

M. TECH CYBER SECURITY

CURRICULUM & SYLLABUS

2026
REGULATION



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		

PREAMBLE
This course provides advanced knowledge of cryptographic principles, algorithms, and protocols used to secure modern information and communication systems. It emphasizes the mathematical foundations, practical applications, and secure implementation of cryptographic techniques.

RATIONALE
- To develop a strong foundation in number theory, modular arithmetic, finite fields, and mathematical concepts underlying modern cryptography. - To provide advanced knowledge of symmetric and asymmetric encryption, hashing, digital signatures, authentication, and public-key infrastructure. - To enable students to analyze and apply cryptographic protocols for secure communication and real-world cybersecurity 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					

TEACHING AND ASSESSMENT SCHEME												
Teaching Scheme / Week				Self-Learning (S) / Semester	Total Hours / Semester	Credits C	Examination Scheme					
L	T	J	P				Theory			Practical		
							CIA	ESE	Total	CIA	ESE	Total
3	0	0	0	45	90	3	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	Hrs
				C	
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

MODEL QUESTION PAPER

(AFFILIATED TO APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY, THIRUVANANTHAPURAM)

FIRST SEMESTER M. TECH DEGREE END SEMESTER EXAMINATION, (2026 SCHEME)			
Course Code:	M260102/CY100A		
Course Name:	APPLIED CRYPTOGRAPHY		
Max. Marks	60	Duration:	2 hours 30 minutes
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	During a classroom discussion, Rahul asserts that the congruence relation (e.g., congruence modulo n) is an equivalence relation, while Rohit disagrees and claims it lacks the necessary properties. Decide who is correct and justify your answer by formally testing the congruence relation against all three properties of an equivalence relation	CO1	(5)														
2	A government agency needs to securely transmit confidential documents between departments. Their existing system uses a symmetric encryption algorithm that has become vulnerable due to its short key length. To improve security without replacing the entire system, engineers apply the same encryption algorithm multiple times using different secret keys before transmitting the data. Identify the encryption technique used in this approach and discuss two strengths of using this method compared to applying the encryption algorithm only once.	CO2	(5)														
3	Cryptographic Concepts and Applications: Instructions: Match each cryptographic concept in Column A with the appropriate real-world scenario in Column B. Write your answers as pairs (e.g., A-1). <table><tr><th>Column A (Cryptographic Concept)</th><th>Column B (Appropriate Scenario)</th></tr><tr><td>A. SHA-256</td><td>1. A government portal uses an elliptic-curve based method to sign digital documents so that recipients can verify the sender's identity.</td></tr><tr><td>B. HMAC</td><td>2. A banking application generates a verification code using a secret key and message to ensure the data has not been altered during transmission.</td></tr><tr><td>C. CMAC</td><td>3. A software system uses a block-cipher-based method with a shared key to verify the integrity of messages exchanged between two devices.</td></tr><tr><td>D. ECDSA</td><td>4. A modern hashing approach designed using a sponge construction for generating secure message digests.</td></tr><tr><td>E. Public Key Infrastructure (PKI)</td><td>5. An organization <u>issues</u> and manages digital certificates so that users can trust secure websites and encrypted emails.</td></tr><tr><td></td><td>6. A block chain system generates a fixed-length hash of each block to maintain integrity and link blocks securely.</td></tr></table>	Column A (Cryptographic Concept)	Column B (Appropriate Scenario)	A. SHA-256	1. A government portal uses an elliptic-curve based method to sign digital documents so that recipients can verify the sender's identity.	B. HMAC	2. A banking application generates a verification code using a secret key and message to ensure the data has not been altered during transmission.	C. CMAC	3. A software system uses a block-cipher-based method with a shared key to verify the integrity of messages exchanged between two devices.	D. ECDSA	4. A modern hashing approach designed using a sponge construction for generating secure message digests.	E. Public Key Infrastructure (PKI)	5. An organization <u>issues</u> and manages digital certificates so that users can trust secure websites and encrypted emails.		6. A block chain system generates a fixed-length hash of each block to maintain integrity and link blocks securely.	CO3	(5)
Column A (Cryptographic Concept)	Column B (Appropriate Scenario)																
A. SHA-256	1. A government portal uses an elliptic-curve based method to sign digital documents so that recipients can verify the sender's identity.																
B. HMAC	2. A banking application generates a verification code using a secret key and message to ensure the data has not been altered during transmission.																
C. CMAC	3. A software system uses a block-cipher-based method with a shared key to verify the integrity of messages exchanged between two devices.																
D. ECDSA	4. A modern hashing approach designed using a sponge construction for generating secure message digests.																
E. Public Key Infrastructure (PKI)	5. An organization <u>issues</u> and manages digital certificates so that users can trust secure websites and encrypted emails.																
	6. A block chain system generates a fixed-length hash of each block to maintain integrity and link blocks securely.																
4	Fill in the blank for each statement by selecting the correct option provided next to it. i. The Diffie-Hellman protocol is primarily designed for secure _____ (digital signatures, key exchange, data encryption) over an insecure communication channel. ii. The _____ (FTP, SSL/TLS, HTTP) protocol is widely used to provide secure communication and data privacy over the internet for web browsing and messaging. iii. A _____ (Man-in-the-Middle, SQL Injection, Buffer Overflow) attack occurs when an unauthorized adversary secretly intercepts and relays communications between two parties who believe they are directly communicating with each other. iv. In the security evaluation of cryptographic systems, the amount of computational resources required to break a cipher is often measured in	CO4	(5)														

