

Register Number 2 2 5 0 0 1 0 2 9

**Sri Sivasubramaniya Nadar College of Engineering, Kalavakkam – 603 110**

(An Autonomous Institution, Affiliated to Anna University, Chennai)

**Department of Computer Science and Engineering**

**Continuous Assessment Test – I**

**Question Paper**

<b>Degree &amp; Branch</b>	B.E. & CSE				<b>Semester</b>	VI
<b>Subject Code &amp; Name</b>	UCS1603 & INTRODUCTION TO MACHINE LEARNING				<b>Regulation:</b>	2018
<b>Academic Year</b>	2022-2023 EVEN	<b>Batch</b>	2020-2024	<b>Date</b>	01.03.2023	FN
<b>Time: 08:15 - 09:45 a.m (90 Minutes)</b>	<b>Answer All Questions</b>				<b>Maximum: 50 Marks</b>	

**COURSE OUTCOMES**

CO1: Understand the basic concepts of machine learning (K2)

CO2: Apply supervised algorithms for different classification problems (K3)

CO3: Understand the need of ensemble methods (K2)

CO4: Apply unsupervised and reinforcement learning techniques to various problems (K3)

CO5: Understand the requirement of dimensionality reduction and optimization techniques (K2)

**Part – A (6×2 = 12 Marks)**

K1	1. Define activation function with examples.	CO1	1.4.1
K3	2. Consider the credit scoring application, identify the proper features needed to build a machine learning model to give credit to a person. Frame a discriminant rule for the same.	CO1	1.4.1
K2	3. Why do we need <i>bias</i> input for a neural network? What are the possible values of it?	CO2	1.4.1
K3	4. Solve the following. The given dataset has 60 samples in positive and 40 samples in negative classes. Of which 10% in each class is misclassified during testing. Calculate the <i>balanced accuracy</i> using appropriate formula.	CO1	1.1.1, 1.4.1
K2	5. What does ROC curve represent in machine learning?	CO1	1.4.1
K3	6. Identify the suitable learning type for the following applications. Justify your answer. a. Building a robot for surveillance b. Internet content categorization	CO1	2.1.3

Register Number 2 2 5 0 0 1 0 2 9

**Sri Sivasubramaniya Nadar College of Engineering, Kalavakkam – 603 110**

(An Autonomous Institution, Affiliated to Anna University, Chennai)

Department of Computer Science and Engineering

**Continuous Assessment Test – I**

**Question Paper**

<b>Degree &amp; Branch</b>	B.E. & CSE				<b>Semester</b>	VI
<b>Subject Code &amp; Name</b>	UCS1603 & INTRODUCTION TO MACHINE LEARNING				<b>Regulation:</b>	2018
<b>Academic Year</b>	2022-2023 EVEN	<b>Batch</b>	2020-2024	<b>Date</b>	01.03.2023	FN
<b>Time: 08:15 - 09:45 a.m (90 Minutes)</b>	<b>Answer All Questions</b>				<b>Maximum: 50 Marks</b>	

**COURSE OUTCOMES**

CO1: Understand the basic concepts of machine learning (K2)

CO2: Apply supervised algorithms for different classification problems (K3)

CO3: Understand the need of ensemble methods (K2)

CO4: Apply unsupervised and reinforcement learning techniques to various problems (K3)

CO5: Understand the requirement of dimensionality reduction and optimization techniques (K2)

**Part – A (6×2 = 12 Marks)**

K1	1. Define activation function with examples.	CO1	1.4.1
K3	2. Consider the credit scoring application, identify the proper features needed to build a machine learning model to give credit to a person. Frame a discriminant rule for the same.	CO1	1.4.1
K2	3. Why do we need <i>bias</i> input for a neural network? What are the possible values of it?	CO2	1.4.1
K3	4. Solve the following.  The given dataset has 60 samples in positive and 40 samples in negative classes. Of which 10% in each class is misclassified during testing. Calculate the <i>balanced accuracy</i> using appropriate formula.	CO1	1.1.1, 1.4.1
K2	5. What does ROC curve represent in machine learning?	CO1	1.4.1
K3	6. Identify the suitable learning type for the following applications. Justify your answer. a. Building a robot for surveillance b. Internet content categorization	CO1	2.1.3

**Part – B (3×6 = 18 Marks)**

K3	7. Consider the following dataset, to find the suitable activity for the given test case using Bayesian Classifier. Test case: {Deadline = Near & None, Is there a Party = Yes, Lazy = Yes}.	CO1	1.1.1, 1.4.1, 13.3.1																																									
	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Deadline?</th><th>Is there a party?</th><th>Lazy?</th><th>Activity</th></tr> </thead> <tbody> <tr><td>Urgent</td><td>Yes</td><td>Yes</td><td>Party</td></tr> <tr><td>Urgent</td><td>No</td><td>Yes</td><td>Study</td></tr> <tr><td>Near</td><td>Yes</td><td>Yes</td><td>Party</td></tr> <tr><td>None</td><td>Yes</td><td>No</td><td>Party</td></tr> <tr><td>None</td><td>No</td><td>Yes</td><td>Pub</td></tr> <tr><td>None</td><td>Yes</td><td>No</td><td>Party</td></tr> <tr><td>Near</td><td>No</td><td>No</td><td>Study</td></tr> <tr><td>Near</td><td>No</td><td>Yes</td><td>TV</td></tr> <tr><td>Near</td><td>Yes</td><td>Yes</td><td>Party</td></tr> <tr><td>Urgent</td><td>No</td><td>No</td><td>Study</td></tr> </tbody> </table>			Deadline?	Is there a party?	Lazy?	Activity	Urgent	Yes	Yes	Party	Urgent	No	Yes	Study	Near	Yes	Yes	Party	None	Yes	No	Party	None	No	Yes	Pub	None	Yes	No	Party	Near	No	No	Study	Near	No	Yes	TV	Near	Yes	Yes	Party	Urgent
Deadline?	Is there a party?	Lazy?	Activity																																									
Urgent	Yes	Yes	Party																																									
Urgent	No	Yes	Study																																									
Near	Yes	Yes	Party																																									
None	Yes	No	Party																																									
None	No	Yes	Pub																																									
None	Yes	No	Party																																									
Near	No	No	Study																																									
Near	No	Yes	TV																																									
Near	Yes	Yes	Party																																									
Urgent	No	No	Study																																									
8. Discuss and compare supervised, unsupervised learning types with suitable illustrations.																																												
9. Given a sample of 13 pictures which have pictures of cats and dogs. The dataset has 8 cat and 5 dog images, where cats belong to class 1 and dogs belong to class 0. The actual and predicted class labels are shown below. Actual Class = [1,1,1,0,0,0,0,1,0,0,0,0,0] Predicted Class = [0,0,0,1,1,1,1,1,0,0,0,0,0] Construct a confusion matrix and calculate precision, recall and F1 measure.																																												

