MITS Kochi
Muthoot Institute of Technology and Science
(Autonomous)

M. TECH

CYBER SECURITY

CURRICULUM & SYLLABUS

SEMESTER 1&2

2025 REGULATION

MITS Kochi
Muthoot Institute of Technology and Science
(Autonomous)

M.Tech CYBER SECURITY

2025 REGULATION

CURRICULUM & SYLLABUS

PROGRAMME STRUCTURE

SEM	SLOT	COURSE CATEGORY	COURSE CODE	COURSE NAME	L	T	J	P	S	C	CREDIT / SEM
I	A	DC	M250902/CN100A	ADVANCED MACHINE LEARNING	3	0	0	0	2	3	18
	B	PC	M250102/MA100B	FOUNDATIONS OF CRYPTOGRAPHY	3	0	0	0	1	3	
	C	PC	M250102/CY100C	INFORMATION SECURITY	3	0	0	0	2	3	
	D	PE	M250102/CY11*D	PROGRAM ELECTIVE 1	3	0	0	0	2	3	
	E	PE	M250102/CY12*E	PROGRAM ELECTIVE 2	3	0	0	0	2	3	
	S	GC	M250902/CN100S	RESEARCH METHODOLOGY AND IPR	2	0	0	0	1	2	
	T	PL	M250102/CY130T	COMPUTING LAB I	0	0	0	2	1	1	
II	A	DC	M250902/CN200A	ADVANCED DATA STRUCTURES AND ALGORITHMS	3	0	0	0	2	3	18
	B	PC	M250102/CY200B	NETWORK SECURITY	3	0	0	0	2	3	
	C	PE	M250102/CY21*C	PROGRAM ELECTIVE 3	3	0	0	0	2	3	
	D	PE	M250102/CY22*D	PROGRAM ELECTIVE 4	3	0	0	0	2	3	
	E		M250102/CY23*E	INDUSTRY/INTERDISCIPLINARY ELECTIVE/MOOC	3	0	0	0	2	3	
	S	PS	M250902/CN200S	MINI PROJECT	0	0	4	0	2	2	
	T	PL	M250102/CY230T	COMPUTING LAB II	0	0	0	2	1	1	
III	A*		M250902/CN300A	MOOC	-	-	-	-	2	2	16
	B		M250902/CN300B	AUDIT COURSE	3	0	0	0	2	-	
	C		M250902/CN340C	INTERNSHIP	-	-	-	-		3	
	D	PS	M250902/CN340D	DISSERTATION/RESEARCH PROJECT PHASE 1	0	0	17	0	2	11	
IV	A	PS	M250902/CN440D	DISSERTATION/RESEARCH PROJECT PHASE II	0	0	24	0	2	16	16
TOTAL CREDITS											68

*MOOC Course to be successfully completed before the commencement of fourth semester (starting from semester 1).

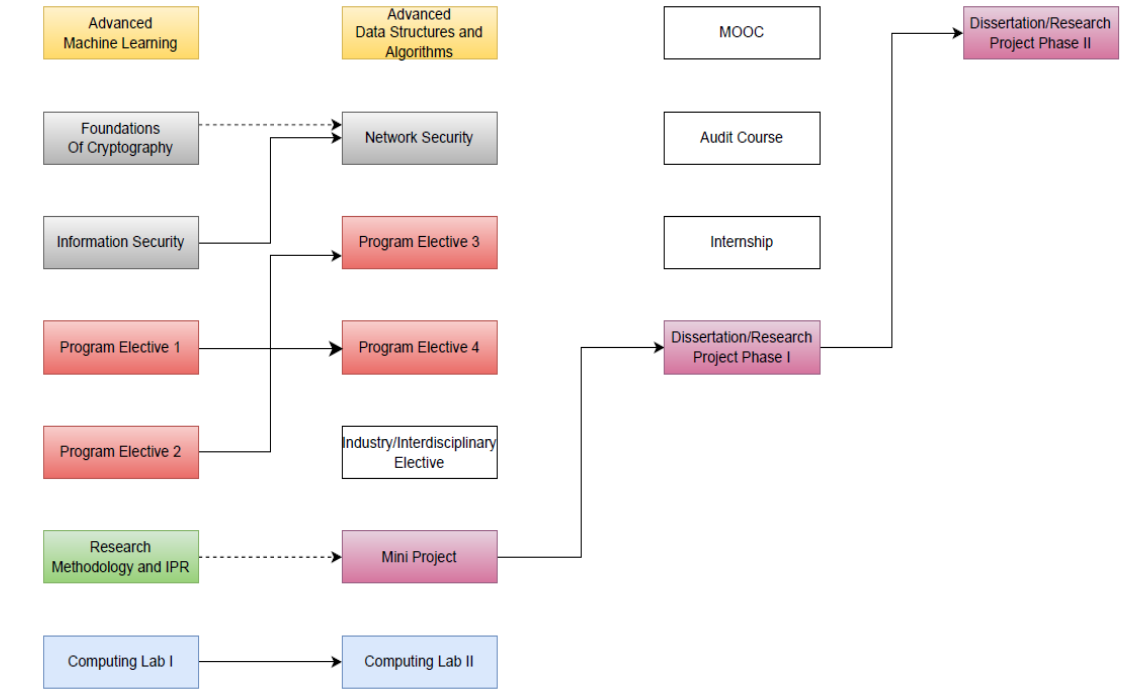
PROGRAM ELECTIVE I		
SL NO	**COURSE CODE**	**COURSE NAME**
1	M250102/CY111D	CYBER FORENSICS AND INCIDENT RESPONSE
2	M250102/CY112D	WEB APPLICATION SECURITY
3	M250102/CY113D	OPTIMIZATION TECHNIQUE
4	M250102/CY114D	TOPICS IN NETWORKS
5	M250102/CY115D	ADVANCED ARCHITECTURE
6	M250902/CN116D	COMPUTATIONAL INTELLIGENCE

PROGRAM ELECTIVE II		
SL NO	**COURSE CODE**	**COURSE NAME**
1	M250102/CY121E	FILE SYSTEM FORENSIC ANALYSIS
2	M250102/CY122E	BLOCK CHAIN
3	M250102/CY123E	SECURE CODING
4	M250102/CY124E	CLOUD COMPUTING AND SECURITY
5	M250102/CY125E	FORMAL METHODS IN SECURITY
6	M250102/CY126E	LINEAR ALGEBRA

PROGRAM ELECTIVE III		
SL NO	**COURSE CODE**	**COURSE NAME**
1	M250102/CY231C	SECURITY OF CYBER PHYSICAL SYSTEM
2	M250102/CY232C	BIOMETRIC SECURITY
3	M250102/CY233C	STEGANOGRAPHY AND MALWARE ANALYSIS
4	M250102/CY234C	OPERATING SYSTEM FORENSICS
5	M250102/CY235C	INFORMATION THEORY AND CODING

PROGRAM ELECTIVE IV		
SL NO	**COURSE CODE**	**COURSE NAME**
1	M250102/CY241D	ETHICAL HACKING
2	M250102/CY242D	SECURE SOFTWARE ENGINEERING
3	M250102/CY243D	INFORMATION SECURITY AND APPLIED CRYPTOGRAPHY
4	M250102/CY244D	MACHINE LEARNING IN SECURITY
5	M250102/CY245D	CYBERLAW AND INTELLECTUAL PROPERTY RIGHTS

COURSE FLOW



Program Elective 1	Program Elective 2	Program Elective 3	Program Elective 4
Wed Application Security	Block Chain	Security of Cyber Physical System	Ethical Hacking
Programming and Data Structures	File System Foresnic Analysis	Biometric Security	Secure Software Engineering
Cyber Forensics and Incident Response	Cloud Computing and Security	Steganography and Malware Analysis	Information Security and Applied Cryptography
Optimization Technique	Formal Methods in Security	Operating System Forensics	Machine Learning in Security
Computational Intelligence	Secure Coding	Information Theory and Coding	Cyberlaw and Intellectual Property Rights
Topics in Networks			

SEMESTER I

APPROVAL

This is to certify that the syllabus titled "syllabus for M.Tech Cyber Security" implemented from the academic year **2025–2026**, is prepared in accordance with the regulations, academic framework, and Outcome Based Education guidelines prescribed by the Institution and the affiliating University.

The syllabus has been **discussed, reviewed, and approved** by the following statutory bodies.

BOARD OF STUDIES (BOS)

Approved in the Board of Studies Meeting of the M.Tech Cyber Security held on 02/09/2025

Chairperson, BoS

Name: Dr. Vicky Nair Designation: HoD Department of Cyber Security

Signature: Date: 03/09/2025

ACADEMIC COUNCIL

Approved by the **Academic Council** in its meeting held on 10/09/2025

PRINCIPAL

Recommended for implementation from the Academic year 2025-2026.

Name: Dr. Neelakandan P C

Signature: Date:

SEMESTER I

CURRICULUM

SLOT	COURSE CATEGORY	COURSE CODE	COURSE NAME	L	T	J	P	S	C
A	DC	M250902/CN100A	ADVANCED MACHINE LEARNING	3	0	0	0	2	3
B	PC	M250102/MA100B	FOUNDATIONS OF CRYPTOGRAPHY	3	0	0	0	1	3
C	PC	M250102/CY100C	INFORMATION SECURITY	3	0	0	0	2	3
D	PE	M250102/CY11*D	PROGRAM ELECTIVE 1	3	0	0	0	2	3
E	PE	M250102/CY12*E	PROGRAM ELECTIVE II	3	0	0	0	2	3
K	GC	M250902/CN100S	RESEARCH METHODOLOGY & IPR	2	0	0	0	1	2
U	LAB1	M250102/CY130T	COMPUTING LAB I	0	0	0	2	1	1
*(**L**- Lecture, **T**-Tutorial, **J**-Project, **P**-Practical, **S**-Self-learning & Team Work, **C**- Credit)*									

COURSE DESCRIPTION							
Regulation	**2025**	**L-T-J-P-S**	**3-0-0-0-2**	**Version**	**25/0**	**Credits**	**3**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)							
Course Code		**Course Name**					**Course Category**
M250902/CN100A		**ADVANCED MACHINE LEARNING**					**DC**

COURSE OBJECTIVES	
1	Introduce supervised, unsupervised and reinforcement learning
2	Familiarize students with basic parameter estimation methods and Gradient Descent Algorithm
3	Enable students to identify, apply suitable machine learning algorithms for classification and regression
4	Equip students to compare and evaluate the performance of machine learning algorithms.
5	Familiarize students with machine learning based solutions for real world problems.

COMPETENCY STATEMENTS	
CC1	Demonstrate foundational understanding of machine learning paradigms and apply parameter estimation techniques and optimization algorithms such as Gradient Descent to solve classification and regression problems.
CC2	Evaluate and compare the performance of machine learning algorithms using appropriate metrics, and design ML-based solutions to address real-world problems across multiple domains.

COURSE OUTCOMES

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

CO	CO Statement	Competency Mapping	Cognitive (C)
CO1	Apply the Machine Learning concepts and basic parameter estimation methods for the solution of problems of different domains. (Cognitive Knowledge Level: Apply)	CC1	A
CO2	Use regression and classification techniques to build models for real world scenarios (Cognitive Knowledge Level: Apply)	CC1	A
CO3	Apply unsupervised learning algorithms and dimensionality reduction techniques to analyse and interpret complex datasets for pattern discovery and feature extraction. (Cognitive Knowledge Level: Apply)	CC1	A
CO4	Implement support vector machine algorithms and graphical modelling techniques to solve real world problems (Cognitive Knowledge Level: Apply)	CC1	A
CO5	Choose suitable model parameters for different machine learning techniques and to evaluate a model performance. (Cognitive Knowledge Level: Apply)	CC2	A
CO6	Design, implement and analyse machine learning solution for a real-world problem. (Cognitive Knowledge Level: Create)	CC2	C

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

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

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

TEACHING AND ASSESSMENT SCHEME													
Teaching Scheme / Week				**Self-Learning (S) / Semester**	**Total Hours / Semester**	**Credits C**	**Examination Scheme**						
							Theory			**Practical**			**Total**
L	**T**	**J**	**P**				**CIA**	**ESE**	**Total**	**CIA**	**ESE**	**Total**	
3	0	0	0	30	70	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	Parameter Estimation and Regression	MLE), Maximum a Posteriori Estimation (MAP). Gradient Descent Algorithm, Regression	8
2	Regularization techniques and Classification algorithms	linear and non-linear algorithms	9
3	Unsupervised learning	K-means, Density-based spatial clustering	8
4	Support Vector Machine and Graphical Models	SVM, Bayesian networks, Hidden Markov model	7
5	Evaluation Metrics and Sampling Methods	Metrics for classification, clustering, Resampling methods	8

SELF-LEARNING / TEAM WORK		
Sl. No	Self-learning / Team Work Description	Hrs/Semester
1	Micro project/Course based project	20
2	Regularization Techniques, Graphical Models, Gaussian mixture models	6
3	Seminar	4

SUGGESTED LEARNING RESOURCES			
Text Book			
Sl. No.	Title of Book	Author	Publication
1	Machine Learning: A Probabilistic Perspective	Kevin P. Murphy.	MIT Press 2012.
2	Introduction to Machine Learning, 2nd edition	Ethem Alpaydin	MIT Press 2010.
Reference			
Sl. No.	Title of Book	Author	Publication
1	Data Mining Concepts and Techniques	Jiawei Han, Micheline Kamber, Jian Pei.	Third Edition, Morgan Kaufmann
2	Deep Learning	Goodfellow, I., Bengio,Y., and Courville, A.,	MIT Press, 2016.
3	Pattern recognition and machine learning.	Christopher M. Bishop.	Springer 2006
Web Resource			
1	Introduction to Machine Learning, Prof. Balaraman Ravindran, NPTEL, IIT Madras.		
2	Machine Learning and Deep Learning - Fundamentals and Applications, Prof. M. K. Bhuyan, NPTEL, IIT Guwahati.		

DETAILED SYLLABUS

Module	Topic	Mode of Delivery	COs	Learning Domain Level	Hrs
				C	
1	Overview of machine learning: supervised, semi-supervised, unsupervised learning, reinforcement learning.	Lecture	CO1	U	
	Basics of parameter estimation: Maximum Likelihood Estimation (MLE)	Lecture	CO1	U	
	Basics of parameter estimation: Maximum Likelihood Estimation (MLE) – Examples	Lecture	CO1	A	
	Basics of parameter estimation: Maximum a Posteriori Estimation (MAP)	Lecture	CO1	A	
	Basics of parameter estimation: Maximum a Posteriori Estimation (MAP) – Example	Lecture	CO1	A	
	Gradient Descent Algorithm, Batch Gradient Descent, Stochastic Gradient Descent	Lecture	CO1	U	
	Regression algorithms: least squares linear regression, normal equations and closed form solution	Lecture	CO2	A	
	Polynomial regression	Lecture	CO2	A	
2	Regularization techniques - LASSO and RIDGE	Self-Learning	CO2	U	
	Classification algorithms: linear and non-linear algorithms	Lecture	CO2	U	
	Perceptron	Lecture	CO2	A	
	Logistic regression	Lecture	CO2	A	
	Naive Bayes	Lecture	CO2	A	
	Decision trees	Lecture	CO2	A	
	Neural networks: Concept of Artificial neuron	Lecture	CO2	A	
	Feed-Forward Neural Network	Lecture	CO2	U	
	Back propagation algorithm	Lecture	CO2	A	
3	Unsupervised learning: clustering, k-means	Lecture	CO3	U	
	Hierarchical clustering	Lecture	CO3	A	
	Principal component analysis	Lecture	CO3	A	
	Density-based spatial clustering of applications with noise (DBSCAN)	Lecture	CO3	A	
	Gaussian mixture models: Expectation Maximization (EM) algorithm for Gaussian mixture model	Self-Learning	CO3	U	
	Gaussian mixture models: Expectation Maximization (EM) algorithm for Gaussian mixture model	Self-Learning	CO3	A	
	Unsupervised learning: clustering, k-means	Lecture	CO3	A	
	Hierarchical clustering	Lecture	CO3	A	
4	Support vector machines and kernels: Max margin classification	Lecture	CO4	U	
	Support vector machines: Max margin classification	Lecture	CO4	A	
	Nonlinear SVM and the kernel trick, nonlinear decision boundaries	Lecture	CO4	A	
	Kernel functions	Lecture	CO4	U	
	Basics of graphical models - Bayesian networks	Self-Learning	CO4	U	
	Hidden Markov model - Inference and estimation	Self-Learning	CO4	U	
	Hidden Markov model - Inference and estimation	Self-Learning	CO4	A	
	Classification Performance Evaluation Metrics:	Lecture	CO5	A	

5	Accuracy, Precision, Precision, Recall, Specificity, False Positive Rate (FPR), F1 Score, Receiver Operator Characteristic (ROC) Curve, AUC		CO6		
	Regression Performance Evaluation Metrics: Mean Absolute Error (MAE), Root Mean Squared Error (RMSE), R Squared/Coefficient of Determination	Lecture	CO5 CO6	A	
	Clustering Performance Evaluation Metrics: Purity, Jaccard index, Normalized Mutual Information, Clustering Accuracy, Silhouette Coefficient, Dunn's Index	Lecture	CO5 CO6	A	
	Boosting: AdaBoost, gradient boosting machines.	Lecture	CO5 CO6	U	
	Resampling methods: cross-validation, bootstrap.	Lecture	CO5 CO6	U	
	Ensemble methods: bagging, boosting, random forests	Lecture	CO5 CO6	U	
	Practical aspects in machine learning: data preprocessing, overfitting, accuracy estimation, parameter and model selection	Lecture	CO5 CO6	U	
	Bias-Variance tradeoff	Lecture	CO5 CO6	U	

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	Parameter Estimation and Regression	8		✓	✓				12
2	Regularization techniques and Classification algorithms	9		✓	✓				12
3	Unsupervised learning	8		✓	✓				12
4	Support Vector Machine and Graphical Models	7		✓	✓				12
5	Evaluation Metrics and Sampling Methods	8		✓	✓				12

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**

FIRST SEMESTER M. TECH DEGREE (REGULAR) EXAMINATION, DECEMBER 2025 (2025 SCHEME)			
Course Code:	**M250902/CN100A**		
Course Name:	**ADVANCED MACHINE LEARNING**		
Max. Marks	**60**	**Duration**:	2 hours 30 minutes

PART A

(Answer all questions. Each question carries 5 marks)

No.	*Question*	*CO*	*Marks*
1	A set of samples, x=(1,0,1,1,1,0,1,0) is drawn independently from a Bernoulli distribution with unknown parameter θ where θ∈(0,1) a) Write down the likelihood function for θ. b) Derive the log-likelihood function. c) Find the Maximum Likelihood Estimate (MLE) of θ. *(Bernoulli distribution, : $f(x/\theta)=\theta^x(1-\theta)^{1-x}$, $x\in\{0,1\}$*	CO1	(5)
2	Design a multi-layer perceptron for simulating the XOR function.	CO2	(5)
3	Suppose you want to cluster the following eight points using k-means: B1 B2 y1 3 9 y2 2 4 y3 7 3 y4 6 8 y5 8 5 y6 5 2 y7 1 1 y8 4 7 Assume that k = 3 and that initially the points are assigned to clusters as follows: C1 = {y1, y2, y3}, C2 = {y4, y5, y6}, C3 = {y7, y8} Apply the k-means algorithm until convergence, using the Manhattan distance.	CO3	(5)
4	Explain the significance of Support Vector Machines (SVMs) and show that the kernel, K(x,y)=(x·y)2 defines a mapping to a 3-dimensional feature space, where x and y are 2-D input vectors.	CO4	(5)
5	Describe boosting. What is the relation between boosting and ensemble learning?	CO5	(5)

PART B

(Answer any 5 questions. Each question carries 7 marks)

No.	*Question*	*CO*	*Marks*
6	Compare and contrast supervised learning, unsupervised learning, and reinforcement learning in terms of their applications, and describe the major challenges in reinforcement learning and how they are addressed in real-world scenarios.	CO1	(7)
7	Formulate the gradient descent learning rule for the linear model $o^{(d)}=w_0+w_1x_1+\cdots+w_nx_n$ where the parameters are learned from a dataset D. Explicitly state the squared error cost function E, assuming each training example d∈D has a target value $t^{(d)}$.	CO1	(7)
8	Apply linear regression on the given dataset to find the equation of the line. X Y 3 2.5 4 3.2 5 3.8	CO2	(7)

	6 | 6.5 7 | 11.5		
9	Apply the DBSCAN algorithm on Point | X | Y P1 | 3 | 7 P2 | 4 | 6 P3 | 5 | 5 P4 | 6 | 4 P5 | 7 | 3 P6 | 6 | 2 where minimum point = 3 and epsilon = 1.5.	CO3	(7)
10	A factory has three different machines: Machine A, Machine B, and Machine C. Each day, one machine is operating. The quality of the product depends on which machine is running, and the product can only be of two types: Good or Defective. You don't directly know which machine is running on a given day, but you can observe the product quality. The initial state distribution, transition probabilities, and emission probabilities are given below. Initial state distribution (π): π={A:0.4,B:0.35,C:0.25} State transition probability matrix: From/To A B C A 0.5 0.3 0.2 B 0.2 0.6 0.2 C 0.3 0.3 0.4 Emission probability matrix (product quality): State Good Defective Machine A 0.9 0.1 Machine B 0.7 0.3 Machine C 0.6 0.4 a) Draw the HMM. Include the state transition probabilities (between Machine A, B, and C) and the emission probabilities (Good, Defective) for each state. b) What is the probability that the product quality will be Good, Defective, Good on three consecutive days, given that the operating machines are A, B, and C respectively?	CO4	(7)
11	Consider a two-class classification problem of predicting whether a fruit is an apple or an orange. Suppose we have a test dataset of 10 records with expected outcomes and a set of predictions from our classification algorithm. Compute the confusion matrix, accuracy, precision, recall, sensitivity, and specificity on the following data. **Sl. No** | **Actual** | **Predicted** 1 | apple | orange 2 | apple | apple 3 | orange | orange 4 | apple | apple 5 | apple | orange 6 | orange | orange 7 | apple | apple 8 | apple | apple 9 | orange | apple 10 | orange | orange	CO5	(7)

<table>
<tr>
<td>12</td>
<td>You are a data scientist at a banking institution. The bank wants to design, implement, and analyse a machine learning solution to predict whether a loan applicant will default on their loan. You are given the following dataset:
<table>
<tr><th>Age</th><th>Income</th><th>Loan Amount</th><th>Credit Score</th><th>Previous Defaults</th><th>Loan Default (Yes/No)</th></tr>
<tr><td>25</td><td>30,000</td><td>5,000</td><td>650</td><td>0</td><td>No</td></tr>
<tr><td>40</td><td>60,000</td><td>15,000</td><td>720</td><td>0</td><td>No</td></tr>
<tr><td>35</td><td>25,000</td><td>12,000</td><td>580</td><td>1</td><td>Yes</td></tr>
<tr><td>50</td><td>80,000</td><td>20,000</td><td>700</td><td>0</td><td>No</td></tr>
<tr><td>28</td><td>22,000</td><td>7,000</td><td>560</td><td>1</td><td>Yes</td></tr>
<tr><td>45</td><td>55,000</td><td>18,000</td><td>680</td><td>0</td><td>No</td></tr>
<tr><td>30</td><td>40,000</td><td>10,000</td><td>600</td><td>1</td><td>Yes</td></tr>
<tr><td>38</td><td>48,000</td><td>14,000</td><td>710</td><td>0</td><td>No</td></tr>
</table>
a) Describe how you would evaluate model performance (e.g., accuracy, precision, recall, F1-score, confusion matrix). Why might precision and recall be more important than accuracy in this problem?
b) Suggest how the bank could integrate this model into its loan approval system, and how to monitor its performance over time to avoid bias or drift.</td>
<td>CO6</td>
<td>(7)</td>
</tr>
</table>

****

COURSE DESCRIPTION					
Regulation	**2025**	**L-T-J-P-S**	**3-0-0-0-2**	**Credits**	**3**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)					
Course Code	**Course Name**				**Course Category**

M250102/MA100B	FOUNDATIONS OF CRYPTOGRAPHY	PC

COURSE OBJECTIVES	
1	To develop a deep understanding of algebraic structures, including groups, rings, fields, and finite fields and their applications in cryptography.
2	To enable the students to analyze the properties of prime numbers and apply suitable primality testing techniques.
3	To equip students with the skills to solve problems involving linear congruences, quadratic residues, and discrete logarithms.
4	To provide a foundational understanding of elliptic curve arithmetic.
5	To equip students with the skills to apply graph theory concepts, such as Euler graphs, Hamiltonian graphs, spanning trees, and shortest path algorithms, to secure network design.

COMPETENCY & OUTCOMES		
Competency Statements	CC1	Demonstrate the ability to apply advanced mathematical concepts from number theory, algebra, elliptic curves, and graph theory to the design, analysis, and implementation of secure cryptographic systems and networks.

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

CO	CO Statement	Competency Mapping	Cognitive (C)
CO1	Apply integer, modular, and polynomial arithmetic in the construction of finite fields. (Cognitive Knowledge Level: Apply)	CC1	A
CO2	Apply the properties of prime numbers in primality testing algorithms. (Cognitive Knowledge Level: Apply)	CC1	A
CO3	Make use of the properties of congruences and discrete logarithms to solve problems. (Cognitive Knowledge Level: Apply)	CC1	A
CO4	Apply the concept of elliptic curve arithmetic to perform elliptic curve point addition and scalar multiplication. (Cognitive Knowledge Level: Apply)	CC1	A
CO5	Apply graph theoretic algorithms to find Euler Tours, minimal spanning trees and shortest paths. (Cognitive Knowledge Level: Apply)	CC1	A

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

CO	Program Outcomes						
	PO						
	1	2	3	4	5	6	7
1	1	-	-	2	1	1	-
2	1	-	-	2	2	1	-
3	1	-	-	2	1	1	-
4	1	-	-	2	1	1	-
5	1	-	-	2	1	1	-

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

TEACHING AND ASSESSMENT SCHEME														
Teaching Scheme / Week				Self-Learning (S) / Semester	Total Hours / Semester	Credits C	Examination Scheme							
L	T	J	P				Theory			Practical			Total	
3	0	0	0	50	90	3	CIA	ESE	Total	CIA	ESE	Total	100	

							40	60	100	0	0	0	

***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	Algebraic Structures	Integer arithmetic, Greatest Common Divisor, Euclid' s & extended Euclid' s Algorithm, Modular arithmetic, Polynomial Arithmetic, Algebraic Structures-Group Ring Field	8
2	Prime Numbers	Prime numbers, Prime power factorization, Fermat's theorem, Euler's totient function, Euler's theorem, Pseudo primes and Carmichael numbers, Primitive roots.	8
3	Arithmetic of Congruences	Congruences-properties, Linear congruence- Solutions, Chinese Remainder Theorem (CRT), Quadratic Residues, Wilson's theorem, Discrete logarithms**.**	8
4	Elliptic Curve Arithmetic	Elliptic curve arithmetic over real numbers, Prime curves, Binary curves, Addition of two points, Multiplication of a point by a constant.	8
5	Graph Theory	Graphs, Euler Graphs, Hamiltonian graphs, Planar Graphs, Trees, Shortest Path algorithms.	8

SELF-LEARNING / TEAM WORK		
Sl. No	Self-learning / Team Work Description	Hrs/Semester 50
1	Algebraic structures-Group	3
2	Programming Assignment - Write a simple four-function (addition, subtraction, multiplication and division) calculator in $GF(2^8)$ using Python.	3
3	Practice problems from Module 1	4
4	RSA Cryptosystem	3
5	Primality Testing-Deterministic Algorithms-Divisibility Test, AKS Algorithm	3
6	Programming Assignment - Write a computer program that implements the Miller-Rabin algorithm for a user specified n.	2
7	Practice problems from Module 2	4
8	Applications of CRT in Secret Sharing Schemes	3
9	Practice problems from Module 3	4
10	Elliptic Curve Encryption/Decryption	3
11	Security of Elliptic Curve Cryptography- ECC Discrete Logarithm Problem	2
12	Programming Assignment – Construct an elliptic curve calculator using python.	4
13	Practice problems from Module 4	3
14	Graphs- Basic Terminology	2
15	Shortest Path algorithm – Dijkstra's Algorithm	3
16	Practice problems from Module 5	4

SUGGESTED LEARNING RESOURCES			
Text Book			
Sl. No.	Title of Book	Author	Publication

1	Cryptography and Network Security,3rd Edition	Behrouz A Forouzan	Tata McGraw-Hill.
2	Cryptography and Network Security Principles and Practices,4th Edition	William Stallings	Pearson Ed.
3	Elementary Number Theory	G.A. Jones and J.M. Jones	Springer UTM,2007
4	Elliptic curves, Number theory and Cryptography	Lawrence C Washington	Chapman & Hall/CRC
5	A first look at Graph Theory	J. Clark and D. A Holton	Allied Publishers (World Scientific) New Delhi 1991.

Reference

Sl. No.	Title of Book	Author	Publication
1	Introduction to Analytic Number Theory	Tom M. Apostol	Springer Verlag
2	A first course in Abstract Algebra (7th edition)	John B Fraleigh	Pearson Education
3	A Course in Number Theory and Cryptography	Neal Koblitz	Springer Verlag

DETAILED SYLLABUS

Module	Topic	Mode of Delivery	COs	Learning Domain Level C	Hrs
1	Integer arithmetic-Divisibility, Greatest Common Divisor, Euclidean Algorithm	Lecture	CO1	A	1
	Extended Euclidean Algorithm	Lecture	CO1	A	1
	Modular arithmetic - Operations, Properties	Lecture	CO1	U	1
	Polynomial Arithmetic	Lecture	CO1	U	1
	Algebraic structures-Group				
	Ring, Field	Lecture	CO1	U	1
	Construction of Finite fields	Lecture	CO1	A	1
	Operations in Finite Fields -Addition and Multiplication	Lecture	CO1	A	1
	Operations in Finite Fields- Division				
2	Prime Numbers, Fundamental Theorem of arithmetic	Lecture	CO2	U	1
	Fermat's Theorem	Lecture	CO2	U	1
	Euler's Totient Function, Euler's Theorem	Lecture	CO2	U	1
	RSA Cryptosystem	Lecture	CO2	A	1
	Pseudo primes and Carmichael numbers	Lecture	CO2	A	1
	Primality Testing-Deterministic Algorithms-Divisibility Test, AKS Algorithm	Lecture	CO2	A	1
	Primality Testing- Fermat's Test, Square root Test	Lecture	CO2	A	1
	Miller-Rabin Test	Lecture	CO2	A	1
	Primitive Roots	Lecture	CO2	U	1
	Existence of primitive roots	Lecture	CO2	A	1
3	Congruences- Definition and properties	Lecture	CO3	A	1
	Linear congruence- Solutions	Lecture	CO3	A	1
	Chinese Remainder Theorem (CRT)	Lecture	CO3	A	1
	Applications of CRT	Lecture	CO3	A	1
	Quadratic Residues, Euler's Criterion, Legendre symbol	Lecture	CO3	U	1
	Quadratic Reciprocity Law	Lecture	CO3	A	1

	Jacobi Symbol	Lecture	CO3	A	1
	Wilson' s theorem	Lecture	CO3	U	1
	Discrete logarithms	Lecture	CO3	U	1
4	Elliptic curves over real numbers	Lecture	CO4	U	1
	Arithmetic of elliptic curves over real numbers	Lecture	CO4	U	1
	Addition and scalar multiplication of points- problems	Lecture	CO4	A	1
	Prime curves -Definition	Lecture	CO4	U	1
	Prime Curves – Addition of two points	Lecture	CO4	A	1
	Prime Curves – Scalar multiplication of a point	Lecture	CO4	A	1
	Binary Curves- Definition	Lecture	CO4	U	1
	Binary Curves- Addition and scalar multiplication of points	Lecture	CO4	A	1
	Elliptic Curve Encryption/Decryption	Lecture	CO4	A	1
	Security of Elliptic Curve Cryptography- ECC Discrete Logarithm Problem	Lecture	CO4	A	1
5	Graphs- Basic Terminology	Lecture	CO5	U	1
	Euler Graph	Lecture	CO5	U	1
	Fleury's Algorithm	Lecture	CO5	A	1
	Hamiltonian Graphs	Lecture	CO5	U	1
	Planar Graphs	Lecture	CO5	A	1
	Euler's Formula	Lecture	CO5	A	1
	Tree, Spanning tree	Lecture	CO5	U	1
	Connector Problems	Lecture	CO5	A	1
	Shortest Path algorithm – Dijkstra's Algorithm	Lecture	CO5	A	1
	Shortest Path algorithm – BFS Algorithm	Lecture	CO5	A	1

TABLE OF SPECIFICATIONS (ToS) FOR QUESTION PAPER DESIGN

Module	Module Title	Teaching Hours	Distribution of Marks (Revised Bloom's Level)						Total Marks
			R	U	A	An	E	C	
1	Algebraic Structures	8	✓	✓	✓				12
2	Prime Numbers	8	✓	✓	✓				12
3	Arithmetic of Congruences	8	✓	✓	✓				12
4	Elliptic Curve Arithmetic	8	✓	✓	✓				12
5	Graph Theory	8	✓	✓	✓				12

This ToS shall be treated as a general guideline for students and teachers for distribution of marks.

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

FIRST SEMESTER M. TECH DEGREE (REGULAR) EXAMINATION, DECEMBER 2025 (2025 SCHEME)	
Course Code:	**M250102/MA100B**
Course Name:	**FOUNDATIONS OF CRYPTOGRAPHY**

Max. Marks	**60**	**Duration**:	2 hours 30 minutes

PART A

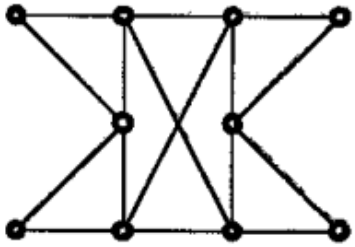
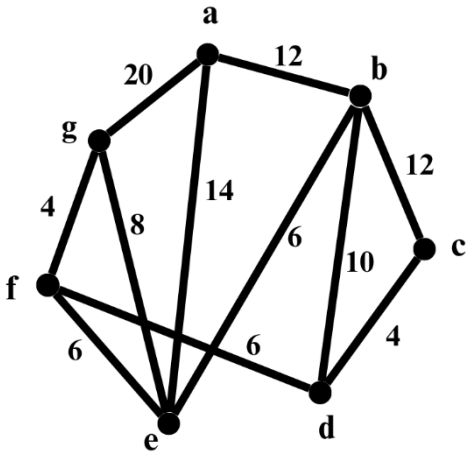
(Answer all questions. Each question carries 4 marks)

No.	***Question***	***CO***	***Marks***
1	Using the extended Euclidean algorithm, obtain two integers s and t such that $13\,s + 20\,t = 1$.	CO1	(4)
2	Show that 2 is a primitive root modulo 25.	CO2	(4)
3	State Wilson's theorem. Find the remainder obtained when $27! - 1$ is divided by 29.	CO3	(4)
4	Find all the points in the elliptic curve $E_7(2,1)$, the curve defined by the equation $y^2 \equiv x^3 + 2x + 1 \pmod 7$.	CO4	(4)
5	Differentiate between Euler graph and Hamiltonian graph. Construct a graph that is Euler but not Hamiltonian.	CO5	(4)

PART B

(Answer any one full question from each module, each question carries 8 marks)

No.		***Question***	***CO***	***Marks***
MODULE 1				
6	a)	Explain the construction of finite fields and the operations in it.	CO1	(4)
	b)	Consider the finite field $\mathrm{GF}(2^8)$ with irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$. Let $f(x) = x^6 + x^4 + x^2 + x + 1$ and $g(x) = x^7 + x + 1$. Compute the following over $\mathrm{GF}(2^8)$; i. $f(x) + g(x)$ ii. $f(x) \times g(x)$	CO1	(4)
OR				
7	a)	Describe modulo operator and the properties of modular arithmetic.	CO1	(4)
	b)	Find the multiplicative inverse of 550 in $GF(1759)$.	CO1	(4)
MODULE II				
8	a)	State and prove Fermat's theorem.	CO2	(4)
	b)	Define Carmichael number. Show that 2821 is a Carmichael number.	CO2	(4)
OR				
9	a)	Explain the Miller-Rabin algorithm for primality testing. While using Miller-Rabin test, how can you reduce the probability of incorrectly identifying a composite number as a prime?	CO2	(5)
	b)	Check whether the number 27 pass Miller-Rabin test to the base 2?	CO2	(3)
MODULE III				
10	a)	Using Chinese remainder theorem solve the following set of simultaneous congruences; $x \equiv 2 \pmod 3, x \equiv 3 \pmod 5, x \equiv 2 \pmod 7$	CO3	(5)
	b)	Explain any one application of Chinese remainder theorem in cyber security.	CO3	(3)
OR				
11	a)	Is 219 a quadratic residue modulo the prime number 383? Justify your answer.	CO3	(4)
	b)	Given that 2 is a primitive root modulo 13. Construct a table of discrete logarithm and using it find a solution for $x^7 \equiv 6 \pmod{13}$.	CO3	(4)
MODULE IV				
12		Consider the points $P = (3,3), Q = (2,0), R = (3,8)$ in the elliptic curve $E_{11}(1,1)$. Calculate the following; i) $P + Q$ ii) $2P$ iii) $P + R$	CO4	(8)
OR				
13		Consider $\mathrm{GF}(2^3)$ with irreducible polynomial $f(x) = x^3 + x + 1$. Let g be a root of $f(x) = 0$ and a generator of $\mathrm{GF}(2^3)$. Let $P = (0,1)$ and $Q = (g^2, 1)$ be two points in the binary elliptic curve $y^2 + xy = x^3 + g^3x^2 + 1$ over $\mathrm{GF}(2^3)$. Find i) $P + Q$ ii) $2Q$.	CO4	(8)
MODULE V				

14	Determine whether the following graph is Euler. If so find an Euler tour using Fleury's algorithm. 	CO5	(8)
	OR		
15	Explain Dijkstra's algorithm and use it to find the lengths of the shortest paths from the vertex a to each of the other vertices and give examples of such paths. 	CO5	(8)

****

COURSE DESCRIPTION					
Regulation	**2025**	**L-T-J-P-S**	**3-0-0-0-2**	**Credits**	**3**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)					
Course Code	**Course Name**				**Course Category**
M250102/ CY100C	**INFORMATION SECURITY**				**PC**

COURSE OBJECTIVES	
1	Apply foundational principles of confidentiality, integrity, and availability in digital systems
2	Implement cryptographic techniques and secure communication protocols to protect data and communications.
3	Analyse vulnerabilities and threats across network, system, and application layers using security tools and technologies.
4	Design secure identity and access control mechanisms using authentication methods and access models.
5	Evaluate risk management strategies, governance policies, and compliance standards for effective organizational security auditing.

COMPETENCY & OUTCOMES		
Competency Statements	CC1	Apply core security principles, threat models, and countermeasures in real-world scenarios
	CC2	Utilize cryptographic methods to enhance digital security.
	CC3	Evaluate governance, ethics, and compliance in the context of cybersecurity laws and standards.