	terms of _____ (physical, operational, computational) security.		
	v. Protocols like Diffie-Hellman and ElGamal rely heavily on the mathematical difficulty of solving _____ (binary, discrete, floating-point) logarithms.		
PART B			
(Answer all questions. Each question carries 10 marks)			
No.	Question	CO	Marks
5	A cryptographic algorithm performs arithmetic operations over the finite field $GF(2^4)$ using the irreducible polynomial $p(x) = x^4 + x + 1.$ Let $A(x) = x^3 + x + 1$ and $B(x) = x^2 + x + 1.$ a) Perform the multiplication $A(x)B(x)$ over $GF(2)$. (3 marks) b) Reduce the resulting polynomial modulo $p(x)$ to obtain the corresponding element in $GF(2^4)$. (4 marks) c) Explain how finite-field arithmetic supports the security and implementation of modern cryptographic algorithms. (3 marks)	CO1	10
OR			
6	Imagine you are a cybersecurity engineer developing an end-to-end encrypted messaging application. During user onboarding, the system generates a pair of cryptographic keys. For a specific user session, the system selects a public parameter $a = 43$ and a system modulus $m = 128$. To successfully derive the corresponding private key required to decrypt incoming messages, the application must compute a modular multiplicative inverse. a) Use the Extended Euclidean Algorithm to determine whether the multiplicative inverse of the parameter $a = 43$ modulo $m = 128$ exists. Show all your working steps clearly. [4 marks] b) If the inverse exists, calculate its exact value so the messaging application can successfully finalize the user's private key component. [3 marks] c) In the context of this messaging application, explain how this computed inverse functions within the key-generation process, and discuss why the mathematical condition $\gcd(a, m) = 1$ is strictly mandatory to prevent system failure. [3 marks]	CO1	10
7	An e-commerce platform encrypts sensitive customer information before transmitting it to its server using the RSA algorithm. The system administrator selects two prime numbers and a public exponent to generate the public key. A small message representing a transaction code must be encrypted before being sent. Given: P=3, Q=11, e=3, and message M=9. Perform RSA encryption to determine the cipher text C. Show the necessary calculations.	CO2	10
OR			
8	During a covert military mission, two field commanders stationed in different locations need to establish a secure communication channel to coordinate their strategy. Since their messages are transmitted over an open network that could be intercepted by enemy forces, they decide to generate a common secret key using the Diffie-Hellman key exchange. Both commanders publicly agree on the following parameters: - Prime number $q=353$ - Primitive root $g=3$ Each commander then secretly selects a private key: - Commander A chooses $X_a=97$ - Commander B chooses $X_b=233$ They exchange their computed public values over the insecure channel and then independently compute the same shared secret key, which will later be used to encrypt their military messages.	CO2	10

	i. Calculate the public value of Commander A Y_a ii. Calculate the public value of Commander B Y_b iii. Determine the shared secret key K generated by both commanders. Show all intermediate steps involved in the Diffie–Hellman key exchange process.		
9	A company stores user passwords in its database using SHA-256 instead of saving them in plain text. Explain how SHA-256 works as a cryptographic hash function and how it helps protect user passwords.	10	CO3
OR			
10	A software company is deploying a secure web portal where users must safely exchange encrypted information with the server. To ensure that users can trust the server's public key and prevent impersonation attacks, the system implements Public Key Infrastructure using Digital Certificate. As a cyber-security engineer, you are asked to analyze how the system ensures secure key distribution. Using the concept of PKI, illustrate how digital certificates enable the secure distribution and management of public keys in this system.	10	CO3
11	A company is developing an online banking application that requires secure communication between customers and the bank server. The application must establish a secure session over an insecure public network and protect the exchanged data from eavesdropping and man-in-the-middle attacks. a) Explain how a key exchange protocol can be used to establish a shared secret key between the client and server. (4 marks) b) Describe how SSL/TLS uses the established cryptographic parameters to provide confidentiality, integrity, authentication, and secure communication. (4 marks) c) Identify one possible attack during the key-exchange/handshake process and state how TLS can mitigate it. (2 marks)	10	CO4
OR			
12	A healthcare organization uses a cryptographic protocol to securely transmit patient information between two servers. During a security audit, it is suspected that an attacker may intercept, modify, and replay messages exchanged between the servers. a) Apply your knowledge of cryptographic protocol attacks to explain how a man-in-the-middle or replay attack could be carried out against the communication protocol. (4 marks) b) Propose suitable modifications to the protocol to prevent the identified attack. (3 marks) c) Describe three security properties/criteria that should be evaluated to determine whether the cryptographic system provides adequate security. (3 marks)	10	CO4

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						
L	T	J	P	S	120	C	Theory			Practical			Total
							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 Deliver y	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 √)

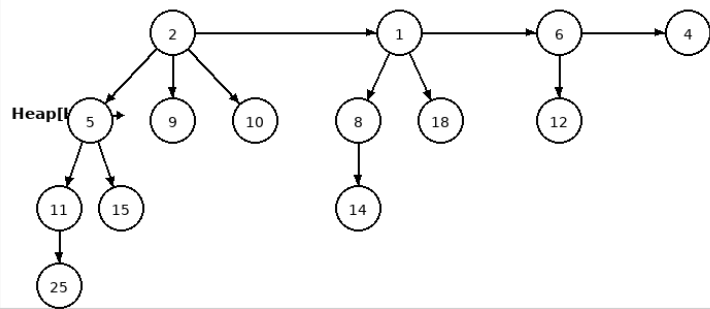
Module	Module Title	Distribution of Marks (RBL)						Total Marks
		R	U	A	An	E	C	
1	Amortized analysis and String matching		X	X				15
2	Advanced data structures		X	X				15
3	Network flow		X	X				15
4	Probabilistic algorithms & Approximation algorithms		X	X				15
<i>This ToS shall be treated as a general guideline for students and teachers for distribution of marks.</i>								

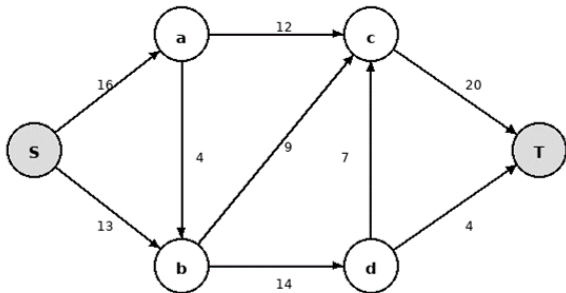
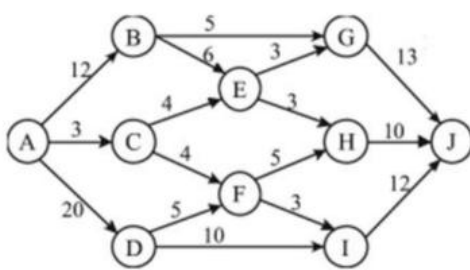
ASSESSMENT PATTERN

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

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. (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	(6)
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. (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	(6)
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: Flow Network  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. (b) Describe the Monte Carlo algorithm for verifying matrix multiplication $AB = C$ for $n \times n$ matrices. Explain how a random vector $r \in \{0,1\}^n$ is used, analyse the one-sided error probability, and state the time complexity advantage over the naive $O(n^3)$ method	CO5	(6)
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. (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	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/CY100C	INFORMATION ASSURANCE AND SECURITY	PC
Pre-requisite		
The student should have basic knowledge of software development, operating systems, and version control concepts.		