**Part – C (2×10 = 20 Marks)**

K3	10. Assume two sensors are used to measure the humidity and temperature of the soil four times a day. During morning both the sensors measured the value, afternoon only temperature measured the value, evening only humidity measured the value and night time both the sensors didn't measured / returned any value. Formulate this as a suitable perceptron learning problem by considering bipolar inputs (+1, -1) and the target is a combination of both the sensors. <b>Note:</b> Initialization values: $w_0 = w_1 = w_2 = 0.5$ , $\eta = 0.1$ , bias = -1, $\theta = 1.0$ . Find the updated weight of each sample for one epoch.	CO2	1.4.1, 2.1.3, 2.3.1, 13.3.1
	(OR)		
K3	11. Use the given data to compute the correlation coefficient and build a regression model for finding the weight of a person with the input as height of a person.	CO2	1.4.1, 4.2.1, 13.3.1
	$Height (X): 70, 62, 65, 60, 62, 72, 68, 66$ $Weight (Y): 215, 180, 185, 160, 162, 220, 190, 185$		

	If the <b>height</b> is <b>63 inches</b> , can you predict the weight of this person using the model you built?		
K2	12. Explain the multi-layer perceptron algorithm and how does it work? Also discuss how the error is back propagated.	CO2	1.4.1, 2.1.3, 2.3.1
	(OR)		
K2	<p>13. a. Explain McCulloch and Pitts neuron model with its structure. Why do we need MLP?</p> <p>b. Draw the structure of MLP neural network for the application of "Breast cancer detection". Define the number of the nodes in each layer and the weight matrix between the layers.</p> <p>The Breast Cancer Wisconsin (Original) Data Set has the following features and class label:</p> <ul style="list-style-type: none"> <li>1. Sample code number: id number</li> <li>2. Clump Thickness: 1 - 10</li> <li>3. Uniformity of Cell Size: 1 - 10</li> <li>4. Uniformity of Cell Shape: 1 - 10</li> <li>5. Marginal Adhesion: 1 - 10</li> <li>6. Single Epithelial Cell Size: 1 - 10</li> <li>7. Bare Nuclei: 1 - 10</li> <li>8. Bland Chromatin: 1 - 10</li> <li>9. Normal Nucleoli: 1 - 10</li> <li>10. Mitoses: 1 - 10</li> </ul> <p>Class: (0 for benign, 1 for malignant)</p>	CO2	1.4.1, 4.1.1, 4.2.1

Register Number 

2	0	5	0	0	1	0	2	9
---	---	---	---	---	---	---	---	---

Sri Sivasubramaniya Nadar College of Engineering, Kalavakkam – 603 110

(An Autonomous Institution, Affiliated to Anna University, Chennai)

Department of Computer Science and Engineering

## Continuous Assessment Test – II

## Question Paper

Degree & Branch	B.E. & CSE			Semester	VI
Subject Code & Name	UCS1603 & INTRODUCTION TO MACHINE LEARNING			Regulation:	2018
Academic Year	2022-2023 EVEN	Batch	2020-2024	Date	03.04.2023 FN
Time: 08:15AM-9:45AM (90 Minutes)	Answer All Questions			Maximum: 50 Marks	

## COURSE OUTCOMES

CO1: Understand the basic concepts of machine learning (K2)

CO2: Apply supervised algorithms for different classification problems (K3)

CO3: Understand the need of ensemble methods (K2)

CO4: Apply unsupervised and reinforcement learning techniques to various problems (K3)

CO5: Understand the requirement of dimensionality reduction and optimization techniques (K2)

## Part – A (6×2 = 12 Marks)

K1	1. The optimization problem of support vector machine can be solved using primal and dual methods. Which is preferable? Why?	CO2	1.4.1, 2.3.1
K1	2. Define the polynomial and RBF kernel functions of support vector machine.	CO2	1.4.1, 2.3.1
K3	3. The probabilities of five events are: P(first) = 0.5, P(second)=P(third)=P(fourth)=P(fifth)= 0.125. Calculate entropy using the given probabilities.	CO3	1.4.1, 13.3.1
K1	4. What is meant by CART? When is it preferable to use in ML model creation?	CO3	1.4.1, 2.3.1
K3	5. Five different models are built using different features and different samples, to find whether the given sample image is Cancerous (C) or not Cancerous (NC). The results given by the five models are: $M_1 \rightarrow C, M_2 \rightarrow NC, M_3 \rightarrow C, M_4 \rightarrow C, M_5 \rightarrow NC$ . Identify the suitable strategy to derive the final decision.	CO3	1.4.1, 2.1.3
K1	6. What is the need of dimensionality reduction techniques in machine learning process?	CO5	1.4.1, 2.1.3

## Part – B (3×6 = 18 Marks)

K2	7. Compare Random Forest and Boosting ensemble algorithms.	CO3	2.3.1
K3	8. Construct space splitting and K-d tree representation for the following data points: (5,4), (2,2), (3,7), (4,6), (7,5), (6,1), (6,8)	CO3	1.4.1, 2.1.3, 2.3.1
K3	9. The pattern number and its corresponding data points ( $X$ ) with label ( $Y$ ) for the training set are given in the following table.	CO2	1.4.1, 2.1.3, 13.3.1

Pattern	X	Y
1	1	-1
2	3	-1
3	7	+1

The SVM objective function is " $g(x) = wx + b$ ". Using the training set, find the values of  $x$ ,  $w$  and  $b$  in the objective function. Also, validate the function, for the test data  $x=9$  to find the class label.

**Part - C (2×10 = 20 Marks)**

10. Construct the decision tree for the dataset given in the following table. Use the impurity functions: Entropy and Information gain to draw the first level tree representation.

Height	Hair	Eyes	Attractive?
Small	Blonde	Brown	No
Tall	Dark	Brown	No
Tall	Blonde	Blue	Yes
Tall	Dark	Blue	No
Small	Dark	Blue	No
Tall	Red	Blue	Yes
Tall	Blonde	Brown	No
Small	Blonde	Blue	Yes

K3 CO3 1.4.1,  
2.1.3,  
13.3.1

(OR)

11. Construct the decision tree for the dataset given in the following table. Use the Gini Index impurity function to draw the final decision tree. Write the corresponding rules in the Implication form (if condition – then).

Past Trend	Open Interest	Trading Volume	Return
Positive	Low	High	Up
Negative	High	Low	Down
Positive	Low	High	Up
Positive	High	High	Up
Negative	Low	High	Down
Positive	Low	Low	Down
Negative	High	High	Down
Negative	Low	High	Down
Positive	Low	Low	Down
Positive	High	High	Up

K3 CO3 1.4.1,  
2.1.3,  
13.3.1

K3

12. Explain Linear Discriminant Analysis (LDA) as a sequence of steps with necessary equations and state few applications of LDA.