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

CO	CO Statement	Competency Mapping	Cognitive (C)
CO1	Apply foundational principles of confidentiality, integrity, and availability in digital systems. (Cognitive Knowledge Level: Apply)	CC1	A
CO2	Implement cryptographic techniques and secure communication protocols to protect data and communications. (Cognitive Knowledge Level: Apply)	CC2	A
CO3	Analyse vulnerabilities and threats across network, system, and application layers using security tools and technologies. (Cognitive Knowledge Level: Analyse)	CC1	An
CO4	Design secure identity and access control mechanisms using authentication methods and access models. (Cognitive Knowledge Level: Create)	CC1	C
CO5	Evaluate risk management strategies, governance policies, and compliance standards for effective organizational security auditing. (Cognitive Knowledge Level: Evaluate)	CC3	E

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

CO	Program Outcomes						
	PO						
	1	2	3	4	5	6	7
1	3		3	2			
2	3		3	3	2		
3	3		3	3	3		
4	1		2	3	2		
5	1	2	2	2		3	1

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

TEACHING AND ASSESSMENT SCHEME													
Teaching Scheme / Week				Self-Learning (S) / Semester	Total Hours / Semester	Credits C	Examination Scheme						
L	T	J	P				Theory			Practical			Total
							CIA	ESE	Total	CIA	ESE	Total	
3	0	0	0	25	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	Foundations of Information Security	Introduction to Information Security, Need for Security	6
2	Cryptography and Secure Communication	Identification, Authentication, and Access Control Concepts, Cryptography	10
3	Security Technologies and Tools	Intrusion Detection and Prevention System (IDPS), Security Information and Event Management (SIEM), Scanning and Analysis Tools	11
4	Governance, Risk Management	Information Security Governance and Policy Risk Management	7
5	Security Auditing	Information Security Auditing	6

SELF-LEARNING / TEAM WORK		
Sl. No	**Self-learning / Team Work Description**	**Hrs/Semester**
1	Develop a conceptual understanding of network architectures, protocols, and communication models necessary for secure system design. https://www.cybrary.it/skill-paths/network-fundamentals	10
2	Apply cybersecurity principles to evaluate threats, recognize vulnerabilities, and implement basic security controls in real-world contexts. https://www.cybrary.it/skill-paths/cybersecurity-fundamentals	10
3	Cyber Security Tools, Techniques, and Counter Measures - Course	10

SUGGESTED LEARNING RESOURCES			
Text Book			
Sl. No.	Title of Book	Author	Publication
1	Principles of Information Security	Michael E. Whitman, Herbert J. Mattord	6th edition, Cengage Learning, 2018.
2	Fundamentals of Information Security: A Straightforward Introduction	Jason Andress	No Starch Press, Inc.
3	Information Security Governance: A Practical Development and Implementation Approach	Krag Brotby	John Wiley & Sons,2009
Reference			
Sl. No.	Title of Book	Author	Publication
1	Information Security Governance	S.H. von Solms, Rossouw von Solms	Springer(2008)
2	IT Auditing Using Controls to Protect Information Assets	Mike Kegerreis, Mike Schiller, Chris Davis	McGraw-Hill Education 3rd Edition
3	Information Technology Control and Audit	Angel R Otero	CRC Press / Auerbach Publications5th Edition
Web Resource			
1	Cybersecurity Fundamentals | Cybrary		
2	Lecture Videos | Computer Systems Security | Electrical Engineering and Computer Science | MIT OpenCourseWare		
3	Information Systems Auditing, Controls and Assurance | Coursera		

DETAILED SYLLABUS					
Module	Topic	Mode of Delivery	COs	Learning Domain Level C	Hrs
1	What Is Security? Key Concepts in Information Security	Lecture	CO1	A	1
	Critical Characteristics of Information, Components of an Information System	Lecture	CO1	A	1
	Approaches to Information Security Implementation, Security in the Systems Development Life Cycle	Lecture	CO1	A	1
	Introduction to Threats and Attacks	Lecture	CO1	A	1
	Compromises to Intellectual Property, Deviations in Quality of Service Espionage or Trespass, Forces of Nature, Human Error or Failure, Information Extortion	Lecture	CO1	A	1
	Sabotage or Vandalism, Software Attacks, Technical Hardware and Software Failures, Technological Obsolescence and Theft, Défense in Depth	Lecture	CO1	A	1
2	Introduction to Cryptography, Cipher Methods	Lecture	CO2	A	1
	Cryptographic Algorithms-Symmetric Encryption	Lecture	CO2	A	1
	Cryptographic Algorithms-Asymmetric Encryption	Lecture	CO2	A	1
	Cryptographic Tools and Key Management, Post quantum cryptography	*Self-Learning*	CO2	A	1
	Protocols for Secure Communication	Lecture	CO2	A	1
	Identification and Authentication Concepts	Lecture	CO4	C	1
	Common Authentication Methods: Passwords, Biometrics, Hardware Tokens	Lecture	CO4	C	1
	Introduction to Access Controls- Implementing Access Controls	Lecture	CO4	C	1
	Access Control Models: DAC, MAC, RBAC	Lecture	CO4	C	1
	Physical Access Control Mechanisms	Lecture	CO4	C	1
3	Intrusion Detection and Prevention Systems (IDPS): Purpose, Types	Lecture	CO3	An	1
	IDPS-Detection Methods, Strengths, Limitations, Deployment	Lecture	CO3	An	1
	Security Information and Event Management (SIEM): Concepts, Data Aggregation and Analysis, Operational Interface	Lecture	CO3	An	1
	Port Scanners, Firewall Analysis Tools	Lecture	CO3	An	1
	Operating System Detection Tools	Lecture	CO3	An	1
	Vulnerability Scanners	Lecture	CO3	An	1
	Packet Sniffers, Wireless Security Tools	Lecture	CO4	C	1
	Firewalls: Types and Deployment	Lecture	CO4	C	1
	Firewalls: Types and Deployment	Lecture	CO4	C	1
	Biometric Access Controls	Lecture	CO4	C	1
	Remote Access Security, VPNs, and Their Role in Secure Connections	Lecture	CO3	An	1
	Remote Access Security, VPNs, and Their Role in Secure Connections	Lecture	CO3	An	1
4	Information Security Governance: Concepts and Need Information Security Policy, Standards, and Practices	Lecture	CO5	E	1
	Security Education, Training and Awareness Program	Lecture	CO5	E	1

	Risk Management-Risk Identification, Assessment, and Control	Lecture	CO5	E	1
	Risk Control Strategies: Avoidance, Mitigation, Acceptance	Lecture	CO5	E	1
	Cost Benefit Analysis (CBA) – Conceptual Overview	Lecture	CO5	E	1
	Governance Overview: Governance Definition, Information Security Governance, Six Outcomes of Effective Governance Data, Knowledge, Value of Information, Benefits of Good Governance	Self-Learning	CO5	E	1
	Overview of ISO/IEC 27001 and ISO/IEC 27002	Self-Learning	CO5	E	1
5	Internal Controls and Audit Basics	Lecture	CO5	E	1
	Stages of an Audit	Lecture	CO5	E	1
	Auditing Cyber Security Programs	Lecture	CO5	E	1
	Auditing Networking Devices, Auditing Unix and Linux Operating Systems	Lecture	CO5	E	1
	Auditing End User Computing Devices	Self-Learning	CO5	E	1
	Auditing Cloud Services and Outsourced Environments Auditing New/Other Technologies	Self-Learning	CO5	E	1

TABLE OF SPECIFICATIONS (ToS) FOR QUESTION PAPER DESIGN

Module	Module Title	Teaching Hours	Distribution of Marks (Revised Bloom's Level)						Total Marks
			R	U	A	An	E	C	
1	Foundations of Information Security	6		✓	✓				12
2	Cryptography and Secure Communication	10		✓	✓				12
3	Security Technologies and Tools	11		✓	✓	✓			12
4	Governance and Risk Management	7		✓	✓		✓		12
5	Information Security Auditing	6		✓	✓		✓		12

This ToS shall be treated as a general guideline for students and teachers for distribution of marks.

Assessment	**Marks**
Continuous Internal Assessment	**40**
Learning Activity	5
Internal Examination	10
Course Project	20
End Semester Examination	**60**
Total	**100**

FIRST SEMESTER M. TECH DEGREE (REGULAR) EXAMINATION, DECEMBER 2025 (2025 SCHEME)			
Course Code:	**M250102/ CY100C**		
Course Name:	**INFORMATION SECURITY**		
Max. Marks	**60**	**Duration**:	2 hours 30 minutes

PART A

(Answer all questions. Each question carries 5 marks)

No.	*Question*	*CO*	*Marks*
1	An attacker breaks into a network, copies files, defaces a web page, and steals credit card numbers. Identify which components of the CIA triad are affected and apply your knowledge to explain how each is impacted.	CO1	(5)
2	Encrypt the plaintext 'CRYPTO' using a Caesar cipher with a shift of 5 and then decrypt it to recover the original message	CO2	(5)
3	Examine two main methods of implementing access controls	CO3	(5)
4	Distinguish between trusted VPNs, secure VPNs, and hybrid VPNs	CO4	(5)
5	Analyse the components of risk identification	CO5	(5)

PART B

(Answer any 5 questions. Each question carries 7 marks)

No.	*Question*	*CO*	*Marks*
6	Identify the different categories of security threats in an organizational context and provide a real-world example for each.	CO1	(7)
7	Apply the Security Development Life Cycle (SDLC) to explain how a secure application can be developed	CO1	(7)
8	Compare common identification and authentication methods with their typical applications.	CO2	(7)
9	Analyze how IDPS improves the overall defense strategy of an organization	CO3	(7)
10	Predict the type of access control models used by an organization to protect financial data, employee records, and project files. Explain the major features of the identified model	CO4	(7)
11	Elaborate on scanning and analysis tools used in IT systems.	CO4	(7)
12	Evaluate the stages of an internal audit and discuss how each stage contributes to improving organizational controls and risk management	CO5	(7)

****

COURSE DESCRIPTION					
Regulation	**2025**	**L-T-J-P-S**	**3-0-0-0-2**	**Credits**	**3**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)					
Course Code	**Course Name**				**Course Category**
M250102/CY111D	**CYBER FORENSICS AND INCIDENT RESPONSE**				**PROGRAMME ELECTIVE**

COURSE OBJECTIVES	
1	Develop technical proficiency in digital forensic tools and methodologies for evidence acquisition, analysis of cyber incidents (network/mobile/email), and anti-forensics detection.
2	Evaluate legal and governance frameworks to ensure cyber forensic investigations adhere to judicial standards and ethical guidelines.
3	Design and execute structured incident response procedures, including evidence preservation, reporting, and compliance with organizational policies.

COMPETENCY & OUTCOMES		
Competency Statements	CC 1	Conduct forensic investigations using industry-standard methodologies, tools, and protocols for digital evidence acquisition, analysis, and reporting.
	CC 2	Apply legal and governance frameworks to cyber forensic practices, ensuring compliance with incident response policies, IT laws, and ethical guidelines.

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

CO	CO Statement	Competency Mapping	Cognitive (C)
CO1	Analyze the judicial and governance frameworks of the IT Act 2000 in current cybersecurity contexts. (Cognitive Knowledge Level: Analyse)	CC2	An
CO2	Execute incident response procedures using digital forensic tools to collect and analyze evidence. (Cognitive Knowledge Level: Apply)	CC1	A
CO3	Apply forensic protocols and tools to acquire, preserve, and analyze digital evidence from storage media. (Cognitive Knowledge Level: Apply)	CC1	A
CO4	Reconstruct digital footprints by analyzing network traffic, mobile devices, and email artifacts. (Cognitive Knowledge Level: Analyse)	CC1	An
CO5	Detect anti-forensics techniques and generate structured investigative reports. (Cognitive Knowledge Level: Evaluate)	CC1	E

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

CO	Program Outcomes						
	PO						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1	2	1	2	3	1	2	1
2	3	2	3	3	3	2	1
3	2	1	2	2	3	1	1
4	2	1	2	2	3	1	1
5	3	3	3	3	3	2	2

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

TEACHING AND ASSESSMENT SCHEME

Teaching Scheme / Week				Self-Learning (S) / Semester	Total Hours / Semester	Credits C	Examination Scheme						
L	T	J	P				Theory			Practical			Total
							CIA	ESE	Total	CIA	ESE	Total	
3	0	0	0	30	70	3	40	60	100	0	0	0	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	Cyber Forensics	Cyber Technology- Technological Aspects of Cyber Forensics- Cybercrimes, Types of Cybercrimes - Governance Aspects of Cyber Forensics- Cyber Security Steps taken to protect ICT and prevent Misuse of Internet -Judicial Aspects of Cyber Forensics- Legal Perspective of Cyber Forensic investigations- IT Act 2000, Social Cyber Media.	9
2	Computer Incident Response	Introduction, Incident Response Team, Stages of Incident Response, Security Incident Response Team Members, Incident Evidence, Incident Response Tools, Incident Response Policies and Procedures.	8
3	Forensic Process and Investigations	Preparing for computer investigations, understanding Public and private investigations, Forensics Process and Forensics Investigation Principles - Forensic Protocol for Evidence Acquisition - Digital Forensics Standards and Guidelines - Digital Evidence – Data Acquisition - storage formats for digital evidence, determining the best acquisition method, Whole Disk Encryption Computer Forensic Investigations: -Preparing for computer investigations, understanding Public and private investigations, Forensics Process and Forensics Investigation Principles - Forensic Protocol for Evidence Acquisition - Digital Forensics Standards and Guidelines - Digital Evidence – Data Acquisition - storage formats for digital evidence, determining the best acquisition method, Whole Disk Encryption. Cyber Forensics Tools-Computer Forensics software and hardware tools -Open Source and Proprietary –-Challenges in Cyber Forensics, Skills Required to Become a Cyber Forensic Expert- Physical Requirements of a Cyber forensics Lab, Types of Cyber forensics	11
4	Network and Email Forensics	Network and Mobile Device Forensics: Forensic Footprints, Seizure of Networking Devices, Network Forensic Artifacts, ICMP Attacks, Drive-By Downloads, Network Forensic Analysis Tools, Case Study: Wireshark. Mobile device forensics, acquisition procedures for cell phones and mobile devices Email Forensics: Email Components, Email Protocols. Email Formats: RFC 5322, Multipurpose Internet Mail Extensions. Email Threats and Comprehensive Email Security, S/MIME-Operational Description, Message Content Types, Analysis of Email headers.	7
5	Anti-forensics and report writing	Anti-forensic Practices: Data Wiping, Shredding, Data Remanence, Degaussing, Trail Obfuscation- Spoofing, Data Modification, Encryption, Case Study: VeraCrypt, Data Hiding: Steganography and Cryptography, Case Study: SilentEye, Anti-forensics Detection Techniques, Case Study: Stegdetect Report writing for high tech investigations – importance of reports, guidelines for writing, generating report findings with forensics software tools.	5

SELF-LEARNING / TEAM WORK		
Sl. No	Self-learning / Team Work Description	Hrs/Semester
1	IT Act 2000: Key sections, amendments, and relevance to modern cybercrimes	2
2	Cybercrimes: Types (phishing, ransomware, identity theft) and case studies	1
3	Cybersecurity governance: Steps to protect ICT infrastructure	1
4	Social media forensics: Legal challenges & evidence collection	1
5	Incident Response Lifecycle (NIST SP 800-61)	1
6	IR Team Roles & Tools: Autopsy, FTK Imager	2
7	Evidence Handling: Chain of custody, volatile data collection	2
8	Forensic Acquisition Methods: Disk imaging (dd/FTK)	2
9	Data Storage Formats (AFF4, E01) & Encryption (BitLocker)	2
10	Forensic Tools: Autopsy (open-source) vs. EnCase (proprietary)	2
11	Lab Requirements & Skill Development	2
12	Network Artifacts: ICMP attacks, drive-by downloads	2
13	Mobile Forensics: Acquisition (ADB, Cellebrite)	2
14	Email Header Analysis: Tracing origins, identifying spoofing	3
15	Anti-Forensics Techniques: Steganography (SilentEye), data wiping	2
16	Detection Tools: Steg detect, VeraCrypt analysis	2
17	Forensic Report Writing: Structure, tools (Magnet REPORT)	1

SUGGESTED LEARNING RESOURCES			
Text Book			
Sl. No.	Title of Book	Author	Publication
1	Cyber Forensics in India- A Legal Perspective	Nishesh Sharma	Universal Law Publishing, First Edition, March 2017
2	Computer forensics- Guide to computer forensics and investigations	Bill Nelson, Amelia Philipps and Christopher Steuart	Course Technology Inc, 3rd Edition, 2009
3	Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response	Leighton Johnson	Syngress, First Edition, 2019
4	Network Security Essentials Applications and Standards	William Stallings	Pearson Education, 4th Edition, 2011.
Reference			
Sl. No.	Title of Book	Author	Publication
1	Fundamentals of Network Security	E. Maiwald	McGraw-Hill, First Edition, 2004
2	Practical Cyber Forensics: An Incident-Based Approach to Forensic Investigations	Niranjan Reddy	Apress, First Edition, 2019
3	Cyber Security Principles of Information Security	Michael. E. Whitman, Herbet. J. Mattord	Course Technology Ptr, 4th Edition,2011.
4	Cryptography and Network Security	William Stallings	Pearson, 5th Edition, 2018
Web Resource			
1	https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt		

2	https://www.sans.org/white-papers/digital-forensics/
3	https://tryhackme.com/path/outline/forensics
4	https://www.autopsy.com/documentation/

DETAILED SYLLABUS

Module	Topic	Mode of Delivery	COs	Learning Domain Level C	Hrs
1	Cyber Forensics- Introduction	Lecture	CO1	U	1
	Cyber Technology - Technological Aspects of Cyber Forensics- Lecture 1	Lecture	CO1	U	1
	Technological Aspects of Cyber Forensics-Lecture 2	Lecture	CO1	U	1
	Cybercrimes, Types of Cybercrimes	Lecture	CO1	U	1
	Governance Aspects of Cyber Forensics	Lecture	CO1	U	1
	Cyber Security Steps taken to protect ICT and prevent Misuse of Internet	Lecture	CO1	U	1
	Judicial Aspects of Cyber Forensics	Lecture	CO1	An	1
	Legal Perspective of Cyber Forensic investigations	Lecture	CO1	An	1
	IT Act 2000, Social Cyber Media	Lecture	CO1	An	1
2	Computer Incident Response- Introduction	Lecture	CO2	U	1
	Incident Response Team	Lecture	CO2	U	1
	Stages of Incident Response	Lecture	CO2	A	1
	Security Incident Response Team Members	Lecture	CO2	U	1
	Incident Evidence	Lecture	CO2	A	1
	Incident Response Tools-Lecture 1	Lecture	CO2	U	1
	Incident Response Tools-Lecture 2	Lecture	CO2	A	1
	Incident Response Policies and Procedures	Lecture	CO2	U	1
3	Computer Forensic Investigations: -Preparing for computer investigations	Lecture	CO3	U	1
	Understanding Public and private investigations	Lecture	CO3	U	1
	Forensics Process and Forensics Investigation Principles	Lecture	CO3	A	1
	Forensic Protocol for Evidence Acquisition	Lecture	CO3	U	1
	Digital Forensics Standards and Guidelines	Lecture	CO3	U	1
	Digital Evidence, Data Acquisition	Lecture	CO3	A	1
	Storage formats for digital evidence, Determining the best acquisition method, Whole Disk Encryption	Lecture	CO3	U	1
	Cyber Forensics Tools-Computer Forensics software and hardware tools - Open Source and Proprietary	Lecture	CO3	U	1
	Challenges in Cyber Forensics	Lecture	CO3	U	1
	Skills Required to Become a Cyber Forensic Expert, Physical Requirements of a Cyber forensics Lab		CO3	U	1
	Types of Cyber forensics		CO3	U	1
4	Forensic Footprints, Seizure of Networking Devices, Network Forensic Artifacts	Lecture	CO3	U	1
	ICMP Attacks, Drive-By Download	Lecture	CO4	U	1

	Network Forensic Analysis Tools, Case Study: Wireshark.	Lecture	CO4	An	1
	Mobile device forensics, acquisition procedures for cell phones and mobile devices	Lecture	CO4	U	1
	Email Forensics: Email Components, Email Protocols, Email Formats: RFC 5322, Multipurpose Internet Mail Extensions	Lecture	CO4	U	1
	Email Threats and Comprehensive Email Security, S/MIME-Operational Description, Message Content Types	Lecture	CO4	U	1
	Analysis of Email headers	Lecture	CO4	An	1
5	Anti-forensic Practices - Data Wiping and Shredding, Data Remanence, Degaussing	Lecture	CO5	U	1
	Trail Obfuscation: Spoofing, Data Modification, Encryption Case Study: VeraCrypt	Lecture	CO5	U, E	1
	Data Hiding: Steganography and Cryptography, Case Study: SilentEye	Lecture	CO5	U, E	1
	Anti-forensics Detection Techniques, Case Study: Steg detect	Lecture	CO5	U, E	1
	Report writing for high tech investigations	Lecture	CO5	E	1

TABLE OF SPECIFICATIONS (ToS) FOR QUESTION PAPER DESIGN

Module	Module Title	Teaching Hours	Distribution of Marks (Revised Bloom's Level)						Total Marks
			R	U	A	An	E	C	
1	Cyber Forensics	9		✓		✓			12
2	Computer Incident Response	8		✓	✓				12
3	Forensic Process and Investigations	11		✓	✓				12
4	Network and Email Forensics	7		✓		✓			12
5	Anti-Forensics and Report Writing	5		✓			✓		12
This ToS shall be treated as a general guideline for students and teachers for distribution of marks.									

Assessment	Marks
Continuous Internal Assessment	**40**
Learning Activity	15
Internal Examination	10
Course Project	15
End Semester Examination	**60**
Total	**100**

COURSE DESCRIPTION					
Regulation	**2025**	**L-T-J-P-S**	**3-0-0-0-2**	**Credits**	**3**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)					
Course Code	**Course Name**				**Course Category**
M250102/CY112D	**WEB APPLICATION SECURITY**				**PROGRAMME ELECTIVE**

COURSE OBJECTIVES	
1	Establish mastery over core web application security principles and modern defence paradigms, using OWASP terminology and frameworks.
2	Conduct end-to-end security assessments by systematically gathering reconnaissance, identifying vulnerabilities, and ethically exploiting attack vectors in lab environments.
3	Design and implement risk-driven defenses and operationalize vulnerability management workflows to protect applications against evolving threats.

COMPETENCY & OUTCOMES		
Competency Statements	CC 1	Find and exploit security weaknesses in web applications using standard tools and methods.
	CC 2	Examine how modern web technologies work and identify their security risks

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

CO	CO Statement	Competency Mapping	Cognitive (C)
CO1	Explain core web application security terminology, vulnerabilities, and countermeasures using OWASP standards. (Cognitive Knowledge Level: Understand)	CC 1	U
CO2	Conduct systematic reconnaissance to identify entry points, server/client-side technologies, and functionality using industry-standard tools like Burp Suite, Nmap. (Cognitive Knowledge Level: Apply)	CC 1	A
CO3	Apply offensive techniques to ethically exploit vulnerabilities in simulated web environments Exploit common web vulnerabilities in controlled environments to demonstrate attack impact. (Cognitive Knowledge Level: Apply)	CC 1	A
CO4	Design and implement secure architectures and defenses to mitigate vulnerabilities. (Cognitive Knowledge Level: Evaluate)	CC 2	E
CO5	Develop secure asynchronous JavaScript applications while mitigating client-side risks. (Cognitive Knowledge Level: Apply)	CC 2	A

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

CO	Program Outcomes						
	PO						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1	1	2	2	1	-	2	-
2	2	1	3	2	3	-	-
3	2	-	3	2	3	2	-
4	3	2	3	3	2	2	2
5	3	3	3	3	3	1	3

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

TEACHING AND ASSESSMENT SCHEME													
Teaching Scheme / Week				Self-Learning (S) / Semester	Total Hours / Semester	Credits C	Examination Scheme						
							Theory			Practical			Total
L	T	J	P				CIA	ESE	Total	CIA	ESE	Total	
3	0	0	0	30	70	3	40	60	100	0	0	0	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 Web Application	Web Application Security Terminology, Types of Web Application Security Testing, Web Application Vulnerabilities and Counter measures	6
2	Reconnaissance	Information Gathering, identifying entry points, Identifying Server-Side Technologies, Identifying Server-Side Functionality Detecting Client-side Technologies	9
3	Web Application Offence	Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), XML External Entity (XXE), Injection	9
4	Securing and Hardening Applications	Securing Modern Web Applications, Secure Application Architecture, defending against XSS Attacks, defending against CSRF Attacks, defending against XXE Attacks, defending against Injection, Defending against DOS	7
5	Web Application Development Technologies	Synchronous and Asynchronous JavaScript, Asynchronous programming and callbacks, Promises, Async and Await, React, Node.js, Express	9

SELF-LEARNING / TEAM WORK		
Sl. No	Self-learning / Team Work Description	Hrs/Semester
1	The Evolution of Web Applications, Web Application Security	1
2	The HTTP Protocol	2
3	Web Functionality	2
4	Essential skills Lab	2
5	API testing Lab	3
6	SQL injection Lab	3
7	File upload vulnerabilities Lab	2
8	Authentication Lab	2
9	Access control vulnerabilities Lab	2
10	HTTP Host header attacks Lab	2
11	HTML and CSS	2
12	JavaScript - Expressions, Data Types,	1
13	JavaScript - Variables, Classes	2

14	JavaScript - Functions, this operator Arrow Functions	3
15	JavaScript - Loops, Scopes, Arrays, Template Literals	2

SUGGESTED LEARNING RESOURCES			
Text Book			
Sl. No.	Title of Book	Author	Publication
1	Web Application Security: Exploitation and Countermeasures for Modern Web Applications	Andrew Hoffman	O'Reilly Media
2	The Web Application Hacker's Handbook	Dafydd Stuttard Marcus Pinto	Wiley Publishing, second edition
Reference			
Sl. No.	Title of Book	Author	Publication
1	The Manager's Guide to Web Application Security: A Concise Guide to the Weaker Side of the Web	Ron Lepofsky	Apress, First edition
Web Resource			
1	https://developer.mozilla.org/en-US/docs/Web/HTML		
2	https://developer.mozilla.org/en-US/docs/Web/CSS		
3	https://portswigger.net/		
4	https://react.dev/learn		
5	https://nodejs.org/en/learn/getting-started/introduction-to-nodejs		
6	https://expressjs.com/en/starter/hello-world.html		
7	https://www.mongodb.com/resources/languages/mern-stack		
8	https://www.mongodb.com/resources/languages/mern-stack-tutorial		

DETAILED SYLLABUS					
Module	Topic	Mode of Delivery	COs	Learning Domain Level C	Hrs
1	Web Application Security Terminology	Lecture	CO1	U	1
	Web Application Security Terminology	Lecture	CO1	U	1
	Types of Web Application Security Testing	Lecture	CO1	U	1
	Web Application Vulnerabilities, Types of Attack and Counter measures – 1	Lecture	CO1	U	1
	Web Application Vulnerabilities, Types of Attack and Counter measures – 2	Lecture	CO1	U	1
	Web Application Vulnerabilities, Types of Attack and Counter measures – 3	Lecture	CO1	U	1
2	Information Gathering - Finding Subdomains	Lecture, Lab	CO2	A	1
	Identifying Entry Points -1	Lecture	CO2	U	1
	Identifying Entry Points -2	Lecture	CO2	A	1
	Identifying Server-Side Technologies – 1	Lecture	CO2	U	1

	Identifying Server-Side Technologies – 2	Lecture	CO2	A	1
	Identifying Server-Side Functionality – 1	Lecture	CO2	U	1
	Identifying Server-Side Functionality – 2	Lecture	CO2	A	1
	Detecting Client-side Technologies – 1	Lecture	CO2	U	1
	Detecting Client-side Technologies – 2	Lecture	CO2	A	1
3	Cross-Site Scripting (XSS) – 1	Lecture	CO3	U	1
	XSS – 2	Lecture	CO3	A	1
	XSS – 3	Lab	CO3	A	1
	Cross-Site Request Forgery (CSRF) – 1	Lecture	CO3	U	1
	CSRF – 2	Lab	CO3	A	1
	XML External Entity (XXE) – 1	Lecture	CO3	U	1
	XXE – 2	Lecture	CO3	U	1
	Injection – 1	Lecture	CO3	U	1
	Injection – 2	Lecture	CO3	A	1
4	Securing Modern Web Applications	Lecture	CO4	E	1
	Secure Application Architecture	Lecture	CO4	E	1
	Defending against XSS Attacks - 1	Lecture	CO4	U	1
	Defending against XSS Attacks – 2	Lecture	CO4	E	1
	Defending against CSRF Attacks - 1	Lecture	CO4	E	1
	Defending against CSRF Attacks – 2	Lecture	CO4	U	1
	Defending against XXE Attacks	Lecture	CO4	U	1
5	Synchronous and Asynchronous JavaScript	Lab	CO5	U	1
	Asynchronous programming and callbacks	Lab	CO5	U, A	1
	Promises, Async and Await	Lab	CO5	U, A	1
	React – 1	Lab	CO5	U	1
	React – 2	Lab	CO5	A	1
	Node.js – 1	Lab	CO5	U	1
	Node.js – 2	Lab	CO5	A	1
	Express – 1	Lab	CO5	U	1
	Express – 2	Lab	CO5	A	1

TABLE OF SPECIFICATIONS (ToS) FOR QUESTION PAPER DESIGN				
Module	**Module Title**	**Teaching Hours**	**Distribution of Marks (Revised Bloom's Level)**	**Total Marks**

			R	U	A	An	E	C	
1	Introduction to Web Application	6		✓					12
2	Reconnaissance	9		✓	✓				12
3	Web Application Offence	9		✓	✓				12
4	Securing and Hardening Applications	7		✓	✓		✓		12
5	Web Application Development Technologies	9		✓	✓				12
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	15
Internal Examination	10
Course Project	15
End Semester Examination	**60**
Total	**100**

FIRST SEMESTER M.TECH DEGREE (REGULAR) EXAMINATION, DECEMBER 2025 (2025 CHEME)			
Course Code:	**M250102/CY112D**		
Course Name:	**WEB APPLICATION SECURITY**		
Max. Marks	**60**	**Duration**:	2 hours 30 minutes

PART A

(Answer all questions. Each question carries 5 marks)

No.	***Question***	***CO***	***Marks***
1	Define the terms 'Threat vector' and 'Attack surface' in the context of web application security.	CO1	(5)
2	While assessing a website at https://shop.example.com, you find a URL: https://shop.example.com/exportData.php?format=xml&year=2023. List all the potential entry points for user input in this request and the type of attack possible for each.	CO2	(5)
3	A login form submits a POST request with the parameters username and password. Describe the steps you would take to test this form for SQL Injection vulnerabilities.	CO3	(5)
4	Differentiate between Mitigation and Prevention in application security. Provide a simple example of each in the context of defending against XSS.	CO4	(5)

5	The following code is part of a Node.js application using the Express framework. Identify the critical security vulnerability in this code and explain what an attacker could do to exploit it.
	
	javascript
	app.get('/user', (req, res) => {
	const username = req.query.user;
	res.send('Hello, ' + username);
	});
		CO5	(5)

PART B

(Answer any 5 questions. Each question carries 7 marks)

No.	***Question***	***CO***	***Marks***
6	Explain the principle of "Least Privilege" and "Defense in Depth." How do these two principles complement each other in designing a secure web application architecture?	CO1	(7)
7	You have discovered a website's robots.txt file contains the entry Disallow: /admin/backup/. Describe your subsequent actions to gather information and probe this directory for potential vulnerabilities.	CO2	(7)
8	You are testing a feature that allows users to upload a profile picture. List the	CO3	(7)

	types of possible attacks and the expected outcome of a successful exploit.		
9	A popular news website allows readers to comment on articles. To prevent Cross-Site Request Forgery (CSRF), the developers have implemented a CSRF token on the login page**.** Evaluate the effectiveness of this security measure. Is this sufficient to protect the entire website? Justify your answer.	CO4	(7)
10	A developer writes code that directly inserts user input into a webpage using document.innerHTML(). Why is this dangerous? What is the simple fix for this vulnerability?	CO4	(7)

11	Given the following Express.js route, identify the potential security vulnerability and demonstrate how to fix it.
	javascript
	app.get('/user/data', (req, res) => {
	const userId = req.query.id;
	const query = `SELECT * FROM users WHERE id = ${userId}`;
	db.query(query, (err, result) => {
	if (err) throw err;
	res.json(result);
	});
	});
		CO5	(7)

12	Explain the output of the following JavaScript code snippet and why it behaves that way. Then, modify the code to achieve the intended output (logging 0, 1, 2 after 100 milliseconds each).
	
	javascript
	for (var i = 0; i < 3; i++) {
	setTimeout(function() {
	console.log(i);
	}, 100);
	}
		CO5	(7)

****

COURSE DESCRIPTION					
Regulation	**2025**	**L-T-J-P-S**	**3-0-0-0-2**	**Credits**	**3**
L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)					
Course Code	**Course Name**				**Course Category**
M250102/CY113D	**OPTIMIZATION TECHNIQUE**				**PROGRAMME ELECTIVE**

COURSE OBJECTIVES	
1	Equip students with a robust understanding of core optimization methodologies, including linear programming, duality, transportation, integer programming, and nonlinear programming.
2	Develop the ability to model real-world problems mathematically, apply appropriate algorithms, and interpret solutions effectively.
3	Foster competence in sensitivity analysis, feasibility assessment, and optimization under constraints to support data-driven decision-making.

COMPETENCY & OUTCOMES		
Competency Statements	CC 1	Model complex real-world scenarios as structured optimization problems and solve them algorithmically.
	CC 2	Critically analyze optimization solutions, assess sensitivity/feasibility, and recommend data-driven decisions.

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

CO	CO Statement	Competency Mapping	Cognitive (C)
CO1	Formulate linear programming problems (LPPs), solve them using graphical/simplex methods, and handle exceptional cases via Big-M/Two-Phase techniques. (Cognitive Knowledge Level: Analyse)	CC1	An
CO2	Construct dual LPPs from primal forms, apply dual simplex method, and conduct sensitivity analysis to evaluate solution robustness. (Cognitive Knowledge Level: Apply)	CC2	A
CO3	Optimize balanced/unbalanced transportation/assignment problems using NMCM, LCM, VAM, and Hungarian algorithms, resolving degeneracy. (Cognitive Knowledge Level: Apply)	CC1	A
CO4	Solve integer linear programming problems (Gomory's cutting plane, branch and bound) and network models (TSP, CPM/PERT) for optimal scheduling. (Cognitive Knowledge Level: Analyse)	CC1	An
CO5	Classify quadratic forms, test convexity, and solve convex nonlinear programming problems (CNLPP) using quadratic/separable programming methods. (Cognitive Knowledge Level: Apply)	CC2	A

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

CO	Program Outcomes						
	PO						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1	2	-	3	3	3	1	1
2	3	-	3	2	3	2	2
3	1	-	3	3	3	3	3
4	2	-	3	3	3	2	3
5	3	-	3	3	3	2	2

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

TEACHING AND ASSESSMENT SCHEME

Teaching Scheme / Week				Self-Learning (S) / Semester	Total Hours / Semester	Credits C	Examination Scheme						
L	T	J	P				Theory			Practical			Total
							CIA	ESE	Total	CIA	ESE	Total	
3	0	0	0	30	70	3	40	60	100	0	0	0	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	Linear Programming	Linear Programming Problem (LPP), Slack-Surplus Variable, Graphical solution of a LPP, Exceptional cases in Graphical Method, Formulation of LPP, Simplex Method, Artificial variable method, Big-M method, Two-Phase method	8
2	Duality in Linear Programming	Canonical form of an LPP, Dual of an LPP, Dual Simplex Method, Basics of Sensitivity Analysis.	8
3	Transportation and Assignment Problem	Transportation Problem, Balanced Transportation Problem, Unbalanced Transportation Problem, North-West Corner Method (NMCM), Least Cost Entry Method (LCM), Vogel's Approximation Method (VAM), Degeneracy in Transportation Problems, Assignment Problem, Mathematical Formulation of the Assignment, Hungarian Algorithm to Solve an Assignment Problem	8
4	Integer Linear Programming, Travelling Salesman problem and Networking	All Integer ILPP, Gomory's Cutting Plane Method, Mixed Integer Linear Programming Problems, Branch and Bound Techniques, Travelling Salesman Problem, Networking-Critical Path Method (CPM), Program Evaluation and Review Technique (PERT), Optimum Scheduling by CPM	8
5	Non-Linear Programming	Quadratic Form, Method of Testing of a Quadratic Form, Conventional Method of Optimization, Convex Functions, Convex Nonlinear Programming Problem (CNLPP), Constraint Qualification (CQ), Quadratic Programming, Separable Programming.	8

SELF-LEARNING / TEAM WORK

Sl. No	Self-learning / Team Work Description	Hrs/Semester
1	Parametric Programming	3
2	Stochastic LP	3
3	Economic Interpretation of Dual Variables	2
4	Post-Optimality Analysis	2
5	Vogel's Approximation (VAM) Optimization	2
6	Auction Algorithm for Assignment	2
7	Monte Carlo Simulation in PERT	3
8	Genetic Algorithms for TSP	3
9	KKT Conditions Visualization	3
10	Sequential Quadratic Programming (SQP)	2
11	Optimization in Python	5

12	Real-World Case Studies	4

SUGGESTED LEARNING RESOURCES

Text Book

Sl. No.	Title of Book	Author	Publication
1	Optimization Techniques in Operations Research	C. B. Gupta	I.K. International Publishing House Pvt. Ltd., New Delhi, 2008
2	Introduction to Operations Research	Frederick S Hillier, Gerald J. Lieberman	Seventh Edition, McGraw-Hill Higher Education, 1967.
3	Operations Research	Kanti Swarup, P. K. Gupta, Man Mohan	Sultan Chand & Sons, New Delhi, 2008.

Reference

Sl. No.	Title of Book	Author	Publication
1	Engineering Optimization: Theory and Practice	Singiresu S Rao	New Age International Publishers, 1996
2	Operations research: An introduction	H A Taha	Macmillon Publishing company, 1976
3	Operations Research	B. S. Goel, S. K. Mittal	Pragati Prakashan, 1980
4	Operations Research	S.D Sharma	Kedar Nath and RamNath - Meerut , 2008
5	Operations Research: Principles and Practice	Phillips,Solberg Ravindran	Wiley, 2007

Web Resource

1	https://developers.google.com/optimization
2	https://neos-server.org/
3	https://ocw.mit.edu/courses/15-053-optimization-methods-in-management-science-spring-2013/
4	https://www.gurobi.com/documentation/current/examples/index.html
5	https://benalexkeen.com/tag/optimization/

DETAILED SYLLABUS

Module	Topic	Mode of Delivery	COs	Learning Domain Level	Hrs
				C	
1	Linear Programming Problem (LPP)	Lecture	CO1	A	1
	Slack-Surplus Variable, Graphical solution of a LPP	Lecture	CO1	A	1
	Slack-Surplus Variable, Graphical solution of a LPP - 2	Lecture	CO1	A	1
	Exceptional cases in Graphical Method, Formulation of LPP	Lecture	CO1	An	1
	Simplex Method	Lecture	CO1	A	1
	Artificial variable method	Lecture	CO1	A	1
	Big-M method	Lecture	CO1	An	1

	Two-Phase method	Lecture	CO1	A	1
2	Duality in Linear Programming	Lecture	CO2	A	1
	Duality in Linear Programming - 2	Lecture	CO2	A	1
	Canonical form of an LPP	Lecture	CO2	A	1
	Dual of an LPP	Lecture	CO2	A	1
	Dual of an LPP - 2	Lecture	CO2	A	1
	Dual Simplex Method	Lecture	CO2	A	1
	Dual Simplex Method - 2	Lecture	CO2	A	1
	Basics of Sensitivity Analysis	Lecture	CO2	A	1
3	Transportation Problem	Lecture	CO3	A	1
	Balanced Transportation Problem	Lecture	CO3	A	1
	Unbalanced Transportation Problem	Lecture	CO3	A	1
	North-West Corner Method (NMCM), Least Cost Entry Method (LCM) and Vogel's Approximation Method (VAM)	Lecture	CO3	A	1
	North-West Corner Method (NMCM), Least Cost Entry Method (LCM) and Vogel's Approximation Method (VAM) - 2	Lecture	CO3	A	1
	Degeneracy in Transportation Problems	Lecture	CO3	A	1
	Assignment Problem, Mathematical Formulation of the Assignment	Lecture	CO3	A	1
	Hungarian Algorithm to Solve an Assignment Problem	Lecture	CO3	A	1
4	All Integer ILPP	Lecture	CO4	A	1
	Gomory's Cutting Plane Method	Lecture	CO4	A	1
	Mixed Integer Linear Programming Problems	Lecture	CO4	A	1
	Branch and Bound Techniques	Lecture	CO4	A	1
	Travelling Salesman Problem	Lecture	CO4	A	1
	Critical Path Method (CPM)	Lecture	CO4	A	1
	Program Evaluation and Review Technique (PERT)	Lecture	CO4	An	1
	Optimum Scheduling by CPM.	Lecture	CO4	An	1
5	Quadratic Form	Lecture	CO5	A	1
	Method of Testing of a Quadratic Form	Lecture	CO5	A	1
	Conventional Method of Optimization	Lecture	CO5	A	1
	Convex Functions	Lecture	CO5	A	1
	Convex Nonlinear Programming Problem (CNLPP)	Lecture	CO5	A	1
	CNLPP - 2	Lecture	CO5	A	1
	Constraint Qualification (CQ)	Lecture	CO5	A	1
	Quadratic Programming, Separable Programming	Lecture	CO5	A	1

TABLE OF SPECIFICATIONS (ToS) FOR QUESTION PAPER DESIGN

Module	Module Title	Teaching Hours	Distribution of Marks (Revised Bloom's Level)						Total Marks
			R	U	A	An	E	C	
1	Linear Programming	8			✓	✓			12
2	Duality in Linear Programming	8			✓				12
3	Transportation and Assignment Problem	8			✓				12
4	Integer Linear Programming, Travelling Salesman problem and Networking	8			✓	✓			12
5	Non-Linear Programming	8			✓				12
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	15
Internal Examination	10
Course Project	15
End Semester Examination	**60**
Total	**100**

COURSE DESCRIPTION					
Regulation	**2025**	**L-T-J-P-S**	**3-0-0-0-2**	**Credits**	**3**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)					
Course Code	**Course Name**			**Course Category**	
M250102/CY114D	**TOPICS IN NETWORKS**			**PROGRAMME ELECTIVE**	

COURSE OBJECTIVES

1	Establish mastery over core web application security principles and modern defence paradigms, using OWASP terminology and frameworks.
2	Conduct end-to-end security assessments by systematically gathering reconnaissance, identifying vulnerabilities, and ethically exploiting attack vectors in lab environments.
3	Design and implement risk-driven defences and operationalize vulnerability management workflows to protect applications against evolving threats.