PREAMBLE
This course introduces the fundamental concepts and practices of Information Assurance and Security, focusing on protecting information assets against threats, vulnerabilities, and cyber attacks. It covers security principles, authentication and access control mechanisms, risk assessment, governance and compliance frameworks, incident response, and disaster recovery. The course equips students with the knowledge and skills required to analyze security risks, design secure systems, and implement effective security management strategies in organizational environments.

RATIONALE
- Provides fundamental knowledge of information assurance and cybersecurity principles. - Develops skills to identify, assess, and mitigate security risks. - Introduces authentication, access control, and security governance mechanisms. - Enhances understanding of incident response and disaster recovery practices. - Prepares students to address real-world information security challenges in organizations.

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
CO5	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					

TEACHING AND ASSESSMENT SCHEME									
Teaching Scheme / Week					Credit	Hours / Semester	Examination Scheme		
L	T	J	P	S			Theory		
							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	<i>Information Security: Principles and Practice</i> (2nd ed.)	Mark Stamp	Wiley

Reference			
Sl. No.	Title of Book	Author	Publication
2	<i>Computer Security: Principles and Practice</i> (4th ed.)	William Stallings & Lawrie Brown	Pearson
3	<i>Information Assurance Fundamentals for IT Professionals</i>	Corey Schou & Steven Hernandez	McGraw-Hill Education
4	<i>Security in Computing</i> (5th ed.)	Charles P. Pfleeger & Shari Lawrence Pfleeger	Pearson
5	<i>Network Security Essentials: Applications and Standards</i> (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
2	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
	Multi-factor authentication	Lecture +	CO2	A	M	Val	1

		Demonstration					
	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
3	Risk identification and analysis	Lecture	CO3	A p	M	Val	1
	Vulnerability assessment concepts	Lecture + Demonstration	CO3	A p	P	Val	1
	Threat modelling techniques	Lecture	CO3	A p	P	Val	1
	Risk mitigation strategies	Lecture	CO3	A p	M	Val	1
	Security auditing concepts	Lecture	CO3	A p	M	Val	1
	Compliance standards and frameworks	Lecture	CO3	A p	–	Val	1
	Business continuity planning	Lecture	CO3	A p	M	Val	1
	Enterprise security management	Lecture	CO3	A p	M	Val	1
	Legal and ethical aspects of information security	Discussion	CO3	A p	–	Val	1
	Study a recent cybersecurity compliance framework and prepare a report	Self-learning	CO3	A p	P	Val	1
4	Incident handling process	Lecture	CO4	A p	M	Val	1
	Security operations and monitoring	Lecture	CO4	A p	M	Val	1
	Intrusion detection and prevention concepts	Lecture+ Demonstration	CO4	A p	P	Val	1
	Digital forensics basics	Lecture	CO4	A p	M	Val	1
	Disaster recovery planning	Lecture	CO4	A p	M	Val	1
	Backup and recovery mechanisms	Lecture	CO4	A p	P	Val	1
	Business continuity management	Lecture	CO4	A p	M	Val	1
	Cyber incident reporting	Discussion	CO4	A p	M	Val	1
	Security Operations Center (SOC) overview	Lecture	CO4	A p	–	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

MODEL QUESTION PAPER

(AFFILIATED TO APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY, THIRUVANANTHAPURAM)

FIRST SEMESTER M. TECH DEGREE END SEMESTER EXAMINATION, (2026 SCHEME)			
Course Code:	M260102/CY100C		
Course Name:	INFORMATION ASSURANCE AND SECURITY		
Max. Marks	60	Duration:	2 hours 30 minutes
<i>Use of Data Book / IS codes, etc to be specified by the question paper setter</i>			

PART A													
(Answer all questions. Each question carries 5 marks)													
No.	Question	CO	Marks										
1	A university network uses a firewall to control incoming and outgoing traffic. State two security functions performed by the firewall and mention one limitation of relying only on a firewall.	CO1	(5)										
2	Match the following <table><tr><td>1. Bell-LaPadula model</td><td>a. Role-based access</td></tr><tr><td>2. Biba model</td><td>b. Confidentiality</td></tr><tr><td>3. Clark-Wilson model</td><td>c. Integrity</td></tr><tr><td>4. RBAC</td><td>d. Well-formed transactions</td></tr><tr><td>5. VPN</td><td>e. Secure remote communication f. Availabilitiy</td></tr></table>	1. Bell-LaPadula model	a. Role-based access	2. Biba model	b. Confidentiality	3. Clark-Wilson model	c. Integrity	4. RBAC	d. Well-formed transactions	5. VPN	e. Secure remote communication f. Availabilitiy	CO2	(5)
1. Bell-LaPadula model	a. Role-based access												
2. Biba model	b. Confidentiality												
3. Clark-Wilson model	c. Integrity												
4. RBAC	d. Well-formed transactions												
5. VPN	e. Secure remote communication f. Availabilitiy												
3	A financial organization identifies an unpatched server vulnerability that could be exploited by attackers. Classify the associated security risk and outline the basic steps required to assess and mitigate the risk.	CO3	(5)										
4	A university's central server becomes unavailable following a cyber incident. The security team isolates the affected system and begins restoring services from backups. Identify the relevant incident-response and recovery activities involved in this situation.	CO4	(5)										
PART B													
(Answer all questions. Each question carries 10 marks)													
No.	Question	CO	Marks										
6	A healthcare organization stores electronic patient records on a networked information system. An attacker obtains unauthorized access to some records, modifies several entries, and temporarily makes the system unavailable. Analyze the security objectives affected in this incident and relate each objective to an appropriate security service or control. OR A small company allows employees to use a shared password for accessing its internal systems. Following a security incident, management decides to introduce individual accounts, strong passwords, encryption and security policies. Evaluate the security weaknesses in the existing arrangement and explain the role of these measures in improving information assurance.	CO1	10										