K2 CO5 2.1.3,  
2.4.1

(OR)

13. Explain Principal Component Analysis (PCA) as a sequence of steps with its importance in dimensionality reduction. Compare PCA with LDA (7 + 3)

K2 CO5 2.1.3,  
2.4.1

Register Number 2 0 5 0 0 1 0 2 9

Sri Sivasubramaniya Nadar College of Engineering, Kalavakkam – 603 110

(An Autonomous Institution, Affiliated to Anna University, Chennai)

Department of Computer Science and Engineering

## Continuous Assessment Test – III

## Question Paper

Degree & Branch	B.E. & CSE			Semester	VI
Subject Code & Name	UCS1603 & INTRODUCTION TO MACHINE LEARNING			Regulation:	2018
Academic Year	2022-2023 EVEN	Batch	2020-2024	Date	08.05.2023 FN
Time: 08:15AM-9:45AM (90 Minutes)	Answer All Questions			Maximum: 50 Marks	

## COURSE OUTCOMES

CO1: Understand the basic concepts of machine learning (K2)

CO2: Apply supervised algorithms for different classification problems (K3)

CO3: Understand the need of ensemble methods (K2)

CO4: Apply unsupervised and reinforcement learning techniques to various problems (K3)

CO5: Understand the requirement of dimensionality reduction and optimization techniques (K2)

## Part – A (6×2 = 12 Marks)

K2	1. Compare active and passive Reinforcement Learning methods.	CO4	2.1.3
K3	2. Find the distance between the two vectors (7, 3, 6, 8, 15) and (5, 1, 7, 9, 12) using Manhattan distance.	CO4	1.4.1, 2.3.1, 2.4.1
K2	3. Assume you need to design a GameAI where the program is initially trained on a large database of human expert moves. Further, moves are refined through learning from its own mistakes. Find the suitable machine learning algorithms that provide a solution for the customer? Define the algorithm.	CO4	1.4.1, 13.3.1, 2.4.1
K1	4. What is meant by saddle point in optimization function?	CO5	2.1.3
K1	5. List three basic search approaches in optimization	CO5	2.1.3
K2	6. Write the advantages of Newton method when compared to Stochastic gradient method?	CO5	2.1.3

## Part – B (3×6 = 18 Marks)

K2	7. Explain how the mathematical model of Markov Decision Process is applied in Reinforcement Learning policy.	CO4	2.1.3, 2.3.1									
	8. You are given a 3x3 grid with the following values.  <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td>1</td><td>2</td><td>3</td></tr> <tr> <td>4</td><td>5</td><td>6</td></tr> <tr> <td>7</td><td>8</td><td>9</td></tr> </table>	1	2	3	4	5	6	7	8	9		1.4.1, 2.1.3, 13.3.1
1	2	3										
4	5	6										
7	8	9										
K3	You start at position (1, 1) (top left corner) and your goal is to reach position (3, 3) (bottom right corner). At each time step, you can take one of four actions: up, down, left, or right. If you reach the goal state, you receive a reward of 10, and if you fall off the grid, you receive a reward of -10. All other actions receive a reward of -1. Use Q learning	CO4										

to find the optimal policy for this problem and fill that in the following pseudocode.

```

def simulate_episode():
    # initialize the starting state
    state = (0, 0)
    # loop until the goal state is reached or the agent falls off the grid
    while True:
        # choose an action based on the current state and exploration rate
        action = choose_action(state)
        # execute the action and observe the next state and reward
        if action == 'up':
            next_state = (state[0] - 1, state[1])
        elif action == 'down':
            next_state = _____
        elif action == 'left':
            next_state = _____
        elif action == 'right':
            next_state = _____
        if next_state[0] < 0 or next_state[0] >= GRID_SIZE or
           next_state[1] < 0 or next_state[1] >= GRID_SIZE:
            reward = _____
            next_state = state
        elif next_state == (GRID_SIZE - 1, GRID_SIZE - 1):
            # the agent reached the goal state

```

- K3 9. Let  $f(x) = x^2 - 4x + 3$ . Find the gradient ( $\nabla f$ ) descent function value for three steps. Assume the initial value of  $x_0 = 3$  and the learning rate = 0.1.

CO5

1.4.1,  
2.3.1,  
2.4.1,  
13.3.1

### Part - C (2×10 = 20 Marks)

10. Assume  $K=2$ , and the initial clusters are instance 1 and instance 4. Use K-means clustering to find the cluster for the given data points to their respective clusters. Find the sum of squared errors of the clusters.

Instance	X	Y
1	2	3
2	3	5
3	4	4
4	5	6
5	6	4

CO4

1.4.1,  
2.1.3,  
13.3.1

(OR)

- K3 11. A self-driving car is deployed in a theme park to help the customers to reach various rides. There are 20 different rides with a distance of 1 km apart. Apply Reinforcement Learning, to draw the state diagram and reward matrix of this robot with architecture and discounting factor.

CO4

1.4.1,  
2.1.3,  
13.3.1

- K2 12. Explain the conjugate gradient descent algorithm with its importance in optimization problems.

CO5

2.1.3,  
13.3.1

(OR)

- K2 13. Explain the hill climbing and simulated annealing algorithms as a search process with an example.

CO5

2.1.3,  
13.3.1

Register No: 205001029

Sri Sivasubramaniya Nadar College of Engineering, Kalavakkam – 603 110.

(An Autonomous Institution, Affiliated to Anna University, Chennai)

B.E. / B.Tech. End Semester Theory Examinations, April/May 2023.

### Sixth Semester

Computer Science and Engineering

### UCS1603 INTRODUCTION TO MACHINE LEARNING

(Regulations 2018)

Time: Three Hours

Answer ALL Questions

Maximum: 100 Marks

K1: Remembering

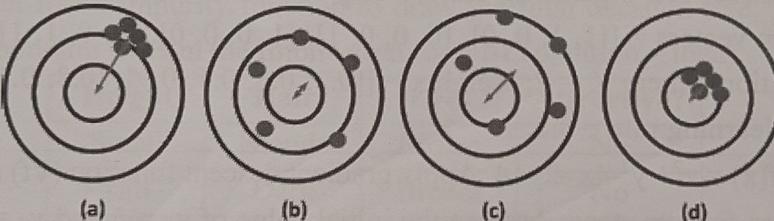
K2: Understanding

K3: Applying

K4: Analyzing

K5: Evaluating

### PART – A (10 × 2 = 20 Marks)

01.	K1	What is meant by semi supervised learning?	CO1
02.	K2	Infer the bias and variance (low or high) for each of the following figures with respect to underfitting and overfitting.  	CO1
03.	K2	Compare Biological Neural Network with Artificial Neural Network.	CO2
04.	K1	What is the purpose of Kernel functions in Support Vector Machine?	CO2
05.	K1	State the univariate and multivariate gaussian functions of Gaussian Mixture Model.	CO3
06.	K1	Consider a data set $S = \{s_1, s_2, s_3, s_4\}$ where $s_1=\text{false}$ , $s_2=\text{true}$ , $s_3=\text{false}$ , $s_4=\text{true}$ and feature set $F = \{f_1, f_2\}$ where $f_1 = \{s_1, s_2\}$ and $f_2 = \{s_3, s_4\}$ . Find the information gain for this dataset.	CO3
07.	K1	Define Q-Learning function in Reinforcement Learning.	CO4
08.	K1	List and write the equations of distance measures used in clustering.	CO4
09.	K1	What is meant by saddle point in optimization function?	CO5
10.	K1	Write the function routine of hill climbing algorithm.	CO5