COMPETENCY & OUTCOMES		
Competency Statements	CC 1	Find and exploit security weaknesses in web applications using standard tools and methods.
	CC 2	Examine how modern web technologies work and identify their security risks

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

CO	CO Statement	Competency Mapping	Cognitive (C)
CO1	Explain core web application security terminology, vulnerabilities, and countermeasures using OWASP standards. (Cognitive Knowledge Level: Understand)	CC 1	U
CO2	Conduct systematic reconnaissance to identify entry points, server/client-side technologies, and functionality using industry-standard tools like Burp Suite, Nmap. (Cognitive Knowledge Level: Apply)	CC 1	A
CO3	Apply offensive techniques to ethically exploit vulnerabilities in simulated web environments Exploit common web vulnerabilities in controlled environments to demonstrate attack impact. (Cognitive Knowledge Level: Apply)	CC 1	A
CO4	Design and implement secure architectures and defenses to mitigate vulnerabilities. (Cognitive Knowledge Level: Evaluate)	CC 2	E
CO5	Develop secure asynchronous JavaScript applications while mitigating client-side risks . (Cognitive Knowledge Level: Apply)	CC 2	A

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

CO	Program Outcomes & Program Specific Outcomes						
	PO						
	1	2	3	4	5	6	7
1	1	2	2	1	-	2	-
2	2	1	3	2	3	-	-
3	2	-	3	2	3	2	-
4	3	2	3	3	2	2	2
5	3	3	3	3	3	1	3

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

Teaching Scheme / Week				Self-Learning (S) / Semester	Total Hours / Semester	Credits C	Examination Scheme						
L	T	J	P				Theory			Practical			Total
							CIA	ESE	Total	CIA	ESE	Total	
3	0	0	0	30	70	3	40	60	100	0	0	0	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	Advanced Internetworking	The Global Internet, Routing Areas, Inter domain Routing -BGP, IP Version 6, Multicast, Multicast Addresses, Multicast Routing – DVMRP, PIM, MSDP Routing to a mobile node, Mobile IPTCP and Mobility, Mobile TCP	8
2	Internetwork Quality of Service	QoS Architectural Framework - Integrated Services Architecture – RSVP - Differentiated Services, Multiprotocol Label Switching-Destination-Based Forwarding - Explicit Routing Virtual Private Networks and Tunnels, Performance issues in networks, Delay Tolerant Networking	8
3	Networking Technologies	Wired: DSL, Cable Networks, SONET, ATM, VLAN, Wireless: Satellite Networks, WiMAX Cellular Networks: Introduction-Wireless links and Network characteristics -CDMA, Cellular Internet access - An overview of cellular network architecture, 3G cellular data networks, 4G LTE Cellular networks - LTE Protocol Stacks -LTE Radio Access Network -Additional LTE functions, 5G Cellular networks, Managing mobility in cellular networks, Wireless and Mobility-Impact on higher level protocols, Personal Area Networks: Bluetooth, Zigbee	9
4	Networking Applications	Multimedia in the Internet: Streaming stored audio/video, Streaming live audio/video, Real time interactive audio/video, Real time Interactive Protocols: RTP- RTCP-SIP-H.323, SCTP Compression: Audio Compression, Image compression- JPEG, Video Compression- MPEG	7
5	Current Topics in Networking	Overlay Networks: Routing overlays -Resilient overlay networks, Peer-Peer Networks – Bit Torrent Distributed Hash Tables, Content Distribution networks, Software Defined Networks: Architecture – Control and Data Planes – Open Flow – SDN Controllers, Network Function Virtualization, Data Center Networking Express	8

SELF-LEARNING / TEAM WORK		
Sl. No	Self-learning / Team Work Description	Hrs/Semester
1	Use Cisco Packet Tracer or GNS3 to simulate BGP, IPv6 routing, and multicast (PIM-DM / SM).	5
2	Investigate how TCP performs in mobile environments and propose modifications.	3
3	Use Mininet or GNS3 to simulate RSVP and DiffServ.	3
4	Compare the architecture and bandwidth capabilities of DSL, Cable, and SONET	2
5	Trace a 4G LTE packet through the protocol stack using Wireshark.	3
6	Set up Bluetooth and ZigBee modules using Arduino or Raspberry Pi and measure communication delay	4
7	Use Wireshark to capture RTP/RTCP packets during a video call or streaming session.	3
8	Use and analyze a BitTorrent client to observe peer behavior and chunk distribution	3
9	Use Mininet + POX/RYU controller to implement OpenFlow-based SDN.	4

SUGGESTED LEARNING RESOURCES			
Text Book			
Sl. No.	Title of Book	Author	Publication
1	Computer Networks - A Systems Approach	Larry Peterson and Bruce Davie	Morgan Kaufmann, 6 th edition, 2022
2	Computer Networking A Top-Down Approach	James F. Kurose and Keith W. Ross	Pearson, 8th edition, 2022
3	Mobile Communications	Jochen Schiller	Addison-Wesley, 2nd edition, 2003
4	Data Communications and Networking	Behrouz A Forouzan	McGraw Hill, 5th edition, 2017
Reference			
Sl. No.	Title of Book	Author	Publication
1	Data and Computer Communications	William Stallings	Pearson, 5th edition, 2017
2	SDN – Software Defined Networks	Thomas D. Nadeau and Ken Gray	, O'Reilly, 2013
Web Resource			
1	https://cs244.stanford.edu/		
2	https://onrc.stanford.edu/		
3	https://datatracker.ietf.org/		
4	https://www.linuxfoundation.org/projects/networking/		
5	https://ant.isi.edu/		
6	https://packetpushers.net/		

DETAILED SYLLABUS					
Module	Topic	Mode of Delivery	COs	Learning Domain Level C	Hrs
1	The Global Internet, Routing Areas	Lecture	CO1	U	1
	Inter domain Routing -BGP	Lecture	CO1	U	1
	IP Version 6	Lecture	CO1	U	1
	Multicast, Multicast Addresses	Lecture	CO1	U	1
	Multicast Routing – DVMRP	Lecture	CO1	U	1
	PIM, MSDP	Lecture	CO1	U	1
	Routing to a mobile node, Mobile IP	Lecture	CO1	U	1
	TCP and Mobility, Mobile TCP	Lecture	CO1	U	1
2	QoS Architectural Framework	Lecture	CO2	U	1
	Integrated Services Architecture	Lecture	CO2	U	1
	RSVP - Differentiated Services	Lecture	CO2	U	1
	Multiprotocol Label Switching,	Lecture	CO2	U	1
	Virtual Private Networks and Tunnels	Lecture	CO2	U	1
	Destination-Based Forwarding - Explicit Routing	Lecture	CO2	U	1

	Performance issues in networks	Lecture	CO2	U	1
	Delay Tolerant Networking	Lecture	CO2	U	1
3	Wired: DSL, Cable Networks, SONET,	Lecture	CO3	U	1
	ATM, VLAN	Lecture	CO3	U	1
	Wireless: Satellite Networks, WiMAX	Lab	CO3	U	1
	Cellular Networks: Introduction-Wireless links and Network characteristics -CDMA,	Lecture	CO3	U	1
	Cellular Internet access-An overview of cellular network architecture, 3G cellular data networks	Lab	CO3	U	1
	4G LTE Cellular networks - LTE Protocol Stacks -LTE Radio Access Network -Additional LTE functions	Lecture	CO3	U	1
	5G Cellular networks	Lecture	CO3	U	1
	Managing mobility in cellular networks, Wireless and Mobility-Impact on higher level protocols	Lecture	CO3	U	1
	Personal Area Networks: Bluetooth, Zigbee	Lecture	CO3	U	1
4	Multimedia in the Internet: Streaming stored audio/video, Streaming live audio/video,	Lecture	CO4	U	1
	Real time interactive audio/video	Lecture	CO4	U	1
	Real time Interactive Protocols: RTP- RTCP	Lecture	CO4	U	1
	H-323	Lecture	CO4	U	1
	SIP, SCTP	Lecture	CO4	U	1
	Compression: Audio Compression, Image compression- JPEG,	Lecture	CO4	U	1
	Video Compression- MPEG	Lecture	CO4	U	1
5	Overlay Networks: Routing overlays	Lecture	CO5	U, A	1
	-Resilient overlay networks,	Lecture	CO5	U, A	1
	Peer-Peer Networks – Bit Torrent – Distributed Hash Tables,	Lecture	CO5	U	1
	Content Distribution networks	Lecture	CO5	A	1
	Software Defined Networks: Architecture – Control and Data Planes	Lecture	CO5	U	1
	Open Flow, SDN Controllers	Lecture	CO5	A	1
	Network Function Virtualization	Lecture	CO5	U	1
	Data Center Networking	Lecture	CO5	A	1

TABLE OF SPECIFICATIONS (ToS) FOR QUESTION PAPER DESIGN

Module	Module Title	Teaching Hours	Distribution of Marks (Revised Bloom's Level)						Total Marks
			R	U	A	An	E	C	
1	Advanced Internetworking	8		✓	✓				12
2	Internetwork Quality of Service	8		✓	✓				12
3	Networking Technologies	9		✓	✓				12
4	Networking Applications	7		✓	✓				12
5	Current Topics in Networking	8		✓	✓				12

This ToS shall be treated as a general guideline for students and teachers for distribution of marks.

Assessment	Marks
Continuous Internal Assessment	**40**
Learning Activity	15
Internal Examination	10
Course Project	15
End Semester Examination	**60**
Total	**100**

COURSE DESCRIPTION					
Regulation	**2025**	**L-T-J-P-S**	**3-0-0-0-2**	**Credits**	**3**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)					
Course Code	**Course Name**				**Course Category**
M250102/CY115D	**ADVANCED ARCHITECTURE**				**PROGRAMME ELECTIVE**

COURSE OBJECTIVES	
1	To provide a solid foundation that furnishes the learner with in-depth knowledge of current and emerging trends in computer architectures, focusing on performance and the hardware/software interface.
2	To design and analyze, memory hierarchy, pipelining, operation of multiprocessors, thread level parallelism, and data level parallelism

COMPETENCY & OUTCOMES		
Competency Statements	CC 1	Analyze and apply the principles of computer design, instruction set architecture, memory hierarchy, and pipelining to evaluate and optimize the performance of modern computing systems.
	CC 2	Apply concepts of multiprocessor and data-level parallelism, including shared memory, synchronization, GPU architectures, and loop-level parallelism, to design efficient solutions for high-performance applications.

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

CO	CO Statement	Competency Mapping	Cognitive (C)
CO1	Solve the advanced issues in design of computer processors, caches and memory. (Cognitive Knowledge Level: Apply)	CC1	A
CO2	Analyze the memory hierarchy design, performance improvement techniques and cache optimization techniques. (Cognitive Knowledge Level: Analyse)	CC1	An
CO3	Analyze the working of pipeline and to understand branching and exception handling in pipelining. (Cognitive Knowledge Level: Analyse)	CC1	An
CO4	State and compare properties of coherence protocol and to understand the operation of multiprocessors and thread level parallelism. (Cognitive Knowledge Level: Evaluate)	CC2	E
CO5	Identify various techniques of data level parallelism including SIMD and GPU processors. (Cognitive Knowledge Level: Apply)	CC2	A

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

CO	Program Outcomes						
	PO						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1	-	-	-	2	-	2	-
2	-	-	-	2	-	2	-
3	-	-	-	2	-	2	-
4	-	-	-	2	-	2	-
5	2	-	-	2	-	2	-

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

TEACHING AND ASSESSMENT SCHEME

Teaching Scheme / Week				Self-Learning (S) / Semester	Total Hours / Semester	Credits C	Examination Scheme						
							Theory			Practical			Total
L	T	J	P				CIA	ESE	Total	CIA	ESE	Total	
3	0	0	0	30	70	3	40	60	100	0	0	0	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	Design and Analysis	Principles of computer design, Fallacies and Pitfalls, Instruction Set Principles- Classifying instruction set architecture, Memory addressing, Type and size of operands, Operations in the instruction set, Instruction for control flow, encoding an instruction set, Role of compiler.	8
2	Memory Hierarchy	Introduction, Cache performance, Basic cache optimizations, Virtual memory–Techniques for fast address translation, Protection via virtual memory, Fallacies and Pitfalls, Case study of Pentium/Linux memory system-Pentium address translation.	8
3	Pipelining	Introduction, Pipeline hazards, Static branch prediction and dynamic branch prediction, Implementation of MITS, Basic pipeline of MITS, Implementing the control in MITS pipeline, Dealing with branches in pipeline, Dealing with exceptions, Handling of multi-cycle operations, Maintaining precise exceptions, Case study of MITS R4000 pipeline.	8
4	Thread Level Parallelism	Introduction, Centralized Shared-Memory Architectures, Performance of Symmetric Shared-Memory Multiprocessors, Distributed Shared-Memory and Directory-Based Coherence, Synchronization: The Basics, Models of Memory Consistency: An Introduction, Crosscutting Issues, Case study of Sun T1 Multiprocessor.	8
5	Data Level Parallelism	Vector architecture, SIMD instruction set, Extension for multimedia, Graphic Processing Units, Case study Envida GPU instruction set architecture, GPU memory structure, Innovations in GPU architecture, Comparisons between vector architecture and GPUs, Comparisons between multimedia SIMD computers and GPUs, Loop level parallelism, finding dependencies, Eliminating dependencies	8

SELF-LEARNING / TEAM WORK		
Sl. No	Self-learning / Team Work Description	Hrs/Semester
1	Survey of modern Instruction Set Architectures (RISC-V, ARM vs x86) – comparison study	5
2	Case study on Cache Mapping Techniques (Direct, Associative, Set-associative) with examples	5
3	Hands-on simulation of Pipeline hazards using a simple simulator tool	5
4	Team study on Synchronization mechanisms (locks, semaphores, barriers) in multiprocessors	5
5	Research and presentation on Real-world GPU architectures (NVIDIA	5

	CUDA vs AMD ROCm)	
6	Analyze performance trade-offs in parallelism (instruction-level, thread-level, data-level) using case studies	5

SUGGESTED LEARNING RESOURCES			
Text Book			
Sl. No.	Title of Book	Author	Publication
1	Computer Architecture- A Quantitative Approach	Hennessy J.L and David A. Patterson	Morgan Kaufmann Publication, Fifth edition, 2002.
2	Computer Systems A programmer's perspective	Randal E Bryant and David O'Hallaron	Pearson Education,2nd edition 2010
Reference			
Sl. No.	Title of Book	Author	Publication
1	Advanced Computer Architecture	Kaihwang and Naresh Jotwani	2nd edition Tata Mcgraw-Hill, 2010
2	Advanced Computer Architecture: A Design Space Approach	Sima D, Fountain T and Kacsuk P	Pearson Education, 1st edition 1997.
Web Resource			
1	https://nptel.ac.in/courses/106/106/106106166/		
2	http://www.cs.cmu.edu/~fp/courses/		
3	https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-823-computer-system-architecture-fall-2005/		
4	http://cs149.stanford.edu/		
5	https://developer.nvidia.com/cuda-zone		

DETAILED SYLLABUS					
Module	Topic	Mode of Delivery	COs	Learning Domain Level C	Hrs
1	Principles of computer design	Lecture	CO1	A	1
	Fallacies and Pitfalls	Lecture	CO1	A	1
	Instruction Set Principles- Classifying instruction set architecture	Lecture	CO1	A	1
	Memory addressing, Type and size of operands	Lecture	CO1	A	1
	Operations in the instruction set	Lecture	CO1	A	1
	Instruction for control flow	Lecture	CO1	A	1
	Encoding an instruction set	Lecture	CO1	A	1
	Role of compiler	Lecture	CO1	A	1
2	Introduction	Lecture	CO2	An	1
	Cache performance	Lecture	CO2	An	1

	Basic cache optimizations	Lecture	CO2	An	1
	Virtual memory –Techniques for fast address translation	Lecture	CO2	An	1
	Protection via virtual memory	Lecture	CO2	An	1
	Fallacies and Pitfalls	Lecture	CO2	An	1
	Case study of Pentium/Linux memory system-Pentium address translation	Lecture	CO2	An	1
	Linux Virtual memory system	Lecture	CO2	An	1
3	Introduction	Lecture	CO3	An	1
	Pipeline hazards	Lecture	CO3	An	1
	Static branch prediction and dynamic branch prediction	Lab	CO3	An	1
	Implementation of MITS, Basic pipeline of MITS	Lecture	CO3	An	1
	Implementing the control in MITS pipeline	Lab	CO3	An	1
	Dealing with branches in pipeline, Dealing with exceptions	Lecture	CO3	An	1
	Handling of multi-cycle operations, Maintaining precise exceptions	Lecture	CO3	An	1
	Case study of MITS R4000 pipeline	Lecture	CO3	An	1
4	Introduction	Lecture	CO4	E	1
	Centralized Shared-Memory Architectures	Lecture	CO4	E	1
	Performance of Symmetric Shared-Memory Multiprocessors	Lecture	CO4	E	1
	Distributed Shared-Memory and Directory-Based Coherence	Lecture	CO4	E	1
	Synchronization: The Basics	Lecture	CO4	E	1
	Models of Memory Consistency: An Introduction	Lecture	CO4	E	1
	Crosscutting Issues	Lecture	CO4	E	1
	Case study Sun T1 Multiprocessor	Lecture	CO4	E	1
5	Vector architecture, SIMD instruction set	Lecture	CO5	A	1
	Extension for multimedia, Graphic Processing Units	Lecture	CO5	A	1
	Case study Envida GPU instruction set architecture	Lecture	CO5	A	1
	GPU memory structure	Lecture	CO5	A	1
	Innovations in GPU architecture, Comparisons between vector architecture and GPUs	Lecture	CO5	A	1
	Comparisons between multimedia SIMD computers and GPUs	Lecture	CO5	A	1
	Loop level parallelism	Lecture	CO5	A	1
	Finding dependencies, Eliminating Dependencies	Lecture	CO5	A	1

TABLE OF SPECIFICATIONS (ToS) FOR QUESTION PAPER DESIGN									
Module	Module Title	Teaching Hours	Distribution of Marks (Revised Bloom's Level)						Total Marks
			R	U	A	An	E	C	
1	Design and Analysis	8		✓	✓				12
2	Memory Hierarchy	8		✓	✓	✓			12
3	Pipelining	8		✓	✓	✓			12
4	Thread Level Parallelism	8		✓	✓	✓	✓		12
5	Data Level Parallelism	8		✓	✓				12
This ToS shall be treated as a general guideline for students and teachers for distribution of marks.									

Assessment	Marks
Continuous Internal Assessment	**40**
Learning Activity	15
Internal Examination	10
Course Project	15
End Semester Examination	**60**
Total	**100**

COURSE DESCRIPTION					
Regulation	**2025**	**L-T-J-P-S**	**3-0-0-0-2**	**Credits**	**3**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)					
Course Code	**Course Name**				**Course Category**
M250902/CN116D	**COMPUTATIONAL INTELLIGENCE**				**PROGRAMME ELECTIVE**

COURSE OBJECTIVES	
1	To understand the fundamental concepts of fuzzy logic, evolutionary computation, and swarm intelligence for handling uncertainty and optimization.
2	To apply soft computing techniques for solving complex optimization and decision-making problems in real-world domains.
3	To compare different soft computing methods in terms of efficiency, convergence, and applicability.

COMPETENCY & OUTCOMES		
Competency Statements	CC 1	Ability to apply fuzzy logic, genetic algorithms, and swarm intelligence techniques to optimize, and solve engineering problems characterized by uncertainty and complexity.
	CC 2	Ability to design, develop, and implement intelligent computational solutions by integrating fuzzy inference, evolutionary algorithms, and swarm optimization methods to address real-world engineering and decision-making challenges.

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

CO	CO Statement	Competency Mapping	Cognitive (C)
CO1	Apply fuzzy logic to handle uncertainty and solve engineering problems. (Cognitive Knowledge Level: Apply)	CC 1	A
CO2	Apply fuzzy logic inference methods in building intelligent machines. (Cognitive Knowledge Level: Apply)	CC 1	A
CO3	Design genetic algorithms for optimized solutions in engineering problems. (Cognitive Knowledge Level: Analyse)	CC 1	An
CO4	Analyse the problem scenarios and apply Ant colony system to solve real optimization problems. (Cognitive Knowledge Level: Apply)	CC 2	An
CO5	Apply PSO algorithm to solve real world problems. (Cognitive Knowledge Level: Apply)	CC 2	A
CO6	Design, develop and implement solutions based on computational intelligence concepts and techniques. (Cognitive Knowledge Level: Create)	CC 2	C

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

CO	Program Outcomes & Program Specific Outcomes						
	PO						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1	-	-	-	2	-	2	-
2	2	-	2	2	2	2	-
3	2	-	2	2	2	2	-
4	2	-	2	2	2	2	-
5	2	-	2	2	2	2	-
6	2	2	2	2	2	2	2

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

TEACHING AND ASSESSMENT SCHEME													
Teaching Scheme / Week				Self-Learning (S) / Semester	Total Hours / Semester	Credits C	Examination Scheme						
							Theory			Practical			Total
L	T	J	P				CIA	ESE	Total	CIA	ESE	Total	
3	0	0	0	30	70	3	40	60	100	0	0	0	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	Fuzzy Logic	Fuzzy Sets and Membership Functions Fuzzy Inference Mechanisms Fuzzy Relations and Composition	6
2	Fuzzy Systems	Linguistic Variables and Fuzzy Rules Fuzzy Inference Systems Fuzzy Reasoning Methods	8
3	Genetic Algorithms	Fundamentals of Genetic Algorithms Genetic Algorithm Operators & Mechanisms Advanced Concepts in GA	9
4	Ant Colony Systems	Fundamentals of Ant Colony Systems Development & Working of Ant Colony Systems Applications of Ant Colony Intelligence	7
5	Particle Swarm Optimization	Fundamentals of PSO PSO Parameters & Mechanisms Advanced Concepts in PSO	10

SELF-LEARNING / TEAM WORK		
Sl. No	Self-learning / Team Work Description	Hrs/Semester
1	Deep Dive into Defuzzification Methods	2
2	Building Mamdani and Sugeno Fuzzy Inference Systems	2
3	Introduction to Fuzzy Logic Control Systems	2
4	Genetic Algorithm Lifecycle: From Initial Population to Final Solution	2
5	Detailed Study of Selection, Crossover, and Mutation Operators	2
6	Comparison of Binary, Real-Valued, and Permutation Representations in GAs	2
7	Implementing a Genetic Algorithm from Scratch	2
8	Probabilistic Path Selection and Pheromone Update Rules in ACO	2
9	Implementing the Ant Colony Optimization (ACO) Metaheuristic	2
10	Ant System vs. Max-Min Ant System vs. Ant Colony System	2
11	Understanding Position, Velocity, and Personal/Best Global Best in PSO	2
12	The Impact of Inertia Weight and Acceleration Coefficients in PSO	2
13	Implementing a Basic PSO Algorithm for a Standard Test Function	2
14	Combining Fuzzy Logic, Genetic Algorithms, and Swarm Intelligence	2
15	Strengths and Weaknesses of GA, ACO, and PSO for Different Problem Types	2

SUGGESTED LEARNING RESOURCES

Text Book			
Sl. No.	Title of Book	Author	Publication
1	Introduction to Soft Computing Neuro-Fuzzy Genetic Algorithms	Samir Roy, Udit Chakraborty	Pearson
2	Artificial Intelligence and Intelligent system	N.P. Padhy	Oxford Press
Reference			
Sl. No.	Title of Book	Author	Publication
1	An Introduction to Genetic Algorithm	Mitchell Melanie	Prentice Hall
2	Ant Colony optimization	Marco Dorigo and Thomas Stutzle	Prentice Hall of India
3	Computational Intelligence: An Introduction	Andries Engelbrecht	Wiley
4	Mathematical Modelling and Applications of Particle Swarm Optimization	Satyobroto Talukder	Blekinge Institute of Technology
5	Nature-Inspired Optimization Algorithms	Xin-She Yang	Elsevier
Web Resource			
1	Introduction to Fuzzy Logic https://www.youtube.com/watch?v=-U-QCX2C8T8		
2	Fuzzy inference system https://www.youtube.com/watch?v=0rXU6qkWK1I		
3	Learning Genetic algorithms https://www.youtube.com/watch?v=kHyNqSnzP8Y		
4	Ant colony optimization https://www.youtube.com/watch?v=ZR2t5qFmxv8		
5	Particle swarm optimization https://www.youtube.com/watch?v=uwXFnzWaCY0		
6	NPTEL: Introduction to soft computing https://nptel.ac.in/courses/106105173		

DETAILED SYLLABUS					
Module	Topic	Mode of Delivery	COs	Learning Domain Level C	Hrs
1	Crisp sets vs fuzzy sets, Operations and properties of Fuzzy sets	Lecture	CO1	U	1
	Membership functions: features of membership functions	Lecture	CO1	U	1
	Fuzzification and methods of membership value assignment	Lecture	CO1	U	1
	Defuzzification-Lambda(alpha) cuts	Lecture	CO1	U	1
	Fuzzy Relation and fuzzy composition	Lecture	CO1	U	1
	Operations on fuzzy relations	Lecture	CO1	U	1
2	Linguistic variables and Hedges	Lecture	CO2	A	1
	Fuzzy Rule Base System-Aggregation of fuzzy rules	Lecture	CO2	A	1
	Fuzzy Inference System: Mamdani FIS	Lecture	CO2	A	1
	Larsen Model	Lecture	CO2	A	1
	Practice Problems on FIS	Lecture	CO2	A	1
	Fuzzy Reasoning – GMP and GMT (lecture 1)	Lecture	CO2	A	1
	Fuzzy Reasoning – GMP and GMT (lecture 2)	Lecture	CO2	A	1

	Practice Problems on Fuzzy Reasoning	Lecture	CO2	A	1
3	Introduction to Genetic algorithm	Lecture	CO3	U	1
	Chromosomes	Lecture	CO3	An	1
	Fitness function, Population	Lecture	CO3	An	1
	GA operators - selection (lecture 1)	Lecture	CO3	A	1
	GA operators - crossover (lecture 2)	Lecture	CO3	A	1
	GA operators - mutation (lecture 3)	Lecture	CO3	A	1
	Elitism, GA parameters, Convergence of GA	Lecture	CO3	U	1
	Multi – objective Genetic Algorithm (lecture 1)	Lecture	CO3	A	1
	Multi – objective Genetic Algorithm (lecture 2)	Lecture	CO3	A	1
4	Introduction, ant colony systems	Lecture	CO4	U	1
	Types of ant colony systems (lecture 1)	Lecture	CO4	U	1
	Types of ant colony systems (lecture 2)	Lecture	CO4	U	1
	Development of the ant colony system	Lecture	CO4	A	1
	Applications of ant colony intelligence	Lecture	CO4	A	1
	Working of ant colony systems (lecture 1)	Lecture	CO4	U	1
	Working of ant colony systems (lecture 2)	Lecture	CO4	U	1
5	Basic Model of PSO algorithm	Lecture	CO5	U	1
	Global Best PSO	Lecture	CO5	A	1
	Local Best PSO, Comparison of ‘gbest’ to ‘lbest’	Lecture	CO5	A	1
	PSO Algorithm Parameters	Lecture	CO5	A	1
	Problem Formulation of PSO algorithm (lecture 1)	Lecture	CO5	A	1
	Problem Formulation of PSO algorithm (lecture 2)	Lecture	CO5	A	1
	Velocity clamping- Inertia weight	Lecture	CO5	A	1
	Constriction Coefficient- Boundary Conditions	Lecture	CO5	A	1
	Guaranteed Convergence PSO (GCPSO)	Lecture	CO5	U	1
	Initialization, Stopping Criteria, Iteration Terms and Function Evaluation	Lecture	CO5	A	1

TABLE OF SPECIFICATIONS (ToS) FOR QUESTION PAPER DESIGN										
Module	Module Title	Teaching Hours	Distribution of Marks (Revised Bloom’s Level)						Total Marks
			R	U	A	An	E	C	

1	Fuzzy Logic	6		✓					12
2	Fuzzy Systems	8		✓	✓				12
3	Genetic Algorithms	9		✓	✓				12
4	Ant Colony Systems	7		✓					12
5	Particle Swarm Optimization	10		✓	✓				12
This ToS shall be treated as a general guideline for students and teachers for distribution of marks.									

Assessment	Marks
Continuous Internal Assessment	**40**
Learning Activity	15
Internal Examination	10
Course Project	15
End Semester Examination	**60**
Total	**100**

COURSE DESCRIPTION					
Regulation	**2025**	**L-T-J-P-S**	**3-0-0-0-2**	**Credits**	**3**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)					
Course Code	**Course Name**				**Course Category**
M250102/CY121E	**FILE SYSTEM FORENSIC ANALYSIS**				**PROGRAMME ELECTIVE**

COURSE OBJECTIVES	
1	To understand the file organization in different Operating Systems.
2	To analyse disk images of various File Systems and identifying data.
3	To recognize and interpret specific artifacts critical in forensic investigations.

COMPETENCY & OUTCOMES		
Competency Statements	CC 1	Students will be able to evaluate different file system structures and determine their forensic significance in digital investigations.
	CC 2	Students will be able to analyze data organization in diverse storage architectures to interpret and present digital evidence.

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

CO	CO Statement	Competency Mapping	Cognitive (C)
CO1	Analyse volume and partition structures in different operating systems. (Cognitive Knowledge Level: Analyse)	CC2	An
CO2	Apply knowledge of FAT file system structures to perform forensic analysis. (Cognitive Knowledge Level: Apply)	CC1	A
CO3	Evaluate the NTFS file system to identify and interpret forensic artifacts. (Cognitive Knowledge Level: Evaluate)	CC1	E
CO4	Evaluate Ext X file systems for data recovery and consistency checks. (Cognitive Knowledge Level: Evaluate)	CC1	E
CO5	Analyze data organization in Flash memory, HFS+, and Android mobile file systems. (Cognitive Knowledge Level: Analyse)	CC2	An

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

CO	Program Outcomes						
	PO						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1	2	-	1	2	3	-	-
2	2	1	2	3	3	-	-
3	3	2	3	3	3	-	-
4	3	2	3	3	3	-	-
5	2	-	2	3	3	-	-

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

TEACHING AND ASSESSMENT SCHEME													
Teaching Scheme / Week				**Self-Learning (S) / Semester**	**Total Hours / Semester**	**Credits C**	**Examination Scheme**						
							Theory			**Practical**			**Total**
L	**T**	**J**	**P**				**CIA**	**ESE**	**Total**	**CIA**	**ESE**	**Total**	
3	0	0	0	30	70	3	40	60	100	0	0	0	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	Digital Investigation Basics and Volume Analysis	Digital Investigations and Evidence**,** Digital Crime Scene Investigation Process, Data Analysis, Data Organizations, Booting Process, Hard Disk Technology, Hard disk data Acquisition - Reading the source data, Writing the output data, A Case Study. PC based partitions - DOS partitions, Analysis considerations, Apple partitions, Removable media, Server based partitions- GPT partitions, Multiple disk volumes- RAID, Disk Spanning - Linux MD, Linux LVM, Windows LDM	8
2	FAT File System Analysis	File system, File system category, Content category, Metadata category, File name category, Application category, FAT concepts and analysis- Introduction, File system category, Content category, Metadata category, File name category, File recovery, determining type, Consistency check, FAT data structure-Boot sector, FAT 32 FS info, directory entries, Long file name directory entries, A Case Study.	8
3	NTFS File System Analysis	Introduction, MFT concepts, MFT entry attribute concepts, other attribute concepts, Indexes, NTFS Analysis- File system category, Content category, Metadata category, File name category, File recovery, determining the type, Consistency check, NTFS data structure- Basic concepts, Standard file attributes, Index attributes and data structures, File system metadata files, A Case Study.	8
4	Ext X File Systems	Ext2 & Ext3 concepts- File system category, Content, Metadata category, File name category, File recovery, determining the type, Consistency check, Ext2 and Ext3 data structures, Ext4 data structures, File Recovery possibility in Ext2, Ext3, Ext4.	8
5	Android and MAC File Systems:	Introduction to Flash Memory, Architecture, NAND and NOR, Android Mobile File Systems - Data Organization, YAFFS2, F2FS, MAC File System - HFS+ - Data Organization.	8

SELF-LEARNING / TEAM WORK		
Sl. No	Self-learning / Team Work Description	Hrs/Semester
1	Study and summarize digital forensic investigation standards and guidelines	3
2	Explore open-source forensic tools (e.g., Autopsy, Sleuth Kit, FTK Imager) and prepare a usage report	3
3	Perform volume/partition analysis using sample disk images.	4
4	Prepare a comparative study of FAT, NTFS, ExtX, HFS+ file systems highlighting differences in metadata, file recovery and artifacts	4
5	Perform FAT file recovery using a forensic tool.	3
6	Prepare a report on NTFS Master File Table (MFT) artifacts and their importance in investigations.	3
7	Explore file recovery methods in Ext4 vs Ext2/3	3
8	Evaluate Android mobile file system forensics (YAFFS2, F2FS) and its applications in cybercrime cases.	3
9	Study on Flash memory forensic challenges (wear levelling, garbage collection, TRIM).	2
10	Prepare an end-to-end forensic investigation workflow (from acquisition	2

	to reporting) based on real case studies.	

SUGGESTED LEARNING RESOURCES			
Text Book			
Sl. No.	Title of Book	Author	Publication
1	File System Forensic Analysis	Brian Carrier	Addison Wesley, 2005
2	Android Forensics Investigation, Analysis and Mobile Security for Google Android	Andrew Hoog	Syngress, 2011
Reference			
Sl. No.	Title of Book	Author	Publication
1	Digital Evidence and Computer Crime	Eoghan Casey	Edition 2, Academic Press, 2004
2	Forensic Discovery	Dan Farmer & Wietse Venema	Addison Wesley, 2005
Web Resource			
1	https://msdf.ucf.edu/syllabus/CIS6386_CS_Spring2023_GRAD.pdf		
2	https://www.cs.nmt.edu/~df/lectures/3%20HDD%20Media%20Continued.pdf		

DETAILED SYLLABUS					
Module	Topic	Mode of Delivery	COs	Learning Domain Level	Hrs
				C	
1	Digital Investigations and Evidence, Digital crime scene investigation process	Lecture	CO1	An	1
	Data Analysis, Data organizations, Booting Process, Hard Disk Technology	Lecture	CO1	U	1
	Hard disk data acquisition - Reading the source data, Writing the output data, A Case Study	Lecture	CO1	U	1
	PC based partitions- DOS partitions, Analysis considerations	Lecture	CO1	An	1
	Apple partitions, removable media	Lecture	CO1	U	1
	Server based partitions- GPT partitions	Lecture	CO1	U	1
	Multiple disk volumes- RAID, Disk Spanning - Linux MD, Linux LVM, Windows LDM – 1	Lecture	CO1	U	2
2	File system, File system category, Content category, Metadata category, File name category, Application category	Lecture, Lab	CO2	A	1
	FAT concepts and analysis- Introduction, File system category, Content category	Lecture	CO2	A	1
	Metadata category, File name category	Lecture	CO2	A	1
	File recovery, determining type, Consistency check	Lecture	CO2	A	1
	FAT data structure-Boot sector, FAT 32 FS	Lecture	CO2	A	1

	info, directory entries				
	Long file name directory entries	Lecture	CO2	A	1
	A Case Study - 1	Lecture	CO2	A	2
3	Introduction, MFT concepts	Lecture	CO3	A	1
	MFT entry attribute concepts, other attribute concepts, Indexes	Lecture	CO3	A	1
	NTFS Analysis- File system category, Content category, Metadata category, File name category	Lab	CO3	A	1
	File recovery, determining the type, Consistency check	Lecture	CO3	A	1
	NTFS data structure- Basic concepts, Standard file attributes, Index attributes and data structures	Lab	CO3	U	1
	File system metadata files	Lecture	CO3	A	1
	A Case Study	Lecture	CO3	E	2
4	Ext2 & Ext3 concepts – File system category, content, metadata category, file name category	Lecture	CO4	A	2
	File recovery, determining the type, Consistency check	Lecture	CO4	A	1
	Ext2 and Ext3 data structures	Lecture	CO4	A	2
	Ext4 data structures	Lecture	CO4	A	2
	File Recovery possibility in Ext2, Ext3, Ext4	Lecture	CO4	E	1
5	Introduction to Flash Memory, Architecture, NAND and NOR	Lecture	CO5	U	2
	Android Mobile File Systems - Data Organization	Lecture	CO5	A	2
	YAFFS2	Lecture	CO5	A	1
	F2FS	Lecture	CO5	A	1
	MAC File System – HFS+ - Data Organization	Lecture	CO5	An	2

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	Digital Investigation Basics and Volume	8		✓	✓	✓			12

	Analysis								
2	FAT File System Analysis	8		✓	✓				12
3	NTFS File System Analysis	8		✓	✓	3	3		12
4	Ext X File Systems	8		✓	✓	3	3		12
5	Android and MAC File Systems	8		✓	✓	✓			12
This ToS shall be treated as a general guideline for students and teachers for distribution of marks.									

Assessment	Marks
Continuous Internal Assessment	**40**
Learning Activity	15
Internal Examination	10
Course Project	15
End Semester Examination	**60**
Total	**100**

COURSE DESCRIPTION					
Regulation	**2025**	**L-T-J-P-S**	**3-0-0-0-2**	**Credits**	**3**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)					
Course Code	**Course Name**				**Course Category**

M250102/CY122E	BLOCKCHAIN	Program Elective

COURSE OBJECTIVES	
1	Describe the basic concepts of Blockchain and different Consensus approaches.
2	Impart knowledge about building and deploying smart contracts.
3	Explore the tools used in decentralized application development.
4	Integrate on-chain and off-chain data using Web3 APIs.
5	Apply blockchain concepts in real-world use cases.

COMPETENCY & OUTCOMES		
Competency Statements	CC1	Explain cryptography, consensus mechanisms, smart contracts, Dapps, and Web3 in building secure decentralized systems.
	CC2	Apply blockchain tools and techniques to design, deploy, and evaluate practical decentralized solutions for real-world use cases.