7	A small company allows employees to use a shared password for accessing its internal systems. Following a security incident, management decides to introduce individual accounts, strong passwords, encryption and security policies. Evaluate the security weaknesses in the existing arrangement and explain the role of these measures in improving information assurance. OR A defence organization stores information at different security levels. Users are provided with different security clearances, and users at a lower level must not access information at a higher level. Apply the relevant security model to this scenario and explain the security properties involved.	CO2	10
8	An organization allows employees to access applications according to their job responsibilities. The organization also plans to introduce fingerprint authentication and one-time passwords for sensitive applications. Analyze the suitability of RBAC and multi-factor authentication for this environment and explain their security benefits. OR An online banking organization identifies phishing, malware, insider misuse and an unpatched web server as potential threats. Develop a basic risk-assessment process for the organization covering threat identification, vulnerability assessment, risk analysis and risk mitigation.	CO3	10
9	A multinational company is preparing for a security audit and must demonstrate compliance with organizational policies and applicable security requirements. The management also wants to improve employee security awareness. Construct a security-governance plan covering policies, auditing, compliance, monitoring and security awareness training. OR A manufacturing company loses access to its primary data centre following a major infrastructure failure. Critical business applications must be restored with minimum interruption. Design a disaster-recovery and business-continuity strategy incorporating backup, recovery priorities, restoration procedures and incident reporting.	CO4	10

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		

PREAMBLE
This course provides advanced knowledge of the principles, techniques, and technologies used to secure computer networks and operating systems against evolving cyber threats. It emphasizes the analysis of security vulnerabilities, implementation of defense mechanisms, and effective response to security incidents.

RATIONALE
- To develop advanced skills in analyzing network and system vulnerabilities, attacks, and security threats. - To provide knowledge of firewalls, IDS/IPS, VPNs, authentication, access control, and system hardening. - To develop the ability to design effective security mechanisms and respond to modern cyberattacks and security incidents.

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	
							CIA	ESE	Total	CI A	ESE
4	0	0	0	4	120	4	40	60	100		
										Total	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 Hijacking, DNS Attacks	L	CO1	A	M	Rs	3
	Secure Network Design Principles	L	CO1	U	I	Re	3
	Firewall Architecture and Types	L	CO2	U	I	Re	3
2	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
	Operating System Security Concepts, Authentication and Authorization	L	CO3	U	I	Re	3
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			
<i>Use of Data Book / IS codes, etc to be specified by the question paper setter</i>			
PART A			
<i>(Answer all questions. Each question carries 5 marks)</i>			
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			
<i>(Answer one full question from each module, each carries 10 marks.)</i>			
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

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

FIRST SEMESTER M. TECH DEGREE (REGULAR) EXAMINATION, (2026 SCHEME)			
Course Code:	M260102/CY110E		
Course Name:	CYBER SECURITY AND SECURE CODING		
Max. Marks	60	Duration:	2 hours 30 minutes
Computer Science and Engineering (Cyber Security)			

Questions (All Questions have OR Part)				CO	Marks
1)	a.			1	3
	Column A – Security Concept	Column B - Description	Column C – Tool / Technique		
	1. Buffer Overflow	A. Tracks the flow of untrusted data	P. ASan		
	2. Taint Tracking	B. Arithmetic result exceeds the permitted range	Q. UBSan		
	3. Integer Overflow	C. Writing beyond the boundary of a memory region	R. Taint Analysis		
		D. Converts untrusted data into a safe representation	S. SCA		
		E. Identifies vulnerable third-party dependencies	T. Output Encoding		
b. Choose the most appropriate answer from the following options: Options: ASan, UBSan, SCA, Output Encoding, DevSecOps, CERT C i. _____ can detect memory-related errors such as buffer overflows during program execution. ii. _____ is used to identify known vulnerabilities in third-party software components. iii. _____ converts potentially dangerous characters into a safe representation before displaying untrusted data.				1	3
c. A C/C++ application accepts a username from a user and copies it into a fixed-size character buffer. When a very long username is supplied, the application crashes. i. Identify the most likely vulnerability. (1 mark) ii. Suggest two secure coding practices to prevent this vulnerability. (2 marks)				1	3
d. A software company is developing a payment application. During a security review, the following problems are identified: User input is directly used by application components. Third-party libraries are included without security verification. Security testing begins only after development is completed. C/C++ modules occasionally contain memory-safety errors. As the security engineer: i. Recommend a suitable approach for validating untrusted input. (2 marks) ii. Suggest an approach for identifying vulnerable third-party dependencies. (1 mark) iii. Recommend one suitable static or dynamic analysis technique/tool for identifying memory-safety problems. (1 mark) iv. Suggest two ways of integrating security into the DevSecOps pipeline.				1	6

	(2 marks)				
OR					
2)	Column A – Secure Coding Concept	Column B – Description	Column C – Suitable Practice / Tool	1	3
	1. Input Validation	A. Integrates security into development and operations	P. DevSecOps		
	2. Output Encoding	B. Restricts data to an expected format or range	Q. CERT C		
	3. Software Composition Analysis	C. Safely represents untrusted data in its output context	R. Allow-list Validation		
		D. Identifies vulnerable software dependencies	S. Context-Aware Encoding		
		E. Detects malicious network traffic	T. SCA		
b. Choose the most appropriate answer from the following options: Options: Input Validation, Taint Tracking, Integer Overflow, CERT C, ASan, Secure SDLC i. _____ provides secure coding guidelines for C/C++ programmers. ii. _____ occurs when an arithmetic result exceeds the range supported by its data type. iii. _____ tracks the movement of untrusted data through a program.				1	3
c. A web application accepts user comments and displays them directly on a webpage without appropriate encoding. A security tester observes that specially crafted input is interpreted by the browser as executable code. i. Identify the likely vulnerability. (1 mark) ii. Suggest two suitable mitigation techniques. (2 marks)				1	3
d. A healthcare application is being developed using several open-source libraries. A security audit identifies inadequate input validation, unsafe output handling, outdated dependencies, and security testing being performed only before release. As the security engineer: i. Recommend suitable input validation and output encoding practices. (2 marks) ii. Suggest a method for identifying vulnerabilities in third-party components. (1 mark) iii. Recommend one suitable code-analysis technique for identifying security defects early. (1 mark) iv. Suggest two security activities that can be incorporated into a DevSecOps pipeline. (2 marks)				1	6
3)	a. An online banking application constructs a database query using user input: SELECT * FROM users WHERE username = 'USER_INPUT' AND password = 'PASSWORD_INPUT'; A penetration tester observes that specially crafted input changes the behaviour of the query. i. Identify the vulnerability. (1 mark) ii. Describe how the application could be protected against this			2	4

