Learn Research
Innovate

UNITED INSTITUTE OF TECHNOLOGY

(An Autonomous Institution)
(Approved by AICTE | Affiliated to Anna University |
Accredited by NAAC with A+ Grade | Certified by ISO 9001:2015)
Periyanaickenpalayam, Coimbatore – 641020

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (CYBER SECURITY)

QUESTION BANK

II YEAR

EVEN SEMESTER

ACADEMIC YEAR 2024 – 2025

INDEX

HEAD OF THE DEPARTMENT

ACOE **PRINCIPAL** **CHAIRMAN**

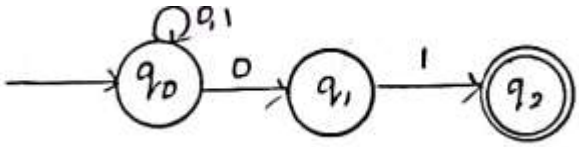
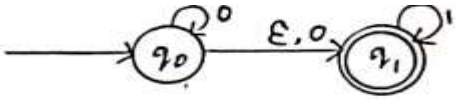
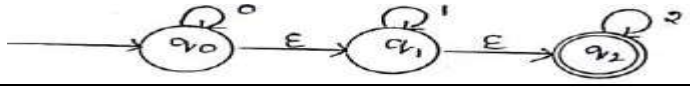
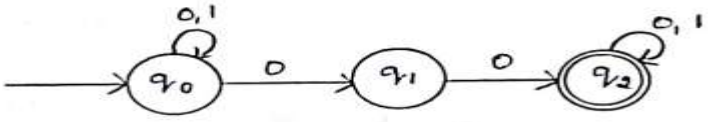
CS3452

THEORY OF COMPUTATION

UNIT I

AUTOMATA AND REGULAR EXPRESSIONS

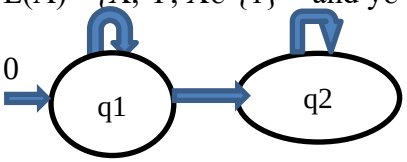
Need for automata theory - Introduction to formal proof – Finite Automata (FA) – Deterministic Finite Automata (DFA) – Non-deterministic Finite Automata (NFA) – Equivalence between NFA and DFA Finite Automata with Epsilon transitions – Equivalence of NFA and DFA- Equivalence of NFAs with and without ε-moves- Conversion of NFA into DFA – Minimization of DFA'S

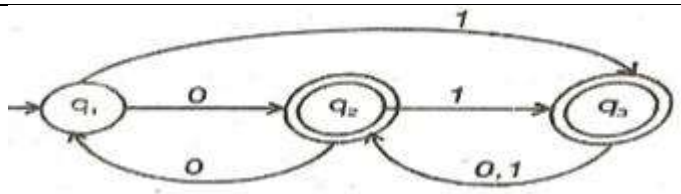
Q.No	Question	CO	BTL	Marks
	PART A			
1.	Define Finite Automata.	1	1	2
2.	Distinguish between DFA and NFA.	1	4	2
3.	List any four types of proofs.	1	1	2
4.	Outline a DFA to accept strings over = {a,b} containing a substring aabb. 	1	2	2
5.	What is the regular expression to represent exponential constants of 'C' language?	1	1	2
6.	Define extended transition diagram.	1	1	2
7.	How to identify NFA -E to represent a*b|c?	1	1	2
8.	Define Epsilon transitions.	1	1	2
	PART B			
1.	Construct DFA equivalent to the NFA given 	1	6	16
2.	Construct a NFA without **ε** moves from NFA with **ε** moves  .	1	6	16
3.	Construct a NFA given below and find the **δ**(q0,01). 	1	6	16
4.	Construct the NFA to check whether ω=01001 is valid or not. 	1	6	16

UNIT II

REGULAR EXPRESSIONS AND LANGUAGES

Regular expression – Regular Languages- Equivalence of Finite Automata and regular expressions Proving languages to be not regular (Pumping Lemma) – Closure properties of regular languages.