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

CO		Competency Mapping	Cognitive (C)
CO1	State the key differentiators for blockchain from other technology systems**.** (Cognitive Knowledge Level: Apply)	CC1	A
CO2	Summarize the classification of consensus algorithms. (Cognitive Knowledge Level: Apply)	CC1	A
CO3	Design, develop, deploy and test smart contract. (Cognitive Knowledge Level: Evaluate)	CC2	E
CO4	Design, deploy and test Dapp. (Cognitive Knowledge Level: Evaluate)	CC2	E
CO5	Explore on-chain and off-chain data. (Cognitive Knowledge Level: Apply)	CC2	A

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

CO	Program Outcomes						
	PO						
	1	2	3	4	5	6	7
1	1	2	2			2	
2	2	1	2			2	
3	2	1	3		2	3	
4	2	2	3		3	3	
5	1	1	2			3	

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

TEACHING AND ASSESSMENT SCHEME

Teaching Scheme / Week				Self-Learning (S) / Semester	Total Hours / Semester	Credits C	Examination Scheme						
							Theory			Practical			Total
L	T	J	P				CIA	ESE	Total	CIA	ESE	Total	
3	0	0	0	12	40	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	Foundations of	Cryptography basics: Symmetric key cryptography, Asymmetric key cryptography, Introduction to Hashing- Applications of	7

	Cryptography and Blockchain	cryptographic hash functions – Merkle trees, Distributed hash tables, Block Chain, Bitcoin to Block Chain, Blockchain programming: Decentralized infrastructure, Disintermediation protocol, Trust enabler Motivating scenarios: Automatic and consistent data collection, Timely information sharing, Auditable actions for provenance, Guidance for governance, Pandemic management	
2	Consensus and Decentralization	Consensus – definition, types, consensus in blockchain. Decentralization – Decentralization using blockchain, Methods of decentralization, Routes to decentralization, Blockchain and full ecosystem decentralization. Consensus Algorithms, Crash fault-tolerance (CFT) algorithms – Paxos, Raft. Byzantine fault tolerance (BFT) algorithms – Practical Byzantine Fault Tolerance (PBFT), Proof of work (PoW), Proof of stake (PoS), Types of PoS.	6
3	Smart Contracts and Ethereum	The concept of a smart contract: Bitcoin transactions versus smart contract transactions, Design of a smart contract, A use case diagram for the counter, Development of a smart contract code: Solidity language, Smart contract code for Counter, Deploying and testing the smart contract, Introduction to remix IDE, Use case of Decentralized airline system, The relevance of public-key cryptography to blockchain, Transaction signing, Deploying smart contracts on Ropsten, Using the private key in mnemonic form, populating a blockchain wallet, Deploying and transacting on Ropsten.	12
4	Decentralized Applications	Dapp development using Truffle: The development process, Installing Truffle, Building the Dapp stack, Install Ganache test chain, Develop the smart contract, Deploy the smart ontract, Develop and configure the web application	8
5	Web3 and Blockchain Data	On-chain data, Blind auction use case, Off-chain data, External data sources ASK airline system use case study, Web3 API: Web3 in Dapp stack, Web3 packages, The channel concept: Micropayment channel, Micropayment channel use case.	7

SELF-LEARNING / TEAM WORK		
Sl. No	Self-learning / Team Work Description	Hrs/Semester
1	Study SHA-256 and Keccak hash function design; Read Satoshi Nakamoto's Bitcoin whitepaper	2
2	Study how the EOS blockchain implements DPoS as its consensus mechanism, and compare it with Ethereum's transition from PoW to PoS.	2
3	Explore ERC-20 (fungible token) and ERC-721 (NFT) standards; Study Gas fees & optimization strategies in Solidity; Read about vulnerabilities	3
4	Explore IPFS and decentralized storage integration in DApps.	2
5	Explore decentralized identity (DID), study interoperability solutions like Polkadot and Cosmos, and learn how real-world assets are tokenized on blockchain.	3

SUGGESTED LEARNING RESOURCES			
Text Book			
Sl. No.	Title of Book	Author	Publication

1	Blockchain in Action	Bina Ramamurthy	Manning Publications First Edition 2020
2	Mastering Blockchain: A Deep Dive into Distributed ledgers, Consensus Protocols, Smart Contracts, Dapps, Cryptocurrencies, Ethereum and more	Imran Bashir	Packt. Publishing, Third Edition 2020

Reference

Sl. No.	Title of Book	Author	Publication
1	'Blockchain: The Blockchain for Beginnings, Guild to Blockchain Technology and Blockchain Programming	Josh Thompson	Create Space Independent Publishing Platform, 2017
2	Solidity Programming Essentials: A beginner's guide to build smart contracts for Ethereum and blockchain	Ritesh Modi	Packt Publishing, First edition, 2018.
3	Blockchain Technology: Concepts and Applications	Kumar Saurabh, Ashutosh Saxena	Wiley Publications, First edition, 2020.
4	Blockchain Technology	Chandramouli Subramanian, Asha A George, et al	Universities Press (India) Pvt. Ltd, First edition, August 2020.
5	Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications	Lorne Lantz, Daniel Cawrey	O'Reilly Media, First edition, 2020.
6	Mastering Ethereum: Building Smart Contracts and DApps,	Andreas M. Antonopoulos, Gavin Wood,	O'Reilly Media, First edition, 2018

Web Resource

1	Blockchain and its Applications, IIT Kharagpur, Prof. Sandip Chakraborty, Prof. Shamik Sural https://nptel.ac.in/courses/106105235

DETAILED SYLLABUS

Module	Topic	Mode of Delivery	COs	Learning Domain Level C	Hrs
1	Cryptography basics: Symmetric key cryptography, Asymmetric key cryptography	Lecture	CO1	U	1
	Introduction to Hashing	Lecture	CO1	U	1
	Applications of cryptographic hash functions – Merkle trees, Distributed hash tables	Lecture	CO1	A	1
	Block Chain, Bitcoin to Block Chain	Lecture	CO1	U	1
	Blockchain programming: Decentralized infrastructure	Lecture	CO1	A	1
	Disintermediation protocol, Trust enabler	Lecture	CO1	U	1
	Motivating scenarios: Automatic and consistent data collection, Timely information sharing, Auditable actions for provenance, Guidance for governance, Attribution of actions, Pandemic management	Lecture	CO1	U	1
2	Consensus – definition, types, consensus in blockchain	Lecture	CO2	U	1
	Decentralization using blockchain, Methods of decentralization	Lecture	CO2	A	1
	Routes to decentralization, Blockchain and full ecosystem decentralization.	Lecture	CO2	A	1
	Consensus Algorithms, Crash fault-tolerance (CFT)	Lecture	CO2	A	1

	algorithms – Paxos, Raft				
	Byzantine fault tolerance (BFT) algorithms – Practical Byzantine Fault Tolerance (PBFT)	Lecture	CO2	A	1
	Proof of work (PoW), Proof of stake (PoS), Types of PoS.	Lecture	CO2	A	1
3	The concept of a smart contract: Bitcoin transactions versus smart contract transactions	Lecture	CO3	A	1
	Design of a smart contract	Lecture	CO3	E	1
	A use case diagram for the counter	Lecture	CO3	E	1
	Development of a smart contract code: Solidity language	Lecture, Lab	CO3	E	1
	Smart contract code for Counter	Lecture, Lab	CO3	E	1
	Deploying and testing the smart contract	Lecture, Lab	CO3	E	1
	Introduction to remix IDE	Lecture, Lab	CO3	A	1
	Use case of Decentralized airline system	Lecture	CO3	E	1
	The relevance of public-key cryptography to blockchain	Lecture	CO3	U	1
	Generating Ethereum addresses	Lecture	CO3	A	1
	Transaction signing, Deploying smart contracts on Ropsten	Lecture	CO3	E	1
	Using the private key in mnemonic form, populating a blockchain wallet, Deploying and transacting on Ropsten	Lecture	CO3	E	1
4	Dapp development using Truffle: The development process	Lecture, Lab	CO4	E	1
	Installing Truffle	Lecture, Lab	CO4	E	1
	Building the Dapp stack	Lecture, Lab	CO4	E	1
	Install Ganache test chain	Lecture, Lab	CO4	E	1
	Familiarizing Ganache test chain	Lecture, Lab	CO4	E	1
	Develop the smart contract	Lecture, Lab	CO4	E	1
	Deploy the smart contract	Lecture, Lab	CO4	E	1
	Develop and configure the web application	Lecture, Lab	CO4	E	1
5	On-chain data	Lecture	CO5	A	1
	Blind auction use case	Lecture	CO5	A	1
	Off-chain data	Lecture	CO5	A	1
	External data sources ASK airline system use case study	Lecture	CO5	A	1
	Web3 API: Web3 in Dapp stack	Lecture	CO5	A	1
	Web3 packages	Lecture	CO5	A	1
	The channel concept: Micropayment channel, Micropayment channel use case	Lecture	CO5	A	1

TABLE OF SPECIFICATIONS (ToS) FOR QUESTION PAPER DESIGN										
Module	Module Title	Teaching Hours	Distribution of Marks (Revised Bloom's Level)						Total Marks
			R	U	A	An	E	C	

1	Foundations of Cryptography and Blockchain	7		✓	✓				12
2	Consensus and Decentralization	6		✓	✓				12
3	Smart Contracts and Ethereum	12		✓	✓	✓	✓		12
4	Decentralized Applications	8		✓	✓	✓	✓		12
5	Web3 and Blockchain Data	7		✓	✓				12
This ToS shall be treated as a general guideline for students and teachers for distribution of marks.									

Assessment	**Marks**
Continuous Internal Assessment	**40**
Learning Activity	15
Internal Examination	10
Course Project	15
End Semester Examination	**60**
Total	100

FIRST SEMESTER M. TECH DEGREE (REGULAR) EXAMINATION, DECEMBER 2025(2025 CHEME)			
Course Code:	**M250102/CY122E**		
Course Name:	**Blockchain**		
Max. Marks	**60**	**Duration**:	2 hours 30 minutes

PART A

(Answer all questions. Each question carries 5 marks)

No.	***Question***	***CO***	***Marks***
1	Differentiate between symmetric key and asymmetric key cryptography with examples from blockchain applications.	CO1	(5)
2	Explain how Proof of Work ensures security in blockchain.	CO2	(5)
3	Compare Bitcoin transactions with smart contract transactions, highlighting their similarities and differences.	CO3	(5)
4	Illustrate how Truffle facilitates the development of DApps, and the role of Ganache in testing smart contracts.	CO4	(5)
5	Provide one real-world blockchain use case where both on-chain and off-chain data are used.	CO5	(5)

PART B

(Answer any 5 questions. Each question carries 7 marks)

No.	***Question***	***CO***	***Marks***
6	Determine how the principles of disintermediation and decentralization in blockchain-based systems replace traditional intermediaries and support the development of a fully decentralized ecosystem.	CO1	(7)
7	Illustrate the use of Paxos, PBFT, and Raft consensus algorithms in achieving reliable consensus under varying fault conditions and scalability requirements in distributed systems	CO2	(7)
8	Evaluate the effectiveness of using a Solidity smart contract for maintaining student records (name, ID, grade) and the deployment, testing process on the Ropsten network.	CO3	(7)
9	Evaluate the role of Ganache on a simple voting DApp using Truffle Suite.	CO4	(7)
10	Explain the working of micropayment channels in blockchain with an example to enable off-chain scalability.	CO5	(7)
11	Infer the role of Web3 APIs in DApp development. Explain Web3 packages and their use in interacting with Ethereum blockchain	CO4	(7)
12	Explain how blind auction can be implemented using smart contracts.	CO3	(7)

****

COURSE DESCRIPTION

Regulation	2025	L-T-J-P-S	3-0-0-0-2	Credits	3
(*L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work*)					
Course Code	**Course Name**			**Course Category**	
M250102/CY123E	**SECURE CODING**			**PROGRAMME ELECTIVE**	

COURSE OBJECTIVES	
1	To establish a foundational understanding of core security goals (CIA triad), malware, and the taxonomy of common cyber-attacks and software vulnerabilities.
2	To equip students with the knowledge to embed security throughout the software development process, from secure design principles to structured threat modelling.
3	To develop practical skills in writing secure code, identifying critical security flaws in databases and web applications, and effectively testing software for security weaknesses before deployment.

COMPETENCY & OUTCOMES		
Competency Statements	CC 1	Write secure code that identifies and prevents common vulnerabilities.
	CC 2	Test applications for security weaknesses and propose effective fixes.

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

CO	CO Statement	Competency Mapping	Cognitive (C)
CO1	Identify and classify fundamental security threats, attacks, and vulnerabilities based on the CIA triad security model. (Cognitive Knowledge Level: Understand)	CC1	U
CO2	Apply the principles of the Secure Software Development Lifecycle (S-SDLC) and threat modelling methodologies to integrate security into each phase of software development. (Cognitive Knowledge Level: Apply)	CC1	A
CO3	Implement secure coding techniques in specific programming contexts to mitigate common vulnerabilities such as denial-of-service attacks, ARP spoofing, and buffer overruns. (Cognitive Knowledge Level: Apply)	CC1	A
CO4	Analyse and remediate database and web-specific security flaws, including SQL injection, race conditions, and cross-site scripting (XSS) attacks, through rigorous input validation and secure coding practices. (Cognitive Knowledge Level: Apply)	CC2	A
CO5	Design and develop comprehensive security test plans and strategies to evaluate the security posture of applications, including testing for HTTP-based, file-based, and client-server vulnerabilities. (Cognitive Knowledge Level: Apply)	CC2	A

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

CO	Program Outcomes & Program Specific Outcomes						
	PO						
	1	2	3	4	5	6	7
1	-	-	3	1	3	3	-
2	3	2	3	3	3	3	2
3	-	-	3	3	3	1	-
4	3	1	3	3	3	3	-
5	3	3	3	3	3	3	1

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

TEACHING AND ASSESSMENT SCHEME

Teaching Scheme / Week				Self-Learning (S) / Semester	Total Hours / Semester	Credits C	Examination Scheme						
L	T	J	P				Theory			Practical			Total
							CIA	ESE	Total	CIA	ESE	Total	
3	0	0	0	30	70	3	40	60	100	0	0	0	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 Security Goals and various threats and attacks	Introduction: Security, CIA Triad, Viruses, Trojans, and Worms In a Nutshell, Security Concepts. Malware Terminology: Active and Passive Security Attacks. IP Spoofing, Tear drop, DoS, DDoS, XSS, SQL injection, Smurf, Man in middle, Format String attack. Types of Security Vulnerabilities- buffer overflows, Invalidated input, race conditions, access control problems, weaknesses in authentication, authorization, or cryptographic practices.	8
2	Security development process and threat modelling.	Secure Software Development Cycle (S-SDLC), Security issues while writing SRS, Design phase security, Development Phase, Test Phase, Maintenance Phase, Writing Secure Code – Best Practices SD3 (Secure by design, default and deployment), Security principles and Secure Product Development Timeline. Threat modelling process and its benefits:	8
3	Secure Coding Techniques	Secure Coding Techniques: Protection against DoS attacks, Application Failure Attacks, CPU Starvation Attacks, Insecure Coding Practices In Java Technology. ARP Spoofing and its countermeasures. Buffer Overrun- Security Issues in C Language: Avoiding Server Hijacking, Securing RPC, ActiveX and DCOM	8
4	Database and Web specific issues	Database and Web-specific issues: SQL Injection Techniques and Remedies, Race conditions, Time of Check Versus Time of Use and its protection mechanisms. Validating Input and Inter-process Communication, Securing Signal Handlers and File Operations. XSS scripting attack and its types	8
5	Testing secure applications.	Testing Secure Applications: Security code overview, secure software installation. The Role of the Security Tester, Building the Security Test Plan. Testing HTTP-Based Applications, Testing File-Based Applications, Testing Clients with Rogue Servers.	8

SELF-LEARNING / TEAM WORK		
Sl. No	Self-learning / Team Work Description	Hrs/Semester
1	Cryptography for Developers	2
2	OWASP Top 10 Overview	2
3	Secure Authentication & Session Management	2
4	Secure Configuration Management	2
5	DevSecOps & Security Tooling (SAST/SCA)	2
6	Secrets Management	2
7	Secure Error Handling & Logging	2
8	Cloud-Native Security Fundamentals	2
9	API Security (REST/GraphQL)	2
10	Practical Cryptography Implementation Lab	2
11	Secure Code Review Techniques	2
12	Incident Response for Developers	2

13	Container Security (Docker/Kubernetes)	2
14	Secure Agile Development	2
15	Capture The Flag (CTF) Practical Lab	2

SUGGESTED LEARNING RESOURCES

Text Book

Sl. No.	Title of Book	Author	Publication
1	Writing Secure Code	Michael Howard and David LeBlanc	Microsoft Press US , (2004)
2	Buffer Overflow Attacks: Detect, Exploit, Prevent	Vitaly Osipov	Syngress, 2005

Reference

Sl. No.	Title of Book	Author	Publication
1	Threat Modelling	Eoghan Casey Frank Swiderski and Window Snyder	Microsoft Professional, First Edition (2004)
2	Secure Coding – Principles & Practices	Mark G. Graff and Kenneth R. van Wyk	O'Reilly (2003).
3	Secure Coding in C and C++ (Sei Series in Software Engineering)	Robert C. Seacord	Pearson Addison-Wesley Professional (2013)

Web Resource

1	https://owasp.org/
2	https://www.sans.org/software-security/
3	https://cwe.mitre.org/
4	https://www.crypto101.io/
5	https://portswigger.net/web-security

DETAILED SYLLABUS

Module	Topic	Mode of Delivery	COs	Learning Domain Level	Hrs
				C	
1	Introduction by discussing Security, CIA Triad, Viruses, Trojans, and Worms In a Nutshell, Security Concepts- exploit, threat, vulnerability, risk, attack.	Lecture	CO1	U	1
	Malware Terminology: Rootkits, Trapdoors, Botnets, Key loggers, Honeypots	Lecture	CO1	U	1
	Active and Passive Security Attacks. IP Spoofing, Tear drop, DoS, DDoS	Lecture	CO1	U	1
	XSS, SQL injection, Smurf, Man in middle, Format String attack.	Lecture	CO1	U	1
	Types of Security Vulnerabilities- buffer overflows, Invalidated input	Lecture	CO1	U	1
	race conditions, access control problems	Lecture	CO1	U	1
	weaknesses in authentication, authorization, or cryptographic practices.	Lecture	CO1	U	1
	Security in software requirements	Lecture	CO1	U	1
2	Secure Software Development Cycle (S-SDLC), Security issues while writing SRS.	Lecture	CO1	U	1
	Design phase security, Development Phase, Test Phase, Maintenance Phase,	Lecture	CO2	U	1
	Writing Secure Code – Best Practices SD3 (Secure by design, default and deployment),	Lecture	CO2	A	1
	Secure Product Development Timeline	Lecture	CO2	U	1

	Security principles and. Threat modelling process and its benefits: Identifying the Threats by Using Attack Trees and rating threats using DREAD	Lecture	CO2	A	1
	Risk Mitigation Techniques and Security Best Practices	Lecture	CO2	U	1
	Security techniques, authentication, authorization.	Lecture	CO2	U	1
	Defence in Depth and Principle of Least Privilege.	Lecture	CO2	U	1
3	Secure Coding Techniques: Protection against DoS attacks,	Lecture	CO3	U	1
	Application Failure Attacks, CPU Starvation Attacks	Lecture	CO3	U	1
	Insecure Coding Practices In Java Technology	Lecture	CO3	U	1
	ARP Spoofing and its countermeasures.	Lecture	CO3	U	1
	Buffer Overrun- Stack overrun, Heap Overrun, Array Indexing Errors, Format String Bugs.	Lecture	CO3	U	1
	Security Issues in C Language: String Handling, Avoiding Integer Overflows and Underflows	Lecture	CO3	A	1
	Type Conversion Issues- Memory Management Issues, Code Injection Attacks	Lecture	CO3	U	1
	Canary based countermeasures using Stack Guard and Propolice. Socket Security, Avoiding Server Hijacking, Securing RPC, ActiveX and DCOM	Lecture	CO3	U	1
4	SQL injection – attack scenario : SQL Injection Techniques and Remedies,	Lecture	CO4	U	1
	Solutions – blacklisting, whitelisting, escaping, Second order SQL injection.	Lecture	CO4	U	1
	Prepared statements and bind variables, mitigating the impact of SQL injection attacks.	Lecture	CO4	U	1
	Race conditions, Time of Check Versus Time of Use and its protection mechanisms	Lecture	CO4	U	1
	Validating Input and Inter-process Communication, Securing Signal Handlers and File Operations.	Lecture	CO4	U	1
	XSS scripting attack and its types	Lecture	CO4	A	1
	Persistent and Non persistent attack XSS Countermeasures	Lecture	CO4	U	1
	Bypassing the XSS Filters.	Lecture	CO4	A	1
5	Security code overview	Lecture	CO5	U	1
	Secure software installation	Lecture	CO5	U	1
	The Role of the Security Tester	Lecture	CO5	U	1
	Building the Security Test Plan	Lecture	CO5	A	1
	Testing HTTP-Based Applications	Lecture	CO5	A	1
	Testing File-Based Applications – 1	Lecture	CO5	U	1
	Testing File-Based Applications – 2	Lecture	CO5	A	1
	Testing Clients with Rogue Servers	Lecture	CO5	A	1

TABLE OF SPECIFICATIONS (ToS) FOR QUESTION PAPER DESIGN

Module	Module Title	Teaching Hours	Distribution of Marks (Revised Bloom's Level)						Total Marks
			R	U	A	An	E	C	
1	Introduction to Security Goals and various threats and attacks	8		✓					12

2	Security development process and threat modelling.	8		✓	✓				12
3	Secure Coding Techniques	8		✓	✓				12
4	Database and Web specific issues	8		✓	✓				12
5	Testing secure applications.	8		✓	✓				12
This ToS shall be treated as a general guideline for students and teachers for distribution of marks.									

Assessment	Marks
Continuous Internal Assessment	**40**
Learning Activity	15
Internal Examination	10
Course Project	15
End Semester Examination	**60**
Total	**100**

COURSE DESCRIPTION					
Regulation	**2025**	**L-T-J-P-S**	**3-0-0-0-2**	**Credits**	**3**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)					
Course Code	**Course Name**				**Course Category**
M250102/CY124E	**CLOUD COMPUTING AND SECURITY**				**PROGRAMME ELECTIVE**

COURSE OBJECTIVES	
1	To introduce fundamental concepts of cloud computing, including service and deployment models, characteristics, and benefits.
2	To develop practical understanding of virtualization techniques and cloud programming models for processing large-scale data.
3	To provide insights into cloud security challenges and familiarize students with leading cloud platforms like AWS and GCP.

COMPETENCY & OUTCOMES		
Competency Statements	CC 1	Learners will be able to design, implement, and manage cloud-based solutions using appropriate service models, virtualization techniques, and cloud programming frameworks.
	CC 2	Learners will be equipped to assess cloud security requirements and compare cloud service providers to recommend suitable platforms for diverse application needs.

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

CO	CO Statement	Competency Mapping	Cognitive (C)
CO1	Examine the various cloud computing models and services.	CC1	A
CO2	Experiment the implementing virtualization techniques.	CC1	A
CO3	Use appropriate cloud programming methods to solve big data problems.	CC1	A
CO4	Examine the need for security mechanisms in cloud.	CC2	An
CO5	Compare the different popular cloud computing platforms	CC2	A

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

CO	Program Outcomes & Program Specific Outcomes						
	PO						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1	3	3	2		2		1
2	3	2	3		3		1
3	3	2	3	2	3		1
4	3	3	2	2	2	2	1
5	3	3	2		3		1

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

TEACHING AND ASSESSMENT SCHEME

Teaching Scheme / Week				Self-Learning (S) / Semester	Total Hours / Semester	Credits C	Examination Scheme						
L	T	J	P				Theory			Practical			Total
							CIA	ESE	Total	CIA	ESE	Total	
3	0	0	0	30	70	3	40	60	100	0	0	0	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	Cloud Computing Fundamentals	Overview of Computing Paradigms-Grid Computing, Cluster Computing, Distributed Computing, Utility Computing, Cloud Computing. NIST reference Model-Basic terminology and concepts. Cloud characteristics, benefits and challenges, Roles and Boundaries. Cloud delivery (service) models-Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), XaaS (Anything-as-a-service)-Cloud deployment models- Public cloud, Community cloud, Private cloud, Hybrid cloud.	6
2	Virtualization	Introduction to component virtualization Basics of Virtualization - Types of Virtualizations - Implementation Levels of Virtualization - Virtualization of CPU, Memory, I/O Devices - Desktop Virtualization – Server Virtualization Storage Virtualization – Network Virtualization.	8
3	Architectural Design of Compute and Storage Clouds	Layered Cloud Architecture Development – Design Challenges - Inter Cloud Resource Management – Resource Provisioning and Platform Deployment – Global Exchange of Cloud Resources. Cloud Programming - Parallel Computing and Programming Paradigms. Map Reduce – Hadoop Library from Apache, HDFS, Pig Latin High Level Languages, Apache Spark.	8
4	Fundamental Cloud Security	Basic terms and concepts in security-– Cloud Security Challenges Software-as-a-Service Security – Security Governance - Threat agents, Cloud security threats/risks, Trust. Operating system security-Virtual machine security-Security of virtualization- Security Risks Posed by Shared Images, Security Risks Posed by Management OS. Infrastructure security Network Level Security, Host Level Security, Data Security, Application-level security, Security of the Physical Systems- Virtual Machine Security Identity & Access Management- Access Control.	8
5	Popular Cloud Platforms	Amazon Web Services (AWS): AWS ecosystem- Computing services, Amazon machine images, Elastic Compute Cloud (EC2), Advanced compute services. Storage services-Simple Storage System (Amazon S3), Elastic Block Store (Amazon EBS), Database Services, Amazon CDN Services and Communication services. Google Cloud Platform IaaS Offerings: Compute Engine (GCE), Cloud Storage, PaaS Offerings: Google App Engine (GAE), Storage services, Application services, Compute services, Database Services, SaaS Offerings: Gmail, Docs, Google Drive. Microsoft Azure: Azure Platform Architecture, Hyper-V, Azure Virtual Machine, Compute services, Storage services.	10

SELF-LEARNING / TEAM WORK		
Sl. No	Self-learning / Team Work Description	Hrs/Semester
1	Students explore free tiers of AWS, GCP, or Azure to launch and configure a simple VM or deploy a basic web app.	3
2	Set up VirtualBox or VMware and create a virtual environment with different OSes.	1
3	Research recent cloud security breaches and analyse how they could have been prevented	1
4	Create a small project using Hadoop or Spark and document the steps.	5
5	Encourage students to complete online micro-courses (e.g., AWS Cloud Practitioner Essentials).	1
6	Use MapReduce/Spark in teams to solve a big data problem (e.g., log analysis)	5
7	Cloud Migration Strategies	2
8	Infrastructure as Code (IaC)	3
9	Serverless Architecture	3
10	DevSecOps & CI/CD Security	6

SUGGESTED LEARNING RESOURCES

Text Book

Sl. No.	Title of Book	Author	Publication
1	Cloud Computing	K. Saurabh	1st edition, Wiley India Pvt. Ltd., 2013.
2	Cloud Computing: Principles and Paradigms	R. Buyya, J. Broberg, and A. M. Goscinski	Wiley, 2011.

Reference

Sl. No.	Title of Book	Author	Publication
1	Distributed and Cloud Computing, From Parallel Processing to the Internet of Things	Kai Hwang, Geoffrey C Fox, Jack G Dongarra	Morgan Kaufmann Publishers, 2012.
2	Cloud Computing: Implementation, Management, and Security	John W.Rittinghouse and James F.Ransome,	CRC Press, 2010.
3	Cloud Computing, A Practical Approach	Toby Velte, Anthony Velte, Robert Elsenpeter	TMH, 2009
4	Cloud Application Architectures: Building Applications and Infrastructure in the Cloud	George Reese	O'Reilly, 2009
5	Computing, A Practical Approach	Anthony T. Velte, Toby Velte, Robert Elsenpeter	McGraw-Hill Osborne
6	Cloud Computing Strategies	Dimitris N. Chorafas	CRC Press
7	Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance	Tim Mather, Subra Kumaraswamy, Shahed Latif	O'Reilly Media
8	Cloud Security: A Comprehensive Guide to Secure Cloud Computing	Ronald L. Krutz	John Wiley & Sons
9	Mastering cloud computing: foundations and applications programming	Buyya, R., Vecchiola, C., & Selvi, S. T	Morgan Kaufmann, 2017 Edition
10	Cloud computing	Bhowmik S.	Cambridge University Press.

Web Resource

1	https://www.ibm.com/cloud/learn/cloud-computing, Microsoft Azure – What is Cloud Computing:
2	https://www.oracle.com/cloud/cloud-deployment-models/, Oracle Cloud Deployment Models Explained

3	https://www.virtualbox.org/manual/UserManual.html, Oracle VirtualBox Documentation:
4	https://hadoop.apache.org/docs/stable/, Apache Hadoop Documentation
5	Google Cloud MapReduce Explained: https://cloud.google.com/architecture/mapreduce-pattern/
6	Microsoft Cloud Security Overview: https://learn.microsoft.com/en-us/security/
7	Coursera – Cloud Computing Specializations: https://www.coursera.org/specializations/cloud-computing
8	edX – Cloud Computing Courses: https://www.edx.org/learn/cloud-computing

DETAILED SYLLABUS

Module	Topic	Mode of Delivery	COs	Learning Domain Level C	Hrs
1	Traditional computing: Limitations.	Lecture	CO1	A	1
	Overview of Computing Paradigms: Grid Computing, Cluster Computing, Distributed Computing, Utility Computing, Cloud Computing.	Lecture	CO1	A	1
	NIST reference Model Basic terminology and concepts	Lecture	CO1	A	1
	Cloud characteristics and benefit s, challenges. Roles and Boundaries.	Lecture	CO1	A	1
	Cloud delivery (service) models: Infrastructure-as-a-Service (IaaS), Platform-asa-Service (PaaS), Software-as-a-Service (SaaS), XaaS (Anything-as-a-service).	Lecture	CO1	A	1
	Cloud deployment models: Public cloud, Community cloud, Private cloud, Hybrid cloud	Lecture	CO1	A	1
2	Introduction to virtualization, Virtualizing physical computing resources Virtual Machines (Machine virtualization):- non-virtualized v/s virtualized machine environments.	Lecture	CO2	A	1
	Types of VMs: process VM v/s system VM, Emulation, interpretation and binary translation	Lecture	CO2	A	1
	Hardware-level virtualization: Hypervisors/VMM, Types of Hypervisors.	Lecture	CO2	A	1
	Full Virtualization, Para-Virtualization, Hardware-assisted virtualization, OS level virtualization.	Lecture	CO2	A	1
	Basics of Network Virtualization	Lecture	CO2	A	1
	Storage Virtualization and Desktop Virtualization, Pros and cons of virtualization.	Lecture	CO2	A	1
	Case Study: Xen: Para-virtualization.	Lecture	CO2	A	1
	Case Study: VMware: full virtualization.	Lecture	CO2	A	1
3	Architectural Design of Compute and Storage Clouds	Lecture	CO3	A	1
	Layered Cloud Architecture Development – Design Challenges	Lecture	CO3	A	1
	Inter Cloud Resource Management – Resource Provisioning and Platform Deployment	Lecture	CO3	A	1

	Global Exchange of Cloud Resources.	Lecture	CO3	A	1
	Cloud Programming: Parallel Computing and Programming Paradigms.	Lecture	CO3	A	1
	Map Reduce.	Lecture	CO3	A	1
	Hadoop Library from Apache, HDFS.	Lecture	CO3	A	1
	Pig Latin High Level Languages, Apache Spark	Lecture	CO3	A	1
4	Basic terms and concepts in security	Lecture	CO4	An	1
	Cloud Security Challenges Software-as-a-Service Security, Security Governance	Lecture	CO4	An	1
	Threat agents, Cloud security threats/risks, Trust.	Lecture	CO4	An	1
	Operating system security-Virtual machine security-	Lecture	CO4	An	1
	Security of virtualization- Security Risks Posed by Shared Images, Security Risks Posed by Management OS.	Lecture	CO4	An	1
	Infrastructure security Network Level Security, Host Level Security, Data Security , Application level security,	Lecture	CO4	An	1
	Security of the Physical Systems- Virtual Machine Security.	Lecture	CO4	An	1
	Identity & Access Management- Access Control.	Lecture	CO4	An	1
5	Amazon Web Services (AWS):- AWS ecosystem, Computing services: Amazon machine images, Elastic Compute Cloud (EC2).	Lecture	CO5	A	1
	Advanced computing services, Storage services: Simple Storage System (Amazon S3), Elastic Block Store (Amazon EBS).	Lecture	CO5	A	1
	Database Services, Amazon CDN Services and Communication services.	Lecture	CO5	A	1
	Google Cloud Platform:- IaaS Offerings: Compute Engine (GCE), Cloud Storage	Lecture	CO5	A	1
	PaaS Offerings: Google App Engine (GAE), Storage services.	Lecture	CO5	A	1
	Application services, Compute services.	Lecture	CO5	A	1
	Database Services, SaaS Offerings: Gmail, Docs, Google Drive.	Lecture	CO5	A	1
	Microsoft Azure: Azure Platform Architecture	Lecture	CO5	A	1
	Hyper-V, Azure Virtual Machine.	Lecture	CO5	A	1
	Azure Compute services, Storage services.	Lecture	CO5	A	1

TABLE OF SPECIFICATIONS (ToS) FOR QUESTION PAPER DESIGN

Module	Module Title	Teaching Hours	Distribution of Marks (Revised Bloom's Level)						Total Marks
			R	U	A	An	E	C	
1	Cloud Computing Fundamentals	6		✓	✓				12

2	Virtualization	8		✓	✓				12
3	Architectural Design of Compute and Storage Clouds, Cloud Programming	8		✓	✓				12
4	Fundamental Cloud Security	8		✓	✓				12
5	Popular Cloud Platforms	10		✓	✓				12
This ToS shall be treated as a general guideline for students and teachers for distribution of marks.									

Assessment	Marks
Continuous Internal Assessment	**40**
Learning Activity	15
Internal Examination	10
Course Project	15
End Semester Examination	**60**
Total	**100**

COURSE DESCRIPTION					
Regulation	**2025**	**L-T-J-P-S**	**3-0-0-0-2**	**Credits**	**3**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)					
Course Code	**Course Name**				**Course Category**
M250102/CY125E	**FORMAL METHODS IN SECURITY**				**PROGRAMME ELECTIVE**

COURSE OBJECTIVES	
1	Understand the core concepts of formal logic and verification methods for proving software and security protocols are correct.
2	Learn to apply techniques like model-checking and theorem proving to find security vulnerabilities in programs and protocols.
3	Gain experience with professional tools used to automate the analysis of security properties and models.

COMPETENCY & OUTCOMES		
Competency Statements	CC 1	Model security problems using formal logic and mathematical frameworks.
	CC 2	Use automated tools to verify systems and find security vulnerabilities.

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

CO	CO Statement	Competency Mapping	Cognitive (C)
CO1	Analyze and apply fundamental formal methods, including propositional/predicate logic and fixed-point theorems, to model and verify security policies such as the Clark-Wilson and Chinese Wall models.	CC1	A
CO2	Construct formal specifications and verify the correctness of sequential programs using weakest preconditions, and of concurrent/reactive systems using model-checking techniques with temporal logics.	CC2	An
CO3	Employ static/dynamic analysis and model-checking tools to identify, analyze, and mitigate common security vulnerabilities in software and communication protocols, evaluating goals like secrecy and authentication.	CC2	An
CO4	Model and analyze advanced security properties, including information flow in web applications, mobility using pi-calculus, and complex protocol goals like non-repudiation and anonymity.	CC1	An
CO5	Utilize specialized formal verification tools to implement and analyze security protocols based on established formal models like Dolev-Yao and BAN logic.	CC2	U

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

CO	Program Outcomes						
	PO						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1	2	-	3	2	1	2	-
2	2	1	3	2	3	2	-
3	2	1	3	3	3	2	1
4	2	1	3	2	2	2	-
5	1	2	3	3	3	2	1

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

TEACHING AND ASSESSMENT SCHEME													
Teaching Scheme / Week				**Self-Learning (S) / Semester**	**Total Hours / Semester**	**Credits C**	**Examination Scheme**						
L	**T**	**J**	**P**				**Theory**			**Practical**			**Total**
							CIA	**ESE**	**Total**	**CIA**	**ESE**	**Total**	
3	0	0	0	30	70	3	40	60	100	0	0	0	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	Formal Methods	Formal Methods – Propositional and Predicate logic, and theorem-proving, Fixed-points and their role in program analysis and model-checking, Formal methods in secure computing- Clark Wilson model and Chinese wall model.	8
2	Verification	Verification of sequential programs using weakest preconditions and inductive methods, and verification of concurrent and reactive programs/systems using model-checking and propositional temporal logic (CTL and LTL). Modelling security protocol, trustworthy processes, data types for models, modelling an intruder.	8
3	Formal methods applications	Application of static and dynamic program analysis and model-checking for detecting common security vulnerabilities in programs and communication protocols. Protocol goals-Yahalom protocol, secrecy, External threat authentication.	8
4	Formal modelling	Information flow and taint analysis for the security of web applications, pi-calculus for formal modelling of mobile systems and their security. Non -repudiation Zhou-Gollmann protocol, anonymity and Dining cryptographers' analysis.	8
5	Familiarization	SPIN, PVS, TAMARIN, Frama-C and Isabelle tools familiarization. Introduction of secure computing protocol model-Dolev Yao model, BAN logic and derivatives.	8

SELF-LEARNING / TEAM WORK		
Sl. No	Self-learning / Team Work Description	Hrs/Semester
1	Set Theory and Functions for Formal Methods	2
2	Introduction to Lattices and Order Theory	2
3	Hoare Logic Fundamentals	2
4	Verifying Blockchain Smart Contracts	2
5	Introduction to Differential Privacy	2
6	The Applied Pi-Calculus	2
7	Symbolic Execution for Vulnerability Discovery	2
8	Introduction to Side-Channel Analysis	2
9	Intermediate Representations for Static Analysis	2
10	Lightweight Formal Methods: TLA+ and Alloy	2
11	Version Control and CI for Formal Models	2
12	Debugging and Interpreting Tool Output	2
13	Economics of Formal Verification	2
14	Usable Security and Formal Methods	2

15	Writing and Reviewing Formal Specifications	2

SUGGESTED LEARNING RESOURCES			
Text Book			
Sl. No.	Title of Book	Author	Publication
1	Model Checking	Edmund M. Clarke, Orna Grumberg and Doron Peled	MIT Press, 1999.
2	Logic and Learning: Knowledge Representation, Computation and Learning in Higher-order Logic	Lloyd, J.W.	Springer Berlin Heidelberg, 2003.
3	Logic in Computer Science - Modelling and Reasoning about Systems	M. Ruth and M. Ryan	Cambridge University Press, 2004
4	Formal Correctness of Security Protocols	G. Bella	Springer, 2009
5	Analysis Techniques for Information Security	Datta A, Jha S, Li N, Melski D and Reps T	Synthesis Lectures on Information Security, Privacy, and Trust, 2010.
Reference			
Sl. No.	Title of Book	Author	Publication
1	Modelling and Analysis of Security Protocols	Peter Ryan, Steve Schneider, M. H. Goldsmith	Pearson Education, 2010
2	Formal Aspects In Security And Trust: Ifip TN Wg1.7	Theo Dimitrakos, Fabio Martinelli	Workshop on Formal Aspects in Security, Springer, 2005
3	Modern Cryptography: Theory & Practice	W. Mao	Pearson Education, 2004
4	Formal Verification of Security Protocols	Giampaolo Bella	Springer, 2007
5	Protocols for Authentication and Key Establishment	Colin Boyd, Anish Mathuria	Springer, 2003
6	Formal Correctness of Security Protocols (Information Security and Cryptography)	Giampaolo Bella	Springer, 1e, 2007.
Web Resource			
1	https://tamarin-prover.github.io/manual/		
2	http://spinroot.com/spin/whatispin.html		
3	https://isabelle.in.tum.de/documentation.html		
4	https://cvc5.github.io/		
5	https://frama-c.com/html/documentation.html		

DETAILED SYLLABUS					
Module	Topic	Mode of Delivery	COs	Learning Domain Level	Hrs
				C	
1	Formal Methods in security	Lecture	CO1	U	1
	Propositional and Predicate logic	Lecture	CO1	U	1
	Theorem-proving logic	Lecture	CO1	U	1
	Fixed-points	Lecture	CO1	U	1
	Fixed points in program analysis	Lecture	CO1	U	1

	Fixed points in model checking	Lecture	CO1	A	1
	Formal methods in secure computing	Lecture	CO1	A	1
	Clark Wilson model and Chinese wall model	Lecture	CO1	A	1
2	Introduction to Verification	Lecture	CO2	U	1
	Verification of sequential programs using weakest preconditions	Lecture	CO2	A	1
	Verification using inductive methods	Lecture	CO2	A	1
	Verification of concurrent and reactive programs	Lecture	CO2	A	1
	Verification using model checking		CO2	An	1
	Propositional temporal logic (CTL and LTL)	Lecture	CO2	U	1
	Modelling security protocol	Lecture	CO2	U	1
	Modelling an intruder	Lecture	CO2	U	1
3	Application of static and dynamic program analysis	Lecture	CO3	A	1
	Model-checking for detecting common security vulnerabilities	Lecture	CO3	An	1
	Communication protocols model checking	Lecture	CO3	U	1
	Protocol goals- Yahalom protocol, secrecy	Lecture	CO3	U	1
	External threat authentication	Lecture	CO3	U	1
4	Information flow	Lecture	CO4	U	1
	Taint analysis for the security of web applications	Lecture	CO4	An	1
	pi-calculus for formal modelling of mobile systems	Lecture	CO4	U	1
	pi-calculus for formal modelling of mobile system security	Lecture	CO4	A	1
	Zhou Gollmann and Dining cryptographers' analysis-anonymity	Lecture	CO4	An	1
5	SPIN familiarization	Lecture	CO5	U	1
	PVS familiarization	Lecture	CO5	U	1
	TAMARIN familiarization	Lecture	CO5	U	1
	Frama-C familiarization	Lecture	CO5	U	1
	Isabelle tools familiarization	Lecture	CO5	U	1
	Dolev Yao model	Lecture	CO5	U	1
	BAN logic and derivatives	Lecture	CO5	U	1

TABLE OF SPECIFICATIONS (ToS) FOR QUESTION PAPER DESIGN

Module	Module Title	Teaching Hours	Distribution of Marks (Revised Bloom's Level)						Total Marks
			R	U	A	An	E	C	
1	Formal Methods	8		✓	✓				12
2	Verification	8		✓	✓				12
3	Formal methods applications	8		✓		✓			12
4	Formal modelling	8		✓		✓			12
5	Familiarization	8		✓					12
This ToS shall be treated as a general guideline for students and teachers for distribution of marks.									

Assessment	**Marks**
Continuous Internal Assessment	**40**
Learning Activity	15

Internal Examination	10
Course Project	15
End Semester Examination	**60**
Total	**100**

COURSE DESCRIPTION					
Regulation	**2025**	**L-T-J-P-S**	**3-0-0-0-2**	**Credits**	**3**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)					
Course Code	**Course Name**				**Course Category**
M250102/CY126E	**LINEAR ALGEBRA**				**PROGRAMME ELECTIVE**

COURSE OBJECTIVES	
1	To provide students with a rigorous foundation in the abstract theory of finite-dimensional vector spaces and linear transformations, emphasizing proof-based understanding.
2	To develop the ability to connect theoretical concepts to practical computational techniques, enabling students to solve complex problems in engineering, computer science, and data analysis.
3	To equip students with the skills to analyze the structure of linear systems and matrices through decomposition methods and to evaluate the appropriate technique for a given application.

COMPETENCY & OUTCOMES		
Competency Statements	CC 1	Execute key linear algebra calculations and decompositions to solve applied problems.
	CC 2	Translate theoretical problems into a linear algebra framework to analyze their structure.

