**Title**	**Major Topics**	**Hrs**
1	**Secure Coding Fundamentals**	Introduction to Cyber Security and Secure Coding, OWASP Top 10 Vulnerabilities, Secure Coding Standards (CERT C/C++, SEI Guidelines), Input Validation & Output Encoding, Memory Safety - Buffer Overflows, Heap Exploits, Integer Overflows, Static and Dynamic Code Analysis (ASan, UBSan, Taint Tracking), Software Composition Analysis and Supply Chain Security, Secure SDLC and DevSecOps Pipeline	12
2	**Web Security and Vulnerability Testing**	Web Application Architecture and Attack Surface, SQL Injection - Types, Detection and Prevention, Cross-Site Scripting (XSS) and CSRF, Authentication and Session Management Flaws, Secure REST and GraphQL API Development (OWASP API Top 10), Server-Side Request Forgery (SSRF) and XXE Injection, TLS/SSL Configuration and Web Security Headers, DAST and Web Application Firewalls (WAF)	12
3	**Malware Analysis and Penetration Testing**	Malware Classification and Behaviour (MITRE ATT&CK, IOCs), Static Malware Analysis, Dynamic Malware Analysis and Sandboxing, Reverse Engineering and Memory Forensics, Penetration Testing Methodology (PTES, OWASP Testing Guide), Reconnaissance and Exploitation, Cloud and Container Attack Techniques, Ransomware Analysis and Incident Response	12
4	**Linux Security, Authentication and Hardening**	Linux Security Architecture (DAC/MAC, Capabilities, seccomp), Linux Firewall and Audit Tools, Secure Authentication Mechanisms (MFA, FIDO2, OAuth 2.0), Public Key Infrastructure (PKI) and Mutual TLS, Security Hardening and Compliance Automation (CIS, DISA STIG), Network Intrusion Detection and Prevention (IDS/IPS, HIDS), Container and Cloud Security Hardening, SIEM and Zero Trust Architecture (NIST SP 800-207)	12

Sl. No	**Self-learning / Team Work Description**
1	Study the OWASP Top 10 (latest edition) and prepare a comparative report on changes from the previous edition.
2	Explore a recent CVE (Common Vulnerability and Exposure) entry, analyse its impact, and present a mitigation strategy.
3	Perform a self-directed walkthrough of a TryHackMe or HackTheBox free room and document the approach and findings.
4	Study the MITRE ATT&CK framework and map three real-world attack campaigns to ATT&CK tactics and techniques.

SUGGESTED LEARNING RESOURCES

Text Book			
Sl. No.	**Title of Book**	**Author**	**Publication**
1	Secure Coding in C and C++	Robert C. Seacord	Addison-Wesley, 2nd Ed., 2013
2	Writing Secure Code	Michael Howard & David LeBlanc	Microsoft Press, 2nd Ed., 2002
3	The Web Application Hacker's Handbook	Dafydd Stuttard & Marcus Pinto	Wiley, 2nd Ed., 2011
4	Practical Malware Analysis	Michael Sikorski & Andrew Honig	No Starch Press, 2012
5	Hacking: The Art of Exploitation	Jon Erickson	No Starch Press, 2nd Ed., 2008
6	Web Security for Developers	Malcolm McDonald	No Starch Press, 2020

7	Metasploit: The Penetration Tester's Guide	David Kennedy et al.	No Starch Press, 2011

Reference			
Sl. No.	**Title of Book**	**Author**	**Publication**
1	Penetration Testing	Georgia Weidman	No Starch Press, 2014
2	Black Hat Python	Justin Seitz	No Starch Press, 2nd Ed., 2021
3	The Hacker Playbook 3	Peter Kim	Secure Planet, 2018

Web Resource	
1	https://owasp.org/www-project-web-security-testing-guide/
2	https://portswigger.net/web-security
3	https://tryhackme.com