	vulnerability. (2 marks) iii. Name one testing technique that can be used to identify this vulnerability. (1 mark)		
	b. A shopping website stores customer reviews and later displays them to other users. The application does not properly encode the stored content. i. Identify the likely attack. (1 mark) ii. Suggest two appropriate mitigation measures. (2 marks)	2	3
	c. During a security assessment, a web application is found to have the following weaknesses: Session identifiers remain valid after logout. Password-reset tokens remain valid for a long time. Identify the two weaknesses and suggest an appropriate remediation for each. (3 marks)	2	3
	d. A REST API used by a mobile banking application exposes customer information. During testing, a user changes an object identifier in an API request and obtains another customer's information. i. Identify the API security weakness. (1 mark) ii. Suggest two authorization controls to prevent the issue. (2 marks) iii. Illustrate how API authentication and authorization should be separately enforced. (2 marks)	2	5
OR			
4)	a. An e-commerce application uses an account-number parameter directly in a database query. A tester discovers that manipulating the parameter allows additional database records to be returned. i. Identify the likely vulnerability. (1 mark) ii. Suggest two secure coding controls to prevent it. (2 marks) iii. Name one suitable security-testing approach for detecting it. (1 mark)	2	4
	b. A logged-in banking user is tricked into visiting a malicious webpage. The webpage causes a request to the bank's application using the user's existing session. i. Identify the attack. (1 mark) ii. Suggest two controls to prevent this attack. (2 marks)	2	3
	c. A web application allows unlimited login attempts and uses predictable session identifiers. Identify the two security weaknesses and suggest one suitable control for each. (3 marks)	2	3
	d. A GraphQL API allows clients to request highly nested objects and exposes several sensitive fields. An attacker sends an extremely large query that causes excessive server resource consumption. i. Identify the security concern. (1 mark) ii. Suggest two controls to limit abusive GraphQL requests. (2 marks) iii. Suggest two practices for securely exposing sensitive data through APIs. (2 marks)	2	5
5)	a. A suspicious executable is recovered from an employee's workstation. The security team does not want to execute it on the organization's production network. i. Identify the most appropriate initial malware-analysis approach. (1 mark) ii. Identify two characteristics or artifacts that can be examined without executing the sample. (2 marks) iii. State one advantage of this approach. (1 mark)	3	4
	b. During malware investigation, an analyst observes that a malicious program creates a new process, establishes an outbound connection, and modifies system configuration. i. Illustrate the purpose of the MITRE ATTACK framework in such an investigation? (1 mark) ii. Identify two possible Indicators of Compromise from the scenario. (2 marks)	3	3
	c. During an authorized penetration test, the tester first gathers information about domains, subdomains, IP addresses, technologies, exposed services, and publicly available organizational information.	3	3

	i. Identify the penetration-testing phase. (1 mark) ii. State two reasons why this phase is important before exploitation. (2 marks)		
	d. A cloud-hosted application is compromised because a container runs with excessive privileges and has access to sensitive host resources. i. Identify the security weakness. (1 mark) ii. Suggest two container-hardening measures. (2 marks) iii. Illustrate how least privilege can reduce the impact of container compromise. (2 marks)	3	5
OR			
6)	a. A security analyst executes a suspicious executable inside an isolated environment and monitors file creation, process activity, registry modifications, and network connections. i. Identify the malware-analysis approach being used. (1 mark) ii. Identify two types of behavioural evidence that can be collected. (2 marks) iii. State one advantage of using an isolated sandbox. (1 mark)	3	4
	b. A malware sample attempts to maintain persistence and communicate with a command-and-control server. i. State the role of MITRE ATTACK in documenting the observed malware behaviour. (1 mark) ii. Identify two possible IOCs that could be collected. (2 marks)	3	3
	c. A penetration tester has identified an exposed service and attempts to determine whether a known vulnerability can be exploited in the authorized target environment. i. Identify the stage of penetration testing represented by this activity. (1 mark) ii. State two precautions that should be followed before exploitation. (2 marks)	3	3
	d. A cloud application uses an overly permissive identity role. After compromising the application, an attacker is able to access storage resources that are unrelated to the application. i. Identify the security weakness. (1 mark) ii. Suggest two controls to reduce excessive cloud permissions. (2 marks) iii. Describe how proper IAM design can limit the impact of a compromised workload. (2 marks)	3	5
7)	a. A Linux server contains sensitive configuration files. The administrator wants to restrict processes from accessing resources beyond their intended privileges. i. Differentiate DAC and MAC in Linux security. (2 marks) ii. Name one Linux mechanism that can provide stronger access restrictions. (1 mark)	4	3
	b. An organization wants to provide phishing-resistant passwordless authentication for employees accessing critical applications. i. Identify the most suitable technology for phishing-resistant passwordless authentication: MFA, FIDO2, or OAuth 2.0. (1 mark) ii. Give two reasons for your choice. (2 marks) iii. State one limitation of relying only on passwords for critical applications. (1 mark)	4	4
	c. A Linux server administrator wants to monitor security-relevant activities and control unauthorized network connections. i. Name one Linux firewall technology that can be used to control network traffic. (1 mark) ii. Name one auditing mechanism/tool that can record security-relevant events. (1 mark) iii. State one benefit of maintaining security audit logs. (1 mark)	4	3