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

CO	CO Statement	Competency Mapping	Cognitive (C)
CO1	Apply the concepts of basis, dimension, and coordinate vectors to solve problems related to the row space, column space, and null space of a matrix. . (Cognitive Knowledge Level: Apply)	CC 1	A
CO2	Apply the properties of linear transformations, including the Rank-Nullity Theorem, to find kernel, range, and matrix representations, and execute change-of-basis operations. (Cognitive Knowledge Level: Apply)	CC 1	A
CO3	Apply the techniques of eigenvalues, eigenvectors, and diagonalization to determine whether a matrix is diagonalizable and to represent linear transformations with diagonal matrices. (Cognitive Knowledge Level: Apply)	CC 1	A
CO4	Analyse vector spaces equipped with an inner product by constructing orthonormal bases, decomposing spaces into orthogonal complements, and interpreting geometric properties like length and orthogonality. (Cognitive Knowledge Level: Analyse)	CC 2	An
CO5	Select appropriate matrix decomposition methods (LU, QR, SVD) to efficiently solve practical problems such as solving linear systems, performing curve fitting, and approximating eigenvalues. (Cognitive Knowledge Level: Evaluate)	CC 2	E

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

CO	Program Outcomes						
	PO						
	1	2	3	4	5	6	7
1	-	-	3	1	2	1	-
2	-	-	3	2	2	1	-
3	1	-	3	2	2	1	-
4	2	-	3	3	2	1	-
5	3	2	3	3	3	2	1
Correlation levels: 1 - Low; 2 - Medium; 3 - High; No Correlation - "-"							

TEACHING AND ASSESSMENT SCHEME

Teaching Scheme / Week				Self-Learning (S) / Semester	Total Hours / Semester	Credits C	Examination Scheme						
							Theory			Practical			Total
L	T	J	P				CIA	ESE	Total	CIA	ESE	Total	
3	0	0	0	30	70	3	40	60	100	0	0	0	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	Vector spaces	Vector Spaces-Definition and Examples. Subspaces, Spanning sets and linear independence. Basis and dimension, Co-ordinates with respect to a given basis. Row space, Column space and null space of a matrix	8
2	Transformations	Linear transformations between vector spaces and their properties, Kernal and range of linear transformations, Rank Nullity theorem, matrix representation of linear transformation, invertible transformations and their matrix representation, co-ordinates and linear transformations under change of basis , similar matrices. Isomorphism between n-space and finite dimensional vector spaces	8
3	Eigenvalues and Eigenvectors	Eigen values, eigenvectors and eigen spaces of matrices and linear transformation, Properties of eigen values and eigen vectors, Diagonalization of matrices, orthogonal diagonalization of real symmetric matrices, representation of linear transformation by diagonal matrix	8
4	Orthogonality	Real Inner Product spaces, properties of inner product, length and distance, Cauchy-Schwarz inequality, Orthogonality, Orthonormal basis, Gram Schmidt orthogonalization process. Orthogonal subspaces, Orthogonal projection. orthogonal compliment and direct sum representation.	8
5	Decomposition	LU-decomposition of matrices, QR-decomposition, Singular value decomposition, Least squares solution of inconsistent linear systems, curve-fitting by least square method. Power method for finding dominant eigen value	8

SELF-LEARNING / TEAM WORK

Sl. No	Self-learning / Team Work Description	Hrs/Semester
1	Applications in Computer Graphics	6
2	Introduction to Numerical Linear Algebra	8
3	Principal Component Analysis (PCA)	6
4	Quantum Computing Basics	5
5	Markov Chains & Eigenvectors	5

SUGGESTED LEARNING RESOURCES			
Text Book			
Sl. No.	Title of Book	Author	Publication
1	Linear Algebra-an introduction	Richard Bronson, Gabriel B. Costa,	2nd edition, Academic Press, 2007
2	Linear Algebra with Applications	Gareth Williams	Jones and Bartlett Publishers, Eighth edition, 2014
Reference			
Sl. No.	Title of Book	Author	Publication
1	Linear Algebra and It's Applications	Gilbert Strang	4th edition, Cengage Learning, 2006
2	Schaum's outline of linear algebra	Seymour Lipschutz, Marc Lipson	3rd Ed., Mc Graw Hill Edn, 2017
3	Linear algebra and its applications	David C Lay	3rd edition, Pearson
4	Introduction to Applied Linear Algebra: Vectors, Matrices, and Least Squares	Stephen Boyd, Lieven Vandenberghe	Cambridge University Press, 2018
5	Linear Algebra with applications	W. Keith Nicholson	4th edition, McGraw-Hill, 2002
Web Resource			
1	https://www.youtube.com/playlist?list=PLZHQObOWTQDPD3MizzM2xVFitgF8hE_ab		
2	https://ocw.mit.edu/courses/18-06-linear-algebra-spring-2010/		
3	https://math.stackexchange.com/		
4	https://linear.axler.net/		
5	https://tutorial.math.lamar.edu/		

DETAILED SYLLABUS					
Module	Topic	Mode of Delivery	COs	Learning Domain	Hrs

				Level C	
1	Vector spaces, Definition and example	Lecture	CO1	U	1
	Linear dependence, Basis , dimension	Lecture	CO1	U	1
	Row space, column space, rank of a matrix - 1	Lecture	CO1	U	1
	Row space, column space, rank of a matrix – 2	Lecture	CO1	A	1
	Row space, column space, rank of a matrix – 3	Lecture	CO1	A	1
	Co-ordinates with respect to a given basis – 1	Lecture	CO1	U	1
	Co-ordinates with respect to a given basis – 2	Lecture	CO1	A	1
	Co-ordinate representation	Lecture	CO1	U	1
2	General linear transformation, Matrix of transformation – 1	Lecture	CO2	U	1
	General linear transformation, Matrix of transformation – 2	Lecture	CO2	A	1
	Kernel and range of a linear mapping	Lecture	CO2	U	1
	Properties of linear transformations,	Lecture	CO2	U	1
	Rank Nullity theorem – 1	Lecture	CO2	U	1
	Change of basis - 1	Lecture	CO2	U	1
	Change of basis – 2	Lecture	CO2	A	1
	Isomorphism	Lecture	CO2	U	1
3	Eigen values and Eigen vectors of a linear transformation and matrix - 1	Lecture	CO3	U	1
	Eigen values and Eigen vectors of a linear transformation and matrix - 2	Lecture	CO3	A	1
	Properties of Eigen values and Eigen vectors	Lab	CO3	U	1
	Diagonalization., orthogonal diagonalization - 1	Lecture	CO3	U	1
	Diagonalization., orthogonal diagonalization – 2	Lab	CO3	U	1
	Diagonalization., orthogonal diagonalization – 3	Lecture	CO3	A	1
	Diagonalizable linear transformation – 1	Lecture	CO3	U	1
	Diagonalizable linear transformation – 2	Lecture	CO3	A	1
4	Inner Product: Real and complex inner product spaces – 1	Lecture	CO4	U	1
	Properties of inner product, length and distance	Lecture	CO4	U	1
	Triangular inequality, Cauchy-Schwarz inequality	Lecture	CO4	U	1
	Orthogonality, Orthogonal complement, Orthonormal bases - 1	Lecture	CO4	U	1
	Orthogonality, Orthogonal complement, Orthonormal bases – 2	Lecture	CO4	U	1
	Gram Schmidt orthogonalization process, orthogonal projection - 1	Lecture	CO4	A	1
	Gram Schmidt orthogonalization process, orthogonal projection - 2	Lecture	CO4	An	1
	Direct sum representation		CO4		1
5	LU decomposition, QR Decomposition – 1	Lecture	CO5	U	1
	LU decomposition, QR Decomposition – 2	Lecture	CO5	A	1
	Singular value decomposition - 1	Lecture	CO5	U	1
	Singular value decomposition - 2	Lecture	CO5	A	1
	Least square solution - 1	Lecture	CO5	U	1
	Least square solution - 2	Lecture	CO5	A	1
	Curve fitting	Lecture	CO5	E	1
	Power method	Lecture	CO5	A	1

TABLE OF SPECIFICATIONS (ToS) FOR QUESTION PAPER DESIGN				
Module	Module Title	Teaching	Distribution of Marks	Total

		Hours	(Revised Bloom's Level)						Marks
			R	U	A	An	E	C	
1	Vector spaces	8		✓	✓				12
2	Transformations	8		✓	✓				12
3	Eigenvalues and Eigenvectors	8		✓	✓				12
4	Orthogonality	8		✓	✓				12
5	Decomposition	8		✓	✓				12
This ToS shall be treated as a general guideline for students and teachers for distribution of marks.									

Assessment	**Marks**
Continuous Internal Assessment	**40**
Learning Activity	15
Internal Examination	10
Course Project	15
End Semester Examination	**60**
Total	**100**

COURSE DESCRIPTION							
Regulation	**2025**	**L-T-J-P-S**	**2-0-0-0-1**	**Version**	**25/0**	**Credits**	**2**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)							

Course Code	Course Name	Course Category
M250902/CN100S	**RESEARCH METHODOLOGY & IPR**	**GENERAL COURSE**

COURSE OBJECTIVES	
1	Approach research projects with enthusiasm and creativity.
2	Conduct literature survey and define research problem.
3	Adopt suitable methodologies and tools to design experiments, develop models, analyze data, and validate research findings.
4	Deliver well-structured technical presentations and write technical reports.
5	Evaluate publication quality and Publish/Patent research outcome.

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	Communicate Research Effectively – Present research findings clearly and persuasively through well-structured written documents and engaging oral presentations tailored to diverse audiences.
CC3	Protect and Publish Intellectual Work – Select appropriate publication avenues, evaluate their quality using recognized metrics, and apply Intellectual Property Rights principles to safeguard innovations.

COURSE OUTCOMES

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

CO	CO Statement	Competency Mapping	Cognitive (C)
CO1	Approach research projects with enthusiasm and creativity. (Cognitive Knowledge Level: Understand)	CC1	U
CO2	Conduct literature survey and define research problem. (Cognitive Knowledge Level: Apply)	CC1	A
CO3	Adopt suitable methodologies and tools to design experiments, develop models, analyze data, and validate research findings. (Cognitive Knowledge Level: Apply)	CC1	A
CO4	Deliver well-structured technical presentations and write technical reports. (Cognitive Knowledge Level: Create)	CC2	C
CO5	Evaluate publication quality and Publish/Patent research outcome. (Cognitive Knowledge Level: Evaluate	CC3	E

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

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

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

TEACHING AND ASSESSMENT SCHEME													
Teaching Scheme / Week				**Self-Learning (S) / Semester**	**Total Hours / Semester**	**Credits C**	**Examination Scheme**						
							Theory			**Practical**			**Total**
L	**T**	**J**	**P**				**CIA**	**ESE**	**Total**	**CIA**	**ESE**	**Total**	
2	0	0	0	10	44	2	40	60	100				100

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

SYLLABUS (Major Topics)			
Module	Title	Major Topics	Contact Hours
1	Introduction to Research Methodology	Meaning of Research, Research process, Research ethics, Thinking skills	6
2	Literature Survey and Problem Definition	Literature survey process, Sources of literature, Identifying research gaps and formulating research objectives/hypotheses.	9
3	Experimental and Modelling Skills	Principles of experimental design, Scientific method, Mathematical and computational modelling approaches. Validation and verification of results.	5
4	Effective Communication	Principles of technical writing, Oral presentation skills, Types of intellectual property, Research metrics-Journal Level	6
5	Publication/Patents	Types of intellectual property, Research metrics-Journal Level	8

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	Conduct a study of the documentation tool -LaTeX	1
5	Peer Review Process and Journal Selection tools -Group Activity	1
6	Open access vs. subscription-based publishing -Prepare a report	1
7	Conduct a study and prepare a report about various research visibility tools.	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	Design and Analysis of Experiments	Montgomery, D.C	Wiley, 9th Ed., 2017
3	Applied Multivariate Statistical Analysis	Johnson, R.A., Wichern, D.W.	Pearson, 6th Ed., 2014.
4	The Craft of Scientific Writing	Michael Alley	Springer, 4th Ed., 2018
5	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 C	Hrs
1	Meaning and significance of research, Types of research	Lecture	CO1	U	1
	Characteristics of good research, Research process	Lecture	CO1	U	1
	Role of research in technological and societal development.	Lecture	CO1	U	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	1
	Creativity: Some definitions, illustrations from day to day life, intelligence versus creativity, creative process, requirements for creativity	Lecture	CO1	U	1
	Motivation for research: Motivational talks on research: "You and Your Research"- Richard Hamming	Self - Learning	CO1	U	1
2	Literature survey process: Planning, searching, screening, analyzing, and synthesizing.	Lecture	CO2	U	1
	Information gathering – reading, searching and documentation, types of literature, Sources of literature	Lecture	CO2	U	1
	Integration of research literature and identification of research gaps	Lecture	CO2	U	1
	Attributes and sources of research problems, problem formulation, Research question, multiple approaches to a problem	Lecture	CO2	U	1
	Problem solving strategies – reformulation or rephrasing, techniques of representation, Importance of graphical representation, examples. Defining research scope and limitations.	Lecture	CO2	U	1
	Tools for literature management: Mendeley, Zotero, EndNote.	Self-Learning	CO2	A	1
	Identify a standard research paper in respective area and summarize it based on the problem addressed, methods used, advantages, disadvantages and future directions	Self-Learning	CO1	A	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	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	1
	Sampling methods and sample size determination.	Lecture	CO3	U	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	1
	Continuum/meso/micro scale approaches for numerical simulation,	Lecture	CO3	U	1
4	Preparing visual aids (figures, tables, charts) for papers and presentations.	Lecture	CO4	A	1
	Guidelines for preparation of good presentation slides.	Self-Learning	CO4	U	1
	Oral presentation skills: Structure, delivery, handling Q&A	Lecture	CO4	A	1
	Principles of technical writing: Structure, clarity, conciseness	Lecture	CO4	U	1
	Rules of scientific writing, form, content and language, layout, typography and illustrations, nomenclature, reference and citation styles, contexts for writing – paper, thesis, reports etc.	Lecture	CO4	A	1
	Common errors in typing and documentation	Lecture	CO4	U	1
	Tools for document preparation-LaTeX.	Self-Learning	CO4	U	1
5	Relative importance of various forms of publication, Choice of journal and reviewing process, Stages in the realization of a paper.	Lecture	CO5	A	1
	Research metrics-Journal level, Article level and Author level, Plagiarism and research ethics .	Lecture	CO5	U	1
	Introduction to IPR, Concepts of IPR, Types of IPR	Lecture	CO5	U	1
	Common rules of IPR practices, Types and Features of IPR Agreement, Trademark, trade secrets	Lecture	CO5	U	1
	Patents- Concept, Objectives and benefits, features, Patent search, filing process, and case studies in India & abroad.	Lecture	CO5	An	1
	Peer-review process and journal selection.	Self-Learning	CO5	U	1
	Open access vs. subscription-based publishing.	Self-Learning	CO5	U	1
	Research visibility: ORCID, ResearchGate, Google Scholar profiles.	Self-Learning	CO5	U	1

TABLE OF SPECIFICATIONS (ToS) FOR QUESTION PAPER DESIGN										
Module	Module Title	Teaching Hours	Distribution of Marks (Revised Bloom's Level)						Total Marks
			R	U	A	An	E	C	

1	Introduction to Research Methodology	6		✓	–	–	–	–	6
2	Literature Survey and Problem Definition	9	–	✓	✓	–	–	–	6
3	Experimental and Modelling Skills	5	–	–	✓	✓	–	–	6
4	Effective Communication	6	–	–	✓	✓		–	6
5	Publication/Patents	8			✓	✓	–	–	6
Research Paper Analysis						✓			30
This ToS shall be treated as a general guideline for students and teachers for distribution of marks.									

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

FIRST SEMESTER M. TECH DEGREE (REGULAR) EXAMINATION, DECEMBER 2025 (2025 SCHEME)			
Course Code:	**M250902/CN100S**		
Course Name:	**RESEARCH METHODOLOGY AND IPR**		
Max. Marks	**60**	**Duration**:	2 hours 30 minutes
Common to M.Tech S1 CC, AI&DS			

PART A

(Answer all questions. Each question carries 5 marks)

No.	*Question*	*CO*	*Marks*
1	Discuss the characteristics of good research.	CO1	(5)
2	Explain various problem-solving strategies.	CO2	(5)
3	Explain the basic principles of experimental designs.	CO3	(5)
4	You are asked to deliver the keynote speech at a national seminar. Outline how you would plan and structure your speech, keeping in mind the importance of audience analysis, delivery style, and context.	CO4	(5)
5	You are deciding where to submit your research article. Two journals are available: Journal A has an Impact Factor of 6.5 and a Cite Score of 5.8, but it is published only twice a year. Journal B has an Impact Factor of 4.2 and a Cite Score of 7.1, and it publishes monthly. As a researcher, which journal would you choose for your article, and why? Justify your answer with reference to publication metrics, visibility, and long-term academic value.	CO5	(5)
6	Discuss various ethical issues concerning research participants.	CO5	(5)

PART B

(Read the given article and write a report that addresses the following issues)

No.	*Question*	*CO*	*Marks*
7	What is the primary research problem explored in the study?	CO2	(3)
8	Explain the significance of the research problem addressed in this study and how the researchers have justified the need for their investigation.	CO2	(3)
9	Discuss any shortcomings or gaps you have identified in the literature review part of this article.	CO2	(6)
10	How well does the chosen methodology align with the research objectives and problem statement in the study.	CO3	(6)
11	Discuss the significance of the study and summarize the important results and contributions by the authors.	CO4	(6)
12	Critically evaluate the limitations of the research article. Identify any weaknesses in the methodology, data analysis, or scope of the study.	CO3	(6)

****

COURSE DESCRIPTION							
Regulation	**2025**	**L-T-J-P-S**	**0-0-0-2-1**	**Version**	**25/0**	**Credits**	**1**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)							
Course Code	**Course Name**						**Course Category**
M250102 / CY10T	**COMPUTING LAB I**						**LAB 1**

COURSE OBJECTIVES	
1	To provide practical exposure to cybersecurity and forensic tools for securing, acquiring, and analyzing digital evidence.
2	To enable students to implement cryptographic algorithms and secure coding practices for developing secure applications.
3	To develop the ability to identify threats, analyze vulnerabilities, and design effective security solutions in real-world systems.

COMPETENCY STATEMENTS	
CC1	Ability to apply tools, write code, and implement measures to defend software against common vulnerabilities and attacks.
CC2	Ability to identify threats, evaluate security solutions, and make high-level design decisions to protect applications.

COURSE OUTCOMES			
Course Outcomes (CO): At the end of this course, learners will be able to:			
CO	**CO Statement**	**Competency Statement Mapping**	**Cognitive (C)**
CO1	Implement cyber security solutions and use of cyber security, information assurance, and cyber/computer forensics software/tools. (Cognitive Knowledge Level: Apply)	CC1	A
CO2	Demonstrate skills needed to deal with common programming errors that lead to most security problems and to learn how to develop secure applications. (Cognitive Knowledge Level: Apply)	CC1	A
CO3	Identify the nature of the threats to software and incorporate secure coding practices throughout the planning and development of the product. (Cognitive Knowledge Level: Analyse)	CC2	An
CO4	Able to properly handle application faults, implement secure authentication, authorization and data validation controls used to prevent common vulnerabilities. (Cognitive Knowledge Level: Apply)	CC1	A
CO5	Practice with an expertise in academics to design and implement security solutions. (Cognitive Knowledge Level: Evaluate)	CC2	E

	PROGRAM OUTCOMES (PO) CORRELATION MATRIX

	PO						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1	1	1	2	3	3	1	3
2	1	1	3	3	3	1	2
3	3	2	3	2	2	3	1
4	1	1	2	3	3	2	1
5	3	3	2	3	2	2	3

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

TEACHING AND ASSESSMENT SCHEME

Teaching Scheme / Week					**Credit**	**Hours / Semester**	**Examination Scheme**		
							Practical		
L	**T**	**J**	**P**	**S**	**C**		**CIA**	**ESE**	**Total**
0	0	0	2	1	1	30	100	0	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*

PRACTICAL SYLLABUS

Experiment No.	Topic	Objective	CO	Learning Domain Level	Hrs
				C	
1	Generate and Validate Hash Values of Office Files, PDFs, multimedia files using Hasher tool	To understand and validate integrity of digital data using hashing	CO1	A	2
2	Forensic Image Acquisition using TrueBack and Encase Imager	To acquire forensic images from storage media for investigation	CO1	A	2
3	Analyze an Image file using Cyber Check tool and FTK/ProDiscover, Familiarisation of Report Module	To analyte forensic images and generate reports	CO1	A	2
4	Data Hiding Techniques using Hex Workshop/WinHex	To explore data hiding and steganography at binary level	CO1	A	2
5	Analyse Windows Registry Files using FRAN / ProDiscover	To investigate Windows registry for forensic evidence	CO1	A	2
6	Acquisition and Analysis of Live Data using WinLift, Volatility Framework, PS Tools	To perform live data acquisition and volatile memory analysis	CO1	A	2
7	Familiarisation with CRYPTOOL and OpenSSL	To gain exposure to basic cryptographic toolkits	CO1	A	2
8	AES (128-bit), RSA, Secure Hash Algorithm	To implement standard cryptographic algorithms	CO1 CO2	A	2
9	Digital Signature Algorithm, Diffie–Hellman Key Exchange	To implement authentication and secure key exchange	CO4	A	2
10	Elliptic Curve Cryptography	To implement ECC for	CO4	A	2

		secure communication			
11	Secure Mail using PGP and S/MIME	To implement secure email communication protocols	CO4 CO5	E	2
12	Familiarization with Wireshark, Backtrack (Kali Linux)	To analyse packets and security threats using network tools	CO1, CO3	An	2
13	Program to send encrypted string via Bluetooth (PC client → Mobile server)	To implement secure data transfer over wireless communication	CO2 CO4	A	2
14	Program for Distributed Denial of Service (DDoS)	To simulate and understand DoS/DDoS attacks	CO3	An	2
15	SQL Injection	To demonstrate and mitigate SQL injection attacks	CO3 CO4	An	2

SUGGESTED LEARNING RESOURCES			
Text Book			
Sl. No.	Title of Book	Author	Publication
1	Guide to Computer Forensics and Investigations (6th Edition)	Nelson, Phillips, Enfinger, Steuart	Cengage Learning
2	Windows Forensic Analysis DVD Toolkit (2nd Edition)	Harlan Carvey	Syngress Inc., 2009
Reference			
Sl. No.	Title of Book	Author	Publication
1	Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry	Harlan Carvey	Syngress
2	Linux Administration: A Beginner's Guide (6th Edition)	Wale Soyinka	McGraw-Hill Education
3	UNIX Network Programming, Volume I	W. Richard Stevens	Pearson Education
4	Internetworking with TCP/IP, Volume III	D. E. Comer	Pearson Education
5	Java Cryptography Extensions: Practical Guide for Programmers	Jason Weiss	Morgan Kaufmann Publishers
Web Resource			
1	NIST Computer Security Resource Center		
2	CERT-In (Indian Computer Emergency Response Team)		
3	OWASP (Open Web Application Security Project)		
4	Kali Linux Official Documentation		

ASSESSMENT PATTERN	
Assessment	**Marks**
Continuous Internal Assessment	**100**

Continuous Lab Evaluation	60
Internal Examination	40
Total	**100**

SEMESTER II

APPROVAL

This is to certify that the syllabus titled "syllabus for M.Tech Cyber Security" implemented from the academic year **2025–2026**, is prepared in accordance with the regulations, academic framework, and Outcome Based Education guidelines prescribed by the Institution and the affiliating University.

The syllabus has been **discussed, reviewed, and approved** by the following statutory bodies.

BOARD OF STUDIES (BOS)

Approved in the Board of Studies Meeting of the M.Tech Cyber Security held on 03/12/2025

Chairperson, BoS

Name: Dr. Vicky Nair Designation: HoD Department of Cyber Security

Signature: Date: 10/12/2025

ACADEMIC COUNCIL

Approved by the **Academic Council** in its meeting held on 29/12/2025

PRINCIPAL

Recommended for implementation from the Academic year 2025-2026.

Name: Dr. Neelakandan P C

Signature: Date:

SEMESTER II

CURRICULUM

SLOT	COURSE CATEGORY	COURSE CODE	COURSE NAME	L	T	J	P	S	C
A	DC	M250902/CN200A	ADVANCED DATA STRUCTURES AND ALGORITHMS	3	0	0	0	2	3
B	PC	M250102/CY200B	NETWORK SECURITY	3	0	0	0	1	3
C	PE	M250102/CY23*C	PROGRAM ELECTIVE III	3	0	0	0	2	3
D	PE	M250102/CY24*D	PROGRAM ELECTIVE IV	3	0	0	0	2	3
E		M250102/CY25*E	INDUSTRY/INTERDISCIPLINARY ELECTIVE	3	0	0	0	2	3
S	PROJECT	M250902/CN100S	MINI PROJECT	2	0	0	0	1	2
T	LAB2	M250102/CY230T	COMPUTING LAB 2	0	0	0	2	1	1
*(**L**- Lecture, **T**-Tutorial, **J**-Project, **P**-Practical, **S**-Self-learning & Team Work, **C**- Credit)*									

COURSE DESCRIPTION							
Regulation	**2025**	**L-T-J-P-S**	**3-0-0-0-2**	**Version**	**25/0**	**Credits**	**3**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)							
Course Code		**COURSE NAME**					**Course Category**
M250902/CN200A		**ADVANCED DATA STRUCTURES AND ALGORITHMS**					**DC**

COURSE OBJECTIVES	
1	Strengthen understanding of algorithmic design principles and performance analysis.
2	Introduce advanced data structures for efficient data organization and manipulation.
3	Apply amortized analysis techniques in evaluating algorithm efficiency.
4	Explore string matching, network flow, and graph-based algorithmic solutions.
5	Familiarize students with probabilistic and approximation algorithms for complex problems.
6	Enable design and implementation of optimized software solutions using advanced algorithms.

COMPETENCY STATEMENTS	
CC1	Demonstrate the ability to analyze and design efficient algorithms using advanced data structures such as heaps, disjoint sets, and graphs by applying amortized, probabilistic, and approximation techniques for optimal computational performance.
CC2	Develop, implement, and evaluate software solutions for complex real-world problems using suitable algorithmic strategies, ensuring correctness, efficiency, and scalability.

COURSE OUTCOMES			
Course Outcomes (CO): At the end of this course, learners will be able to:			
CO	**CO Statement**	**Competency Mapping**	**Cognitive ©**
CO1	Analyse the relevance of amortized analysis and applications. (Cognitive Level: Apply)	CC1	U
CO2	Illustrate string matching algorithms. (Cognitive Level: Apply)	CC1	A
CO3	Illustrate advanced data structures like Binomial heap, Fibonacci heap Disjoint set and string-matching algorithms. (Cognitive Level: Apply)	CC1	A
CO4	Illustrate network flow algorithms and applications. (Cognitive Level: Apply)	CC1	An
CO5	Make use of probabilistic algorithms and approximation algorithms in computing. (Cognitive Level: Apply)	CC1	An
CO6	Design, develop and implement software using advanced data structures and algorithms. (Cognitive Level: Create))	CC2	C
Cognitive (Revised blooms Level): *-* ***R****: Remember;* ***U****: Understand;* ***A****: Apply;* ***An****: Analyse;* ***E****: Evaluate;* ***C****: Create*			

CO	**PROGRAM OUTCOMES (PO) CORRELATION MATRIX**						
	PO						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1	2	-	2	2	2	1	-
2	2	-	2	3	2	1	-
3	3	-	3	3	3	1	-
4	3	-	3	3	3	1	-
5	3	-	3	2	3	1	-
6	3	3	3	3	3	1	3
Correlation levels: 1 – Low; 2 – Medium; 3 – High; No Correlation – "-"							

TEACHING AND ASSESSMENT SCHEME													
Teaching Scheme / Week				**Self-Learning (S) / Semester**	**Total Hours / Semester**	**Credits C**	**Examination Scheme**						
							Theory			**Practical**			**Total**
L	**T**	**J**	**P**				**CIA**	**ESE**	**Total**	**CIA**	**ESE**	**Total**	
3	0	0	0	30	70	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	Amortized analysis and String matching	Overview of asymptotic notations and complexity analysis, Amortized analysis – aggregate analysis, accounting method, potential method. String matching – introduction, Rabin-Karp algorithm, Knuth-Morris-Pratt algorithm.	8
2	Advanced data structures	Overview of binary heap operations, Binomial tree and heap, Binomial heap operations, Fibonacci heap structure, Fibonacci heap operations, Disjoint set – overview, linked list representation, disjoint set forests.	9
3	Network flow	Network flow properties, examples, residual network, augmenting path, cut of network, maxflow-mincut theorem, Ford-Fulkerson algorithm, Edmonds- Karp algorithm, maximum bipartite matching.	8
4	Probabilistic algorithms	Introduction, types of probabilistic algorithms, Numerical algorithms – Numerical integration, Probabilistic counting, Monte-Carlo algorithms – Verifying matrix multiplication. Number theory fundamentals – modular arithmetic, modular exponentiation, Euler's Theorem and Fermat's Theorem, Primality testing – Miller-Rabin test. Las Vegas algorithms – Probabilistic selection and quick sort.	7
5	Approximation algorithms	Introduction, Vertex-cover problem, Traveling salesman problem, Set- covering problem, Subset-sum problem.	8

SELF-LEARNING / TEAM WORK		
Sl. No	Self-learning / Team Work Description	Hrs/ Semester
1	Micro project/Course based project	20
2	Regularization Techniques, Graphical Models, Gaussian mixture models	6
3	Seminar	4

SUGGESTED LEARNING RESOURCES			
Text Book			
Sl. No.	Title of Book	Author	Publication
1	Introduction to Algorithms	Thomas H Cormen	MIT Press.
2	Algorithm Design	Jon Kleinberg, Eva Tardos	Pearson Education.
Reference			
Sl. No.	Title of Book	Author	Publication
1	Design and Analysis of Algorithm	S. Sridhar	Oxford University Pres

2	Fundamentals of Algorithms	E. Horowitz, S. Sahni, S. Rajasekaran	Universities Press
3	*Design and Analysis of Algorithms	Alfred V. Aho, John E. Hopcroft, Jeffrey D. Ullman.	Pearson Education
Web Resource			
1	*Algorithms Specialization*, Prof. Tim Roughgarden, Coursera, Stanford University.		
2	*Algorithms, Part I & II*, Prof. Robert Sedgewick & Kevin Wayne, Coursera, Princeton University.		

DETAILED SYLLABUS

Module	Topic	Mode of Delivery	Cos	Learning Domain Level C	Hrs
1	Overview of asymptotic notations and complexity analysis.	Lecture	CO1	U	1
	Amortized analysis–aggregate analysis	Lecture	CO1	U	1
	Accounting method	Lecture	CO1	A	1
	Potential method	Lecture	CO1	A	1
	String matching–introduction	Lecture	CO1	A	1
	Rabin-Karp algorithm	Lecture	CO1	U	1
	Knuth-Morris-Pratt algorithm (1)	Lecture	CO2	A	1
	Knuth-Morris-Pratt algorithm (2)	Lecture	CO2	A	1
2	Overview of binary heap operations	Self-Learning	CO2	U	1
	Binomial tree and heap	Lecture	CO2	U	1
	Binomial heap operations (1)	Lecture	CO2	A	1
	Binomial heap operations (2)	Lecture	CO2	A	1
	Fibonacci heap structure	Lecture	CO2	A	1
	Fibonacci heap operations (1)	Lecture	CO2	A	1
	Fibonacci heap operations (2)	Lecture	CO2	A	1
	Disjoint set–overview, LinkedList representation	Lecture	CO2	U	1
	Disjoint set forests	Lecture	CO2	A	1
3	Network flow properties, examples	Lecture	CO3	U	1
	Residual network, augmenting path, cut of network	Lecture	CO3	A	1
	Max-flow,min-cut theorem	Lecture	CO3	A	1
	Ford-Fulkerson algorithm	Lecture	CO3	A	1
	Edmonds-Karp algorithm	Self-Learning	CO3	U	1
	Maximum bipartite matching	Self-Learning	CO3	A	1
4	Introduction, types of probabilistic algorithms	Lecture	CO4	A	1
	Numerical algorithms–Numerical integration, Probabilistic counting	Lecture	CO4	A	1
	Monte-Carlo algorithms–Verifying matrix multiplication	Lecture	CO4	U	1
	Number theory fundamentals–modular arithmetic, modular exponentiation	Self-Learning	CO4	U	1
	Euler's Theorem and Fermat's Theorem	Self-Learning	CO4	U	1
	Primality testing–Miller-Rabin test (1)	Self-Learning	CO4	A	1
	Primality testing–Miller-Rabin test (2)	Lecture	CO4	A	1
	Las Vegas algorithms–Probabilistic selection and quick sort	Lecture	CO4	A	1
	Introduction	Lecture	CO5	A	1

5			CO6		
	Vertex-cover problem	Lecture	CO5 CO6	A	1
	Traveling-salesman problem	Lecture	CO5 CO6	A	1
	Set-covering problem.	Lecture	CO5 CO6	U	1
	Subset-sum problem (1).	Lecture	CO5 CO6	U	1
	Subset-sum problem (1)	Lecture	CO5 CO6	U	1

1

TABLE OF SPECIFICATIONS (ToS) FOR QUESTION PAPER DESIGN

Module	Module Title	Teaching Hours	Distribution of Marks (Revised Bloom's Level)						Total Marks
			R	U	A	An	E	C	
1	Advanced Data Structures – Heaps, Disjoint Sets, Treesnet	8	✓	✓					12
2	Amortized Analysis and Algorithm Complexity	9		✓					12
3	Graph Algorithms – Network Flow, Cut of Network, Shortest Path	8		✓	✓				12
4	String Matching and Dynamic Programming Algorithms	7		✓	✓				12
5	Probabilistic and Approximation Algorithms	7		✓	✓				12

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**

SECOND SEMESTER M. TECH DEGREE (REGULAR) EXAMINATION, DECEMBER 2025(2025 SCHEME)			
Course Code:	**M250902/CN200A**		
Course Name:	**ADVANCED DATA STRUCTURES AND ALGORITHMS**		
Max. Marks	**60**	**Duration**:	2 hours 30 minutes

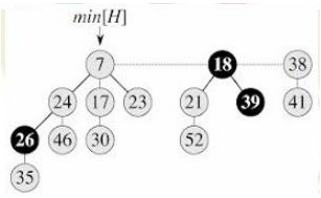
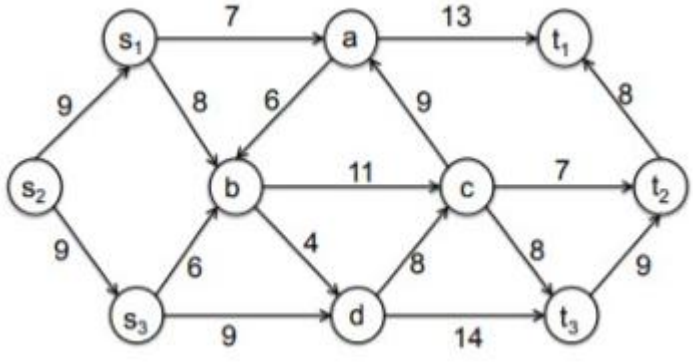
PART A

(Answer all questions. Each question carries 5 marks)

No.	*Question*	*CO*	*Marks*
1	Explain accounting method of amortized analysis with a suitable example.	CO1	(5)
2	Explain the algorithm for uniting two binomial heaps and analyse the running time	CO2	(5)
3	Maximum matching in a bipartite graph G corresponds to a maximum flow in its corresponding flow network G'. Comment on this statement. Explain how maximum flow problem can be used to solve maximum bipartite matching problem.	CO3	(5)
4	Explain the probabilistic algorithm for verifying matrix multiplication problem	CO4	(5)
5	Explain the approximation algorithm for traveling salesperson problem	CO5	(5)

PART B

(Answer any 5 questions. Each question carries 7 marks)

No.	*Question*	*CO*	*Marks*
6	Describe Knuth-Morris-Pratt algorithm and illustrate using given text T = AABAACAADAABAABA and pattern P = AABA	CO1	(7)
7	a) Using potential method, compute the amortized cost of incrementing a binary counter. b) Suppose we perform a sequence of n operations on a data structure in which the i^{th} operation costs i if i is an exact power of 2, and 1 otherwise. Use accounting method of amortized analysis to determine the amortized cost per operation.	CO1	(7)
8	a) Explain how disjoint set data structure is used to find connected components on an undirected graph b) Show the binomial heap that results when a node with key 11 is deleted from the binomial heap shown in figure.	CO2	(7)
9	a) Explain the structure of Fibonacci heap. b) Apply extract minimum operation on the Fibonacci heap shown in figure and show the result 	CO3	(7)
10	Describe Ford-Fulkerson algorithm and apply on the following network. Also obtain minimum cut across the network. 	CO4	(7)
11	a) Apply Miller-Rabin algorithm to test whether the number 34 1is prime or not. (4) b) Explain probabilistic quick sort algorithm. (3)	CO5	(7)

12	a) Describe polynomial-time approximation scheme and fully polynomial-time approximation scheme. (3) b) Give an example of a graph for which APPROX-VERTEX COVER always yields a suboptimal solution(4)	CO6	(7)

COURSE DESCRIPTION					
Regulation	**2025**	**L-T-J-P-S**	**3-0-0-0-2**	**Credits**	**3**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)					
Course Code	**Course Name**				**Course Category**
M250102/CY200B	**NETWORK SECURITY**				**PC**

COURSE OBJECTIVES	
1	To understand the fundamental principles of data and network security, including the concepts of Confidentiality, Integrity, and Availability (CIA Triad).
2	To learn the basic and advanced cryptographic techniques such as symmetric-key, asymmetric-key algorithms, hash functions, and digital signatures
3	To analyze the various threats and vulnerabilities present in computer networks and systems, including malware, denial-of-service, and intrusion attacks..
4	To explore the security protocols and mechanisms used at different layers of the network (IPSec, SSL/TLS, SSH) for secure data transmission
5	To develop practical skills in configuring security devices like Firewalls, Intrusion Detection Systems (IDS), and Virtual Private Networks (VPNs).

COMPETENCY & OUTCOMES		
Competency Statements	CC1	Demonstrate the ability to design, implement, and maintain a secure network infrastructure by applying cryptographic algorithms, defense mechanisms, and security protocols to ensure the Confidentiality, Integrity, and Availability of data and network resources.