**PART – B (5 × 6 = 30 Marks)**

11.	K3	<p>The samples of “<b>cats and dogs classification</b>”, with its actual and predicted labels are given below.</p> <p>Actual labels = [‘dog’, ‘cat’, ‘dog’, ‘cat’, ‘dog’, ‘cat’, ‘dog’, ‘cat’, ‘dog’, ‘dog’, ‘dog’, ‘cat’, ‘dog’, ‘cat’, ‘dog’, ‘dog’, ‘cat’, ‘dog’, ‘cat’, ‘dog’, ‘cat’]</p> <p>Predicted labels = [‘dog’, ‘dog’, ‘dog’, ‘cat’, ‘dog’, ‘dog’, ‘cat’, ‘cat’, ‘cat’, ‘dog’, ‘dog’, ‘cat’, ‘dog’, ‘cat’, ‘dog’, ‘cat’, ‘dog’, ‘cat’]</p> <p>Construct a confusion matrix and calculate accuracy, sensitivity and specificity.</p>	CO1
12.	K3	<p>Consider two vectors X and Y, find the Sum of Squared Error using Linear Regression with appropriate equations.</p> <p>X = [2, 4, 6, 8] Y = [3, 7, 5, 10]</p>	CO2
13.	K2	Compare random forest with boosting ensemble algorithms.	CO3
14.	K3	Construct self-organizing feature map and find the suitable cluster for the given vectors = [[1, 1, 0, 0], [0, 0, 0, 1], [1, 0, 0, 0], [0, 0, 1, 1]] after first iteration, where K = 2, weights = [[0.2, 0.6, 0.5, 0.9], [0.8, 0.4, 0.7, 0.3]] and learning rate = 0.5.	CO4
15.	K3	Let $f(x) = x^2 + y^2 - 4x - 2y + 4$ . Apply gradient descent function ( $\nabla f$ ) and find the values for two steps. Assume the initial value of $x_0 = 5$ and $y_0 = -3$ and the learning rate = 0.1.	CO5

**PART – C (5 × 10 = 50 Marks)**

16.	K2	Explain three types of learning with appropriate diagram, uniqueness and any two applications in each type.	CO1
(OR)			
17.	K2	Explain the importance of the curse of dimensionality, ROC curve and AUC curve in machine learning process.	CO1
18.	K3	<p>Consider the inputs <math>X_1, X_2</math> and output T given in the below table with learning rate = 0.1, theta = 1.0, <math>W_0 = W_1 = W_2 = \text{bias} = 0.5</math>.</p> <p>Output = 1 if <math>y_j \geq \theta</math> -1 if <math>y_j &lt; \theta</math></p> <p>Apply the Perceptron learning algorithm for the OR network to estimate the updated weights and output of each sample for two epochs.</p> <p>Note: <math>y_j</math> = output of weighted linear function and output = <math>g(y_j)</math></p>	CO2

X <sub>1</sub>	X <sub>2</sub>	T
1	1	1
1	-1	1
-1	1	1
-1	-1	-1

(OR)

19.	K3	<p>A set of data points are given between 1 and 15, where the data points 3 and 7 belong to class 1 (+1) and data point 12 belong to class 2 (-1). Let the SVM objective function is "<math>g(x) = wx + b</math>". Using the given data points, find the values of x, w and b in the objective function. Also, validate the function, for the test data "<math>x = 9</math>" to find the class label.</p>	CO2
-----	----	---	-----

20.	K3	<p>Construct the decision tree for the dataset given in the following table. Use the Gini Index impurity function to draw the final decision tree. Write the corresponding rules in the Implication form (if condition – then).</p> <table border="1"> <thead> <tr> <th>Height</th><th>Hair</th><th>Eyes</th><th>Attractive?</th></tr> </thead> <tbody> <tr> <td>Small</td><td>Blonde</td><td>Brown</td><td>No</td></tr> <tr> <td>Tall</td><td>Dark</td><td>Brown</td><td>No</td></tr> <tr> <td>Tall</td><td>Blonde</td><td>Blue</td><td>Yes</td></tr> <tr> <td>Tall</td><td>Dark</td><td>Blue</td><td>No</td></tr> <tr> <td>Small</td><td>Dark</td><td>Blue</td><td>No</td></tr> <tr> <td>Tall</td><td>Red</td><td>Blue</td><td>Yes</td></tr> <tr> <td>Tall</td><td>Blonde</td><td>Brown</td><td>No</td></tr> <tr> <td>Small</td><td>Blonde</td><td>Blue</td><td>Yes</td></tr> </tbody> </table>	Height	Hair	Eyes	Attractive?	Small	Blonde	Brown	No	Tall	Dark	Brown	No	Tall	Blonde	Blue	Yes	Tall	Dark	Blue	No	Small	Dark	Blue	No	Tall	Red	Blue	Yes	Tall	Blonde	Brown	No	Small	Blonde	Blue	Yes	CO3
Height	Hair	Eyes	Attractive?																																				
Small	Blonde	Brown	No																																				
Tall	Dark	Brown	No																																				
Tall	Blonde	Blue	Yes																																				
Tall	Dark	Blue	No																																				
Small	Dark	Blue	No																																				
Tall	Red	Blue	Yes																																				
Tall	Blonde	Brown	No																																				
Small	Blonde	Blue	Yes																																				

21.	K3	<p>Construct space splitting and K-d tree representation for the following 2D data points in the given sequence. Explain the procedure for these representations.</p> <p>(3, 6), (17, 15), (13, 15), (6, 12), (9, 1), (2, 7), (10, 19)</p>	CO3
-----	----	--	-----

22.	K3	<p>Assume K=2, and the initial clusters are instance 1 and instance 4. Use K-means clustering to find the cluster for the given 2D data points (X, Y) into respective clusters. Find the sum of squared errors of the clusters.</p> <table border="1"> <thead> <tr> <th>Instance</th><th>X</th><th>Y</th></tr> </thead> <tbody> <tr> <td>1</td><td>1.0</td><td>1.5</td></tr> </tbody> </table>	Instance	X	Y	1	1.0	1.5	CO4
Instance	X	Y							
1	1.0	1.5							

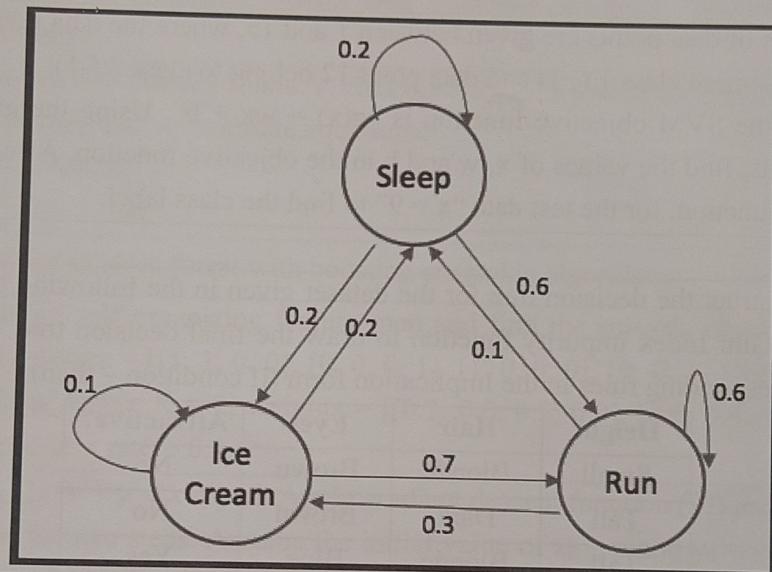
2	1.0	4.5
3	2.0	1.5
4	2.0	3.5
5	3.0	2.5

(OR)

Convert the given Markov chain into reward matrix representation of reinforcement learning. Define the possible Markov sequences with its reward value.