Q.No	Question	CO	BTL	Marks
	PART A			
1.	Illustrate regular expression to recognize the set of strings over {a,b} having an odd number of a's and b's and that starts with 'a'	2	3	2
2.	When two states are said to be distinguished? Give an example.	2	1	2
3.	Demonstrate a regular expression that recognize the set of all strings (0+1) * that do not contain the substring 00 and 11 over the alphabet ∑= {0,1}.	2	3	2
4.	Explain that reversal of any regular language is also regular.	2	2	2
5.	Recall the term Regular expression. Give a regular expression for any language containing symbols (0,1) and strictly ends with '1'. Illustrate the following two languages: $L_1 = \{a^n b a^n \mid n > 0\}$ $L_2 = \{a^n b a^n b^{n+1} \mid n > 0\}$ Check whether the above languages are context free or not.	2	1	2
6.	Define Pumping Lemma for regular languages.	2	1	2
7.	Outline an NFA equivalent to (0+1) * (00+11).	2	2	2
8.	What are the various methods for conversion of DFA to RE?	2	1	2
	PART B			
1.	What are the types of closure properties? Explain them.	2	4	16
2.	Construct and t Find R and A where the L(A)= {X, Y, X€ {1} * and y€ {0,1} *  	2	6	16
3.	Construct and Find R for finite automata given below?	2	6	16

				
4.	(i) State and prove pumping lemma? (ii) Show that the set L ={a(i2) |i≥|}is not regular.	2	6	16
5.	Construct a DFA with reduce state equation to the regular expression RE = 10 +(0+11) 0*1	2	6	16

UNIT III

CONTEXT FREE GRAMMAR AND PUSH DOWN AUTOMATA

Types of Grammar - Chomsky ‘s hierarchy of languages -Context-Free Grammar (CFG) and Languages – Derivations and Parse trees –Ambiguity in grammars and languages – Push Down Automata (PDA): Definition – Moves - Instantaneous descriptions - Languages of pushdown automata – Equivalence of pushdown automata and CFG-CFG to PDA-PDA to CFG – Deterministic Pushdown Automata.

Q.No	Question	CO	BTL	Marks
	PART A			
1.	Outline CFG to accept the language defined by, L={a(i)b(j)c(k)|i,j,k>=0 and i=j+k}.	3	2	2
2.	List out the steps for performing LL parsing.	3	1	2
3.	Illustrate a regular expression that recognize the set of all strings (0+1) * that do not contain the substrings 00 and 11 over the alphabet ∑= {0,}.	3	3	2
4.	Define Pumping lemma for context free language	3	1	2
5.	Mention a few points regarding the Chomsky hierarchy with illustration.	3	1	2
6.	Explain the context free grammar representing the set of palindromes over (0+1) *.	3	2	2
7.	Define Chomsky ‘s hierarchy.	3	1	2
8.	What is Deterministic pushdown automata?	3	1	2
	PART B			
1.	For the grammar given below give the parse tree for leftmost and rightmost derivation of the string 1001.	3	6	16
2.	Let L = {a (n) b(n) c (m) d(m) | n,m ≥ 1} find a PDA for L?	3	5	16
3.	Let L = { a(i) b(j) c (k) | i, j, k ≥ 0 i + j = k} Prove the transition function. i) . Accepted by final state. ii). Accepted by empty state (LN).	3	5	16
4.	Construct PDA to CFG M=({p,q},{0,1},{x,z},{q,z,⦰}	3	6	16
5.	Construct CFG to PDA. M=({q0,q1},{0,1},{z0,xx},δ,qo,z0,⦰}) δ(q0,1,z0)={q0,xz0} δ(q0,1,x)={qo,xzo} δ(q0,0,x)={q1,x} δ(q0,ε,z0)={q0,ϵ } δ(q1,1,x)-{q1,ϵ } δ(q1,0,z0)=(q0,zo)	3	6	16

UNIT IV

NORMAL FORMS AND TURING MACHINE

Normal forms for CFG – Simplification of CFG- Chomsky Normal Form (CNF) and Grei bach Normal Form (GNF) – Pumping lemma for CFL – Closure properties of Context Free Languages – Turing Machine: Basic model – definition and representation –Instantaneous Description – Language acceptance by TM – TM as Computer of Integer functions – Programming techniques for Turing machines (subroutines).