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

CO	CO Statement	Competency Mapping	Cognitive ©
CO1	Analyze the key security issues and procedures in computer and mobile communication networks (Cognitive Knowledge Level: Analyze)	CC1	A
CO2	Implement the security at the physical level, operating system level and network level (Cognitive Knowledge Level: Apply)	CC1	A
CO3	Introduces the threats to computer networks through the exploitation of network infrastructure design weaknesses (Cognitive Knowledge Level: Analyze)	CC1	A
CO4	Analyze the security flaws in the network infrastructure protocol (Cognitive Knowledge Level: Evaluate)	CC1	A
CO5	Analyze the security flaws in the network infrastructure protocol (Cognitive Knowledge Level: Evaluate)	CC1	A

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

CO	Program Outcomes						
	PO						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1	2	-	3	2	2	1	-
2	2	-	3	3	3	1	-
3	3	-	3	3	3	1	-
4	3	2	3	3	3	2	-
5	3	2	3	3	3	2	3

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

TEACHING AND ASSESSMENT SCHEME													
Teaching Scheme / Week				Self-Learning (S) / Semester	Total Hours / Semester	Credits C	Examination Scheme						
							Theory			Practical			Total
L	T	J	P				CIA	ESE	Total	CIA	ESE	Total	
3	0	0	0	30 SECURITY OF CYBER PHYSICAL SYSTEM	90	3	40	60	100	0	0	0	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 Network Security	CIA in Network Security, Threats and attacks (Eavesdropping, Alteration, Denial-of-service, Masquerading, Repudiation, Correlation and trace back), Symmetric Key Cryptography, Public-key cryptography, Digital Signatures, Hash Functions, Message Authentication Codes, Digital Certificates, Passwords, Password Complexity, Social Engineering.	8
2	Physical Security and Operating System Security	Physical Security: Authentication, TEMPEST, RFID, Biometrics, Operating System Concepts and Buffer overflow, operating System Security, Application Program Security.	8
3	Malware, Email Security, IP Security	Malware: Insider Attacks, Malware, Privacy-Invasive Software, Counter measures Electronic Mail Security: Pretty good privacy, S/MIME.IP Security: Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations, Key management.	8
4	Network Security	Network Security: ARP, ICMP, Sniffing, IP Spoofing, TCP, UDP, NAT, TCP Session Hijacking, DoS, DNS, SSH, VPN, IPSec, SSL, Firewall, Wireless Security Multiplication of a point by a constant.	8
5	Web Security	Web Security: Web Security considerations, Secure Socket Layer and Transport layer Security, Secure Electronic Transaction. Firewalls, Packet filters, Application-Level Gateway, Encrypted Tunnels	8

SELF-LEARNING / TEAM WORK		
Sl. No	**Self-learning / Team Work Description**	**Hrs./Semester**
1	Study the basic concepts of cryptography — plaintext, ciphertext, encryption, and decryption.	2
2	Prepare a comparative study of symmetric and asymmetric key cryptography.	3
3	Programming Assignment – Implement Caesar Cipher and Vigenère Cipher in Python.	3
4	Case Study – Analyze real-world applications of symmetric encryption (e.g., AES).	3
5	Demonstration – Configure SSL/TLS for a sample web application.	3
6	Study the working of Diffie–Hellman key exchange protocol.	2
7	Programming Assignment – Implement RSA encryption and decryption using Python.	3

8	Prepare a report on hash functions and message authentication codes (MD5, SHA-256, HMAC).	3
9	Simulate network attacks such as ARP spoofing or DoS using tools like Wireshark or Kali Linux (demo-based).	3
10	Study session – Intrusion Detection and Prevention Systems (IDS/IPS) architecture.	3
11	Group Activity – Analyze a case of ransomware or phishing attack and present mitigation strategies.	3
12	Programming Task – Implement a simple authentication system using hashing and salting.	3
13	Prepare a short report on firewalls and packet filtering techniques.	2
14	Discussion – Study VPNs and secure tunneling protocols (IPSec, L2TP).	3
15	Research mini-topic – Blockchain security and its relevance to network trust models.	3
16	Practice problems and MCQs covering all modules for revision and peer discussion.	3

SUGGESTED LEARNING RESOURCES

Text Book

Sl. No.	Title of Book	Author	Publication
1	Introduction to Computer Security, ISBN-13: 978-0-321-51294-9, ISBN-10: 0-321-51294-4	Michael T. Goodrich & Roberto Tamassia	Pearson, 2011
2	Cryptography and Network Security	William Stallings	Pearson Education, 2014

Reference

Sl. No.	Title of Book	Author	Publication
1	Computer Networks: A System Approach 5th Edition	Larry Peterson and Bruce S Davisl	Elsevier-2014
2	Internetworking with TCP/IP, Principles, Protocols & Architecture (6th Edition,)	Douglas E Comer,	PHI– 2014.
3	Computer Networks, Protocols, Standards and Interfaces	Uyless Black	PHI

DETAILED SYLLABUS

Module	Topic	Mode of Delivery	Cos	Learning Domain Level	Hrs
				C	
1	CIA in Network Security	Lecture	CO1	A	1
	Threats and attacks	Lecture	CO1	A	1
	Symmetric Key Cryptography	Lecture	CO1	U	1
	Public-key cryptography	Lecture	CO1	U	1
	Digital Signatures	Lecture	CO1	U	1
	Hash Functions	Lecture	CO1	U	1
	Message Authentication Codes, Digital Certificates	Lecture	CO1	A	1
	Passwords, Password Complexity, Social Engineering	Lecture	CO1	A	1
2	Physical Security: Authentication	Lecture	CO2	U	1
	TEMPEST	Lecture	CO2	U	1
	Biometrics,	Lecture	CO2	U	1
	Operating system concepts	Lecture	CO2	A	1

	Buffer-overflow	Lecture	CO2	A	1
	Operating System Security	Lecture	CO2	A	1
	RFID	Lecture	CO2	A	1
	Application Program Security	Lecture	CO2	A	1
3	Malware, Privacy-Invasive Software	Lecture	CO3	A	1
	Countermeasures Electronic Mail Security	Lecture	CO3	A	1
	Pretty good privacy, S/MIME.	Lecture	CO3	A	1
	IP Security: Architecture,	Lecture	CO3	U	1
	Authentication Header	Lecture	CO3	U	1
	Encapsulating Security, Payload	Lecture	CO3	A	1
	Combining Security Associations, Key management	Lecture	CO3	A	1
4	ARP, ICMP	Lecture	CO4	U	1
	Sniffing, IP Spoofing	Lecture	CO4	U	1
	TCP, UDP	Lecture	CO4	A	1
	NAT, TCP Session Hijacking	Lecture	CO4	U	1
	DoS, DNS	Lecture	CO4	A	1
	SSH, VPN	Lecture	CO4	A	1
	IPSec, SSL	Lecture	CO4	U	1
	Firewall, Wireless security	Lecture	CO4	A	1
5	Web security considerations	Lecture	CO5	U	1
	Secure Socket Layer	Lecture	CO5	U	1
	Transport Layer Security	Lecture	CO5	A	1
	Secure Electronic Transaction	Lecture	CO5	U	1
	Firewalls	Lecture	CO5	A	1
	Packet filters	Lecture	CO5	A	1
	Application-Level Gateway	Lecture	CO5	U	1
	Encrypted Tunnels	Lecture	CO5	A	1

TABLE OF SPECIFICATIONS (ToS) FOR QUESTION PAPER DESIGN

Module	Module Title	Teaching Hours	Distribution of Marks (Revised Bloom's Level)						Total Marks
			R	U	A	An	E	C	
1	Introduction to Network Security – Security Attacks, Services, and Mechanisms	8	✓	✓					12
2	Symmetric Key Cryptography – DES, AES, Stream Ciphers	8	✓	✓	✓				12
3	Public Key Cryptography – RSA, Diffie–Hellman, Key Management	8	✓	✓	✓				12
4	Authentication, Integrity, and Hash Functions – MD5, SHA, HMAC, Digital Signatures	7	✓	✓	✓				12
5	Network Security Practices – Firewalls, IDS, VPN, IP Security, Web and Email Security	7	✓	✓	✓				12

This ToS shall be treated as a general guideline for students and teachers for distribution of marks.

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

SECOND SEMESTER M. TECH DEGREE (REGULAR) EXAMINATION, DECEMBER 2025 (2025 SCHEME)			
Course Code:	**M250102/CY200B**		
Course Name:	**NETWORK SECURITY**		
Max. Marks	**60**	**Duration**:	2 hours 30 minutes

PART A

(Answer all questions. Each question carries 5 marks)

No.		***Question***	***CO***	***Marks***
1		What is Network Security? How does network security work?	CO1	(4)
2		Explain Eavesdropping and Denial of Service	CO2	(4)
3		Write note on RFID.	CO3	(4)
4		Discuss ICMP and PGP.	CO4	(4)
5		What are Intrusion prevention systems (IPS)?	CO5	(4)

PART B

(Answer any 5 questions. Each question carries 7 marks)

No.	***Question***	***CO***	***Marks***
6	a) Write down the principles of security. (4) b) Discuss the role of digital signatures in modern communication. Also discuss the differences between the digital certificates with digital signatures in authentication. (3)	CO1	(7)
7	a) Write notes on the following (4) i. Repudiation ii. VPN iii. iii. Intrusion detection b) Discuss in detail the types of phishing attacks (3)	CO1	(7)
8	How do PGP create a secure network? Write the general structure of Private Key Ring used in Pretty Good Privacy (PGP).	CO3	(7)
9	Discuss the cryptographic algorithms used in S/MIME. Why S/MIME is better than MIME	CO3	(7)
10	Explain the sequence of steps used in Secure Socket Layer handshake protocol for establishing a new session. Draw a diagram which shows the action of Handshake Protocol	CO4	(7)
11	What is firewall? Describe how firewall can be used to protect the network?	CO5	(7)

COURSE DESCRIPTION					
Regulation	**2025**	**L-T-J-P-S**	**3-0-0-0-2**	**Credits**	**3**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)					
Course Code	**Course Name**				**Course Category**
M250102/CY231C	**SECURITY OF CYBER PHYSICAL SYSTEM**				**PROGRAMME ELECTIVE**

COURSE OBJECTIVES	
1	Develop technical proficiency in digital forensic tools and methodologies for evidence acquisition, analysis of cyber incidents (network/mobile/email), and anti-forensics detection.
2	Evaluate legal and governance frameworks to ensure cyber forensic investigations adhere to judicial standards and ethical guidelines.
3	Design and execute structured incident response procedures, including evidence preservation, reporting, and compliance with organizational policies.

COMPETENCY & OUTCOMES		
Competency Statements	CC1	Conduct forensic investigations using industry-standard methodologies, tools, and protocols for digital evidence acquisition, analysis, and reporting.
	CC2	Apply legal and governance frameworks to cyber forensic practices, ensuring compliance with incident response policies, IT laws, and ethical guidelines.

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

CO	CO Statement	Competency Mapping	Cognitive ©
CO1	Use Embedded system concepts to solve real word problems. (Cognitive Knowledge Level: Apply)	CC2	An
CO2	Present solution to automated systems to make life easier. (Cognitive Knowledge Level: Apply)	CC1	A
CO3	Illustrate concepts of embedded systems and microcontroller to enhance existing systems. (Cognitive Knowledge Level: Evaluate)	CC1	A
CO4	Develop concepts, logics towards solving a unknown problem in research and industry. (Cognitive Knowledge Level: Analyze)	CC1	An

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

CO	Program Outcomes						
	PO						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1	3	-	3	2	-	-	-
2	3	-	3	3	2	-	-
3	3	-	3	3	3	-	-
4	1	-	2	3	2	-	-

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

TEACHING AND ASSESSMENT SCHEME													
Teaching Scheme / Week				**Self-Learning (S) / Semester**	**Total Hours / Semester**	**Credits C**	**Examination Scheme**						
							Theory			**Practical**			**Total**
L	**T**	**J**	**P**				**CIA**	**ESE**	**Total**	**CIA**	**ESE**	**Total**	
3	0	0	0	25	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	Cyber-physical Systems and their security risks	Architecture, characteristics of cps, protections against natural events and accidents, Protections Against Natural Events and Accidents, security and privacy concerns.	9
2	Cybersecurity Terminology and Frameworks	Terminology: Core Terminology, Scope, Assets, confidentiality, Integrity, Availability. Risk Assessment Terminology: Threats, Vulnerabilities, Probability, Impact	8
3	Crosscutting security	preventing attacks, detecting attacks, mitigating attacks. Policy and political aspects of cps security – incentives and regulation, cyber-conflict, industry practices and standards.	11
4	Security of Cyber-Physical Systems	Introduction to CPS Securities, Basic Techniques in CPS Securities, Cyber Security Requirements, Attack Model and Countermeasures, Advanced Techniques in CPS Securities	7
5	CPS Application	Health care and Medical Cyber-Physical Systems, Smart grid and Energy Cyber Physical Systems, WSN based Cyber-Physical Systems, Smart Cities guidelines for writing, generating report findings with forensics software tools.	5

SELF-LEARNING / TEAM WORK		
Sl. No	**Self-learning / Team Work Description**	**Hrs/Semester**
1	Develop a conceptual understanding of network architectures, protocols, and communication models necessary for secure system design. https://www.cybrary.it/skill-paths/network-fundamentals	10
2	Apply cybersecurity principles to evaluate threats, recognize vulnerabilities, and implement basic security controls in real-world contexts. https://www.cybrary.it/skill-paths/cybersecurity-fundamentals	10
3	Cyber Security Tools, Techniques, and Counter Measures – Course	10

SUGGESTED LEARNING RESOURCES			
Text Book			
Sl. No.	Title of Book	Author	Publication
1	Cyber Security for Cyber Physical Systems	Saqib Ali, Taiseera Al Balushi, Zia Nadir, and Omar Khadeer Hussain	Springer International Publishing, 2018.
2	Cyber Physical Systems – Advances and Applications	Anitha Kumari K. and Avinash Sharma	Bentham Science Publishers, 2024
Reference			
Sl. No.	Title of Book	Author	Publication
1	Security and Resilience of Cyber Physical Systems	Krishan Kumar, Sunny Behal, Abhinav Bhandari, Sajal Bhatia.	Chapman & Hall, 2022.
2	Security Analytics: A Data Centric Approach to Information Security	Mehak Khurana and Shilpa Mahajan	CRC Press LLC, 2022
Web Resource			
1	What Is Cybersecurity? | IBM		
2	Cybersecurity Framework | NIST – National Institute of Standards and Technology		
3	Cybersecurity Best Practices | Cybersecurity and Infrastructure Security Agency CISA		

DETAILED SYLLABUS					
Module	Topic	Mode of Delivery	Cos	Learning Domain Level C	Hrs
1	Architecture	Lecture	CO1	A	1
	protections against natural events and accidents	Lecture	CO1	A	1
	Protections Against Natural Events and Accidents	Lecture	CO1	A	1
	Layers of protection for safety-critical ICS.	Lecture	CO1	A	1
	Security and privacy concerns.	Lecture	CO1	A	1
	Attacks Against CPSs	Lecture	CO1	A	1
	Attack Points in a CPS.	Lecture	CO1	A	1
	High-Profile, Real-World Attacks Against CPSs	Lecture	CO1	A	1
2	Cybersecurity Terminology and Frameworks	Lecture	CO2	A	1
	Terminology	Lecture	CO2	A	1
	Core Terminology, Scope	Lecture	CO2	A	1
	Assets, Confidentiality	*Lecture*	CO2	A	1
	Integrity, Availability	Lecture	CO2	A	1
	Risk Assessment Terminology	Lecture	CO4	C	1
	Threats, Vulnerabilities,	Lecture	CO4	C	1
	Probability, Impact	Lecture	CO4	C	1
3	Crosscutting security – Introduction	Lecture	CO3	An	1
	Preventing attacks	Lecture	CO3	An	1
	detecting attacks	Lecture	CO3	An	1
	Remote Attestation	Lecture	CO3	An	1
	mitigating attacks 1	Lecture	CO3	An	1
	Policy and political aspects of cps security 1	Lecture	CO3	An	1
	Cyber-conflict	Lecture	CO4	C	1
	Industry practices and standards	Lecture	CO4	C	1
4	Introduction	Lecture	CO5	E	1
	Introduction to CPS Securities	Lecture	CO5	E	1
	Basic Techniques in CPS Securities	Lecture	CO5	E	1
	Techniques	Lecture	CO5	E	1
	Cyber Security Requirements	Lecture	CO5	E	1
	Attack Model	Lecture	CO5	E	1
	Countermeasures	Lecture	CO5	E	1
	Advanced Techniques in CPS Securities	Lecture	CO5	E	1
5	Health care	Lecture	CO5	E	1
	Medical Cyber	Lecture	CO5	E	1
	Physical Systems	Lecture	CO5	E	1
	Smart grid	Lecture	CO5	E	1
	Energy Cyber Physical Systems	Lecture	CO5	E	1
	WSN based Cyber	Lecture	CO5	E	1
	Physical Systems	Lecture	CO5	E	1
	Smart Cities	Lecture	CO5	E	1

TABLE OF SPECIFICATIONS (ToS) FOR QUESTION PAPER DESIGN									
Module	Module Title	Teaching Hours	Distribution of Marks (Revised Bloom's Level)						Total Marks
			R	U	A	An	E	C	
1	Foundations of Information Security	6		✓	✓				12
2	Cryptography and Secure Communication	10		✓	✓				12
3	Security Technologies and Tools	11		✓	✓	✓			12
4	Governance and Risk Management	7		✓	✓		✓		12
5	Information Security Auditing	6		✓	✓		✓		12
This ToS shall be treated as a general guideline for students and teachers for distribution of marks.									

Assessment	Marks
Continuous Internal Assessment	**40**
Learning Activity	5
Internal Examination	10
Course Project	20
End Semester Examination	**60**
Total	**100**

SECOND SEMESTER M. TECH DEGREE (REGULAR) EXAMINATION, DECEMBER 2025 (2025 SCHEME)			
Course Code:	**M250102/CY231C**		
Course Name:	**SECURITY OF CYBER PHYSICAL SYSTEM**		
Max. Marks	**60**	**Duration**:	2 hours 30 minutes

PART A			
(Answer all questions. Each question carries 5 marks)			
No.	***Question***	***CO***	***Marks***
1	What all are the three most common requirements of cyber security?	CO1	(5)
2	For each identified risk, an organization can consider a number of possible responses. Explain.	CO2	(5)
3	Give details about the Risk Assessment Terminology used in Physical Cyber Security.	CO3	(5)
4	Define the term Remote Attestation.	CO4	(5)
5	Transduction attacks represent one of the novel ways in which CPS security is different from classical IT security. Explain	CO5	(5)
PART B			
(Answer any 5 questions. Each question carries 7 marks)			
No.	***Question***	***CO***	***Marks***
6	Illustrate the General architecture of cyber-physical systems and explain the characteristics of CPS.	CO1	(7)
7	Differentiate the two main types of mitigating technologies: i) proactive ii) reactive	CO1	(7)
8	Give details about the Risk Assessment Terminology used in Physical Cyber Security	CO2	(7)
9	Summarize some of the industry- and government-led efforts to try to improve the security of CPSs, and how to leverage the new field of CPS security for attacks and wars.	CO3	(7)
10	Define about the Security of Cyber-Physical Systems.	CO4	(7)
11	Write a note about the fundamental based Cyber-Physical Systems	CO4	(7)
12	Can a cyber-physical system have a soul ultimately? Why? How? Why not?	CO5	(7)

COURSE DESCRIPTION					
Regulation	**2025**	**L-T-J-P-S**	**3-0-0-0-2**	**Credits**	**3**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)					
Course Code	**Course Name**				**Course Category**
M250102/CY232C	**BIOMETRIC SECURITY**				**PROGRAMME ELECTIVE**

COURSE OBJECTIVES	
1	Develop a comprehensive understanding of biometric principles, technologies, and performance metrics, distinguishing them from traditional authentication methods.
2	Gain practical knowledge of key biometric modalities—fingerprint, face, iris, ear, and behavioral traits—covering data acquisition, feature extraction, matching, and evaluation processes.
3	Examine the vulnerabilities, attacks, and defense mechanisms in biometric systems, along with industry standards, databases, and ethical considerations in real-world applications.

COMPETENCY & OUTCOMES		
Competency Statements	CC 1	Understand and evaluate biometric principles, technologies, and performance metrics to differentiate biometric systems from traditional authentication methods.
	CC 2	Apply various biometric recognition techniques such as fingerprint, face, iris, and behavioral biometrics to design and assess effective identity verification systems.

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

CO	CO Statement	Competency Mapping	Cognitive ©
CO1	Identify and explain biometric fundamentals, technologies, and performance metrics distinguishing biometrics from traditional systems. (Cognitive Knowledge Level: Understand)	CC1	U
CO2	Apply fingerprint and palm print recognition techniques for feature extraction, matching, and verification in real-world applications. (Cognitive Knowledge Level: Apply)	CC2	A
CO3	Analyze facial, signature, and keystroke recognition methods to interpret their roles in user identification and authentication. (Cognitive Knowledge Level: Analyse)	CC2	An
CO4	Examine iris, ear, gait, and hand geometry features to understand segmentation, normalization, and performance evaluation processes.(Cognitive Knowledge Level: Analyse)	CC2	An
CO5	Evaluate the security, privacy, and adversary attack models in biometric systems, including biometric standards and databases. (Cognitive Knowledge Level: Evaluate)	CC3	E

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

CO	Program Outcomes						
	PO						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1	3	2					1
2	3	2	3	2	2		
3	3	3	2	2	2		1
4	3	3	2	3	2		
5	3	3	2	3	2	3	2
Correlation levels: 1 – Low; 2 – Medium; 3 – High; No Correlation – "-"							

TEACHING AND ASSESSMENT SCHEME												
Teaching Scheme / Week				**Self-Learning (S) / Semester**	**Total Hours / Semester**	**Credits C**	**Examination Scheme**					
L	**T**	**J**	**P**				**Theory**			**Practical**			**Total**
							CIA	**ESE**	**Total**	**CIA**	**ESE**	**Total**	
3	0	0	0	30	70	3	40	60	100	0	0	0	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 Biometrics	Biometric fundamentals – Biometric technologies – Biometrics Vs traditional techniques –Characteristics of a good biometric system – Benefits of biometrics – Key biometric processes: verification, identification and biometric matching – Performance measures in biometric systems, FAR, FRR, FTE rate, EER and ATV rate, Applications of Biometric Systems, Security and Privacy Issues, Physiological Biometrics and Behavioral Biometrics.	9
2	Fingerprint Recognition	Fingerprint recognition: Friction ridge patterns, Acquisition, Feature extraction, matching, indexing, synthesis, palm print.	8
3	Face Recognition	Face recognition: Introduction, image acquisition, face detection. Feature extraction of face recognition, matching, heterogeneous face recognition. Signature-scan, Keystroke Scan– components, working principles	11
4	Iris and Ear Recognition	Iris recognition, Image acquisition, iris segmentation, normalization. Encoding and matching, quality assessment, performance evaluation, Ear detection and recognition – challenges, gait and hand geometry. Feature extraction and matching	7
5	Hardware Security	Internet of things (IoT) ecosystem and security vulnerabilities-Attacks on cyber-physical systems-Reverse Engineering-Side-channel attacks Intellectual Property (IP) piracy-Hardware Trojan-Electronic counterfeiting, Hardware security primitives-Physical Unclonable Function (PUF) Characterizing PUFs: Strong vs. weak PUFs, Random number generator (RNG),Characterizing RNGs: Pseudo vs True RNG	5

SELF-LEARNING / TEAM WORK		
Sl. No	**Self-learning / Team Work Description**	**Hrs/Semester**
1	IT Act 2000: Key sections, amendments, and relevance to modern cybercrimes	2
2	Cybercrimes: Types (phishing, ransomware, identity theft) and case studies	1
3	Cybersecurity governance: Steps to protect ICT infrastructure	1
4	Social media forensics: Legal challenges & evidence collection	1
5	Incident Response Lifecycle (NIST SP 800-61)	1
6	IR Team Roles & Tools: Autopsy, FTK Imager	2
7	Evidence Handling: Chain of custody, volatile data collection	2
8	Forensic Acquisition Methods: Disk imaging (dd/FTK)	2

9	Data Storage Formats (AFF4, E01) & Encryption (BitLocker)	2
10	Forensic Tools: Autopsy (open-source) vs. EnCase (proprietary)	2
11	Lab Requirements & Skill Development	2
12	Network Artifacts: ICMP attacks, drive-by downloads	2
13	Mobile Forensics: Acquisition (ADB, Cellebrite)	2
14	Email Header Analysis: Tracing origins, identifying spoofing	3
15	Anti-Forensics Techniques: Steganography (Silent Eye), data wiping	2
16	Detection Tools: Steg detect, VeraCrypt analysis	2
17	Forensic Report Writing: Structure, tools (Magnet REPORT)	1

SUGGESTED LEARNING RESOURCES

Text Book

Sl.No.	Title of Book	Author	Publication
1	Introduction to Biometrics	Anil K. Jain, Arun A. Ross, Karthik Nandakumar	Springer,2011.
2	Handbook of Biometrics	Jain, P. Flynn, A. Ross	Springer, 2008

Reference

Sl.No.	Title of Book	Author	Publication
1	Biometric Technologies and Verification Systems	John R. Vacca	Elsevier, 2007
2	"Biometrics – Identity Verification in a Networked World"	Samir Nanavati, Michael Thieme, Raj Nanavati,	Wiley-dream tech India Pvt Ltd, New Delhi, 2003
3	"Biometrics for Network Security"	Paul Reid	Pearson Education, New Delhi, 2004

Web Resource

1	https://www.nist.gov/cyberframework
2	https://www.cert-in.org.in/
3	https://www.cybok.org/

DETAILED SYLLABUS

Module	Topic	Mode of Delivery	Cos	Learning Domain Level C	Hrs
1	Introduction to Biometrics – Definition, Characteristics, and Scope	Lecture	CO1	U	1
	Biometric System Components – Sensor, Feature Extraction, Matcher, Decision Module	Lecture	CO1	U	1
	Performance Measures – FAR, FRR, EER, ROC Curve	Lecture	CO1	U	1
	Applications and Security Issues in Biometric Systems	Lecture	CO1	U	1
2	Fingerprint Recognition – Patterns, Minutiae Features, Acquisition Techniques	Lecture	CO2	U	1
	Fingerprint Feature Extraction and Matching	Lecture	CO2	A	1

	Algorithms				
	Palm Print Recognition – Pre-processing and Feature Extraction	Lecture	CO2	A	1
3	Face Recognition – Detection, Alignment, and Feature Representation	Lecture	CO3	U	1
	Heterogeneous Face Recognition and Challenges	Lecture	CO3	A	1
	Signature and Keystroke Dynamics – Feature Extraction and Classification	Lecture	CO3	A	1
4	Iris Recognition – Segmentation, Normalization, and Encoding Techniques	Lecture	CO4	U	1
	Ear Recognition – Feature Extraction and Matching	Lecture	CO4	U	1
	Gait and Hand Geometry Recognition – Feature Parameters and Applications	Lecture	CO4	A	1
5	Security of Biometric Systems – Adversary Attacks and Countermeasures	Lecture	CO5	U	1
	Biometric Standards and Databases (ISO/IEC 19794)	Lecture	CO5	U	1
	Privacy and Ethical Issues in Biometrics	Lecture	CO5	A	1

TABLE OF SPECIFICATIONS (ToS) FOR QUESTION PAPER DESIGN

Module	Module Title	Teaching Hours	Distribution of Marks (Revised Bloom's Level)						Total Marks
			R	U	A	An	E	C	
1	Biometric Fundamentals & Performance (FAR/FRR/EER, ROC, Applications)	8		✓	✓	✓			12
2	Fingerprint & Palm Print (Acquisition, Feature Extraction, Matching)	8		✓	✓	✓			12
3	Face, Signature & Keystroke (Detection, Features, Classification)	9		✓	✓	✓			12
4	Iris, Ear, Gait & Hand Geometry (Segmentation, Normalization, Encoding)	8		✓	✓	✓			12
5	Security, Attacks, Standards, Databases, Privacy & Ethics	7		✓	✓	✓	✓		12
This ToS shall be treated as a general guideline for students and teachers for distribution of marks.									

Assessment	**Marks**
Continuous Internal Assessment	**40**
Learning Activity	15
Internal Examination	10
Course Project	15
End Semester Examination	**60**
Total	**100**

SECOND SEMESTER M. TECH DEGREE (REGULAR) EXAMINATION, DECEMBER 2025 (2025 SCHEME)			
Course Code:	**M250102/CY232C**		
Course Name:	**BIOMETRIC SECURITY**		
Max. Marks	**60**	**Duration**:	2 hours 30 minutes

PART A

(Answer all questions. Each question carries 5 marks)

No	***Question***	***CO***	***Marks***
1	Define Biometrics. Explain the basic components of a biometric system.	CO1	(5)
2	Describe how performance of a biometric system is evaluated using FAR, FRR, and EER.	CO2	(5)
3	Explain the process of fingerprint feature extraction and matching with a suitable example.	CO3	(5)
4	Discuss the major challenges in face recognition systems under varying lighting and pose conditions.	CO4	(5)
5	Describe the ethical and privacy concerns related to the use of biometric data in security systems.	CO5	(5)

PART B

(Answer any 5 questions. Each question carries 7 marks)

No	***Question***	***CO***	***Marks***
6	With a neat diagram, explain the general architecture and workflow of a fingerprint recognition system.	CO2	(7)
7	Discuss various feature extraction and encoding techniques used in iris recognition systems.	CO4	(7)
8	Compare and contrast face, signature, and keystroke recognition techniques with respect to accuracy and usability.	CO3	(7)
9	Explain how multimodal biometric systems overcome the limitations of unimodal systems.	CO1	(7)
10	Analyze the types of adversary attacks in biometric systems and the mechanisms used for their prevention.	CO5	(7)
11	Describe biometric standards such as ISO/IEC 19794 and their significance in interoperability.	CO5	(7)
12	Explain the role of machine learning in improving the performance of modern biometric recognition systems.	CO3	(7)

****

COURSE DESCRIPTION					
Regulation	**2025**	**L-T-J-P-S**	**3-0-0-0-2**	**Credits**	**3**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)					
Course Code	**Course Name**				**Course Category**
M250102/CY233C	**STEGANOGRAPHY AND MALWARE ANALYSIS**				**PROGRAMME ELECTIVE**

COURSE OBJECTIVES	
1	To provide in-depth understanding of steganography concepts, techniques, and detection methods used for covert communication and malware concealment.
2	To equip students with the knowledge and skills required for program analysis, reverse engineering, and malware behavior investigation using real-world tools.
3	To enable learners to analyze and evaluate malware persistence, execution, and evasion mechanisms to design effective detection and defense strategies.

COMPETENCY & OUTCOMES		
Competency Statements	CC 1	Evaluate and implement steganographic techniques in both spatial and transform domains, and apply steganalysis methods to detect hidden information and prevent covert malware communication.
	CC 2	Analyze, reverse engineer, and interpret malware behavior through static and dynamic program analysis, identifying persistence, execution, and evasion mechanisms using professional tools and frameworks.

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

CO	CO Statement	Competency Mapping	Cognitive ©
CO1	Explain the principles of steganography, its applications in information hiding, and the role of steganalysis in detecting covert channels. (Cognitive Knowledge Level: Understand)	CC1	U
CO2	Apply spatial and transform domain techniques using tools like S-Tool, J-Steg, and OutGuess to embed and extract hidden data. (Cognitive Knowledge Level: Apply)	CC1	A
CO3	Perform static and dynamic program analysis to understand executable behavior and identify malware characteristics. (Cognitive Knowledge Level: Apply)	CC2	A
CO4	Analyze Windows internals, persistence, and privilege escalation mechanisms used by malware for system compromise. (Cognitive Knowledge Level: Analyse)	CC2	An
CO5	Perform malware detection and defense methods including YARA rules, unpacking, and stego-firewall implementation to mitigate threats. Use reverse engineering tools such as Ghidra, IDA Pro, and GDB Debugger to investigate, document, and report malware behavior. (Cognitive Knowledge Level: Apply)	CC2	E

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

CO	Program Outcomes						
	PO						
	1	2	3	4	5	6	7
1	3	2	-	1	1	2	-
2	3	2	-	2	3	-	-
3	2	3	-	3	3	-	-
4	2	3	2	3	2	-	-
5	2	3	2	3	3	2	2

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

TEACHING AND ASSESSMENT SCHEME

Teaching Scheme / Week				Self-Learning (S) / Semester	Total Hours / Semester	Credits C	Examination Scheme						
							Theory			Practical			Total
L	T	J	P				CIA	ESE	Total	CIA	ESE	Total	
3	0	0	0	30	70	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	Introduction to Steganography and Information Hiding	Fundamentals of steganography and information hiding, Steganography vs. cryptography Image steganography principles and metrics (capacity, distortion, imperceptibility), Spatial domain techniques – LSB embedding and extraction, Tool: *S-Tool*, Applications and ethical aspects	7
2	Transform Domain Steganography and Steganalysis	DCT and DWT-based embedding in JPEG/JPEG2000, Transform-domain robustness and perceptual fidelity, Tools: J-Steg, OutGuess, Statistical and ML-based steganalysis, Steg Firewall – concept and prevention of covert malware communication, Comparative analysis: spatial vs. transform domain	8
3	Program Analysis and Reverse Engineering	Static and dynamic program analysis, Information flow analysis, Assembly language basics for reverse engineering, Disassemblers and debuggers, Anti-disassembly and anti-debugging techniques, Code obfuscation and de-obfuscation, Tools: Ghidra, *GDB*, *IDA Pro*	8
4	Windows Internals and Malware Behavior	Windows PE file format – headers, sections, imports/exports, Windows API and COM overview, Malware persistence mechanisms: registry, services, DLL load order hijacking, Rootkits and privilege escalation, Analysis of persistence indicators and sandboxing methods	8

5	Malware Execution, Encoding, and Detection	Malware execution: DLL injection, process hollowing, API hooking, APC-based injection, Malware data encoding: ciphers, custom encoding, and packers, Malware detection: unpacking, *YARA rules*, behavior-based detection, Tools: Ghidra, IDA Pro, GDB Debugger, Wireshark, Peview, Case studies: ransomware, 124rojans, rootkits	9

SELF-LEARNING / TEAM WORK

Sl. No	Self-Learning / Team Work Description	Hrs/Semester
1	Research on history and evolution of information hiding and steganography	2
2	Study and demonstrate simple spatial domain steganography using S-Tool	3
3	Explore transform-domain steganography using J-Steg and OutGuess	3
4	Implement a simple steganalysis technique to detect hidden data in images	2
5	Demonstrate Steg Firewall mechanism for blocking covert channels	2
6	Perform static analysis on a benign executable using Ghidra	3
7	Conduct dynamic analysis using GDB or a sandbox environment	3
8	Analyze Windows PE file format using Peview or CFF Explorer	2
9	Identify and document malware persistence mechanisms (registry, DLL hijacking)	3
10	Write and test basic YARA rules for malware detection	2
11	Compare packing and obfuscation techniques using small executable samples	2
12	Mini team project: Perform a complete malware analysis workflow and prepare report	3

SELF-LEARNING / TEAM WORK

Sl. No	Self-learning / Team Work Description	Hrs/Semester
1	Study the fundamentals and history of information hiding and steganography	2
2	Explore spatial domain steganography using S-Tool and analyze output	3
3	Experiment with transform domain steganography using J-Steg and OutGuess	3

4	Implement a simple steganalysis technique to detect hidden content	3
5	Demonstrate Steg Firewall operation to block stego-malware communication	2
6	Perform static malware analysis using Ghidra on a sample binary	3
7	Conduct dynamic analysis using GDB or sandbox tools	3
8	Analyze Windows PE file structure using Peview	2
9	Create and test YARA rules for malware detection	3
10	Mini project: End-to-end analysis of a benign or simulated malware sample	6

SUGGESTED LEARNING RESOURCES

Text Book			
Sl. No.	Title of Book	Author	Publication
1	Steganography in Digital Media: Principles, Algorithms, and Applications	J. Fridrich	1st Edition, Cambridge University Press, 2010.
2	Surreptitious Software: Obfuscation, Watermarking, and Tamper proofing for Software Protection.	C. Collberg and J. Nagra	Addison-Wesley, 2010.
Reference			
Sl. No.	Title of Book	Author	Publication
1	Practical Malware Analysis	Michael Sikorski and Andrew Honig,	No Starch Press 2012
Web Resource			
1	https://www.nist.gov/cyberframework		
2	https://www.malware-traffic-analysis.net/		

DETAILED SYLLABUS

Module	Topic	Mode of Delivery	Cos	Learning Domain Level	Hrs
				C	
1	Fundamentals of Steganography and Information Hiding	Lecture	CO1	U	1
	Steganography vs Cryptography	Lecture	CO1	U	1
	Image Steganography – Principles, Capacity, and Distortion	Lecture	CO1	U	1
	Spatial Domain Steganography – LSB Technique	Lecture, Lab	CO2	A	1
	Tool Demonstration: *S-Tool*	Lecture, Lab	CO2	A	1

	Ethical Issues and Applications of Steganography	Lecture	CO2	U	1
2	Transform Domain Steganography – DCT and DWT Methods	Lecture	CO2	U	1
	Steganography in JPEG/JPEG2000	Lecture	CO2	U	1
	Tools: *J-Steg*, *OutGuess* – Features and Use	Lecture, Lab	CO2	A	1
3	Steganalysis – Statistical and Machine Learning Methods	Lecture	CO3	A	1
	Steg Firewall – Architecture and Implementation	Lecture, Lab	CO3	A	1
	Static and Dynamic Program Analysis – Overview	Lecture	CO3	U	1
	Information Flow Analysis	Lecture	CO3	U	1
	Assembly Language Basics for Reverse Engineering	Lecture	CO3	U	1
	Disassemblers and Debuggers	Lecture, Lab	CO3	A	1
	Anti-Disassembly and Anti-Debugging Techniques	Lecture	CO3	A	1
4	Windows PE File Format – Structure and Sections	Lecture	CO4	U	1
	Windows API and COM Overview	Lecture	CO4	U	1
	Malware Persistence – Registry, Services, DLL Hijacking	Lecture	CO4	A	1
	Rootkits and Privilege Escalation Techniques	Lecture	CO4	A	1
	Sandbox Analysis of Malware Behavior	Lecture, Lab	CO4	A	1
5	Malware Execution Techniques – DLL Injection, Process Hollowing	Lecture	CO5	U	1
	Malware Execution – API Hooking and APC Injection	Lecture	CO5	U	1
	Malware Data Encoding – Ciphers, Encoders, Packers	Lecture	CO5	A	1
	Malware Detection using *YARA Rules*	Lecture, Lab	CO5	A	1
	Case Studies: Ransomware, Trojans,	Lecture	CO5	E	1

	Rootkits				
	Tools Demonstration – *Ghidra, IDA Pro, Wireshark, Peview*	Lecture, Lab	CO5	A	1

TABLE OF SPECIFICATIONS (ToS) FOR QUESTION PAPER DESIGN

Module	Module Title	Teaching Hours	Distribution of Marks (Revised Bloom's Level)						Total Marks
			R	U	A	An	E	C	
1	Introduction to Steganography & Information Hiding	7	—	✓	✓	—	—	—	12
2	Transform-Domain Steganography & Steganalysis	8	—	✓	✓	✓	—	—	12
3	Program Analysis & Reverse Engineering	8	—	—	✓	✓	—	—	12
4	Windows Internals & Malware Behavior	8	—	—	✓	✓	✓	—	12
5	Malware Execution, Encoding & Detection	9	—	—	✓	✓	✓	—	12

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	15
Internal Examination	10
Course Project	15
End Semester Examination	**60**
Total	**100**

SECOND SEMESTER M. TECH DEGREE (REGULAR) EXAMINATION, DECEMBER 2025 (2025 SCHEME)			
Course Code:	**M250102/CY233C**		
Course Name:	**STEGANOGRAPHY AND MALWARE ANALYSIS**		
Max. Marks	**60**	**Duration**:	2 hours 30 minutes

PART A			
(Answer all questions. Each question carries 5 marks)			
No	***Question***	***CO***	***Marks***
1	Define steganography. Differentiate between steganography and cryptography with suitable examples.	CO1	(5)
2	Explain the Least Significant Bit (LSB) technique used in spatial domain steganography. Illustrate with an example.	CO2	(5)
3	Describe the concept of *Steg Firewall*. How does it prevent covert malware communication?	CO3	(5)
4	Discuss common anti-debugging techniques used by malware and suggest countermeasures.	CO4	(5)
5	What is the role of YARA rules in malware detection? Provide a simple example of a rule.	CO5	(5)
PART B			
(Answer any 5 questions. Each question carries 7 marks)			
No	***Question***	***CO***	***Marks***
6	With a neat diagram, explain the embedding and extraction process in DCT-based image steganography.	CO1	(7)
7	Evaluate the challenges and advantages of using transform-domain steganography compared to spatial domain methods.	CO2	(7)
8	Explain static and dynamic malware analysis techniques. Compare their applications and limitations.	CO3	(7)
9	Analyze the Windows PE file format and explain how it is useful in reverse engineering malware.	CO4	(7)
10	Illustrate malware persistence techniques such as registry modification, DLL hijacking, and service creation.	CO4	(7)
11	Discuss different malware execution techniques such as DLL injection and process hollowing with examples.	CO5	(7)
12	Examine how packers and obfuscation affect malware detection. Suggest approaches to overcome these challenges.	CO5	(7)

COURSE DESCRIPTION					
Regulation	**2025**	**L-T-J-P-S**	**3-0-0-0-2**	**Credits**	**3**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)					
Course Code	**Course Name**				**Course Category**
222ECS033	**OPERATING SYSTEM FORENSICS**				**PROGRAMME ELECTIVE**

COURSE OBJECTIVES	
1	To provide a solid foundation that furnishes the learner with in-depth knowledge of current and emerging trends in computer architectures, focusing on performance and the hardware/software interface.
2	To design and analyze, memory hierarchy, pipelining, operation of multiprocessors, thread level parallelism, and data level parallelism

COMPETENCY & OUTCOMES		
Competency Statements	CC 1	Analyze and apply the principles of computer design, instruction set architecture, memory hierarchy, and pipelining to evaluate and optimize the performance of modern computing systems.
	CC 2	Apply concepts of multiprocessor and data-level parallelism, including shared memory, synchronization, GPU architectures, and loop-level parallelism, to design efficient solutions for high-performance applications.