	d. An organization receives thousands of alerts from firewalls, servers, endpoint systems, and authentication services. The security team wants centralized event correlation and a security architecture in which access is continuously verified. i. Identify the technology used for centralized collection and correlation of security events. (1 mark) ii. Identify the security architecture based on the principle “never trust, always verify.” (1 mark) iii. Suggest two benefits of implementing SIEM in the organization. (2 marks) iv. State one important principle of Zero Trust Architecture. (1 mark)	4	5
OR			
8)	a. A compromised Linux application attempts to perform system calls that are unnecessary for its normal operation. i. Identify one Linux security mechanism that can restrict such system calls. (1 mark) ii. Describe how the mechanism reduces the attack surface. (2 marks)	4	3
	b. Two internal services must authenticate each other before establishing a secure connection. i. Identify the appropriate security mechanism. (1 mark) ii. Describe the role of digital certificates in this mechanism. (2 marks) iii. State one advantage of mutual authentication. (1 mark)	4	4
	c. An organization wants to detect repeated failed authentication attempts and suspicious changes to critical Linux files. i. Identify one suitable Linux auditing mechanism. (1 mark) ii. State one type of event that should be monitored. (1 mark) iii. State one role of audit logs in incident investigation. (1 mark)	4	3
	d. An enterprise allows employees to access applications from offices, homes, and cloud environments. The organization wants access decisions to consider user identity, device security, application, and resource sensitivity rather than simply trusting the internal network. i. Identify the appropriate security architecture. (1 mark) ii. State two principles that should guide the architecture. (2 marks) iii. Identify two ways centralized security monitoring supports this architecture. (2 marks)	4	5

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		

PREAMBLE
Research Methodology and IPR introduces learners to the systematic process of conducting, evaluating, and communicating research. The course develops skills in research thinking, literature survey, problem formulation, research design, data analysis, validation, and scholarly publication, while emphasizing research and publication ethics. It also introduces the responsible use of AI tools in contemporary research practices. The course further familiarizes learners with Intellectual Property Rights and patenting procedures for protecting research and innovation outcomes.

RATIONALE
- Develop the ability to identify, formulate, and systematically investigate research problems using appropriate research methodologies. - Develop skills in literature review, research design, data analysis, modelling, and validation of research outcomes. - Equip learners with competencies for scientific writing, research publication, presentation, and effective communication of research findings. - Create awareness of Intellectual Property Rights (IPR), research ethics, patents, and protection of research outcomes.

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	Explain the significance of enthusiasm and creativity in research projects. (Cognitive Level: Understand)	CC1	U	M	Rs
CO2	Formulate a research problem through a literature survey. (Cognitive Level: Apply)	CC1	A	P	V
CO3	Apply suitable methodologies and tools for conducting research investigations. (Cognitive Level: Apply)	CC1	A	Ar	V
CO4	Create research outcomes in appropriate scholarly forums. (Cognitive Level: Create)	CC2	C	Ar	O
CO5	Evaluate the concepts of Intellectual Property Rights, patents, and patenting procedures in research and innovation. (Cognitive 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					

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
2	0	0	0	15	(30 +15)	2	CIA	ESE	Total	CIA	ESE	Total	100
							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.	8
3	Experimental, Modelling Skills and Publication/Patents	Principles of experimental design, Scientific method, Mathematical and computational modelling approaches. Validation and verification of results, AI tools for data analysis and modelling. Types of intellectual property, Research metrics-Journal Level, AI in publication.	10
4	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	6

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
	Activity 1: Research Motivation, Research Ethics & Responsible Research Reflection	Self Study	CO1	U	M	V	1
2	Literature survey process: Planning, searching, screening, analyzing, and synthesizing.	Lecture	CO2	U	P	V	1
	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)	CO2	A	P	V	1
	Activity 2: Literature Survey, Research-Gap Analysis & Academic Integrity Lab	Self Study	CO2	A	P	V	1
	Activity 3: Research Problem Formulation & Proposal Pitch	Self Study	CO2	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.	Lecture	CO3	U	Ar	V	1
	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, trade secrets	Lecture	CO4	U	P	O	1
	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
	Activity 4: Mini Experimental / Computational Research Design & Analysis	Self Study	CO3	A	Ar	V	1
	Activity 5: Mock Peer Review & Journal Selection Simulation	Self Study	CO4	A	Ar	O	1
	Nature of Intellectual Property: Patents,	Lecture	CO5	U	P	O	1

4	Designs, Trade and Copyright.						
	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
	Activity 6: Patent Development, Filing Procedure & IPR Case Study	Self Study	CO5	A	P	O	1
	Activity 7: e-Portfolio & Researcher Development Log	Self Study	CO5	A	Ar	O	1

ASSESSMENT PATTERN	
Assessment	Marks
Continuous Internal Assessment	100
Internal Examination	40
Continuous Assessment	60
Total	100

Activity-Based Learning and Assessment Plan

Total Activity Marks: 60

The activities are designed to develop practical research competence through literature discovery, responsible use of AI tools, reference management, academic writing, research integrity, experimental design, publication practices, intellectual property rights (IPR), and research communication.

1. Summary of Assessed Activities

Activity	Activity Title	Self-Learning / Preparatory Component	Week(s)	Marks	Mode
A1	Research Motivation, Research Ethics & Responsible Research Reflection	Research motivation; responsible conduct of research; publication ethics (1 hr)	3	5	Individual reflective note + in-class ethics case discussion
A2	Literature Survey, Research-Gap Analysis & Academic Integrity Lab	Scholarly search; literature-review tools; reference management; AI-assisted literature discovery and verification; plagiarism awareness (5 hr)	5–8	10	Individual literature study using Zotero/Mendeley/EndNote and approved AI tools + plagiarism/verification exercise
A3	Research Problem Formulation & Proposal Pitch	Research problem, gap, objectives and proposal structure	8–9	10	Individual 5-minute pitch + 1-page research concept note
A4	Mini Experimental / Computational Research Design & Analysis	Experimental design; datasets; evaluation metrics; basic statistical analysis	10–12	10	Hands-on research-design exercise using Python/R/SPSS/Excel/MATLAB or appropriate domain tools

Activity	Activity Title	Self-Learning / Preparatory Component	Week(s)	Marks	Mode
A5	Mock Peer Review & Journal Selection Simulation	Peer-review process; journal scope; indexing; research/journal metrics; publication ethics (1 hr)	12–13	10	Paired peer review + evidence-based journal-selection analysis
A6	Patent Search, Prior-Art Analysis & Preliminary Claim Drafting	Patent search; prior art; patentability; basic IPR concepts (1 hr)	14	10	Group prior-art search + individual claim/analysis sheet + presentation
A7	e-Portfolio & Researcher Development Log	Open access; responsible use of citation/research metrics; researcher identity and scholarly profile (2 hr)	15	5	Curated digital portfolio + reflective log

COURSE DESCRIPTION							
Regulation	2026	L-T-J-P-S	3-0-0-0-2	VERSION	26/0	CREDITS	0
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)							

COURSE CODE	COURSE NAME	COURSE CATEGORY
	DESIGN THINKING	AUDIT COURSE
PRE-REQUISITE		
Nil		

PREAMBLE
This course offers an introductory exploration of fundamental engineering concepts and techniques, the design process, analytical thinking and creativity, as well as the fundamentals and development of engineering drawings, along with their application in engineering problems.