23. K3

CO4



24. K2

Explain Linear Discriminant Analysis (LDA) algorithm with its importance in dimensionality reduction. Compare LDA with Principle Component Analysis (PCA).

CO5

(OR)

25. K2

List the different gradient descent algorithms and explain the conjugate gradient descent algorithm with its importance in optimization problems.

CO5

#### Course Outcomes:

CO1: Understand the basic concepts of machine learning (K2)

CO2: Apply supervised algorithms for different classification problems (K3)

CO3: Understand the need of ensemble methods (K2)

CO4: Apply unsupervised and reinforcement learning techniques to various problems (K3)

CO5: Understand the requirement of dimensionality reduction and optimization techniques (K2)

Degree & Branch	BE CSE			Semester	VI
Subject Code & Name	UCS1602 Compiler Design				
Academic Year	2022-2023 EVEN	Batch	2020-2024	Date	28.02.2023 FN
Time: 08:15 - 09:45 a.m (90 Minutes)	Answer All Questions			Maximum: 50 Marks	

(K1: Remembering, K2: Understanding, K3: Applying, K4: Analyzing, K5: Evaluating)

CO1:	Design a lexical analyzer for a sample language (K3)
CO2:	Apply different parsing algorithms to develop the parsers for the given grammar (K3)
CO3:	Write syntax directed translation for programming language constructs (K3)
CO4:	Understand and implement a simple code generator (K3)
CO5:	Understand and implement code optimization techniques (K3)
CO6:	Construct a compiler for a simple language using modern tools (K6)

**Part – A (6 × 2 = 12 Marks)**

		KL	CO	PI
1.	Outline the steps of language processing system.	K2	CO1	1.3.1
2.	Illustrate the use of the given terms: yytext, yylval, yylex.	K2	CO1	1.4.1
3.	Define token, lexeme and pattern with suitable examples.	K2	CO1	1.4.1
4.	Convert the following NFA into equivalent grammar.  	K2	CO2	4.1.2
5.	Explain the error recovery strategies used by the parser.	K2	CO2	1.4.1
6.	Show that the given grammar is ambiguous. $S \rightarrow S a S \mid \epsilon$	K2	CO2	1.3.1

**Part – B (3×6 = 18 Marks)**

		KL	CO	PI
7.	Explain the phases of a compiler. Illustrate the output of each phase for the following code segment.  int a,b; float c,d; d=a/c-b+40;	K2	CO1	1.4.1
8.	Explain the algorithm for computing FOLLOW and compute FOLLOW for the non-terminals in the given grammar.  $S \rightarrow cAd$ $A \rightarrow aB$ $B \rightarrow b \epsilon$	K2	CO2	2.1.3
9.	Construct the LL(1) parsing table and check whether the given grammar is LL(1) or not.  $S \rightarrow aAbCD \mid \epsilon$ $A \rightarrow ASD \mid \epsilon$ $B \rightarrow SaC \mid hC \mid \epsilon$ $C \rightarrow Sf \mid Cg$ $D \rightarrow aBD \mid \epsilon$	K3	CO2	2.1.3

**Part – C (2 × 10 = 20 Marks)**

		KL	CO	PI
10.	Develop a code using LEX tool to recognize the tokens in the following code segment.  <code>#include&lt;iostream.h&gt; int main () {     int myarray[10] = { 12,4,3,1,15,45,33,21,10,2};      cout&lt;&lt;"\nInput list is \n";     for(int i=0;i&lt;10;i++)     {         cout &lt;&lt;myarray[i]&lt;&lt;"\t";     }     for(int k=1; k&lt;10; k++)     {         int temp = myarray[k];         int j= k-1;         while(j&gt;=0 &amp;&amp; temp &lt;= myarray[j])         {             myarray[j+1] = myarray[j];             j = j-1;         }         myarray[j+1] = temp;     }     cout&lt;&lt;"\nSorted list is \n";     for(int i=0;i&lt;10;i++)     {         cout &lt;&lt;myarray[i]&lt;&lt;"\t";     }</code>	K3	CO1	2.4.1 4.1.2 13.3.1 14.2.1

	{ }			
(Or)				
11.	Apply direct method to construct DFA for the regular expression $(0/1)^*0011$	K3	CO1	2.4.1 4.1.2 13.3.1 14.2.1
12.	Construct the predictive parsing table for the given grammar and parse the string <b>acbbgf</b> <b>Grammar</b> $S \rightarrow aBDh$ $B \rightarrow Bb \mid c$ $D \rightarrow EF$ $E \rightarrow g \mid \epsilon$ $F \rightarrow f \mid \epsilon$	K3	CO2	4.1.2, 13.3.1 14.2.1
(Or)				
13.	Construct a recursive decent parser for the following grammar and parse the string <b>abfc</b> <b>Grammar</b> $S \rightarrow aB \mid aC \mid Sd \mid Se$ $B \rightarrow bBc \mid f$ $C \rightarrow g$	K3	CO2	4.1.2, 13.3.1 14.2.1

**Sri Sivasubramaniya Nadar College of Engineering,  
 Kalavakkam – 603 110**  
 (An Autonomous Institution, Affiliated to Anna University, Chennai)  
 Department of CSE  
 Continuous Assessment Test – II  
 Regulations – R2018

Degree & Branch	BE CSE			Semester	VI
Subject Code & Name	UCS1602 Compiler Design				
Academic Year	2022-2023 EVEN	Batch	2020-2024	Date	31.03.2023 FN
Time: 08:15 - 09:45 a.m (90 Minutes)	Answer All Questions			Maximum: 50 Marks	

(K1: Remembering, K2: Understanding, K3: Applying, K4: Analyzing, K5: Evaluating)

CO1:	Design a lexical analyzer for a sample language (K3)
CO2:	Apply different parsing algorithms to develop the parsers for the given grammar (K3)
CO3:	Write syntax directed translation for programming language constructs (K3)
CO4:	Understand and implement a simple code generator (K3)
CO5:	Understand and implement code optimization techniques (K3)
CO6:	Construct a compiler for a simple language using modern tools (K6)