DETAILED SYLLABUS *(Self-learning if any to be marked)*

Module	Topic	Mode of Delivery	CO	Learning Domain			Hrs
				C	P	A	
1	Introduction to Cyber Security and Secure Coding	L	CO1	U	M	Rs	1
	OWASP Top 10 Vulnerabilities	L, P	CO1	A	M	Rs	2
	Secure Coding Standards (CERT C/C++, SEI Guidelines)	L, P	CO1	A	M	Rs	1
	Input Validation and Output Encoding	L, P	CO1	A	M	Rs	3
	Memory Safety - Buffer Overflows, Heap Exploits, Integer Overflows	L, P	CO1	An	P	Rs	2
	Static and Dynamic Code Analysis (ASan, UBSan, Taint Tracking)	L, P	CO1	An	P	Rs	1
	Software Composition Analysis and Supply Chain Security	L, P	CO1	A	P	Rs	2
	Secure SDLC and DevSecOps Pipeline	L, P	CO1	A	P	V	1
2	Web Application Architecture & Attack Surface	L, P	CO2	U	M	Rs	3
	SQL Injection - Types, Detection & Prevention	L, P	CO2	An	P	Rs	2
	Cross-Site Scripting (XSS) and CSRF	L, P	CO2	An	P	Rs	1
	Authentication and Session Management Flaws	L, P	CO2	An	P	Rs	2
	Secure REST and GraphQL API Development (OWASP API Top 10)	L, P	CO2	A	P	Rs	1
	Server-Side Request Forgery (SSRF) and XXE Injection	L, P	CO2	An	P	Rs	3
	TLS/SSL Configuration and Web Security Headers	L, P	CO2	A	P	Rs	2
	DAST and Web Application Firewalls (WAF)	L, P	CO2	A	P	V	1
3	Malware Classification and Behaviour (MITRE ATT&CK, IOCs)	L, P	CO3	U	M	Rs	2
	Static Malware Analysis	L, P	CO3	An	P	Rs	1
	Dynamic Malware Analysis and Sandboxing	L, P	CO3	An	P	Rs	3
	Reverse Engineering and Memory Forensics	L, P	CO3	An	P	Rs	2
	Penetration Testing Methodology (PTES, OWASP Testing Guide)	L, P	CO3	A	P	Rs	1
	Reconnaissance and Exploitation	L, P	CO3	An	P	Rs	2
	Cloud and Container Attack Techniques	L, P	CO3	An	P	V	1
	Ransomware Analysis and Incident Response	L, P	CO3	E	Ar	V	3

4	Linux Security Architecture (DAC/MAC, Capabilities, seccomp)	L, P	CO4	U	M	Rs	2
	Linux Firewall and Audit Tools	L, P	CO4	A	P	Rs	1
	Secure Authentication Mechanisms (MFA, FIDO2, OAuth 2.0)	L, P	CO4	A	P	Rs	2
	Public Key Infrastructure (PKI) and Mutual TLS	L, P	CO4	A	P	Rs	1
	Security Hardening and Compliance Automation (CIS, DISA STIG)	L, P	CO4	E	P	V	3
	Network Intrusion Detection and Prevention (IDS/IPS, HIDS)	L, P	CO4	A	P	Rs	2
	Container and Cloud Security Hardening	L, P	CO4	E	P	V	1
	SIEM and Zero Trust Architecture (NIST SP 800-207)	L, P	CO4	E	Ar	V	2