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

CO	CO Statement	Competency Mapping	Cognitive ©
CO1	Explain the basics for operating system (Cognitive Knowledge Level: Understand)	CC1	A
CO2	Determine the challenges, attacks and defence in distributed Operating Systems. (Cognitive Knowledge Level: Apply)	CC1	An
CO3	Illustrate the characteristics and applications of security in OS principles. (Cognitive Knowledge Level: Apply)	CC1	An
CO4	Examine the basic functionalities of Windows and Linux Hardening (Cognitive Knowledge Level: Apply)	CC2	E
CO5	Investigate the vulnerabilities and identify the threats of Hardware security. (Cognitive Knowledge Level: Apply)	CC2	A
CO6	Investigate and review the vulnerabilities and threats in Windows, Linux and Hardware systems and report the measures to be taken (Cognitive Knowledge Level: Evaluate)	CC1	An

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

CO	Program Outcomes						
	PO						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1	-	-	-	2	-	2	-
2	-	-	-	2	-	2	-
3	-	-	-	2	-	2	-
4	-	-	-	2	-	2	-
5	2	-	-	2	--	2	-
6	2	-	-	2	-	2	-

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

TEACHING AND ASSESSMENT SCHEME

Teaching Scheme / Week				Self-Learning (S) / Semester	Total Hours / Semester	Credits C	Examination Scheme						
							Theory			Practical			Total
L	T	J	P				CIA	ESE	Total	CIA	ESE	Total	
3	0	0	0	30	70	3	40	60	100	0	0	0	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	Live Response	Data Collection Introduction, Live Response- Lochard's Exchange Principle Order of Volatility, When to Perform Live Response, What Data to Collect System Time, Logged-on Users ,Open Files, Network Information, Network Connections Process Information, Process-to-Port Mapping, Process Memory, Network Status Nonvolatile Information, Live-Response Methodologies.	8
2	Memory	Collecting Process Memory, Dumping Physical Memory. Analyzing a Physical Memory Dump File Metadata, File Signature Analysis, NTFS Alternate Data Streams Alternative Methods of Analysis. Executable File Analysis- Static Analysis, Dynamic Analysis. Registry Analysis: System Information, Auto start Locations Removable Storage Devices, Mounted Devices, Portable Devices. Finding Users, Tracking User Activity.	8
3	Introduction to malware	MFT, Event logs. Recycle bin, Prefetch files, Scheduled tasks, Jump lists, Hibernation files, Application files. Malware Detection: Malware Characteristics, Detecting Malware: Log analysis, AV scans, Digging deeper Rootkit, Rootkit Detection: Live Detection, GMER, Helios, MS Strider Ghostbuster, F-Secure Backlight, Sophos Anti-Rootkit: Postmortem Detection and Prevention	8
4	Linux Overview	Modern Linux Systems, Forensic Analysis of Linux Systems Linux File Types and Identification. Linux File Analysis Crash and Core Dumps Investigating Evidences From Linux Logs. Linux Time Configuration Analysis, Network Configuration Analysis, Network Security Artifacts. Linux Peripheral Devices, Printers and Scanners, External Attached Storage.	8
5	Recovery	Recovering Items from Web Cache, Recovering Items from plist Files, Recovery of Email artefacts: Popular Email applications, MobileMe (.Mac) and Web-Based E-mail, Recovery of E-mail Data. Popular Chat Applications, Recovery of Chat Data. Locating and Recovering images: Recovering Images. Finding and recovering quick time movies and other video. Microsoft Office, Portable Document Format (PDF),Recovering Office Files, PDFs, and Other Documents.	8

Sl. No	Self-learning / Team Work Description	Hrs/Semester
1	Live Response: Locard's Exchange Principle, Order of Volatility, When to Perform Live Response, and Data Collection Methods	5
2	Memory Forensics: Collecting Process Memory, Dumping and Analyzing Physical Memory using forensic tools	5
3	File System and Registry Analysis: File Metadata, NTFS Alternate Data Streams, Executable File (Static & Dynamic) Analysis, Registry Artefact Investigation	5
4	Windows Forensic Artefacts: MFT, Prefetch, Event Logs, Jump Lists, Rootkit Detection using GMER, Helios, and BlackLight	5
5	Linux Forensics: Log Analysis, Crash Dumps, Network Configuration and Security Artefacts, and Evidence Extraction from Devices	5
6	Data and Artifact Recovery: Web Cache, E-mail, Chat Logs, PDF, Office, and Multimedia File Recovery	5

SUGGESTED LEARNING RESOURCES			
Text Book			
Sl. No.	Title of Book	Author	Publication
1	Windows Forensic Analysis DVD Toolkit	Harlan Carvey	Edition 2, Syngress Inc. ,2009
2	Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry	Harlan Carvey	Pearson Education,2nd edition 2010
Reference			
Sl. No.	Title of Book	Author	Publication
1	Practical Linux Forensics: A Guide For Digital Investigators	Bruce Nikkel	2nd edition Tata McGraw-Hill, 2010
2	Unix and Linux Forensic Analysis DVD Toolkit	Chris Pogue, Cory Altheide, Todd Haverkos	Syngress Inc., 2008
Web Resource			
1	https://www.nist.gov/		
2	https://forensicswiki.xyz/		

DETAILED SYLLABUS

Module	Topic	Mode of Delivery	COs	Learning Domain Level	Hrs
				C	
1	Introduction to Live Response and Evidence Handling	Lecture	CO1	U	1
	Locard's Exchange Principle and Order of Volatility	Lecture	CO1	U	1
	Live Response Procedures – When and How to Collect Data	Lecture	CO1	U	1
	Data Collection: System Time, Logged-On Users, Open Files, Network Information	Lecture, Lab	CO1	A	1
	Network Connections, Process Information, Process-to-Port Mapping	Lecture, Lab	CO1	A	1
	Live-Response Methodologies and Non-Volatile Data	Lecture	CO1	U	1
2	Process Memory and Physical Memory Acquisition	Lecture	CO2	U	1
	Dumping and Analyzing Physical Memory	Lecture, Lab	CO2	A	1
	File Metadata and File Signature Analysis	Lecture, Lab	CO2	A	1
	NTFS Alternate Data Streams and Executable File Analysis	Lecture	CO2	A	1
	Static and Dynamic Analysis of Executables	Lecture, Lab	CO2	A	1
	Registry Analysis: System Information and Autostart Locations	Lecture, Lab	CO2	A	1
3	Windows Artefacts: Event Logs, MFT, Prefetch, Recycle Bin	Lecture	CO3	U	1
	Scheduled Tasks, Jump Lists, and Hibernation Files	Lecture	CO3	U	1
	Rootkits – Characteristics, Live and Postmortem Detection	Lecture	CO3	A	1

	Tools for Rootkit Detection – GMER, Helios, F-Secure, BlackLight	Lecture, Lab	CO3	A	1
	Malware Detection: Log Analysis, AV Scans, Behavioral Analysis	Lecture, Lab	CO3	A	1
4	Linux Forensics Overview	Lecture	CO4	U	1
	File System and Log Analysis in Linux	Lecture, Lab	CO4	A	1
	Crash and Core Dump Analysis	Lecture	CO4	A	1
	Network Configuration and Security Artefact Analysis	Lecture, Lab	CO4	A	1
	Investigating Linux Peripheral Devices and External Storage	Lecture	CO4	U	1
5	Data and Artefact Recovery from Web Cache and Browser Files	Lecture, Lab	CO5	A	1
	Email Artefacts: Recovery from Desktop and Web-based Clients	Lecture, Lab	CO5	A	1
	Chat Artefacts: Recovery from Instant Messaging Applications	Lecture, Lab	CO5	A	1
	Multimedia Artefacts: Image and Video Recovery	Lecture, Lab	CO5	A	1
	Office Documents and PDF Recovery	Lecture, Lab	CO5	A	1

TABLE OF SPECIFICATIONS (ToS) FOR QUESTION PAPER DESIGN

Module	Module Title	Teaching Hours	Distribution of Marks (Revised Bloom's Level)						Total Marks
			R	U	A	An	E	C	
1	Design and Analysis	8		✓	✓				12
2	Memory Hierarchy	8		✓	✓	✓			12
3	Pipelining	8		✓	✓	✓			12
4	Thread Level Parallelism	8		✓	✓	✓	✓		12
5	Data Level Parallelism	8		✓	✓				12

This ToS shall be treated as a general guideline for students and teachers for distribution of marks.

Assessment	**Marks**
Continuous Internal Assessment	**40**
Learning Activity	15
Internal Examination	10
Course Project	15
End Semester Examination	**60**
Total	**100**

SECOND SEMESTER M. TECH DEGREE (REGULAR) EXAMINATION, DECEMBER 2025 (2025 SCHEME)			
Course Code:	**M250102/CY234C**		
Course Name:	**SECURE SOFTWARE ENGINEERING**		
Max. Marks	**60**	**Duration**:	2 hours 30 minutes

(Answer all questions. Each question carries 5 marks)

No	***Question***	***CO***	***Marks***
1	Define *Live Response* in digital forensics. Explain the significance of the Order of Volatility in evidence collection with an example.	CO1	(5)
2	Discuss the process of memory acquisition and explain how registry analysis assists in identifying user activity.	CO2	(5)
3	Describe the forensic significance of Master File Table (MFT) and Prefetch files in malware analysis.	CO3	(5)
4	Explain how Linux log files and time configuration analysis support forensic investigations.	CO4	(5)
5	Outline the procedure to recover deleted email artefacts and chat history from web browsers using forensic tools.	CO5	(5)

PART B

(Answer any 5 questions. Each question carries 7 marks)

No	***Question***	***CO***	***Marks***
6	Illustrate the data collection and live response process with a neat diagram. Discuss tools used for capturing volatile and non-volatile data.	CO1	(7)
7	Explain different methods for memory dump analysis. Compare static and dynamic analysis techniques used in forensic investigation.	CO2	(7)
8	Evaluate various rootkit detection tools such as GMER, Helios, and MS Strider Ghostbuster, highlighting their limitations.	CO3	(7)
9	Evaluate various rootkit detection tools such as GMER, Helios, and MS Strider Ghostbuster, highlighting their limitations.	CO4	(7)
10	Demonstrate the steps involved in recovering deleted media and PDF files from a Windows system.	CO5	(7)
11	Discuss the forensic approach for investigating USB removable devices and mounted drives to trace user activity.	CO2	(7)
12	Examine how malware detection through event logs and scheduled tasks helps in reconstructing the sequence of attack.	CO3	(7)

COURSE DESCRIPTION					
Regulation	**2025**	**L-T-J-P-S**	**3-0-0-0-2**	**Credits**	**3**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)					
Course Code	**Course Name**				**Course Category**
M250102/CY235C	**INFORMATION THEORY AND CODING**				**PROGRAMME ELECTIVE**

COURSE OBJECTIVES	
1	Understand the fundamental concepts, components, and performance metrics (FAR, FRR, EER) of a good biometric system
2	Analyze the working principles, feature extraction, and matching techniques for major physiological biometrics, including Fingerprint, Face, Iris, and Ear recognition.
3	Evaluate the security and privacy challenges in biometric systems, including adversary attacks on the user interface and database.

COMPETENCY & OUTCOMES		
Competency Statements	CC 1	Design and implement a complete biometric authentication pipeline, covering image acquisition, feature extraction, and template matching for a chosen modality (e.g., Fingerprint or Face).
	CC 2	Formulate mitigation strategies to defend a biometric system against common security vulnerabilities, such as spoofing (adversary attacks on user interface) and template tampering (database attacks).

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

CO	CO Statement	Competency Mapping	Cognitive (C)
CO1	Practice measure of information-entropy, mark off model for information source (Cognitive Knowledge Level: Analyze)	CC1	A
CO2	Uses Hannon's source encoding theorem (Cognitive Knowledge)	CC1	A
CO3	Use Huffman coding procedure to analyze the performance (Cognitive Knowledge Level: Analyze)	CC1	An
CO4	Demonstrate linear block codes for error detection and correction (Cognitive Knowledge Level: Analyze)	CC2	An
CO5	Analyze RS codes golay codes and convolution co odes (Cognitive l: Evaluate)	CC2	A

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

CO	Program Outcomes						
	PO						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1	-	-	-	2	-	2	-
2	2	-	2	2	2	2	-
3	2	-	2	2	2	2	-
4	2	-	2	2	2	2	-
5	2	-	2	2	2	2	-
6	2	2	2	2	2	2	2

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

TEACHING AND ASSESSMENT SCHEME													
Teaching Scheme / Week				**Self-Learning (S) / Semester**	**Total Hours / Semester**	**Credits C**	**Examination Scheme**						
							Theory			**Practical**			**Total**
L	**T**	**J**	**P**				**CIA**	**ESE**	**Total**	**CIA**	**ESE**	**Total**	
3	0	0	0	30	70	3	40	60	100	0	0	0	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	Information Theory	Introduction, Measure of information, Average information content of symbols in long independent sequences, Average information content of symbols in long dependent sequences. Mark-off statistical model for information source, Entropy and information rate of mark-off source.	8
2	Source Coding	Encoding of the source output, Shannon's encoding algorithm. Communication Channels, Discrete communication channels, Continuous channels, Source coding theorem.	8
3	Fundamental Limits on Performance	Huffman coding, Discrete memory less Channels, Mutual information, Channel Capacity. Channel coding theorem, Differential entropy and mutual information for continuous ensembles, Channel capacity Theorem	8
4	Introduction to Error Control Coding	Introduction, Types of errors, examples, Types of codes Linear Block Codes: Matrix description, Error detection and correction, Standard arrays and table look up for decoding. Binary Cycle Codes, Algebraic structures of cyclic codes, Syndrome calculation. BCH codes.	8
5	Types of Codes	RS codes, Golay codes, shortened cyclic codes, Burst error correcting codes. Burst and Random Error correcting codes. Convolution Codes, Time domain approach. Transform domain approach.	8

Sl. No	**Self–learning / Team Work Description**	**Hrs/Semester**
1	Study of Information Theory fundamentals — Entropy, Information rate, and Mark-off model	4
2	Implementation of Shannon's Source Coding Theorem using MATLAB/Python	5
3	Comparative study of Huffman Coding and Channel Capacity — Discrete vs Continuous Channels	5
4	Mini Project: Error Control Coding – Implementation of Linear Block Codes, Syndrome Decoding	5
5	Team Presentation on BCH and Cyclic Codes – Encoding and Decoding Process	4
6	Research Paper Review: RS, Golay, and Burst Error Correcting Codes	4
7	Seminar: Transform Domain Coding Approaches in Modern Communication	3

	Systems	

SUGGESTED LEARNING RESOURCES

Text Book			
Sl. No.	Title of Book	Author	Publication
1	*Elements of Information Theory*, 2nd Edition	Thomas M. Cover, Joy A. Thomas	Wiley-Interscience, 2006
2	*Information Theory, Coding and Cryptography*	Ranjan Bose	Tata McGraw Hill, 2008
Reference			
Sl. No.	Title of Book	Author	Publication
1	*Error Control Coding: Fundamentals and Applications*, 2nd Edition	Shu Lin, Daniel J. Costello	Pearson Education, 2004
2	*Digital Communications*	John G. Proakis	McGraw Hill, 2008
3	*Information and Coding Theory*	Gareth A. Jones, J. Mary Jones	Springer, 2000
Web Resource			
1	https://en.wikipedia.org/wiki/Information_theory		
2	https://nptel.ac.in/courses/108/106/108106142/	NPTEL Online Course	IIT Kanpur
3	https://www.shannonentropy.netmark.co/	Online Entropy Simulation Tool	

DETAILED SYLLABUS

Module	Topic	Mode of Delivery	COs	Learning Domain Level	Hrs
				C	
1	Introduction to Information Theory	Lecture	CO1	U	1
	Measure of Information and Average Information Content	Lecture	CO1	U	1
	Information Content of Symbols in Independent & Dependent Sequences	Lecture	CO1	U	1

	Mark-off Statistical Model for Information Source	Lecture	CO1	A	1
	Entropy and Information Rate of Mark-off Source	Lecture	CO1	A	1
	Numerical Examples on Entropy and Information Rate	Lecture, Tutorial	CO1	A	1
2	Source Coding Basics	Lecture	CO2	U	1
	Encoding of Source Output	Lecture	CO2	U	1
	Shannon's Encoding Algorithm	Lecture	CO2	A	1
	Communication Channels and Classification	Lecture	CO2	U	1
	Discrete & Continuous Communication Channels	Lecture	CO2	U	1
	Source Coding Theorem	Lecture	CO2	A	1
	Numerical Problems on Source Coding Efficiency	Lecture, Tutorial	CO2	A	2
3	Huffman Coding and Channel Capacity	Lecture	CO3	U	1
	Discrete Memoryless Channels	Lecture	CO3	U	1
	Mutual Information and Channel Capacity Theorem	Lecture	CO3	A	1
	Differential Entropy and Mutual Information for Continuous Ensembles	Lecture	CO3	A	1
	Performance Limits and Shannon's Channel Coding Theorem	Lecture	CO3	A	1
	Numerical Examples on Channel Capacity	Lecture, Tutorial	CO3	A	2
4	Introduction to Error Control Coding	Lecture	CO4	U	1
	Types of Errors and Codes	Lecture	CO4	U	1
	Linear Block Codes: Matrix Description and Error Detection	Lecture	CO4	A	1
	Standard Arrays and Table Look-up for Decoding	Lecture, Lab	CO4	A	1
	Binary Cyclic Codes and Algebraic Structures	Lecture	CO4	A	1
	Syndrome Calculation and BCH C	Lecture	CO4	A	1

5	RS codes	Lecture	CO5	E	1
	Golay codes	Lecture	CO5	E	1
	Shortened cyclic codes	Lecture	CO5	E	1
	Burst error correcting codes	Lecture	CO5	E	1
	Burst and Random Error correcting codes	Lecture	CO5	E	1
	Convolution Codes	Lecture	CO5	E	1
	Time domain approach	Lecture	CO5	E	1
	Transform domain approach	Lecture	CO5	E	1

TABLE OF SPECIFICATIONS (ToS) FOR QUESTION PAPER DESIGN

Module	Module Title	Teaching Hours	R	U	A	An	E	C	Total Marks
1	Information Theory	6		✓	✓				12
2	Source Coding	8		✓	✓	✓			12
3	Fundamental Limits on Performance	9			✓	✓			12
4	Introduction to Error Control Coding	7			✓	✓	✓		12
5	Types of Codes	10			✓	✓	✓		12

Assessment	Marks
Continuous Internal Assessment	**40**
Learning Activity	15
Internal Examination	10
Course Project	15
End Semester Examination	**60**
Total	**100**

SECOND SEMESTER M. TECH DEGREE (REGULAR) EXAMINATION, DECEMBER 2025 (2025 SCHEME)			
Course Code:	**M250102/CY235C**		
Course Name:	**INFORMATION THEORY AND CODING**		
Max. Marks	**60**	**Duration**:	2 hours 30 minutes

(Answer all questions. Each question carries 5 marks)

No	***Question***	***CO***	***Marks***
1	Define information theory. Explain the concept of entropy and its significance in measuring information content.	CO1	(5)
2	Differentiate between independent and dependent sequences with examples. Describe how the average information content varies between them.	CO1	(5)
3	Explain Shannon's encoding algorithm and its role in source coding.	CO2	(5)
4	Define mutual information and channel capacity. Discuss their relationship using a neat expression.	CO3	(5)
5	Compare linear block codes and cyclic codes. Mention their advantages and applications.	CO54	(5)

PART B

(Answer any 5 questions. Each question carries 7 marks)

No	***Question***	***CO***	***Marks***
6	Explain Mark-off statistical model for information sources. Derive an expression for the information rate of a Mark-off source.	CO1	(7)
7	With a neat block diagram, explain discrete communication channels. Illustrate the concept of source coding theorem with an example.	CO2	(7)
8	Derive the channel capacity theorem for a discrete memory less channel. Explain the importance of the theorem in data transmission.	CO3	(7)
9	Describe error detection and correction using standard array decoding. Provide a suitable example.	CO4	(7)
10	Explain the construction and decoding process of Hamming codes. Show how single-bit errors are detected and corrected.	CO4	(7)
11	Discuss convolutional codes and their time domain representation. How does the transform domain approach improve efficiency?	CO5	(7)
12	Compare and contrast RS codes and BCH codes. State applications where each is preferred.	CO5	(7)

****

COURSE DESCRIPTION					
Regulation	**2025**	**L-T-J-P-S**	**3-0-0-0-2**	**Credits**	**3**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)					
Course Code	**Course Name**				**Course Category**
M250102/CY241D	**ETHICAL HACKING**				**PROGRAMME ELECTIVE**

COURSE OBJECTIVES	
1	Provide practical knowledge and skills in vulnerability assessment and penetration testing to discover weaknesses in applications and infrastructure.
2	Establish a solid knowledge of the main security issues in modern networked computer systems and IT infrastructure.
3	Understand and apply the phases of an attack, including information gathering, scanning, gaining access, maintaining access, and covering tracks (the methodology of ethical hacking).

COMPETENCY & OUTCOMES		
Competency Statements	CC 1	Students will be able to utilize specialized forensic tools and techniques to recover deleted, corrupted, or hidden data from digital media for the purpose of evidence collection.
	CC 2	Students will be able to document and maintain the chain of custody for digital evidence, and prepare a legally sound forensic report to present findings in a clear and professional manner.

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

CO	CO Statement	Competency Mapping	Cognitive (C)
CO1	Evaluate the different methodologies of foot printing. /To discover and collect information about the system. (Cognitive Knowledge Level: Evaluate)	CC2	An
CO2	Evaluate where information networks are most vulnerable. (Cognitive Knowledge Level: Evaluate)	CC1	A
CO3	Perform system vulnerability exploit attacks and produce a security assessment report. (Cognitive Knowledge Level: Create)	CC1	E
CO4	Analyse the different kinds of attacks in the Cloud and methods of Securing. (Cognitive Knowledge Level: Analysis)	CC1	E
CO5	Analyse the methods of Dissecting and fighting against attacks in IoT and Malwares. (Cognitive Knowledge Level: Analysis)	CC2	An

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

CO	Program Outcomes						
	PO						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1	2	-	1	2	3	-	-
2	2	1	2	3	3	-	-
3	3	2	3	3	3	-	-
4	3	2	3	3	3	-	-
5	2	-	2	3	3	-	-

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

TEACHING AND ASSESSMENT SCHEME													
Teaching Scheme / Week				Self-Learning (S) / Semester	Total Hours / Semester	Credits C	Examination Scheme						
							Theory			Practical			Total
L	T	J	P				CIA	ESE	Total	CIA	ESE	Total	
3	0	0	0	30	70	3	40	60	100	0	0	0	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 Ethical Hacking and Reconnaissance	Hacking Concepts, Types and Phases, Ethical Hacking Concepts and Scope, Information Security Controls, Types of Security Policies, Vulnerability Assessment, Penetration Testing, Foot printing, Methodology- Through Search Engines, Social Networking Sites, Website foot printing, Email foot printing, WHOIS , DNS foot printing, Types of attack, Desktop and server OS vulnerabilities, Virtualization and ethical hacking, Foot printing Tools.	8
2	Scanning Networks and Gaining Access	Scanning Methodology, OS Fingerprinting & Banner Grabbing, Enumeration and tools for Enumeration, System Hacking, Sniffing, Denial of Service attacks	8
3	Maintaining Access and Clearing Tracks	Post Exploitation and Maintaining Access with Backdoors, Rootkits, Exploitation tools, Hiding evidence, Hacking- Web Applications, TCP/IP Session Hijacking, SQL Web servers, Hacking Mobile Platforms Injections, Hacking Wireless Networks- Methods, Countermeasures, Hacking	8
4	Non-Tech Hacking and Cloud Computing	Dumpster Diving, Tailgating, Shoulder Surfing, P2P Hacking, People Watching, Kiosks, Vehicle Surveillance, Badge Surveillance, Physical Security, Cloud Computing, Threats, Cloud Computing Attacks, Cloud Security	8
5	IoT and Malware	IoT Concepts and Attacks, Hacking Methodology, Countermeasures, Dissecting Mobile Malware, Ransomware, ATM Malware and Honeypots	8

SELF-LEARNING / TEAM WORK		
Sl. No	Self-learning / Team Work Description	Hrs/Semester
1	Study and summarize digital forensic investigation standards and guidelines	3
2	Explore open-source forensic tools (e.g., Autopsy, Sleuth Kit, FTK Imager) and prepare a usage report	3
3	Perform volume/partition analysis using sample disk images.	4
4	Prepare a comparative study of FAT, NTFS, ExtX, HFS+ file systems highlighting differences in metadata, file recovery and artifacts	4
5	Perform FAT file recovery using a forensic tool.	3
6	Prepare a report on NTFS Master File Table (MFT) artifacts and their importance in investigations.	3
7	Explore file recovery methods in Ext4 vs Ext2/3	3

8	Evaluate Android mobile file system forensics (YAFFS2, F2FS) and its applications in cybercrime cases.	3
9	Study on Flash memory forensic challenges (wear levelling, garbage collection, TRIM).	2
10	Prepare an end-to-end forensic investigation workflow (from acquisition to reporting) based on real case studies.	2

SUGGESTED LEARNING RESOURCES			
Text Book			
Sl. No.	Title of Book	Author	Publication
1	Ethical Hacking and Network Defense	Michael T. Simpson	Cengage Learning, New Delhi, 2012
2	The Basics of Hacking and Penetration Testing	Patrick Engebreston	Syngress, Second Edition
Reference			
Sl. No.	Title of Book	Author	Publication
1	Hacking The Art of Exploitation	Jon Erickson	No Starch Press, Second Edition.
2	Gray Hat Hacking The Ethical Hackers Handbook	Dr. Allen Harper, Stephen Sims, Michael Baucom	Mc Graw Hill Education, Fifth
3	Hacking Exposed 7: Network Security Secrets & Solutions	Stuart McClure, Joel Scambray, George Kurtz	Mc Graw Hill, 2012
Web Resource			
1	https://tryhackme.com/f		
2	https://www.hackthebox.com/		

DETAILED SYLLABUS					
Module	Topic	Mode of Delivery	COs	Learning Domain Level	Hrs
				C	
1	Hacking Concepts, Types and Phases, Ethical Hacking Concepts and Scope	Lecture	CO1	An	1
	Information Security Controls	Lecture	CO1	U	1
	Types of Security Policies	Lecture	CO1	U	1
	Vulnerability Assessment	Lecture	CO1	An	1
	Penetration Testing	Lecture	CO1	U	1
	Foot printing , Methodology- Through Search Engines, Social Networking Sites	Lecture	CO1	U	1
	Website foot printing, Email foot printing	Lecture	CO1	U	1
	WHOIS, DNS foot printing				
	Types of attack. Desktop and server OS	Lecture	CO1	U	1

	vulnerabilities. Virtualization and ethical hacking.				
	Foot printing Tools	Lecture	CO1	U	2
2	Scanning Methodology	Lecture, Lab	CO2	A	1
	OS Fingerprinting & Banner Grabbing	Lecture	CO2	A	1
	Enumeration and tools for Enumeration	Lecture	CO2	A	1
	System Hacking	Lecture	CO2	A	1
	Sniffing	Lecture	CO2	A	1
	Denial of Service attacks	Lecture	CO2	A	1
3	Post Exploitation and Maintaining Access with Backdoors, Rootkits	Lecture	CO3	A	1
	Exploitation tools	Lecture	CO3	A	1
	Hiding evidence	Lab	CO3	A	1
	Hacking- Web Applications	Lecture	CO3	A	1
	TCP/IP Session Hijacking	Lab	CO3	U	1
	SQL Injections	Lecture	CO3	A	1
	Hacking Wireless Networks- Methods, Countermeasures	Lecture	CO3	A	1
	Hacking Web servers	Lecture	CO3	A	1
	Hacking Mobile Platforms	Lecture	CO3	E	2
4	Dumpster Diving, Tailgating, Shoulder Surfing	Lecture	CO4	A	2
	P2P Hacking, People Watching, Kiosks,	Lecture	CO4	A	1
	Vehicle Surveillance, Badge Surveillance	Lecture	CO4	A	2
	Physical Security	Lecture	CO4	A	2
	Cloud Computing Attacks	Lecture	CO4	A	1
	Cloud Security	Lecture	CO4	A	1
	Cloud Computing, Threat	Lecture	CO4	E	1
5	IoT Concepts and Attacks	Lecture	CO5	U	2
	Hacking Methodology	Lecture	CO5	A	2
	Countermeasures	Lecture	CO5	A	1
	Dissecting Mobile Malware, Ransomware	Lecture	CO5	A	1
	ATM Malware and Honeypots	Lecture	CO5	An	2

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	Digital Investigation Basics and Volume Analysis	8		✓	✓	✓			12
2	FAT File System Analysis	8		✓	✓				12
3	NTFS File System Analysis	8		✓	✓	3	3		12
4	Ext X File Systems	8		✓	✓	3	3		12
5	Android and MAC File Systems	8		✓	✓	✓			12
This ToS shall be treated as a general guideline for students and teachers for distribution of marks.									

Assessment	Marks
Continuous Internal Assessment	**40**
Learning Activity	15
Internal Examination	10
Course Project	15
End Semester Examination	**60**
Total	**100**

SECOND SEMESTER M. TECH DEGREE (REGULAR) EXAMINATION, DECEMBER 2025 (2025 SCHEME)			
Course Code:	**M250102/CY241D**		
Course Name:	**ETHICAL HACKING**		
Max. Marks	**60**	**Duration**:	2 hours 30 minutes

(Answer all questions. Each question carries 5 marks)			
No	***Question***	***CO***	***Marks***
1	Define ethical hacking. Explain its phases and how it differs from malicious hacking.	CO1	(5)
2	Explain scanning methodologies and describe how OS fingerprinting is used to identify networked systems.	CO2	(5)
3	Discuss rootkits and backdoors. How are they used to maintain access and what countermeasures exist?	CO3	(5)
4	Describe social engineering attacks such as shoulder surfing and tailgating. Suggest preventive strategies.	CO4	(5)
5	Define IoT malware. Explain how honeypots help in detecting and analyzing IoT-based attacks.	CO5	(5)
PART B			
(Answer any 5 questions. Each question carries 7 marks)			
No	***Question***	***CO***	***Marks***
6	Illustrate the methodology of ethical hacking with a neat diagram. Discuss tools used in reconnaissance.	CO1	(7)
7	Analyze network scanning and enumeration techniques. Explain banner grabbing with an example.	CO2	(7)
8	Explain post-exploitation and clearing tracks. How can attackers use TCP/IP session hijacking?	CO3	(7)
9	Evaluate non-technical hacking methods such as dumpster diving and social media exploitation.	CO4	(7)
10	Discuss threats to cloud environments and explain cloud security countermeasures.	CO4	(7)
11	Describe IoT malware propagation mechanisms and measures to prevent ransomware in smart devices.	CO5	(7)
12	Examine ATM malware and explain how honeypots can detect financial network compromises.	CO5	(7)

****

COURSE DESCRIPTION					
Regulation	**2025**	**L-T-J-P-S**	**3-0-0-0-2**	**Credits**	**3**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)					
Course Code	**Course Name**				**Course Category**
M250102/CY242D	**SECURE SOFTWARE ENGINEERING**				**Program Elective**

COURSE OBJECTIVES	
1	To understand the need for security throughout the software development life cycle.
2	To analyze threats, vulnerabilities, and risks associated with software system
3	To learn secure coding principles and defensive design strategies
4	To explore techniques for software testing, validation, and verification from a security perspective.
5	To study advanced security mechanisms, compliance, and case studies from industry

COMPETENCY & OUTCOMES		
Competency Statements	CC1	Explain cryptography, consensus mechanisms, smart contracts, Dapps, and Web3 in building secure decentralized systems.
	CC2	Apply blockchain tools and techniques to design, deploy, and evaluate practical decentralized solutions for real-world use cases.

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

CO		**Competency Mapping**	**Cognitive (C)**
CO1	Explain the principles and processes of secure software development.	CC1	A
CO2	Apply threat modeling and risk management techniques to software systems.	CC1	A
CO3	Design and implement secure software components using best practices.	CC2	E
CO4	Conduct software security testing and interpret the results effectively.	CC2	E
CO5	Evaluate and improve systems using DevSecOps practices and standards.	CC2	A

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

CO	**Program Outcomes**						
	PO						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1	1	2	2	-	-	2	-
2	2	1	2	-	-	2	-
3	2	1	3	-	2	3	-
4	2	2	3	-	3	3	-
5	1	1	2	-	-	3	-

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

TEACHING AND ASSESSMENT SCHEME													
Teaching Scheme / Week				Self-Learning (S) / Semester	Total Hours / Semester	Credits C	Examination Scheme						
							Theory			Practical			Total
L	T	J	P				CIA	ESE	Total	CIA	ESE	Total	
3	0	0	0	12	40	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	Foundations of Secure Software Engineering	Foundations of Secure Software Engineering (Basics and Process Integration)	7
2	Threat And Risk Management	Threat Modeling and Risk Management.	6
3	Secure designs and coding practices	Secure Design and Coding Practices	12
4	Security testing, verification	Security Testing, Verification, and Validation	8
5	Advanced Topics and case studies	Advanced Topics and Case Studies	7

SELF-LEARNING / TEAM WORK		
Sl. No	**Self-learning / Team Work Description**	**Hrs/Semester**
1	Study SHA-256 and Keccak hash function design; Read Satoshi Nakamoto's Bitcoin whitepaper	2
2	Study how the EOS blockchain implements DPoS as its consensus mechanism, and compare it with Ethereum's transition from PoW to PoS.	2
3	Explore ERC-20 (fungible token) and ERC-721 (NFT) standards; Study Gas fees & optimization strategies in Solidity; Read about vulnerabilities	3
4	Explore IPFS and decentralized storage integration in DApps.	2
5	Explore decentralized identity (DID), study interoperability solutions like Polka dot and Cosmos, and learn how real-world assets are tokenized on blockchain.	3

SUGGESTED LEARNING RESOURCES			
Text Book			
Sl. No.	Title of Book	Author	Publication
1	Software Security Building Security In	Gary McGraw,	Addison-Wesley, 2006.
2	Software Security Engineering: A Guide for Project Managers,	Julia H. Allen et al	Addison-Wesley, 2008.
Reference			
Sl. No.	Title of Book	Author	Publication
1	OWASP Security Considerations in SDLC	Josh Thompson	Create Space Independent Publishing Platform, 2017
2	Security Considerations in SDLC	Ritesh Modi	NIST SP 800-64 Rev.2
5	Web Application Security	Andrew Hoffman	O'Reilly, 2020

Web Resource	
1	Blockchain and its Applications, IIT Kharagpur, Prof. Sandip Chakraborty, Prof. Shamik Sural https://nptel.ac.in/courses/106105235
2	https://www.microsoft.com/en-us/securityengineering/sdl/practices
3	https://www.cert-in.org.in/PDF/Application_Security_Guidelines.pdf

DETAILED SYLLABUS					
Module	Topic	Mode of Delivery	COs	Learning Domain Level C	Hrs
1	Introduction to Software Security – need and importance	Lecture	CO1	U	1
	Secure Software Development Life Cycle (SSDLC)	Lecture	CO1	U	1
	Security touchpoints across SDLC phases	Lecture	CO1	A	1
	Software Assurance and Security Goals (Confidentiality, Integrity, Availability	Lecture	CO1	U	1
	Security Requirements Engineering – identifying misuse and abuse cases	Lecture	CO1	A	1
	Overview of Threats, Vulnerabilities, and Exploits	Lecture	CO1	U	1
2	Introduction to Threat Modeling	Lecture	CO2	U	1
	STRIDE, DREAD, and PASTA Models	Lecture	CO2	A	1
	Attack Trees and Data Flow Diagrams (DFDs)	Lecture	CO2	A	1
	Risk Analysis and Prioritization Techniques	Lecture	CO2	A	1
	Case Study: Threat Modeling for Web/Mobile Applications	Lecture	CO2	A	1
	Integrating Risk Management with Agile and DevSecOps	Lecture	CO2	A	1
3	Secure Design Principles (Least Privilege, Defense in Depth, Fail-Safe Defaults, etc.)	Lecture	CO3	A	1
	Secure Coding Standards (OWASP, CERT)	Lecture	CO3	E	1
	Common Programming Vulnerabilities: Buffer Overflow, Injection, XSS, CSRF, Insecure Deserialization	Lecture	CO3	E	1
	Input Validation, Error Handling, and Logging Practices	Lecture, Lab	CO3	E	1
	Secure Memory Management and Cryptographic Coding Practices	Lecture, Lab	CO3	E	1
	Tools for Secure Code Review and Static Analysis	Lecture, Lab	CO3	E	1
4	Security Testing in SDLC – Unit, Integration, and System Levels	Lecture, Lab	CO4	E	1
	Static vs. Dynamic Analysis	Lecture, Lab	CO4	E	1
	Penetration Testing and Fuzz Testing	Lecture, Lab	CO4	E	1
	Secure Regression Testing	Lecture, Lab	CO4	E	1
	Software Security Metrics and Measurement	Lecture, Lab	CO4	E	1
	Tool-based Approaches: SonarQube, OWASP ZAP, Burp Suite	Lecture, Lab	CO4	E	1
	Verification and Validation Standards (ISO/IEC, NIST SP 800-64)	Lecture, Lab	CO4	E	1
5	Secure Deployment and Configuration Management	Lecture	CO5	A	1
	DevSecOps and Continuous Security Integration	Lecture	CO5	A	1
	Software Supply Chain Security	Lecture	CO5	A	1

	Managing Software Patches and Updates	Lecture	CO5	A	1
	Legal, Ethical, and Compliance Aspects (GDPR, ISO/IEC 27001)	Lecture	CO5	A	1
	Case Studies: Real-world Secure Software Failures and Lessons Learned	Lecture	CO5	A	1
	Future Trends in Secure Software Development	Lecture	CO5	A	1

TABLE OF SPECIFICATIONS (ToS) FOR QUESTION PAPER DESIGN

Module	Module Title	Teaching Hours	Distribution of Marks (Revised Bloom's Level)						Total Marks
			R	U	A	An	E	C	
1	Foundations of Cryptography and Blockchain	7		✓	✓				12
2	Consensus and Decentralization	6		✓	✓				12
3	Smart Contracts and Ethereum	12		✓	✓	✓	✓		12
4	Decentralized Applications	8		✓	✓	✓	✓		12
5	Web3 and Blockchain Data	7		✓	✓				12

This ToS shall be treated as a general guideline for students and teachers for distribution of marks.

Assessment	**Marks**
Continuous Internal Assessment	**40**
Learning Activity	15
Internal Examination	10
Course Project	15
End Semester Examination	**60**
Total	100

SECOND SEMESTER M. TECH DEGREE (REGULAR) EXAMINATION, DECEMBER 2025 (2025 SCHEME)			
Course Code:	**M250102/CY242D**		
Course Name:	**SECURE SOFTWARE ENGINEERING**		
Max. Marks	**60**	**Duration**:	2 hours 30 minutes

PART A

(Answer all questions. Each question carries 5 marks)

No.	***Question***	***CO***	***Marks***
1	Define Secure Software Engineering. Explain the need for integrating security in each phase of the Software Development Life Cycle (SDLC).	CO1	(5)
2	What is threat modeling? Illustrate the STRIDE model with suitable examples.	CO2	(5)
3	Explain any three secure design principles with appropriate examples.	CO3	(5)
4	Differentiate between static and dynamic security testing. Mention their roles in ensuring software assurance..	CO4	(5)
5	Describe the role of DevSecOps in modern software development and how it supports continuous security integration..	CO5	(5)

PART B

(Answer any 5 questions. Each question carries 7 marks)

No.	***Question***	***CO***	***Marks***
6	Discuss the phases and security touchpoints of the Secure Software Development Life Cycle (SSDLC). How do they differ from traditional SDLC?	CO1	(7)
7	Explain the DREAD risk assessment model. How can it be applied in prioritizing software vulnerabilities?	CO2	(7)
8	Illustrate the steps involved in creating an attack tree for a web application. How does it support risk mitigation?	CO3	(7)
9	Explain the common secure coding standards recommended by OWASP and CERT. Give examples of how they prevent vulnerabilities such as SQL injection or buffer overflow.	CO4	(7)
10	Describe the process of conducting penetration testing and fuzz testing. Compare their objectives and outcomes.	CO5	(7)
11	Discuss how security auditing and compliance (such as ISO/IEC 27034 or NIST SP 800-64) help maintain software integrity and trustworthiness.	CO4	(7)
12	Examine the role of software supply chain security and patch management in preventing real-world cyberattacks. Provide examples of failures and lessons learned.	CO3	(7)

****

COURSE DESCRIPTION					
Regulation	**2025**	**L-T-J-P-S**	**3-0-0-0-2**	**Credits**	**3**
(*L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work*)					
Course Code	**Course Name**				**Course Category**
M250102/CY243D	**INFORMATION SECURITY AND APPLIED CRYPTOGRAPHY**				**PROGRAMME ELECTIVE**

COURSE OBJECTIVES	
1	To understand the fundamental principles and goals of information security.
2	To learn classical and modern cryptographic techniques for confidentiality, integrity, and authentication.
3	To analyze symmetric and asymmetric encryption algorithms and their real-world applications.
4	To explore key management, digital signatures, and public key infrastructures (PKI).
5	To study cryptographic protocols and their application in secure communication and data protection.

COMPETENCY & OUTCOMES		
Competency Statements	CC 1	Write secure code that identifies and prevents common vulnerabilities.
	CC 2	Test applications for security weaknesses and propose effective fixes.