**Part – A (6 × 2 = 12 Marks)**

		KL	CO	PI
1.	How precedence and associativity are handled by YACC compiler?	K1	CO2	1.4.1 1.3.1
2.	Explain the difference between Translation Scheme and Syntax Directed Translation.	K2	CO3	1.4.1
3.	What is dependency graph? Draw the dependency graph for the expression $8*9+10$	K1	CO3	2.1.3
4.	Explain L-attributed definition.	K2	CO3	1.4.1
5.	What is synthesized attribute?	K1	CO3	1.4.1
6.	Write the SDT for the following production. $D \rightarrow id: T$	K2	CO3	1.4.1

**Part – B (3×6 = 18 Marks)**

KL	CO	PI

7.	Construct Abstract Syntax Tree (AST) for the following expression and also write the syntax directed translation for the same. $S=a+b*c+d$	K3	CO3	2.1.3
8.	Consider the following SDT to convert the binary number to decimal number. Draw the annotated parse tree for the binary number <b>1011</b>  $N \rightarrow L \{ N.dval=L.dval \}$ $L \rightarrow L B \{ L.dval= L.dval * 2 + B.dval \}$ $L \rightarrow B \{ L.dval=B.dval \}$ $B \rightarrow 0 \{ B.dval=0 \}$ $B \rightarrow 1 \{ B.dval=1 \}$	K2	CO3	13.3.1 14.2.1
9.	Explain the implementation of three address code with suitable examples.	K2	CO3	1.3.1 1.4.1

**Part – C ( $2 \times 10 = 20$  Marks)**

		KL	CO	PI
10.	Construct LR(0) items for the grammar G and also check the given grammar is SLR(1) or not  $G: S \rightarrow 0S0 \mid 1S1 \mid 10$	K3	CO2	2.1.3 13.3.1 14.2.1
11.	Construct CLR parser for the grammar G  $G: S \rightarrow Aa \mid bAc \mid Bc \mid bBa$ $A \rightarrow d$ $B \rightarrow d$	K3	CO2	2.1.3 13.3.1 14.2.1
12.	Construct SLR parser for the grammar G. Parse the string <b>accb</b>  $G: S \rightarrow aSSb \mid aSSS \mid c$	K3	CO2	2.1.3 13.3.1 14.2.1
13.	Construct LALR parser for the grammar G. Parse the string <b>0011</b>  $G: S \rightarrow 0S1 \mid 01$	K3	CO2	2.1.3 13.3.1 14.2.1



**Sri Sivasubramaniya Nadar College of Engineering,  
Kalavakkam – 603 110**  
 (An Autonomous Institution, Affiliated to Anna University, Chennai)  
 Department of CSE  
 Continuous Assessment Test – III  
 Regulations – R2018

Degree & Branch	BE CSE				Semester	VI
Subject Code & Name	UCS1602 Compiler Design					
Academic Year	2022-2023 EVEN	Batch	2020-2024	Date	05/05/2023	FN
Time: 08:15 - 09:45 a.m (90 Minutes)	Answer All Questions				Maximum: 50 Marks	

(K1: Remembering, K2: Understanding, K3: Applying, K4: Analyzing, K5: Evaluating)

CO1:	Design a lexical analyzer for a sample language (K3)
CO2:	Apply different parsing algorithms to develop the parsers for the given grammar (K3)
CO3:	Write syntax directed translation for programming language constructs (K3)
CO4:	Understand and implement a simple code generator (K3)
CO5:	Understand and implement code optimization techniques (K3)
CO6:	Construct a compiler for a simple language using modern tools (K6)

**Part – A (6 × 2 = 12 Marks)**

		KL	CO	PI
1.	Apply the following SDT to predict the output for the input $xxyrr$ . $S \rightarrow xW \{ \text{print} (6) \}$ $S \rightarrow y \{ \text{print}(5) \}$ $W \rightarrow Sr\{\text{print} (4) \}$	K3	CO3	1.4.1 1.3.1
2.	Calculate the total instruction cost for the given target code. MOV m,R0 ADD b,R0 SUB #3,R0 MOV 3(R0), a	K3	CO4	1.3.1 1.4.1
3.	Explain register and address descriptors.	K1	CO4	1.4.1
4.	Explain the usage of <code>getReg</code> function	K1	CO4	1.4.1
5.	List the loop optimization techniques	K2	CO5	1.4.1
6.	Define flow graph.	K2	CO5	1.4.1

**Part – B (3×6 = 18 Marks)**

		KL	CO	PI
7.	<p>Apply SDT for flow of control statements to generate three address code for the following code.</p> <pre> main() {     int i, a, =2,b=5,c=3,d=6;     while(i&lt;=20)     {         i=i+5;         switch(i)         {             case 0:                 a=b*-c +b * -c;                 break;             case 2:                 a=b / c * d                 break;             default:                 a=d+c-b;                 break;         }     } } </pre>	K3	CO3	2.1.3
8.	Explain syntax directed translation for assignment statements with example.	K3	CO3	13.3.1
9.	Explain the algorithm for Directed Acyclic Graph (DAG) generation from basic block and apply DAG to optimize the following code	K2	CO4	2.1.3
	<ol style="list-style-type: none"> <li>1. t1 := c * i</li> <li>2. t2 := a[t1]</li> <li>3. t3 := c * i</li> <li>4. t4 := c * j</li> <li>5. t5 := a[t3]</li> <li>6. t6:=c*j</li> <li>7. p:= t6</li> <li>8. t7 := i + 1</li> <li>9. i := t7</li> <li>10. if i &lt;= 20 goto (1)</li> </ol>			

**Part – C (2 × 10 = 20 Marks)**

	KL	CO	PI
10.	K3	CO5	1.3.1 2.1.3 13.3.1

Construct a flow graph for the following code after converting into three address code and do the necessary optimization.

```

a = 20;

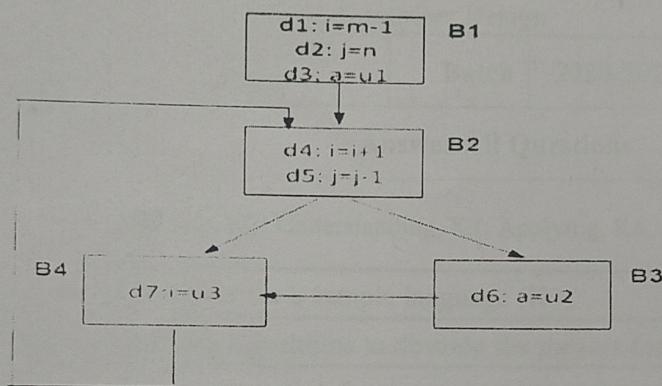
```

```

c = 22/7*a;
while (a<100)
{
    b = x + 0;
    if (a > b)
        a=a+30;
    else
        a=b+30;
}

```

11. Write the reaching definition algorithm and apply the algorithm to the following flow graph



12. Explain code generation algorithm. Translate the given code into three address code and generate assembly code  
 $a = b^* - c + b^* - c$

13. Explain the issues of code generation algorithm in detail.

K3 CO5 1.3.1  
2.1.3  
13.3.1

K2 CO4 13.3.1

K2 CO4 13.3.1

Register No:

2	0	5	0	0	1	0	2	9			
---	---	---	---	---	---	---	---	---	--	--	--

Sri Sivasubramaniya Nadar College of Engineering, Kalavakkam – 603 110.