PRACTICAL SYLLABUS

Module	Objective	CO	Learning Domain			Hrs
			C	P	A	
1	Set up Kali Linux lab; verify GCC hardening flags and binary protections using checksec	CO1	A	M	Rs	3
1	Identify and exploit OWASP Top 10 vulnerabilities on DVWA and WebGoat	CO1	A	M	Rs	3
1	Perform code review and CERT C rule application using Semgrep and Cppcheck	CO1	A	M	Rs	3
1	Write input validation routines in Python/C and perform fuzz testing with AFL++	CO1	A	M	Rs	3
1	Build a DevSecOps CI/CD pipeline integrating Semgrep SAST and Trivy container scan	CO1	A	P	V	3
2	Intercept and map HTTP/S traffic using mitmproxy and Wireshark	CO2	A	M	Rs	3
2	Perform manual and automated SQL injection on DVWA using SQLmap	CO2	An	P	Rs	3
2	Conduct XSS attack and defence exercises; implement CSRF token protection on WebGoat	CO2	An	P	Rs	3
2	Audit TLS configuration with testssl.sh; implement CSP and HSTS headers on Nginx	CO2	A	P	Rs	3
2	Conduct full active scan with OWASP ZAP; write ModSecurity CRS rules	CO2	A	P	V	3
3	Set up REMnux workstation; classify malware samples using YARA rules and ClamAV	CO3	A	M	Rs	3
3	Perform end-to-end penetration test on Metasploitable 2 and write a formal pentest report	CO3	A	P	Rs	3
3	Conduct reconnaissance with Nmap and theHarvester; exploit target using Metasploit Framework	CO3	An	P	Rs	3
3	Perform IAM privilege escalation using CloudGoat; execute Kubernetes RBAC abuse on minikube	CO3	An	P	V	3
3	Analyse defanged ransomware sample using Ghidra and Volatility; conduct IR tabletop simulation	CO3	E	Ar	V	3
4	Configure SELinux and AppArmor policies; apply seccomp-BPF filter using libseccomp	CO4	A	M	Rs	3
4	Write nftables rule sets for multi-tier topology; configure auditd privilege escalation logging	CO4	A	P	Rs	3
4	Implement TOTP-based MFA using pyotp and FreeOTP; set up FIDO2 demo server with python-fido2	CO4	A	P	Rs	3
4	Scan Docker images with Trivy; harden Kubernetes deployment with RBAC and kube-bench audit	CO4	E	P	V	3
4	Ingest system and Suricata logs into ELK Stack; build threat correlation dashboards	CO4	E	Ar	V	3

ASSESSMENT PATTERN

Assessment	Marks
Continuous Internal Assessment	**60**
Internal Examination	10
Continuous Lab Assessment	25
Learning Activity/Seminar	10
Course Project	15
End Semester Examination-Theory	**40**
Total	**100**

COURSE DESCRIPTION							
Regulation	**2026**	**L-T-J-P-S**	**2-0-0-0-1**	**Version**	**26/0**	**Credits**	**2**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)							

Course Code	Course Name	Course Category
M260904/CN100K	**RESEARCH METHODOLOGY AND IPR**	GENERAL COURSE

COURSE OBJECTIVES	
1	Approach research projects with enthusiasm and creativity.
2	Conduct literature survey and define research problem.
3	Adopt suitable methodologies and tools to design experiments, develop models, analyze data, and validate research findings.
4	Evaluate publication quality and Publish/Patent research outcome.
5	Apply the concepts of Intellectual Property Rights, patents, and patenting procedures in research and innovation.

COMPETENCY STATEMENTS	
CC1	Conduct Independent Research – Demonstrate the ability to plan and execute research projects from problem identification to dissemination of results, while adhering to ethical guidelines.
CC2	Disseminate Research and Protect Intellectual Work – Demonstrate the ability to evaluate publication quality, select appropriate publication avenues, and publish or patent research outcomes effectively.
CC3	Apply Intellectual Property Rights in Research – Demonstrate the ability to apply Intellectual Property Rights principles, patents, and patenting procedures to protect research outcomes and technological innovations.

COURSE OUTCOMES

Course Outcomes (CO): At the end of this course, learners will be able to:

CO	CO Statement	CC Mapping	Cognitive (C)	Psychomotor (P)	Affective (A)
CO1	Approach research projects with enthusiasm and creativity. (Cognitive Knowledge Level: Understand)	CC1	U	M	Rs
CO2	Conduct literature survey and define research problem. (Cognitive Knowledge Level: Apply)	CC1	A	P	V
CO3	Adopt suitable methodologies and tools to design experiments, develop models, analyze data, and validate research findings. (Cognitive Knowledge Level: Apply)	CC1	A	Ar	V
CO4	Evaluate publication quality and Publish/Patent research outcome. (Cognitive Knowledge Level: Create)	CC2	C	Ar	O
CO5	Apply the concepts of Intellectual Property Rights, patents, and patenting procedures in research and innovation. (Cognitive Knowledge Level: Evaluate	CC3	E	P	O