RATIONALE
This course provides a foundation in engineering principles, problem-solving, and design thinking essential for engineering practice. It develops analytical and creative skills while introducing engineering drawing as a tool for visualizing and communicating technical ideas. The course prepares students for higher-level engineering studies and real-world engineering applications.

COMPETENCY STATEMENT/s
1. Apply fundamental engineering concepts, design thinking, and problem-solving techniques to address basic engineering challenges.
2. Interpret and prepare engineering drawings using standard conventions for effective technical communication and visualization.

CO	CO Statement	Competency Mapping	Cognitive (C)	Psychomotor (P)	Affective (A)
1	Apply fundamental engineering concepts, analytical thinking, and problem-solving techniques to solve basic engineering problems.	CC1	A	M	Rs
2	Apply the engineering design process and creative thinking approaches to develop solutions for simple engineering problems.	CC1	A	M	V
3	Interpret engineering drawings using standard engineering conventions and graphical communication techniques.	CC2	A	P	V
4	Analyze engineering problems and communicate technical ideas effectively through engineering graphics and visualization techniques.	CC1, CC2	An	Ar	O

TEACHING AND ASSESSMENT SCHEME													
Teaching Scheme / Week					Hours / Semester	Credit	Examination Scheme						
L	T	J	P	S	(45+20)	C	Theory			Practical			Total
							CIA	ESE	Total	CIA	ESE	Total	
3	0	0	0	2		0	100		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	Design process	Traditional design, Design Thinking Approach, Introduction to Design Thinking, History and evolution of Design Thinking, Role of design thinking in the human-centred design process. Design space, Design Thinking in a Team Environment, Team formation.	7
2	Design Thinking Stages	Empathize, Define, Ideate, Prototype and Test. The importance of empathy, Building a user-centred mindset. Problem statement formulation, User needs and pain points, establishing target specifications, Setting the final specifications.	7
3	Ideation	Generating Ideas, Brainstorming techniques, Application of Aesthetics and Ergonomics in Design. Bio-mimicry, Conceptualization, Visual thinking, Drawing/Sketching, Presenting ideas.	7
4	Prototyping, Testing & IPR in design	Use of prototyping, Types of prototypes, Rapid prototyping techniques, User testing and feedback collection, Iterative prototyping, testing to gauge risk and market interest Entrepreneurship/business ideas, Patents and Intellectual Property, Agility in design, Ethical considerations in design. Overcoming common implementation challenges	9

Sl. No	Self-learning / Team Work Description
1	Study and summarize a successful product or service developed using the Design Thinking approach.
2	Explore engineering solutions inspired by nature and present their applications.
3	Investigate recent advancements in 3D printing and rapid prototyping techniques.
4	Study a patent related to an engineering innovation and analyze its key features.
5	Examine the role of ethics and sustainability in modern engineering design through real-world examples.

SUGGESTED LEARNING RESOURCES

Text Book			
Sl. No.	Title of Book	Author	Publication
1	Design Thinking: Understand – Improve – Apply	Christoph Meinel, Larry Leifer and Hasso Plattner	Springer Berlin, Heidelberg, 2011 Edition
2	Design Thinking: Integrating Innovation, Customer Experience, and Brand Value	Thomas Lockwood and Edgar Papke	Allworth Press, 2009 Edition

Reference			
Sl. No.	Title of Book	Author	Publication
1	Design Your Thinking	Pavan Soni	Penguin Random House India Private Limited, 2020 Edition
2	Design Thinking : A Guide to Creative Problem Solving for Everyone	Andrew Pressman	Taylor & Francis, 2018 Edition
3	Design Thinking Techniques an Approaches	N Siva Prasad	Ane Books Pvt. Ltd., 2023 Edition

Web Resource	
1	https://onlinecourses.nptel.ac.in/e-learning/preview/noc22_mg32
2	https://onlinecourses.nptel.ac.in/e-learning/preview/noc21_mg63

DETAILED SYLLABUS								
Module	Title	Topic	Mode of Delivery	CO	Learning Domain			Hrs
					C	P	A	
1	Design process	Design process: Traditional design, Design Thinking	Lecture	2	U	M	Rs	3

		Approach, Introduction to Design Thinking, History and evolution of Design Thinking.						
		Role of design thinking in the human-centred design process. Design space	Lecture, Discussion	2	U	M	V	2
		Design Thinking formation.	Activity Based Learning	2	A	M	V	2
2	Design Thinking Stages	Design Thinking Stages: Empathize, Define, Ideate, Prototype and Test.	Lecture	2	U	M	V	2
		The importance of empathy, Building a user-centred mindset.	Discussion, Case Study	2	A	M	V	2
		Problem statement formulation User needs and pain points, establishing target specifications, Setting the final specifications.	Activity Based Learning	1,2	A	P	V	3
3	Ideation	Generating Ideas, Brainstorming techniques.	Activity Based Learning	2	A	M	V	2
		Application of Aesthetics and Ergonomics in Design. Biomimicry.	Lecture, Case Study	2	U	M	V	3
		Conceptualization, Visual thinking, Drawing/Sketching, Presenting ideas	Workshop	3,4	A	P	O	2
4	Prototyping, Testing and IPR in design	Use of prototyping, Types of prototypes, Rapid prototyping techniques.	Lecture, Demonstration	3	A	P	V	3
		User testing and feedback collection, Iterative prototyping, testing to gauge risk and market interest	Activity Based Learning	4	An	Ar	O	2
		Entrepreneurship/business ideas, Patents and Intellectual Property.	Lecture	1	U	M	V	2
		Agility in design, Ethical considerations in design. Overcoming common implementation challenges	Discussion, Case Study	4	An	M	O	2

COURSE DESCRIPTION							
Regulation	2026	L-T-J-P-S	3-0-0-0-2	Version	26/0	Credits	0
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)							
Course Code	Course Name					Course Category	
	ACADEMIC WRITING					AUDIT COURSE	
PRE-REQUISITE							
Basic proficiency in English language and communication.							