(An Autonomous Institution, Affiliated to Anna University, Chennai)

B.E. / B.Tech. End Semester Theory Examinations, April/May 2023.

**Sixth Semester**

Computer Science and Engineering

**UCS1602 COMPILER DESIGN**

(Regulations 2018)

Time: Three Hours

**Answer ALL Questions**

Maximum: 100 Marks

K1: Remembering

K2: Understanding

K3: Applying

K4: Analyzing

K5: Evaluating

**PART – A (10 × 2 = 20 Marks)**

01.	K1	Define tokens, patterns and lexemes.	CO1
02.	K2	Compare the features of DFA and NFA.	CO1
03.	K1	Define handle pruning.	CO2
04.	K1	What is the main idea of left factoring? Give an example.	CO2
05.	K1	What is annotated parse tree?	CO3
06.	K3	Construct the three-address code sequence for the following assignment statement. $d = (a - b) + (a - c) + (a - c)$	CO3
07.	K1	List the uses of registers in code generation.	CO4
08.	K2	Explain register and address descriptors.	CO4
09.	K1	Define flow graph.	CO5
10.	K2	Explain dead code elimination with an example.	CO5

**PART – B (5 × 6 = 30 Marks)**

11.	K3	Develop a LEX program for recognizing the tokens such as identifiers and arithmetic operators of C language.	CO1
12.	K3	Apply left recursion elimination algorithm for the following grammar. $E \rightarrow E + T \mid E - T \mid T$ $T \rightarrow a \mid b \mid ( E )$	CO2
13.	K2	Describe quadruples and triples in detail.	CO3
14.	K2	Compare and contrast static versus dynamic memory allocation.	CO4
15.	K2	Explain the principle sources of optimization in detail.	CO5

**PART – C ( $5 \times 10 = 50$  Marks)**

16.	K3	Identify output of each of the phases of compiler for the source program given below  $a:=b+c*50$	CO1
		(OR)	
17.	K3	Construct the minimum state DFA for the regular expression $(a/b)^* a (a/b)$	CO1
		(OR)	
18.	K3	Construct predictive parsing table for the following grammar $E \rightarrow E + T \mid T$ $T \rightarrow T * F \mid F$ $F \rightarrow (E) \mid id$	CO2
		(OR)	
19.	K3	Construct the SLR parsing table for the following grammar $S \rightarrow (L) \mid a$ $L \rightarrow L, S \mid S$ Parse the input string $(a, (a, a))$ .	CO2
		(OR)	
20.	K3	Apply SDT for flow of control statements to generate three address code for the following code.  <pre> main() {     int i, x=1, y=2, z=3, m, n;     while(i&lt;=x*y)     {         i=i+1;         switch(i)         {             case 0:                 m = x*z+y;                 break;             case 2:                 m=x/z+y;                 break;             default:                 n=x+z-y;                 break;         }     } } </pre>	CO3

21.	K3	Write the SDT for constructing syntax tree and apply the same for the following expression $a+b*5$	CO3
22.	K2	Explain the issues of code generation with example.	CO4
		(OR)	
23.	K2	Explain code generation algorithm. Translate the given statement into three address code and generate assembly code: $D:=(a-b)*(a-c)+(a-c)$	CO4
24.	K3	Write the algorithm for DAG generation from the basic block and apply DAG to optimize the following code:  1: $t1 := 4 * i$ 2: $t2 := a [t1]$ 3: $t3 := 4 * i$ 4: $t4 := b [t3]$ 5: $t5 := t2 * t4$ 6: $t6 := \text{Prod} + t5$ 7: $\text{Prod} := t6$ 8: $t7 := i + 1$ 9: $i := t7$ 10: if $i \leq 20$ goto (1)	CO5
		(OR)	
25.	K3	Construct a flow graph for the following source code after converting into three address code and do the necessary optimization.  $a = 20;$ $c = a * 22 / 7;$ <b>while</b> ( $a < 100$ ) { $b = x + 0;$ <b>if</b> ( $a > b$ ) $a = a + 15;$ <b>else</b> $a = a + 15;$ }	CO5

## Course Outcomes:

- CO1: Design a lexical analyzer for a sample language (K3)  
 CO2: Apply different parsing algorithms to develop the parsers for the given grammar (K3)  
 CO3: Write syntax directed translation for programming language constructs (K3)  
 CO4: Understand and implement a simple code generator (K3)  
 CO5: Understand and implement code optimization techniques (K3)

Register No:

2	0	5	0	0	1	0	2	9			
---	---	---	---	---	---	---	---	---	--	--	--

Sri Sivasubramaniya Nadar College of Engineering, Kalavakkam – 603 110.

(An Autonomous Institution, Affiliated to Anna University, Chennai)

B.E. / B.Tech. End Semester Theory Examinations, November/December 2022.

Fifth Semester

Computer Science and Engineering

### UCS1503 THEORY OF COMPUTATION

(Regulations 2018)

Time: Three Hours

Answer ALL Questions

Maximum: 100 Marks

K1: Remembering

K2: Understanding

K3: Applying

K4: Analyzing

K5: Evaluating

#### PART – A (10 × 2 = 20 Marks)

01.	K2	Show that $L = \{ 0^n 1^{2n} \mid n \geq 1 \}$ is not regular.	CO1
02.	K2	Write regular expressions for the following: Strings of A's and B's with no consecutive A's.	CO1
03.	K1	Find the language generated by: $S \rightarrow 0S1 \mid 0A \mid 0 \mid 1B \mid 1$	CO2
04.	K2	Translate the following grammar into an equivalent one with no unit productions and no useless symbols $S \rightarrow ABA \quad A \rightarrow aAA \mid aBC \mid bB \quad B \rightarrow A \mid bB \mid Cb \quad C \rightarrow CC \mid Cc$	CO2
05.	K2	Show a PDA that accepts the language generated by the grammar. $S \rightarrow aSbb$ $S \rightarrow aab$	CO3
06.	K1	Define Deterministic Pushdown Automata.	CO3
07.	K2	Differentiate Turing Machine and Finite Automata.	CO4
08.	K2	Show a Turing machine with no more than three states that accepts the language $a(a+b)^*$ .	CO4
09.	K1	What is Universal Turing machine?	CO5
10.	K1	Define Rice's theorem.	CO5

#### PART – B (5 × 6 = 30 Marks)

11.	K2	If L is accepted by an NFA with $\epsilon$ -transition then show that L is accepted by an NFA without $\epsilon$ -transition.	CO1
12.	K3	Solve: Remove $\epsilon$ productions from the grammar $S \rightarrow ABaC, A \rightarrow BC, B \rightarrow b \mid \epsilon, C \rightarrow D \mid \epsilon, D \rightarrow d$	CO2