Cognitive (Revised blooms Level): *- **R**: Remember; **U**: Understand; **A**: Apply; **An**: Analyse; **E**: Evaluate; **C**: Create*
Psychomotor Domain (Dave's): *- **I**-Imitation, **M**-Manipulation, **P**-Precision, **Ar**-Articulation, **N**-Naturalisation*
***Affective (Krathwohl)**: - **Re**-Receiving, **Rs**-Responding, **V**-Valuing, **O**-Organization, **Ch**-Characterization*

CO	PROGRAM OUTCOMES (PO) CORRELATION MATRIX						
	PO						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1	3	2	2	1	1	3	2
2	3	2	2	2	2	2	1
3	3	2	3	3	3	2	1

4	2	3	2	1	1	2	1
5	3	3	3	2	3	2	2
Correlation levels: 1 - Low; 2 - Medium; 3 - High; No Correlation - "-"							

TEACHING AND ASSESSMENT SCHEME

Teaching Scheme / Week				Self-Learning (S) / Semester	Total Hours / Semester	Credits C	Examination Scheme						
L	T	J	P				Theory			Practical			Total
							CIA	ESE	Total	CIA	ESE	Total	
2	0	0	0	10	(34+10)	2	40	60	100				100

***L**: Lecture (One unit is of one-hour duration), **T**: Tutorial (One unit is of one-hour duration), **P**: Practical (One unit is of one-hour duration), **J**: Project (One unit is of one-hour duration), **S**: Self-Learning & Team Work (One unit is of one-hour duration), **CIA**: Continuous Internal Assessment, **ESE**: End Semester Examination*

SYLLABUS (Major Topics)

Module	Title	Major Topics	Contact Hours
1	Introduction to Research Methodology	Meaning of Research, Research process, Thinking skills, Introduction to Research Ethics and Publication Ethics, Overview of AI in research.	6
2	Literature Survey and Problem Definition	Literature survey process, Sources of literature, Identifying research gaps and formulating research objectives/hypotheses, AI tools for literature survey.	9
3	Experimental and Modelling Skills	Principles of experimental design, Scientific method, Mathematical and computational modelling approaches. Validation and verification of results, AI tools for data analysis and modelling.	5
4	Publication/Patents	Types of intellectual property, Research metrics-Journal Level, AI in publication.	7
5	IPR	Nature of Intellectual Property, Process of Patenting and Development, International Scenario, Procedure for grants of patents, Patenting under PCT, Patent Rights, Geographical Indications, IPR issues related to AI-generated content, Ownership of AI-assisted research outputs	7

SELF-LEARNING / TEAM WORK

Sl. No	Self-learning / Team Work Description	Hrs/Semester
1	Write a summary of "You and Your Research"-by Richard Hamming	1
2	Read a research paper of their interest and summarize it .	3
3	Make a study about tools of literature management and present it.	2
4	Analyze the peer review process and explore journal quality metrics (impact factor, indexing). (Group Activity)	1
5	Prepare a report comparing open access vs. subscription-based publishing.	1
6	Conduct a study and prepare a report on research visibility tools and citation metrics.	1
7	Study the patenting process and prepare a report on patent filing procedures, including PCT and Geographical Indications.	1

SUGGESTED LEARNING RESOURCES

Text Book

Sl. No.	Title of Book	Author	Publication
1	Research Methodology: Methods and Techniques	C.R. Kothari & Gaurav Garg	New Age International, 4th Ed., 2019.