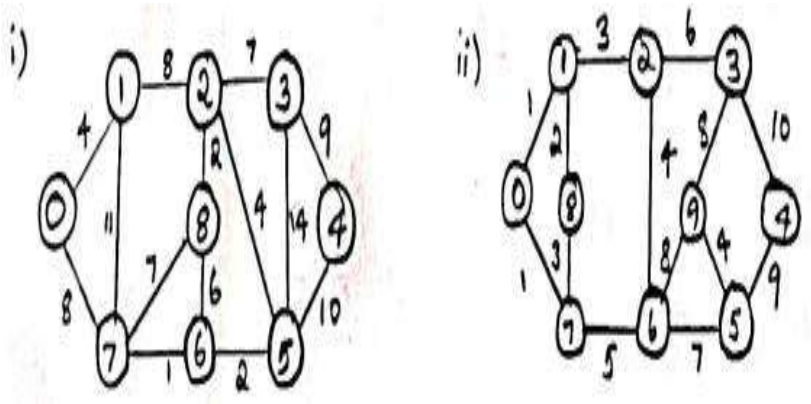
Q.No	Question	CO	BTL	Marks
	PART A			
1.	Tabulate the difference between CNF and GNF.	4	2	2
2.	Illustrate the philosophy behind the Pumping lemma for CFLs.	4	3	2
3.	List the different types of mouse events.	4	2	2
4.	What is the role of checking off symbols in a Turing Machine?	4	1	2
5.	Define a Turing Machine	4	1	2
6.	What is meant by a Turing Machine with two-way infinite tape?	4	1	2
7.	Explain the multi tape Turing Machine mode. Is it more power than the basic turing machine? justify your answer	4	2	2
8.	Define instantaneous description of a Turing Machine?	4	1	2
	PART B			
1.	Find GNF for the following Grammar S→AB; A→Bs|b; B→SA|a |b; B→SA|a	4	6	16
2.	Write Programming Techniques for Turning Machines construction and explain.	4	4	16
3.	Design a Turing Machine that accepts all the strings of the form a (n) b(n)for n≥1 and reject all the strings.	4	6	16
4.	Find a grammar in Chomsky Normal Form (CNF) equivalent to S→aAbB; A→aA|a; B→bB|b	4	5	16
5.	Let G be the grammar S→OB| 1 A| A→O|OS|1AA; B→1|1S|OBB. For the string 00110101	4	5	16

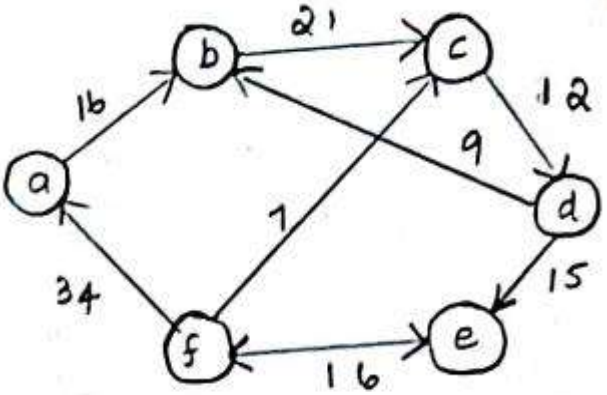
	Find i) Leftmost derivation ii) Right most derivation iii) Derivation Tree for the string 0110 iv) Find a rightmost derivation And construct.			

UNIT V

UNDECIDABILITY

Unsolvable Problems and Computable Functions –PCP-MPCP-Recursive and recursively enumerable languages – Properties -Universal Turing machine -Tractable and Intractable problems – P and NP completeness – Kruskal's algorithm – Travelling Salesman Problem-3-CNFSAT problems.

Q.No	Question	CO	BTL	Marks
	PART A			
1.	What are tractable problems?	5	1	2
2.	Define class P and NP problems.	5	1	2
3.	When is a language L recursively enumerable?	5	1	2
4.	Explain that the union of recursive language is recursive language.	5	2	2
5.	What is undecidability problem? Give an example for an undecidable problem.	5	1	2
6.	Differentiate between recursive and recursively enumerable languages.	5	2	2
7.	Define Diagonal languages.	5	1	2
8.	Mention any two undecidability properties for recursively enumerable language.	5	1	2
	PART B			
1.	Solve the given problem using Kruskal's algorithm? 	5	6	16

2.	State recursive and non-recursive enumerable languages and Explain it.	5	4	16
3.	State rice theorem.	5	4	16
4.	State halting problem is undecidable.	5	4	16
5.	Discuss travelling salesman problem in terms of P and NP completeness? 	5	6	16

-----END----

CS3491
ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

UNIT I

PROBLEM SOLVING

Introduction to AI - AI Applications - Problem solving agents – search algorithms – uninformed search strategies – Heuristic search strategies – Local search and optimization problems – adversarial search – constraint satisfaction problems (CSP)