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

CO	CO Statement	Competency Mapping	Cognitive (C)
CO1	To provide a strong foundation in the principles, goals, and architecture of information security systems.	CC1	U
CO2	To develop the ability to apply classical and modern cryptographic algorithms to achieve data confidentiality and integrity.	CC1	A
CO3	To equip students with analytical skills for evaluating symmetric and asymmetric encryption mechanisms.	CC1	A
CO4	To familiarize students with digital signatures, key management, and public key infrastructure (PKI).	CC2	A
CO5	To enable students to design and implement secure communication protocols and advanced cryptographic systems for real-world applications.	CC2	A

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

CO	Program Outcomes & Program Specific Outcomes						
	PO						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1	-	-	3	1	3	3	-
2	3	2	3	3	3	3	2
3	-	-	3	3	3	1	-
4	3	1	3	3	3	3	-
5	3	3	3	3	3	3	1

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

TEACHING AND ASSESSMENT SCHEME													
Teaching Scheme / Week				Self-Learning (S) / Semester	Total Hours / Semester	Credits C	Examination Scheme						
							Theory			Practical			Total
L	T	J	P				CIA	ESE	Total	CIA	ESE	Total	
3	0	0	0	30	70	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	Foundations of Information Security	Security goals: Confidentiality, Integrity, Availability, Threats, vulnerabilities, and attacks, Information security principles and policies, Security services and mechanisms, Introduction to cryptography and cryptanalysis, Overview of modern security architecture	8
2	Classical and Modern Cryptography	Substitution and transposition ciphers, Block ciphers and stream ciphers, Feistel structure and product ciphers, DES, 3DES, and AES algorithms, Modes of operation (ECB, CBC, CFB, OFB, CTR),Random number generation and its importance	8
3	Public Key Cryptography and Key Management	Concept of public key systems, RSA algorithm and mathematical foundations, Diffie–Hellman key exchange, ElGamal cryptosystem Key distribution and management, Digital signatures and authentication techniques	8
4	Cryptographic Protocols and Applications	Message authentication and integrity mechanisms, Hash functions (SHA, MD5) and MACs, Digital certificates and Public Key Infrastructure (PKI) Secure Socket Layer (SSL/TLS) and HTTPS Email security (PGP, S/MIME) IP security (IPsec)	8
5	Advanced Cryptography and Security Applications	Elliptic Curve Cryptography (ECC) Quantum cryptography basics Blockchain-based cryptographic systems Cryptographic attacks and countermeasures Case studies: Secure communication, e-Commerce, and digital currency systems	8

SELF-LEARNING / TEAM WORK		
Sl. No	**Self-learning / Team Work Description**	**Hrs/Semester**
1	Cryptography for Developers	2
2	OWASP Top 10 Overview	2
3	Secure Authentication & Session Management	2
4	Secure Configuration Management	2
5	DevSecOps & Security Tooling (SAST/SCA)	2
6	Secrets Management	2
7	Secure Error Handling & Logging	2
8	Cloud-Native Security Fundamentals	2
9	API Security (REST/GraphQL)	2
10	Practical Cryptography Implementation Lab	2
11	Secure Code Review Techniques	2
12	Incident Response for Developers	2
13	Container Security (Docker/Kubernetes)	2
14	Secure Agile Development	2
15	Capture The Flag (CTF) Practical Lab	2

SUGGESTED LEARNING RESOURCES			
Text Book			
Sl. No.	Title of Book	Author	Publication
1	Cryptography and Network Security: Principles and Practice	William Stallings	Pearson, 8th Edition, 2023
2	Cryptography and Network Security	Behrouz A. Forouzan	McGraw Hill, 3rd Edition, 2021
3	Handbook of Applied Cryptography	Alfred J. Menezes	CRC Press, 2018
Reference			
Sl. No.	Title of Book	Author	Publication
1	Applied Cryptography	Bruce Schneier	Wiley, 2020
2	Network Security: Private Communication in a Public World	Charlie Kaufman et al.	Pearson, 3rd Edition, 2015
3	SP 800-175B – Guidelines for Cryptography Management	NIST	(N/A - This is a government publication/standard)
Web Resource			
1	https://owasp.org/		
2	https://www.sans.org/software-security/		
3	https://cwe.mitre.org/		
4	https://www.crypto101.io/		
5	https://portswigger.net/web-security		

DETAILED SYLLABUS

Module	Topic	Mode of Delivery	COs	Learning Domain Level	Hrs
				C	
1	Introduction by discussing Security, CIA Triad, Viruses, Trojans, and Worms In a Nutshell, Security Concepts- exploit, threat, vulnerability, risk, attack.	Lecture	1	U	1
	Malware Terminology: Rootkits, Trapdoors, Botnets, Key loggers, Honeypots	Lecture	1	U	1
	Active and Passive Security Attacks. IP Spoofing, Tear drop, DoS, DDoS	Lecture	1	U	1
	XSS, SQL injection, Smurf, Man in middle, Format String attack.	Lecture	1	U	1
	Types of Security Vulnerabilities- buffer overflows, Invalidated input	Lecture	1	U	1
	race conditions, access control problems	Lecture	1	U	1
	weaknesses in authentication, authorization, or cryptographic practices.	Lecture	1	U	1
	Security in software requirements	Lecture	1	U	1
2	Secure Software Development Cycle (S-SDLC), Security issues while writing SRS.	Lecture	2	U	1
	Design phase security, Development Phase, Test Phase, Maintenance Phase,	Lecture	2	U	1
	Writing Secure Code – Best Practices SD3 (Secure by design, default and deployment),	Lecture	2	A	1
	Secure Product Development Timeline	Lecture	2	U	1
	Security principles and. Threat modelling process and its benefits: Identifying the Threats by Using Attack Trees and rating threats using DREAD	Lecture	2	A	1
	Risk Mitigation Techniques and Security Best Practices	Lecture	2	U	1

	Security techniques, authentication, authorization.	Lecture	2	U	1
	Defence in Depth and Principle of Least Privilege.	Lecture	2	U	1
3	Secure Coding Techniques: Protection against DoS attacks,	Lecture	3	U	1
	Application Failure Attacks, CPU Starvation Attacks	Lecture	3	U	1
	Insecure Coding Practices In Java Technology	Lecture	3	U	1
	ARP Spoofing and its countermeasures.	Lecture	3	U	1
	Buffer Overrun- Stack overrun, Heap Overrun, Array Indexing Errors, Format String Bugs.	Lecture	3	U	1
	Security Issues in C Language: String Handling, Avoiding Integer Overflows and Underflows	Lecture	3	A	1
	Type Conversion Issues- Memory Management Issues, Code Injection Attacks	Lecture	3	U	1
	Canary based countermeasures using Stack Guard and Propolice. Socket Security, Avoiding Server Hijacking, Securing RPC, ActiveX and DCOM	Lecture	3	U	1
4	SQL injection – attack scenario : SQL Injection Techniques and Remedies,	Lecture	4	U	1
	Solutions – blacklisting, whitelisting, escaping, Second order SQL injection.	Lecture	4	U	1
	Prepared statements and bind variables, mitigating the impact of SQL injection attacks.	Lecture	4	U	1
	Race conditions, Time of Check Versus Time of Use and its protection mechanisms	Lecture	4	U	1
	Validating Input and Inter-process Communication, Securing Signal Handlers and File Operations.	Lecture	4	U	1
	XSS scripting attack and its types	Lecture	4	A	1
	Persistent and Non persistent attack XSS Countermeasures	Lecture	4	U	1
	Bypassing the XSS Filters.	Lecture	4	A	1
5	Security code overview	Lecture	5	U	1
	Secure software installation	Lecture	5	U	1
	The Role of the Security Tester	Lecture	5	U	1
	Building the Security Test Plan	Lecture	5	A	1
	Testing HTTP-Based Applications	Lecture	5	A	1
	Testing File-Based Applications – 1	Lecture	5	U	1
	Testing File-Based Applications – 2	Lecture	5	A	1
	Testing Clients with Rogue Servers	Lecture	5	A	1

TABLE OF SPECIFICATIONS (ToS) FOR QUESTION PAPER DESIGN

Module	Module Title	Teaching Hours	Distribution of Marks (Revised Bloom's Level)						Total Marks
			R	U	A	An	E	C	
1	Introduction to Security Goals and various threats and attacks	8		✓					12
2	Security development process and threat modelling.	8		✓	✓				12
3	Secure Coding Techniques	8		✓	✓				12
4	Database and Web specific issues	8		✓	✓				12
5	Testing secure applications.	8		✓	✓				12

This ToS shall be treated as a general guideline for students and teachers for distribution of marks.

Assessment	Marks
Continuous Internal Assessment	**40**
Learning Activity	15
Internal Examination	10
Course Project	15
End Semester Examination	**60**
Total	**100**

SECOND SEMESTER M. TECH DEGREE (REGULAR) EXAMINATION, DECEMBER 2025 (2025 SCHEME)			
Course Code:	**M250102/CY243D**		
Course Name:	**INFORMATION SECURITY AND APPLIED CRYPTOGRAPHY**		
Max. Marks	**60**	**Duration**:	2 hours 30 minutes

PART A

(Answer all questions. Each question carries 5 marks)

No.	***Question***	***CO***	***Marks***
1	Define Information Security. Explain the goals of security: confidentiality, integrity, and availability with examples.	CO1	(5)
2	Differentiate between block ciphers and stream ciphers. Give examples of each.	CO2	(5)
3	Explain the RSA algorithm with an example. Mention its applications in secure communication.	CO3	(5)
4	What is a message authentication code (MAC)? Describe its role in maintaining data integrity.	CO4	(5)
5	Define Elliptic Curve Cryptography (ECC). Discuss why ECC is preferred over RSA for modern security systems.	CO5	(5)

PART B

(Answer any 5 questions. Each question carries 7 marks)

No.	***Question***	***CO***	***Marks***
6	Illustrate the security architecture of an organization. Discuss the principles of security policies and services.	CO1	(7)
7	Explain the Feistel cipher structure. Compare the working principles of DES, 3DES, and AES algorithms.	CO2	(7)
8	Discuss key distribution and management mechanisms in public key cryptography. Explain Diffie–Hellman key exchange.	CO3	(7)
9	Describe the process of digital signature generation and verification. Why is non-repudiation important?	CO3	(7)
10	Explain the working of SSL/TLS protocol. How does it ensure authentication and confidentiality?	CO4	(7)
11	Describe blockchain-based cryptographic systems. Explain how they ensure data integrity in distributed environments.	CO5	(7)
12	Examine various cryptographic attacks (e.g., brute force, man-in-the-middle) and explain their countermeasures.	CO5	(7)

****

COURSE DESCRIPTION					
Regulation	**2025**	**L-T-J-P-S**	**3-0-0-0-2**	**Credits**	**3**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)					
Course Code	**Course Name**				**Course Category**
M250102/CY244D	**MACHINE LEARNING IN SECURITY**				**PROGRAMME ELECTIVE**

COURSE OBJECTIVES	
1	Introduce and explain the fundamental concepts of Machine Learning (ML) and its real-world applications in security..
2	Compare and contrast the primary types of ML and deep learning algorithms, including supervised, unsupervised, and reinforcement learning
3	Apply and differentiate various classification and clustering ML algorithms, such as Linear/Logistic Regression, Decision Trees, SVM, Naive Bayes, K-NN, and K-Means

COMPETENCY & OUTCOMES		
Competency Statements	CC 1	Understand the role of Machine Learning in Cybersecurity and explain the limitations and challenges when applying ML to security problems.
	CC 2	Design and implement appropriate ML algorithms (e.g., SVM, Random Forest, Gradient Boosting) to solve specific security challenges.

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

CO	CO Statement	Competency Mapping	Cognitive (C)
CO 1	Identify the different machine learning models (Cognitive Knowledge Level: Apply)	CC1	A
CO 2	Examine the application of machine learning models in security (Cognitive Knowledge Level: Analyze	CC1	A
CO 3	Implement intrusion detection system in machine learning (Cognitive Knowledge Level: Apply	CC1	A
CO 4	Implement the machine learning security model biometric system (Cognitive Knowledge Level: Evaluate)	CC2	An
CO 5	Design and Implement software error metrics and solution for software errors using machine learning (Cognitive Knowledge Level: Evaluate)	CC2	A

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

CO	Program Outcomes & Program Specific Outcomes						
	PO						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1	3	3	2		2		1
2	3	2	3		3		1
3	3	2	3	2	3		1
4	3	3	2	2	2	2	1
5	3	3	2		3		1

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

TEACHING AND ASSESSMENT SCHEME													
Teaching Scheme / Week				Self-Learning (S) / Semester	Total Hours / Semester	Credits C	Examination Scheme						
							Theory			Practical			Total
L	T	J	P				CIA	ESE	Total	CIA	ESE	Total	
3	0	0	0	30	70	3	40	60	100	0	0	0	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	Machine Learning	What Is Machine Learning? Why Machine Learning and Security? Real-World Uses of Machine Learning in Security, Limitations of Machine Learning in Security, Classification and Clustering-Machine Learning: Problems and Approaches, Main types of machine learning algorithms-Supervised, Unsupervised, Semi-supervised and Reinforcement learning	6
2	ML Algorithms	Linear regression, Logistic regression, Decision tree, SVM algorithm, Naive Bayes algorithm, KNN algorithm, K-means, Random forest algorithm, Dimensionality reduction algorithms, Gradient boosting algorithm and AdaBoosting algorithm.	8
3	Intrusion Detection Techniques	Intrusion Detection system-The problem of intrusion detection-ML techniques for intrusion detection-Network IDS, Host IDS, Protocol IDS, Application IDS, Hybrid IDS, Signature-based method, Anomaly-based method, Comparison of IDS with firewalls.	8
4	Biometric Authentication Systems	Biometric Systems, Introduction to biometric systems, An implementation of Biometric IRIS system, Performance-errors-security-technology-advantages applications	8
5	Machine Learning for Software Security	Software security-searching for software errors-Machine learning techniques for searching software errors, Error metrics in machine learning, How does machine learning change software engineering? Code Obfuscation, ML techniques to obfuscation, obfuscated command line detection using ML.	10

SELF-LEARNING / TEAM WORK		
Sl. No	**Self-learning / Team Work Description**	**Hrs/Semester**
1	Students explore free tiers of AWS, GCP, or Azure to launch and configure a simple VM or deploy a basic web app.	3
2	Set up VirtualBox or VMware and create a virtual environment with different OSes.	1
3	Research recent cloud security breaches and analyze how they could have been prevented	1
4	Create a small project using Hadoop or Spark and document the steps.	5
5	Encourage students to complete online micro-courses (e.g., AWS Cloud Practitioner Essentials).	1
6	Use MapReduce/Spark in teams to solve a big data problem (e.g., log analysis)	5
7	Cloud Migration Strategies	2
8	Infrastructure as Code (IaC)	3
9	Serverless Architecture	3

10	DevSecOps & CI/CD Security	6

SUGGESTED LEARNING RESOURCES			
Text Book			
Sl. No.	Title of Book	Author	Publication
1	Machine Learning and Security	Clarence Chio, David Freeman,	O'ReillyMedia, Inc.,2018.
2	Hands-On Artificial Intelligence for Cyber security	Alessandro Parisi,	PacktPublishingLimited.,2019
Reference			
Sl. No.	Title of Book	Author	Publication
1	Machine Learning	Tom Mitchell	McGrawHill,1997.
2	Cloud Computing: Implementation, Management, and Security	John W. Rittenhouse and James Ransome,	CRC Press, 2010.
3	Machine learning for computer and cybersecurity: principle, algorithms, and practices	Gupta, Brij B and QuanZ.Sheng, eds	CRC Press,2019
4	Artificial Intelligence and Data Mining Approach in Security Frameworks	Neeraj Bhargava, Ritu Bhargava, Pramod Singh Rathore, Rashmi Agrawal	2021
5	Machine learning in cyber trust: security, privacy, and reliability.	Tsai, JeffreyJP, andS.YuPhilip, eds	2009
6	Machine Learning: A Probabilistic Perspective	Kevin P Murphy	MIT Press.
7	Pattern Recognition and Machine Learning	Christopher Bishop.	Springer2006
Web Resource			
1	**https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/**		
2	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-64r2.pdf		

Module	Topic	Mode of Delivery	COs	Learning Domain Level C	Hrs
1	What is Machine Learning? Why machine learning and security?	Lecture	CO1	A	1
	Real world uses of machine learning in security	Lecture	CO1	A	1
	Limitations of machine learning in security	Lecture	CO1	A	1
	Classification-Machine learning problems and approaches	Lecture	CO1	A	1
	Clustering- Machine learning problems and approaches	Lecture	CO1	A	1
	Supervised, Unsupervised	Lecture	CO1	A	1
	Semi-supervised and Reinforcement learning	Lecture	CO1	A	1
	Classification versus Clustering	Lecture	CO1	A	1
2	Linear regression, Logistic regression	Lecture	CO2	A	1
	Decision tree algorithm,	Lecture	CO2	A	1
	Naïve Bayes algorithm, KNN algorithm	Lecture	CO2	A	1
	KNN algorithm, K-means	Lecture	CO2	A	1

	Random Forest Algorithm	Lecture	CO2	A	1
	Dimensionality reduction algorithms	Lecture	CO2	A	1
	Gradient boosting algorithm	Lecture	CO2	A	1
	Ada Boosting algorithm	Lecture	CO2	A	1
3	Intrusion Detection system	Lecture	CO3	A	1
	The problem of intrusion detections	Lecture	CO3	A	1
	ML techniques for intrusion detection	Lecture	CO3	A	1
	Network IDS, Host IDS	Lecture	CO3	A	1
	Protocol IDS, Application IDS	Lecture	CO3	A	1
	Hybrid IDS	Lecture	CO3	A	1
	Signature-based method, Anomaly-based method	Lecture	CO3	A	1
	Comparison of IDS with firewall	Lecture	CO3	A	1
4	Introduction to biometric systems	Lecture	CO4	An	1
	An implementation of Biometric IRIS system	Lecture	CO4	An	1
	Biometric system-performance-errors-security	Lecture	CO4	An	1
	Technology-advantages	Lecture	CO4	An	1
	Technology-disadvantages	Lecture	CO4	An	1
	Biometric Systems applications	Lecture	CO4	An	1
5	Software security issues	Lecture	CO5	A	1
	Searching and detecting software errors	Lecture	CO5	A	1
	Machine learning techniques for searching software errors	Lecture	CO5	A	1
	Error metrics in machine learning	Lecture	CO5	A	1
	How does machine learning change software engineering?	Lecture	CO5	A	1
	Code Obfuscation	Lecture	CO5	A	1
	ML techniques to obfuscation	Lecture	CO5	A	1
	Obfuscated command line detection using ML	Lecture	CO5	A	1

TABLE OF SPECIFICATIONS (ToS) FOR QUESTION PAPER DESIGN

Module	Module Title	Teaching Hours	Distribution of Marks (Revised Bloom's Level)						Total Marks
			R	U	A	An	E	C	
1	Cloud Computing Fundamentals	6		✓	✓				12
2	Virtualization	8		✓	✓				12
3	Architectural Design of Compute and Storage Clouds, Cloud Programming	8		✓	✓				12
4	Fundamental Cloud Security	8		✓	✓				12
5	Popular Cloud Platforms	10		✓	✓				12

This ToS shall be treated as a general guideline for students and teachers for distribution of marks.

Assessment	Marks
Continuous Internal Assessment	**40**
Learning Activity	15
Internal Examination	10
Course Project	15
End Semester Examination	**60**
Total	**100**

SECOND SEMESTER M. TECH DEGREE (REGULAR) EXAMINATION, DECEMBER 2025 (2025 SCHEME)				
Course Code:	**M250102/CY244D**			
Course Name:	**MACHINE LEARNING IN SECURITY**			
Max. Marks	**60**	**Duration**:	2 hours 30 minutes	
PART A				
(Answer all questions. Each question carries 5 marks)				
No.	***Question***		***CO***	***Marks***
1	Define Machine Learning (ML). Explain the role of ML in cybersecurity and list its main learning types.		CO1	(5)
2	Compare Supervised and Unsupervised learning with suitable examples.		CO2	(5)
3	Differentiate between signature-based IDS and anomaly-based IDS. Mention their advantages and limitations.		CO3	(5)
4	Explain the working of a Biometric IRIS recognition system. Discuss its performance and security aspects.		CO4	(5)
5	What is Code Obfuscation? How does ML help in detecting obfuscated commands or code patterns?		CO5	(5)
PART B				
(Answer any 5 questions. Each question carries 7 marks)				
No.	***Question***		***CO***	***Marks***
6	Discuss classification and clustering techniques in ML and their applications in cybersecurity.		CO1	(7)
7	Explain the working principle and use cases of Decision Tree and Random Forest algorithms in intrusion detection.		CO2	(7)
8	Compare Naive Bayes and Support Vector Machine (SVM) algorithms. Explain where each is best applied in security systems.		CO3	(7)
9	Describe various types of Intrusion Detection Systems (IDS) — Network, Host, Protocol, Application, and Hybrid — with examples.		CO4	(7)
10	Discuss Error metrics used in ML for identifying software vulnerabilities. How does ML change modern software security practices?		CO5	(7)
11	Explain Gradient Boosting and AdaBoost algorithms. Compare their performance in classification tasks.		CO4	(7)
12	Evaluate the role of Machine Learning in Biometric Authentication Systems. Discuss accuracy, security, and privacy trade-offs.		CO3	(7)

****

COURSE DESCRIPTION					
Regulation	**2025**	**L-T-J-P-S**	**3-0-0-0-2**	**Credits**	**3**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)					
Course Code	**Course Name**				**Course Category**
M250102/CY245D	**CYBERLAW AND INTELLECTUAL PROPERTY RIGHTS**				**PROGRAMME ELECTIVE**

COURSE OBJECTIVES	
1	Highlight the basics and importance of Cyber space and IT act.(Cognitive Knowledge Level: Understand)
2	Analyse electronic governance. Understanding the importance and need for DSC, internet service providers and their liability. (Cognitive Knowledge Level: Analyse)
3	Use the provision of Cyber law to deal with Types of Cyber Crime, Cyber-crime Complaints, National cyber security policy. (Cognitive Knowledge Level: Apply)
4	Demonstrate the procedure for registration, Characteristics, publication, infringement and term of copyright and also know the other forms of IP. (Cognitive Knowledge Level: Apply)
5	Analyse European Position, Legal position and Indian position on Computer related Patents. Evaluate IPR cases. (Cognitive Knowledge Level: Analyse)

COMPETENCY & OUTCOMES		
Competency Statements	CC 1	Model security problems using formal logic and mathematical frameworks.
	CC 2	Use automated tools to verify systems and find security vulnerabilities.

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

CO	CO Statement	Competency Mapping	Cognitive (C)
CO1	Illustrate cyberspace and explain the interface of technology and law, and analyse the need for the Information Technology Act along with an explanation of the Information Technology Act, 2000	CC1	A
CO2	Analyse the concept of Digital Signature Certificate and define cybercrime along with a list and explanation of cybercrimes under the Indian Penal Code.	CC2	An
CO3	Demonstrate of hacking, child pornography, cyber stalking, denial of service attack, and virus dissemination, and explain data protection and privacy with suitable examples.	CC2	An
CO4	Describe the various types of intellectual property rights along with their objectives, and evaluate issues relating to authorship and assignment.	CC1	An
CO5	Define patent and explain the European position on computer-related patents, and differentiate between the legal position on computer-related patents and the Indian position on patents.	CC2	U

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

CO	Program Outcomes						
	PO						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1	2	-	3	2	1	2	-
2	2	1	3	2	3	2	-
3	2	1	3	3	3	2	1
4	2	1	3	2	2	2	-
5	1	2	3	3	3	2	1

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

TEACHING AND ASSESSMENT SCHEME													
Teaching Scheme / Week				Self-Learning (S) / Semester	Total Hours / Semester	Credits C	Examination Scheme						
							Theory			Practical			Total
L	T	J	P				CIA	ESE	Total	CIA	ESE	Total	
3	0	0	0	30	70	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	Cyber Space	Fundamental definitions-Interface of Technology and Law– Jurisprudence and-Jurisdiction in Cyber Space- Indian context of Jurisdiction Enforcement agencies– Need for IT act-UNCITRAL– E-Commerce basics. Information Technology Act, 2000- Aims and Objects — Overview of the Act– Jurisdiction	8
2	Electronic Governance	Legal Recognition of Electronic Records and Electronic Evidence-Digital Signature Certificates- Securing Electronic records and secure digital signatures- Duties of Subscribers-Role of Certifying Authorities Regulators under the Act-The Cyber Regulations Appellate Tribunal Internet Service Providers and their Liability– Powers of Police under the Act– Impact of the Act on other Laws. Cyber Crimes-Meaning of Cyber Crimes–Different Kinds of Cyber-crimes Cyber-crimes under IPC	8
3	Cr.P.C and Indian Evidence Law	Cyber-crimes under the Information Technology Act 2000-Cyber-crimes under International Law– Hacking, Child Pornography, Cyber Stalking, Denial of service Attack, Virus Dissemination, Software Piracy, Internet Relay Chat (IRC) Crime, Credit Card Fraud, Net Extortion, Phishing etc. Cyber Terrorism Violation of Privacy on Internet- Data Protection and Privacy– Indian Court cases.	8
4	Intellectual Property Rights	Copyrights- Software– Copyrights vs Patents debate-Authorship and Assignment Issues- Copyright in Internet-Multimedia and Copyright issues- Software Piracy-Trademarks- Trademarks in Internet– Copyright and Trademark cases.	8
5	Patents	Understanding Patents- European Position on Computer related Patents, Legal position on Computer related Patents-Indian Position on Patents - Case Law, Domain names-registration- Domain Name Disputes-Cyber Squatting-IPR cases.	8

SELF-LEARNING / TEAM WORK		
Sl. No	**Self-learning / Team Work Description**	**Hrs/Semester**
1	Set Theory and Functions for Formal Methods	2
2	Introduction to Lattices and Order Theory	2
3	Hoare Logic Fundamentals	2
4	Verifying Blockchain Smart Contracts	2
5	Introduction to Differential Privacy	2
6	The Applied Pi-Calculus	2
7	Symbolic Execution for Vulnerability Discovery	2

8	Introduction to Side-Channel Analysis	2
9	Intermediate Representations for Static Analysis	2
10	Lightweight Formal Methods: TLA+ and Alloy	2
11	Version Control and CI for Formal Models	2
12	Debugging and Interpreting Tool Output	2
13	Economics of Formal Verification	2
14	Usable Security and Formal Methods	2
15	Writing and Reviewing Formal Specifications	2

SUGGESTED LEARNING RESOURCES

Text Book

Sl. No.	Title of Book	Author	Publication
1	Model Checking	Edmund M. Clarke, Orna Grumberg and Doron Peled	MIT Press, 1999.
2	Logic and Learning: Knowledge Representation, Computation and Learning in Higher-order Logic	Lloyd, J.W.	Springer Berlin Heidelberg, 2003.
3	Logic in Computer Science - Modelling and Reasoning about Systems	M. Ruth and M. Ryan	Cambridge University Press, 2004
4	Formal Correctness of Security Protocols	G. Bella	Springer, 2009
5	Analysis Techniques for Information Security	Datta A, Jha S, Li N, Melski D and Reps T	Synthesis Lectures on Information Security, Privacy, and Trust, 2010.

Reference

Sl. No.	Title of Book	Author	Publication
1	Modelling and Analysis of Security Protocols	Peter Ryan, Steve Schneider, M. H. Goldsmith	Pearson Education, 2010
2	Formal Aspects In Security And Trust: Ifip TN Wg1.7	Theo Dimitrakos, Fabio Martinelli	Workshop on Formal Aspects in Security, Springer, 2005
3	Modern Cryptography: Theory & Practice	W. Mao	Pearson Education, 2004
4	Formal Verification of Security Protocols	Giampaolo Bella	Springer, 2007
5	Protocols for Authentication and Key Establishment	Colin Boyd, Anish Mathuria	Springer, 2003
6	Formal Correctness of Security Protocols (Information Security and Cryptography)	Giampaolo Bella	Springer, 1e, 2007.

Web Resource

1	https://tamarin-prover.github.io/manual/
2	http://spinroot.com/spin/whatispin.html
3	https://isabelle.in.tum.de/documentation.html
4	https://cvc5.github.io/
5	https://frama-c.com/html/documentation.html

DETAILED SYLLABUS					
Module	Topic	Mode of Delivery	COs	Learning Domain Level	Hrs
				C	
1	Fundamental definitions, Interface of Technology and Law	Lecture	CO1	U	1
	Jurisprudence and-Jurisdiction in Cyber Space, Indian Context of jurisdiction	Lecture	CO1	U	1
	Enforcement agencies	Lecture	CO1	U	1
	Need for IT act, UNCITRAL	Lecture	CO1	U	1
	E-Commerce basics	Lecture	CO1	U	1
	InformationTechnologyAct,2000	Lecture	CO1	A	1
	Aims and Objects—Overview of the Act	Lecture	CO1	A	1
	Jurisdiction	Lecture	CO1	A	1
2	Legal Recognition of Electronic Records and Electronic Evidence	Lecture	CO2	U	1
	Digital Signature Certificates-Securing Electronic records and secure digital signatures	Lecture	CO2	A	1
	Duties of Subscribers-Role of Certifying Authorities	Lecture	CO2	A	1
	Regulators under the Act	Lecture	CO2	A	1
	The Cyber Regulations Appellate Tribunal, Internet ServiceProvidersandtheirLiability		CO2	An	1
	Powers of police under the Act, Impact of the Act on other laws	Lecture	CO2	U	1
	Meaning of Cyber Crimes–Different Kinds of Cyber crimes	Lecture	CO2	U	1
	Cyber-crimes under IPC	Lecture	CO2	U	1
3	Introduction	Lecture	CO3	A	1
	Cyber-crimes under the Information Technology Act 2000	Lecture	CO3	An	1
	Cyber-crimes under International Law	Lecture	CO3	U	1
	Hacking, Child Pornography, Cyber Stalking,	Lecture	CO3	U	1
	Denial of service Attack, Virus Dissemination, Software Piracy	Lecture	CO3	U	1
	Internet Relay Chat (IRC)Crime, Credit Card Fraud, Net Extortion, Phishing	Lecture	CO3	U	1
	Cyber Terrorism Violation of Privacy on internet	Lecture	CO3	U	1
	Data Protection and Privacy–Indian Court cases.	Lecture	CO3	U	1
4	Introduction	Lecture	CO4	U	1
	Copyrights	Lecture	CO4	An	1
	Copyrights vs Patents debate	Lecture	CO4	U	1
	Authorship and Assignment Issues	Lecture	CO4	A	1
	Copyright in Internet	Lecture	CO4	U	1
	Multimedia and Copyright issues	Lecture	CO4	U	1
	Software Piracy- Trademarks	Lecture	CO4	U	1
	Trademarks in Internet, Copyright and Trademark cases.	Lecture	CO4	An	1
5	Understanding Patents- European Position on Computer related Patents	Lecture	CO5	U	1
	Legal position on Computer related Patents	Lecture	CO5	U	1
	Indian Position on Patents	Lecture	CO5	U	1
	Case Law, Domain names	Lecture	CO5	U	1
	Domain name registration	Lecture	CO5	U	1

	Domain Name Disputes	Lecture	CO5	U	1
	Cyber Squatting	Lecture	CO5	U	1
	IPR cases	Lecture	CO5	U	1

TABLE OF SPECIFICATIONS (ToS) FOR QUESTION PAPER DESIGN									
Module	Module Title	Teaching Hours	Distribution of Marks (Revised Bloom's Level)						Total Marks
			R	U	A	An	E	C	
1	Formal Methods	8		✓	✓				12
2	Verification	8		✓	✓				12
3	Formal methods applications	8		✓		✓			12
4	Formal modelling	8		✓		✓			12
5	Familiarization	8		✓					12
This ToS shall be treated as a general guideline for students and teachers for distribution of marks.									

Assessment	Marks
Continuous Internal Assessment	**40**
Learning Activity	15
Internal Examination	10
Course Project	15
End Semester Examination	**60**
Total	**100**

Course Code:	M250102/CY245D		
Course Name:	CYBERLAW AND INTELLECTUAL PROPERTY RIGHTS		
Max. Marks	60	Max. Marks	60

PART A

(Answer all questions. Each question carries 5 marks)

No.	Question	CO	Marks
1	Define cyber space. Explain the interface between technology and law in the context of cyber jurisprudence.	CO1	(5)
2	What is threat modeling? Describe the process of digital signature certification and discuss the duties of certifying authorities. the STRIDE model with suitable examples.	CO2	(5)
3	What are cyber-crimes under the Information Technology Act, 2000? List and explain any four types.	CO3	(5)
4	Explain intellectual property rights (IPR) in cyberspace. How are copyrights and software piracy regulated?	CO4	(5)
5	Define patent. Discuss the relevance of patent law in India and its relation to computer software.	CO5	(5)

PART B

nswer any 5 questions. Each question carries 7 marks)

No.	Question	CO	Marks
6	Discuss the Information Technology Act, 2000 — its aims, objectives, and jurisdiction in cyber space.	CO1	(7)
7	Explain the legal recognition of electronic records and evidence under the IT Act. How does this impact Indian court proceedings?	CO2	(7)
8	Describe the role and liability of Internet Service Providers (ISPs) under the IT Act.	CO2	(7)
9	Examine cyber-crimes under international law with reference to hacking, cyber stalking, and data theft.	CO3	(7)
10	Discuss the powers of police and enforcement agencies in investigating cyber-crimes under Cr.P.C. and IT Act.	CO3	(7)
11	Explain copyright issues in multimedia and Internet-based content. Give examples of relevant case studies.	CO4	(7)
12	Compare Indian and European patent systems. Discuss cyber-related patent disputes and domain name registrations.	CO5	(7)

****

COURSE DESCRIPTION							
Regulation	**2025**	**L-T-J-P-S**	**0-0-4-0-2**	**Version**	**25/0**	**Credits**	**2**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)							
Course Code	**Course Name**						**Course Category**
M250902/CN200S	**MINIPROJECT**						**PROJECT**

COURSE OBJECTIVES	
1	Enable the students to apply advanced software engineering principles and research methodologies in the design, development, and implementation of a mini project that addresses real-world problems or research challenges.

COMPETENCY STATEMENTS	
CC1	Students can identify real-world problems, study related solutions, analyze requirements, and develop simple, effective software using modern tools, while preparing clear reports and applying basic engineering and management skills

COURSE OUTCOMES

CO	CO Statement	Competency Statement Mapping	Cognitive (C)
CO1	Identify technically and economically feasible problems (Cognitive Knowledge Level: Apply)	CC1	A
CO2	Identify and survey the relevant literature for getting exposed to related solutions and get familiarized with software development processes. (Cognitive Knowledge Level: Apply)	CC1	A
CO3	Perform requirement analysis for identifying design methodologies and developing adaptable and reusable solutions of minimal complexity by using modern tools and advanced programming techniques. (Cognitive Knowledge Level: Analyse)	CC1	A
CO4	Prepare a technical report after the project presentation. (Cognitive Knowledge Level: Apply)	CC1	A
CO5	Apply engineering and management principles to achieve the goal of the project.. (Cognitive Knowledge Level: Apply)	CC1	A

CO	PROGRAM OUTCOMES (PO) CORRELATION MATRIX						
	PO						
	1	2	3	4	5	6	7
1	3	3	3	3	3	3	3
2	3	3	3	3	3	3	3
3	3	3	3	3	3	3	3
4	3	3	3	3	3	3	3
5	3	3	3	3	3	3	3
Correlation levels: 1 - Low; 2 - Medium; 3 - High; No Correlation - "-"							

TEACHING AND ASSESSMENT SCHEME									
Teaching Scheme / Week					Credit	Hours / Semester	Examination Scheme		
							Practical		
L	T	J	P	S	C		CIA	ESE	Total
0	0	4	0	2	2	30	100	0	100

ASSESSMENT PATTERN	
Assessment	**Marks**
Continuous Internal Assessment	**100**
Interim evaluation 1	20
Interim evaluation 2	20
Final evaluation by a committee	35
Report	15
Supervisor/Guide	10
Total	**100**

COURSE DESCRIPTION							
Regulation	**2025**	**L-T-J-P-S**	**0-0-0-2-1**	**Version**	**25/0**	**Credits**	**1**
(L- Lecture, T-Tutorial, J-Project, P-Practical, S-Self-learning & Team Work)							
Course Code	**Course Name**						**Course Category**
M250102 / CY10T	**COMPUTING LAB II**						**LAB 1**

COURSE OBJECTIVES	
1	Enable students to implement and test core network and security primitives (sockets, hashing, authentication) using C/Java and evaluate their security properties.
2	Train students to use standard security tools and analysis workflows (traffic capture, protocol inspection, vulnerability scanning, simulation) ethically and in controlled environments
3	Develop student capability to analyze common vulnerabilities (buffer overflow, weak password hashing, insecure network services), demonstrate remediation, and document secure design choices.

COMPETENCY STATEMENTS	
CC1	Apply core concepts of computer and network security to design, implement, and evaluate secure communication programs using C/Java, including socket programming, encryption, and secure network configurations in a controlled laboratory environment.
CC2	Analyze, simulate, and assess real-world security mechanisms and vulnerabilities using standard tools (such as Nmap, Wireshark, NS2/NS3, and intrusion detection systems) to develop practical skills in vulnerability scanning, traffic analysis, and performance evaluation while adhering to ethical and legal standards.

COURSE OUTCOMES			
CO	**CO Statement**	**Competency Statement Mapping**	**Cognitive (C)**
CO1	Implement and test fundamental computer and network security programs using C/Java for secure communication, encryption, and authentication in a controlled lab environment. (Cognitive Knowledge Level: Apply)	CC1	A
CO2	Demonstrate the configuration of Linux-based systems and use of security tools (e.g., Wireshark, Nmap) to analyze and monitor network activities safely. (Cognitive Knowledge Level: Apply)	CC1	A
CO3	Analyze the vulnerabilities and threats in communication networks using scanning, simulation, and performance evaluation tools like NS2/NS3. (Cognitive Knowledge Level: Analyse)	CC2	An
CO4	Apply methods to detect and mitigate attacks such as buffer overflow, password cracking, and injection in a controlled environment, emphasizing defensive strategies. (Cognitive Knowledge Level: Apply)	CC1	A

CO5	Evaluate the effectiveness of network security mechanisms (firewalls, IDS/IPS, honeypots) through case studies and propose improvements for secure system design. (Cognitive Knowledge Level: Evaluate)	CC2	E

CO	**PROGRAM OUTCOMES (PO) CORRELATION MATRIX**						
	PO						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1	2	2	3	3	3	2	3
2	2	2	3	3	3	2	2
3	3	3	3	3	3	3	2
4	2	2	3	3	2	3	2
5	3	3	3	3	3	3	3
Correlation levels: 1 - Low; 2 - Medium; 3 - High; No Correlation - "-"							

TEACHING AND ASSESSMENT SCHEME									
Teaching Scheme / Week					**Credit**	**Hours / Semester**	**Examination Scheme**		
							Practical		
L	**T**	**J**	**P**	**S**	**C**		**CIA**	**ESE**	**Total**
0	0	0	2	1	1	30	100	0	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									

PRACTICAL SYLLABUS					
Experiment No.	Topic	Objective	CO	Learning Domain Level	Hrs
				C	
1	Implement TCP and UDP Socket Programming using C/Java	To understand secure communication and socket programming principles	CO1	A	2
2	Secure File Transfer using Encryption in C/Java	To implement encryption-based file transfer ensuring data confidentiality	CO1	A	2
3	Linux Firewall Configuration using iptables	To configure and test firewall rules to restrict unauthorized access	CO2	A	2

4	Network Traffic Capture and Analysis using Wireshark	To monitor and analyze live network packets ethically for anomalies	CO2	A	2
5	Controlled Network Scanning using Nmap	To identify open ports and assess vulnerabilities in a safe lab setup	CO3	A	2
6	Network Simulation and Performance Evaluation using NS2/NS3	To simulate network topologies and analyze protocol behavior	CO3	An	2
7	Demonstration of Buffer Overflow and Mitigation Techniques	To understand memory exploitation and protection mechanisms	CO4	A	2
8	Implementation of Secure Password Hashing (PBKDF2/bcrypt)	To secure user credentials using cryptographic hashing algorithms	CO4	A	2
9	Intrusion Detection using Snort/Suricata	To detect and analyze intrusion attempts using IDS tools	CO5	E	2
10	Honeypot Deployment and Analysis (Cowrie/Kippo)	To deploy a honeypot and analyze attack patterns in a controlled setup	CO5	E	2

Text Book

Sl. No.	Title of Book	Author	Publication
1	*Computer Security: Principles and Practice* (4th Edition)	William Stallings, Lawrie Brown	Pearson Education, 2021
2	*Network Security Essentials: Applications and Standards* (6th Edition)	William Stallings	Pearson Education, 2020

Reference

Sl. No.	Title of Book	Author	Publication
1	*Practical Network Scanning and Penetration Testing with Nmap*	Abhinav Singh	Packt Publishing, 2021
2	*Wireshark for Security Professionals: Using Wireshark and the Metasploit Framework*	Jessey Bullock, Jeff T. Parker	Wiley, 2017
3	*The Art of Memory Forensics*	Michael Hale Ligh, Andrew Case, Jamie Levy, A.	Wiley, 2014

		Walters	
4	*Hands-On Ethical Hacking and Network Defense* (4th Edition)	Michael T. Simpson, Kent Backman	Cengage Learning, 2019
5	*Cybersecurity Blue Team Toolkit*	Nadean Tanner	Wiley, 2019

Web Resource			
Sl. No.	Resource	Organization / Author	Link
1	NIST Computer Security Resource Center	National Institute of Standards and Technology	https://csrc.nist.gov
2	CERT-In (Indian Computer Emergency Response Team)	Govt. of India	https://www.cert-in.org.in
3	OWASP (Open Web Application Security Project)	OWASP Foundation	https://owasp.org
4	Wireshark Official Documentation	Wireshark Foundation	https://www.wireshark.org/docs/
5	Kali Linux Official Documentation	Offensive Security	https://www.kali.org/docs/

ASSESSMENT PATTERN	
Assessment	**Marks**
Continuous Internal Assessment	**100**
Continuous Lab Evaluation	60
Internal Examination	40
Total	**100**