2	Research and Publication Ethics	Santosh Kumar Yadav	Springer Nature, 2023
3	Institutional guide to using AI for research	Xue Zhou & Hosam Al-Samarraie	Springer, 2025
4	Design and Analysis of Experiments	Montgomery, D.C	Wiley, 9th Ed., 2017
5	Applied Multivariate Statistical Analysis	Johnson, R.A., Wichern, D.W.	Pearson, 6th Ed., 2014.
6	The Craft of Scientific Writing	Michael Alley	Springer, 4th Ed., 2018
7	Intellectual Property: The Law of Trademarks, Copyrights, Patents, and Trade Secrets	Deborah E. Bouchoux	Cengage Learning, 6th Ed., 2020.
Reference			
Sl. No.	Title of Book	Author	Publication
1	Research Methodology: A Step-by-Step Guide for Beginners	Ranjit Kumar	Sage Publications, 5th Ed., 2022.
2	Writing Your Thesis	Paul Oliver	Sage Publications, 4th Ed., 2014
3	Intellectual Property Rights: Unleashing the Knowledge Economy	Prabuddha Ganguli	McGraw-Hill, 2nd Ed., 2011.
Web Resource			
1	https://nptel.ac.in/courses/12110600		
2	https://ocw.mit.edu		
3	https://www.youtube.com/watch?v=6BArSbZ2Gcw		

DETAILED SYLLABUS

Module	Topic	Mode of Delivery	COs	Learning Domain Level			Hrs
				C	P	A	
1	Meaning and significance of research, Types of research	Lecture	CO1	U	M	Rs	1
	Characteristics of good research, Research process	Lecture	CO1	U	M	Rs	1
	Role of research in technological and societal development, Introduction to Research Ethics and Publication Ethics, Overview of AI in research.	Lecture	CO1	U	M	V	1
	Thinking skills: Levels and styles of thinking, common-sense and scientific thinking, examples, logical thinking, division into sub-problems, verbalization and awareness of scale.	Lecture	CO1	U	M	Rs	1
	Creativity: Some definitions, illustrations from day to day life, intelligence versus creativity, creative process, requirements for creativity	Lecture	CO1	U	M	V	1
	Motivation for research: Motivational talks on research: "You and Your Research"- Richard Hamming	Tutorial (Self Study)	CO1	U	M	V	1
2	Literature survey process: Planning,	Lecture	CO2	U	P	V	1

	searching, screening, analyzing, and synthesizing.						
	Information gathering – reading, searching and documentation, types of literature, Sources of literature	Lecture	CO2	U	P	V	1
	Integration of research literature and identification of research gaps	Lecture	CO2	U	P	V	1
	Attributes and sources of research problems, problem formulation, Research question, multiple approaches to a problem	Lecture	CO2	U	P	V	1
	Problem solving strategies – reformulation or rephrasing, techniques of representation, Importance of graphical representation, examples. Defining research scope and limitations.	Lecture	CO2	U	P	V	1
	Tools for literature management: Mendeley, Zotero, EndNote, AI tools for literature survey (Scite, Semantic Scholar, ChatGPT, Connected Papers)	Tutorial (Self Study)	CO2	A	P	V	1
	Identify a standard research paper in respective area and summarize it based on the problem addressed, methods used, advantages, disadvantages and future directions	Tutorial (Self Study)	CO1	A	P	V	1
3	Scientific method, role of hypothesis in experiment, units and dimensions, dependent and independent variables, Principles of experimental design: Control, randomization, replication.	Lecture	CO3	U	Ar	V	1
	Precision and accuracy, need for precision, definition, detection, estimation and reduction of random errors, Statistical tools for data analysis Validation and verification of results, definition, detection and elimination of systematic errors.	Lecture	CO3	U	Ar	V	1
	Sampling methods and sample size determination.	Lecture	CO3	U	P	V	1
	Mathematical and computational modelling approaches. Types of models, stages in modelling, curve fitting, the role of approximations, problem representation, logical reasoning, mathematical skills.	Lecture	CO3	U	Ar	V	1
	Continuum/meso/micro scale approaches for numerical simulation, AI tools for data analysis and modelling(SPSS, R, Pandas, NumPy, Power BI, Tableau).	Lecture	CO3	U	Ar	V	1
4	Relative importance of various forms of publication, Choice of journal and reviewing process, Stages in the realization of a paper.	Lecture	CO4	A	Ar	O	1
	Research metrics -Journal level, Article level and Author level, Plagiarism and research ethics.	Lecture	CO4	U	P	O	1
	Introduction to IPR, Concepts of IPR, Types of IPR	Lecture	CO4	U	P	O	1
	Common rules of IPR practices, Types and Features of IPR Agreement, Trademark,	Lecture	CO4	U	P	O	1