Q.No	Question	CO	BTL	Marks
	PART A			
1.	What is Artificial Intelligence?	1	1	2
2.	What are various applications of AI? or What today? can AI do	1	1	2
3.	What are the advantages of heuristic function?	1	1	2
4.	Is AI a science, or is it engineering? Or neither or both? Explain.	1	2	2
5.	How will you measure the problem-solving performance?	1	1	2
6.	State on which basis search algorithms are chosen?	1	1	2
7.	List some of the uninformed search techniques.	1	1	2
8.	What do you mean by local maxima with respect to search technique?	1	1	2
	PART B			
1.	Solve the following problems. What types of control strategy is used in the following problem? i. The Tower of Hanoi ii. Crypto-arithmetic iii. The missionaries and cannibals' problems iv. 8-puzzle problem	1	4	16
2.	(i) Explain the A* search and give the proof of optimality of A* (ii) Explain AO* algorithm with a suitable example. State the limitations in the algorithm?	1 1	4 4	8 8
3.	Explain the nature of heuristics with example. What is the effect of heuristics accuracy?	1	4	16
4.	Discuss about constraint satisfaction problem with an algorithm for solving a crypt arithmetic Problem. CROSS +ROADS DANGER ----------	1	6	16

UNIT II

PROBABILISTIC REASONING

Acting under uncertainty – Bayesian inference – naïve bayes models. Probabilistic reasoning – Bayesian networks – exact inference in BN – approximate inference in BN – causal networks.

Q.No	Question	CO	BTL	Marks
	PART A			
1.	Define principle of maximum expected utility (MEU)	2	1	2
2.	Mention the needs of probabilistic reasoning in AI.	2	1	2
3.	State Bayes' Theorem in Artificial Intelligence.	2	1	2
4.	What is Bayesian Belief Network?	2	1	2
5.	Given that P(A)=0.3, P(A|B) =0.4 and P(B)=0.5, Compute P(B|A).	2	2	2
6.	Differentiate uncertainty with ignorance	2	2	2
7.	What is the need for utility theory in uncertainty?	2	1	2
8.	Why does uncertainty arise?	2	2	2
	PART B			
1.	Explain variable elimination algorithm for answering queries on Bayesian networks?	2	4	16
2.	Construct a Bayesian Network and define the necessary CPTs for the given scenario. We have a bag of three biased coins a, b and c with probabilities of coming up heads of 20%, 60% and 80% respectively. One coin is drawn randomly from the bag (with equal likelihood of drawing each of the three coins) and then the coin is flipped three times to generate the outcomes X1, X2 and X3 a. Draw a Bayesian network corresponding to this setup and define the relevant CPTs b. Calculate which coin is most likely to have been drawn if the flips come up HHT	2	6	16
3.	Discuss about Bayesian Theory and Bayesian network.	2	6	16
4.	Explain how does Bayesian statistics provide reasoning under various kinds of uncertainty?	2	4	16

UNIT III

SUPERVISED LEARING

Introduction to machine learning – Linear Regression Models: Least squares, single & multiple variables, Bayesian linear regression, gradient descent, Linear Classification Models: Discriminant function – Probabilistic discriminative model - Logistic regression, Probabilistic generative model – Naive Bayes, Maximum margin classifier – Support vector machine, Decision Tree, Random forests.

Q.No	Question	CO	BTL	Marks
	PART A			
1.	What is Machine Learning?	3	1	2
2.	What is 'Over fitting' in Machine learning?	3	1	2
3.	What are the different Algorithm techniques in Machine Learning?	3	1	2
4.	What is the main key difference between supervised and unsupervised machine learning?	3	1	2
5.	What is 'Training set' and 'Test set'?	3	1	2
6.	What is a Linear Regression?	3	1	2
7.	Why is random forest better than SVM?	3	1	2
8.	Difference between stochastic gradient descent (SGD) and gradient descent (GD)?	3	2	2
	PART B			
1.	Explain Naïve Bayes Classifier with an Example.	3	4	16
2.	Explain the following. a) Linear regression b) Logistic Regression	 3 3	 4 4	 8 8
3.	(i) Explain SVM Algorithm in Detail. (ii) Explain Decision Tree Classification.	3 3	4 4	8 8
4.	Explain the principle of the gradient descent algorithm. Accompany your explanation with a diagram. Explain the use of all the terms and constants that you introduce and comment on the range of values that they can take.	3	4	16

UNIT IV

ENSEMBLE TECHNIQUES AND UNSUPERVISED LEARNING

Combining multiple learners: Model combination schemes, Voting, Ensemble Learning - bagging, boosting, stacking, Unsupervised learning: K-means, Instance Based Learning: KNN, Gaussian mixture models and Expectation maximization.