13.	K3	Construct the Context Free Grammar (CFG) for the following PDA $\delta(q_0, a, z_0) \rightarrow (q_1, z_1 z_0)$ $\delta(q_0, b, z_0) \rightarrow (q_1, z_2 z_0)$ $\delta(q_1, a, z_1) \rightarrow (q_1, z_1 z_1)$ $\delta(q_1, b, z_1) \rightarrow (q_1, \lambda)$ $\delta(q_1, b, z_2) \rightarrow (q_1, z_2 z_2)$ $\delta(q_1, a, z_2) \rightarrow (q_1, \lambda)$ $\delta(q_1, \lambda, z_2) \rightarrow (q_1, \lambda) // accepted by the empty stack$	CO3
14.	K3	Construct a Turing Machine for the language $L = \{a^n b^n \mid n \geq 1\}$ .	CO4
15.	K2	What are undecidable problems? Explain the undecidability of halting problem of Turing machine.	CO5

**PART – C (5 × 10 = 50 Marks)**

16.	K3	Construct a DFA equivalent to the NFA. $M = (\{p, q, r, s\}, \{0, 1\}, \delta, p, \{q, s\})$ Where $\delta$ is defined in the following table.	CO1
OR			

17.	K3	Construct the NFA for the following $\epsilon$ -NFA	CO1
OR			

18.	K3	Simplify the following context free grammar. (Here, $\Lambda$ stands for epsilon ( $\epsilon$ )). $S \rightarrow TU V$ $T \rightarrow aTb \Lambda$ $U \rightarrow cU \Lambda$ $V \rightarrow aVc W$ $W \rightarrow bW \Lambda$	CO2
OR			

19.	K3	Construct the following grammar into Chomsky Normal Form. $S \rightarrow abSb \mid a \mid aAb$ $A \rightarrow bS \mid aAAb \mid \epsilon$	CO2
20.	K3	Develop a Pushdown Automata (PDA) to accept a language $\{a^n b^{2n} \mid n \geq 1\}$ . Show the validation of $w = aabb$ .	$L =$ CO3
		OR	
21.	K3	Use the CFL pumping lemma to show that $L = \{a^i b^j c^k \mid i < j < k\}$ is not a context free grammar with theorem and proof.	CO3
22.	K3	Construct a Turing machine for proper subtraction, which is defined as $m - n$ if $m > n$ and 0 otherwise.	CO4
		OR	
23.	K3	Construct a Turing Machine to accept strings formed with 0 and 1 and having substring 000.	CO4
24.	K2	Prove that Universal language is recursively enumerable but not recursive. Also prove that the language $L_d$ is not recursive or recursively enumerable.	CO5
		OR	
25.	K2	What is PCP? Check and explain whether the PCP with two lists X and Y have solution, where $X = \{b, bab^3, ba\}$ and $Y = \{b^3, ba, b\}$ .	CO5

**Course Outcomes:**

CO1: Construct automata, regular expression for any given pattern (K3)

CO2: Understand the need of formal languages, and grammars (K3)

CO3: Design pushdown automata for any CFL (K3)

CO4: Design Turing machines for any Languages (K3)

CO5: Explain the Decidability or undecidability of various problems (K2).

Register No:

2	0	5	0	0	1	0	2	9			
---	---	---	---	---	---	---	---	---	--	--	--

Sri Sivasubramaniya Nadar College of Engineering, Kalavakkam – 603 110.

(An Autonomous Institution, Affiliated to Anna University, Chennai)

B.E. / B.Tech. End Semester Theory Examinations, November/December 2022.

Fifth Semester

Computer Science and Engineering

**UCS1505 INTRODUCTION TO CRYPTOGRAPHIC TECHNIQUES**

(Regulations 2018)

Time: Three Hours

Answer ALL Questions

Maximum: 100 Marks

K1: Remembering

K2: Understanding

K3: Applying

K4: Analyzing

K5: Evaluating

**PART – A (10 × 2 = 20 Marks)**

01.	K1	What are the functionalities of private-key encryption schemes?	CO1
02.	K1	What is Pseudo-randomness?	CO1
03.	K1	What is message integrity?	CO2
04.	K1	Define collusion resistance.	CO2
05.	K1	What is a confusion diffusion approach?	CO3
06.	K1	What is a Feistel network?	CO3
07.	K1	What is the result of a prime number theorem?	CO4
08.	K1	What are the limitations of private key cryptography?	CO4
09.	K1	Why are public-key encryption algorithms asymmetric?	CO5
10.	K1	What is a hybrid encryption?	CO5

**PART – B (5 × 6 = 30 Marks)**

11.	K1	List and briefly explain the basic types of attacks against encryption schemes in the order of severity.	CO1
12.	K2	Outline the differences between encryption and message authentication.	CO2
13.	K2	Briefly explain the reasons for pseudorandom permutation to be instantiated with a completely heuristic construction.	CO3
14.	K2	Briefly explain the need of number theory in cryptography.	CO4
15.	K2	Briefly explain the steps in the Eavesdropping experiment.	CO5

**PART – C (5 × 10 = 50 Marks)**

16.	K2	Explain the basic principles of modern cryptography.  (OR)	CO1
17.	K2	Briefly explain the difference between the concrete and asymptotic approaches of computational security.	CO1
18.	K2	Explain the construction of basic CBC-MAC.  (OR)	CO2
19.	K2	Explain the generic “Birthday” attack for collusion resistance.	CO2
20.	K2	Explain the different cases of substitution-permutation networks.  (OR)	CO3
21.	K2	Explain the different stages in the rounds of AES encryption algorithm.	CO3
22.	K3	Users Alice and Bob choose a common prime $q = 353$ and a primitive root $\alpha = 3$ . If user Alice has private key $X_A = 97$ , what is A's public key $Y_A$ ? If user B has private key $X_B = 223$ , what is B's public key $Y_B$ ? What is the shared secret key K? Apply Diffie Hellman Algorithm for the key exchange with detailed algorithmic steps.  (OR)	CO4
23.	K3	Apply Miller-Rabin primality testing algorithm and check whether the number $n=29$ is prime.	CO4
24.	K3	Construct the ciphertext using El Gamal encryption scheme for the message $M=1299$ with the prime number $p=2579$ , primitive root $\alpha = 2$ , and private key $d=765$ .  (OR)	CO5
25.	K2	Apply RSA digital signature algorithm, to sign and verify the message $M=35$ , with $p=7$ , $q=13$ and $e=5$ . Illustrate the procedure.	CO5

**Course Outcomes:**

- CO 1: Describe and implement classical and symmetric ciphers (K2)
- CO 2: Describe the authentication schemes and hash algorithms (K2)
- CO 3: Understand the number theoretic foundations of cryptography (K3)
- CO 4: Compare and contrast various Public key cryptographic techniques (K3)
- CO 5: Illustrate various Public key cryptographic techniques (K3)