	trade secrets						
	Patents- Concept, Objectives and benefits, features, Patent search, filing process, and case studies in India & abroad.	Lecture	CO4	An	Ar	O	1
	Peer-review process and journal selection.	Tutorial (Self Study)	CO4	U	Ar	O	1
	Open access vs. subscription-based publishing, Research visibility: ORCID, ResearchGate, Google Scholar profiles, AI in publication: Use of AI writing tools (ChatGPT, Grammarly), Journal policies on AI-generated content.	Tutorial (Self Study)	CO4	U	Ar	O	1
5	Nature of Intellectual Property: Patents, Designs, Trade and Copyright.	Lecture	CO5	U	P	O	1
	Process of Patenting and Development: technological research	Lecture	CO5	U	P	O	1
	Innovation, patenting, development.	Lecture	CO5	U	P	O	1
	International Scenario: International cooperation on Intellectual Property	Lecture	CO5	U	P	O	1
	Procedure for grants of patents	Lecture	CO5	An	P	O	1
	Patenting under PCT	Tutorial (Self Study)	CO5	U	P	O	1
	Patent Rights: Scope of Patent Rights, Geographical Indications, IPR issues related to AI-generated content, Ownership of AI-assisted research outputs.	Tutorial (Self Study)	CO5	U	P	O	1

TABLE OF SPECIFICATIONS (ToS) FOR QUESTION PAPER DESIGN

Module	Module Title	Teaching Hours	Distribution of Marks (Revised Bloom's Level)						Total Marks
			R	U	A	An	E	C	
1	Introduction to Research Methodology	6	X	X	–	–	–	–	6
2	Literature Survey and Problem Definition	9	–	X	X	–	–	–	6
3	Experimental and Modelling Skills	5	–	–	X	X	–	–	6
4	Publication/Patents	7		X	X	X	–	–	6
5	IPR	7		X		X			6
Research Paper Analysis						X			30
This ToS shall be treated as a general guideline for students and teachers for distribution of marks.									

ASSESSMENT PATTERN	
Assessment	**Marks**
Continuous Internal Assessment	**40**
Learning Activity	30
Internal Examination	10
End Semester Examination	**60**
Total	**100**

MODEL QUESTION PAPER

Total Pages: …….			
Register No.:	……	Name:	……

(AN AUTONOMOUS COLLEGE AFFILIATED TO APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY, THIRUVANATHAPURAM)

FIRST SEMESTER M. TECH DEGREE (REGULAR) EXAMINATION, NOV 2026 (2026 SCHEME)			
Course Code:	**M260904/CN100K**		
Course Name:	**RESEARCH METHODOLOGY AND IPR**		
Max. Marks	**60**	**Duration**:	2 hours 30 minutes
Specify if the question paper is common to different programmes			
Use of Data Book / IS codes, etc to be specified by the question paper setter			

Answer all questions. Each question carries 5 marks

No.	*Question*	*CO*	*Marks*
1	Discuss the salient recommendations for great research recommended by Richard Hamming in his famous talk "You and Your Research".	CO1	5
2	What are the characteristics of a good research question? Discuss with an example.	CO2	5
3	Explain the difference between continuum, meso-scale and micro-scale approaches for numerical simulation.	CO3	5
4	Discuss any four rules of scientific writing.	CO4	5
5	What are the requirements for patentability?	CO5	5
6	What are the differences between copyright and trademark protection?	CO5	5
7	What is the main research problem addressed?	CO2	3
8	Identify the type of research.	CO2	3
9	Outline the process of transforming a research innovation into a patentable outcome and compare it with the publication process	CO4	6
10	Evaluate the role of Intellectual Property Rights in academic research and industrial innovation	CO5	6
11	Compare and evaluate the suitability of patents, copyrights, trademarks, and trade secrets for protecting different types of intellectual property.	CO5	6
12	Propose the major steps involved in converting a research outcome into a publishable journal article.	CO4	6

****