Q.No	Question	CO	BTL	Marks
	PART A			
1.	What is bagging and boosting in ensemble learning?	4	1	2
2.	What type of classifiers are used in weighted voting method?	4	1	2
3.	What are examples of unsupervised learning?	4	1	2
4.	What are Gaussian mixture models. How is expectation maximization used in it?	4	1	2
5.	What is the principle of maximum likelihood?	4	1	2
6.	What is expectation maximization algorithm used for?	4	1	2
7.	How do you implement expectation maximization algorithm?	4	1	2
8.	What is the advantage of Gaussian process?	4	1	2
	PART B			
1.	List the applications of clustering and identify advantages and disadvantages of clustering algorithm.	4	4	16
2.	Explain various learning techniques involved in unsupervised learning?	4	4	16
3.	What is Gaussian process? And explain in detail of Gaussian parameter estimates with suitable examples.	4	4	16
4.	List non-parametric techniques and Explain K-nearest neighbour estimation.	4	4	16

UNIT V

NEURAL NETWORKS

Perceptron - Multilayer perceptron, activation functions, network training – gradient descent optimization – stochastic gradient descent, error backpropagation, from shallow networks to deep networks –Unit saturation (aka the vanishing gradient problem) – ReLU, hyper parameter tuning, batch normalization, regularization, dropout.

Q.No	Question	CO	BTL	Marks
	PART A			
1.	What is perceptron and its types?	5	1	2
2.	What are the advantages of Multilayer Perceptron?	5	1	2
3.	What are the three main types gradient descent algorithm?	5	1	2
4.	Does stochastic gradient descent lead to faster training?	5	1	2
5.	What are the types of activation function?	5	1	2
6.	Why is ReLU used in deep learning?	5	1	2
7.	Is stochastic gradient descent same as gradient descent?	5	1	2
8.	What are the activation functions of MLP?	5	1	2
	PART B			
1.	(i) List the factors that affect the performance of multilayer feed-forward neural network. (ii) Difference between a Shallow Net & Deep Learning Net.	5 5	4 4	8 8
2.	Develop a Back-propagation algorithm for Multilayer Feed forward neural network consisting of one input layer, one hidden layer and output layer from first principles.	5	4	16
3.	Draw the architecture of a Multilayer perceptron (MLP) and explain its operation. Mention its advantages and disadvantages.	5	5	16
4.	Write the flowchart of error back-propagation training algorithm.	5	5	16

-----END----

CB3401

DATABASE MANAGEMENT SYSTEMS AND SECURITY

UNIT I

RELATIONAL DATABASES

Data Models – Relational Data Models – Relational Algebra – Structured Query Language – Entity-Relationship Model – Mapping ER Models to Relations – Distributed Databases – Data Fragmentation – Replication.

Q.No	Question	CO	BTL	Marks
	PART A			
1.	Define a data model.	1	1	2
2.	What is the relational data model?	1	1	2
3.	What is relational algebra?	1	1	2
4.	What is SQL?	1	1	2
5.	What is an entity in the ER model?	1	1	2
6.	What is data fragmentation?	1	1	2
7.	Define replication in distributed databases.	1	1	2
8.	What is the purpose of mapping ER models to relations?	1	1	2
	PART B			
1.	Explain the various types of data models with examples.	1	4	16
2.	(i) Explain the process of Mapping an Entity-Relationship (ER) Model to a Relational Model. (ii) Explain Relational Algebra and its fundamental operations with examples.	1 1	4 4	8 8
3.	Describe Structured Query Language (SQL) and its various types of commands with examples.	1	4	16
4.	Describe Data Fragmentation and Replication in Distributed Databases.	1	4	16

UNIT II

DATABASE DESIGN

ER Diagrams – Functional Dependencies – Non-Loss Decomposition Functional Dependencies – First Normal Form – Second Normal Form – Third Normal Form – Dependency Preservation – Boyce/Codd Normal Form – Multi-Valued Dependencies and Fourth Normal Form – Join Dependencies and Fifth Normal Form