PREAMBLE	
- Introduces the principles of reader-centric writing, scholarly communication, scientific documentation, and technical reporting. - Develops the ability to prepare research papers, project proposals, review articles, and technical reports that meet academic and professional standards.	

RATIONALE	
This course equips the students with - The ability to communicate research findings effectively through academic and technical documents using accepted scholarly conventions. - Competence in preparing research papers, project proposals, and technical reports that meet academic and professional standards. - Knowledge of citation practices, academic ethics, and publication standards, along with the critical thinking and communication skills required for research careers.	

COMPETENCY STATEMENT/s			
CC1	Develop scholarly documents using principles of academic and scientific writing.		
CC2	Prepare research manuscripts, project proposals and technical reports conforming to academic standards.		
COURSE OUTCOMES			
Course Outcomes (CO): At the end of this course, learners will be able to:			
CO	CO Statement	Competency Mapping	Cognitive (C)
CO 1	Apply the principles of reader-centric academic writing to improve clarity and readability of scholarly documents.	CC1	A
CO 2	Analyse writing structures and progression techniques used in scientific literature.	CC1	An
CO 3	Develop titles, abstracts, introductions, conclusions, and visual elements for research publications.	CC1, CC2	A
CO 4	Evaluate and apply referencing, citation, and technical grammar standards in academic documents.	CC1	E
CO 5	Prepare project proposals, review papers, extended abstracts, and technical reports for research dissemination.	CC2	C
Cognitive (Revised blooms Level): - R: Remember; U: Understand; A: Apply; An: Analyse; E: Evaluate; C: Create			

TEACHING AND ASSESSMENT SCHEME												
Teaching Scheme / Week					Credit	Hours / Semester	Examination Scheme					
							Theory			Practical		
L	T	J	P	S	C		CIA	ESE	Total	CIA	ESE	Total
3	0	0	0	2	0	(45+20)	100		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	Fundamentals of Academic Writing	Reader-centric writing, memory load in reading, acronyms, pronouns, synonyms, disconnected phrases, background ghetos, abusive detailing, cryptic captions, long sentences, reader motivation and engagement.	10
2	Fluid Reading and Progression Techniques	Setting expectations, progression tracks, topic and non-topic progression, sentence fluidity, reading energy consumption, readability enhancement.	8
3	Structure of Research Articles	Writing titles, abstracts, introductions, headings, subheadings, organization of research papers, coherence and logical flow.	10
4	Visuals, References and Technical Grammar, Scholarly and Technical Documents	Visual communication, conclusions, references, bibliography, citation styles, grammar in technical writing, active/passive voice, common writing errors. Extended abstracts, project proposals, review papers, research papers, technical reports.	17

SELF-LEARNING / TEAM WORK		
Sl. No	Self-learning / Team Work Description.	Hrs
1	Review and critique of a published journal paper.	4
2	Analysis of titles, abstracts and introductions from reputed journals.	4
3	Preparation of an extended abstract on a selected research topic.	4
4	Citation and referencing exercises using IEEE/APA styles.	3
5	Technical grammar and proofreading activities.	3
6	Preparation of visuals, tables and figures for a research article.	3

SUGGESTED LEARNING RESOURCES			
Text Book			
Sl. No.	Title of Book	Author	Publication
1	Scientific Writing 2.0: A Reader and Writer's Guide	Jean-Luc Lebrun	World Scientific Publishing, 2011
2	How to Write and Publish a Scientific Paper	Barbara Gastel & Robert A. Day	Greenwood Publishers, 2016
Reference			
Sl. No.	Title of Book	Author	Publication
1	The Craft of Research	Wayne C. Booth et al.	University of Chicago Press
2	Academic Writing for Graduate Students	John M. Swales & Christine B. Feak	University of Michigan Press
3	Writing for Peer Reviewed Journals	Pat Thomson & Barbara Kamler	Routledge
4	Publication Manual	American Psychological Association	Latest Edition
Web Resource			
1	https://owl.purdue.edu		
2	https://writingcenter.unc.edu		
3	https://authorservices.wiley.com		
4	https://www.springer.com/gp/authors-editors		

DETAILED SYLLABUS

Module	Major Topic & Sub Topic	Mode of Delivery	COs	Learning Domain Level	Hours
				C	
1	Reader-centric academic writing and reading toolkit	L	1	U	1
	Acronyms, pronouns, synonyms and memory burden	Activity	1	A	2
	Disconnected phrases, background ghettos and abusive detailing	L	1	A	1
	Cryptic captions and long sentences	L	1	A	1
	Sustaining reader attention and maintaining flow	L	1	A	1
	Creating reader motivation and reducing knowledge gaps	Activity	1	A	2
	Case studies and writing exercises	Activity	1	A	2
2	Setting expectations through grammar and themes	L	2	U	1
	Topic-based and non-topic-based progression tracks	L	2	A	1
	Detection of sentence fluidity problems	L	2	U	1
	Reading energy consumption and readability	L	2	A	1
	Abstract writing: structure, coherence and precision	L, Activity	3	A	2
	Exercises on progression and coherence	L, Activity	3	A	2
3	Title writing: qualities, purpose and metrics	L	3	A	2
	Abstract writing: structure, coherence and precision	L	3	A	2
	Headings and sub-headings: principles and syntax	L	3	A	2
	Introduction writing: scope, definitions and reader questions	L, Activity	3	A	2
	Analysis of published research papers	L, Activity	3	A	2
4	Visuals in research papers: principles and metrics	L	4	A	1
	Writing effective conclusions	L, Activity	4	A	2
	References and bibliography: citation styles and ethics	L, Activity	4	A	2
	Grammar in technical writing	L, Activity	4	A	2
	Active and passive voice, common mistakes	L	4	A	1
	Extended abstract preparation	L, Activity	5	C	1
	Project proposal preparation	L, Activity	5	C	2
	Writing review papers and overview articles	L, Activity	5	C	2
	Research paper preparation	L, Activity	5	C	2
	Technical report writing	L, Activity	5	C	2