Q.No	Question	CO	BTL	Marks
	PART A			
1.	What is an ER diagram?	2	1	2
2.	Define functional dependency.	2	1	2
3.	What is non-loss decomposition?	2	1	2
4.	What is the First Normal Form (1NF)?	2	1	2
5.	What is the Second Normal Form (2NF)?	2	1	2
6.	What is Boyce-Codd Normal Form (BCNF)?	2	1	2
7.	What is a multi-valued dependency?	2	1	2
8.	Define Fifth Normal Form (5NF).	2	1	2
	PART B			
1.	(i) Explain ER diagrams with components and examples. (ii)What are Functional Dependencies? Explain with examples.	2 2	4 4	8 8
2.	(i) Explain First Normal Form (1NF), Second Normal Form (2NF), and Third Normal Form (3NF) with examples. (ii) What is Boyce-Codd Normal Form (BCNF), and how is it different from 3NF?	2 2	4 4	8 8
3.	Explain Dependency Preservation in Normalization? How does it relate to database decomposition?	2	4	16
4.	Explain the Multi-Valued Dependencies and Fourth Normal Form (4NF)? Explain Join Dependencies and Fifth Normal Form (5NF).	2	4	16

UNIT III

TRANSACTION MANAGEMENT

Transaction Concepts – ACID Properties – Serializability – Transaction Isolation Levels – Concurrency Control – Need for Concurrency – Lock-Based Protocols – Deadlock Handling – Recovery System – Failure Classification – Recovery Algorithm.

Q.No	Question	CO	BTL	Marks
	PART A			
1.	What is a transaction in a database?	3	1	2
2.	Define ACID properties.	3	1	2
3.	What is serializability?	3	1	2
4.	What is a transaction isolation level?	3	1	2
5.	Why is concurrency control needed?	3	1	2
6.	What is a lock in a database?	3	1	2
7.	Define deadlock in a database.	3	1	2
8.	What is failure classification in a recovery system?	3	1	2
	PART B			
1.	Explain Transaction Concepts and the importance of ACID properties in database systems.	3	4	16
2.	(i) Explain concurrency control and lock-based protocols. (ii) What is Serializability in database transactions? Explain its types.	3 3	4 4	8 8
3.	Explain about the deadlock handling in databases.	3	4	16
4.	Analyse on the recovery system and recovery algorithms.	3	4	16

UNIT IV

DATABASE SECURITY

Need for database security – SQL Injection Attacks – The Injection Technique – SQLi Attack Avenues and Types

Q.No	Question	CO	BTL	Marks
	PART A			
1.	Why is database security important?	4	1	2
2.	What is SQL injection?	4	1	2
3.	What is the injection technique in SQLi?	4	1	2
4.	List the common avenues of SQL injection attacks.	4	1	2
5.	What are the types of SQL injection attacks?	4	1	2
6.	Define blind SQL injection.	4	1	2
7.	What is an error-based SQL injection?	4	1	2
8.	What is a union-based SQL injection?	4	1	2
	PART B			
1.	Explain the need for database security in detail.	4	4	16
2.	Describe SQL injection attacks and their types with examples.	4	4	16
3.	Discuss SQL injection attack avenues and preventive measures.	4	6	16
4.	Explain the impacts and mitigation techniques of SQL injection attacks.	4	4	16

UNIT V

ACCESS CONTROL AND ENCRYPTION

Database Access Control – SQL based access definition – Cascading Authorizations – Role- based access control – Inference – Database encryption

Q.No	Question	CO	BTL	Marks
	PART A			
1.	What is database access control?	5	1	2
2.	What is SQL-based access definition?	5	1	2
3.	Define cascading authorizations.	5	1	2
4.	What is role-based access control (RBAC)?	5	1	2
5.	What is inference in database security?	5	1	2
6.	What is database encryption?	5	1	2
7.	Differentiate between symmetric and asymmetric encryption	5	2	2
8.	What are the advantages of role-based access control?	5	1	2
	PART B			
1.	Explain database access control mechanisms.	5	4	16
2.	Discuss role-based access control (RBAC) in detail.	5	6	16
3.	Discuss the SQL-based access control mechanisms with examples.	5	6	16
4.	Explain the role of encryption in database security.	5	4	16

-----END----

CB3402
OPERATING SYSTEMS AND SECURITY

UNIT I

OPERATING SYSTEM OVERVIEW

Computer-System Organization – Architecture – Operating-System Operations – Resource Management – Security and Protection – Distributed Systems – Kernel Data Structures – Operating-System Services – System Calls – System Services – Why Applications Are Operating System Specific – Operating-System Design and Implementation - Operating-System Structure – Building and Booting an Operating System

Q.No	Question	CO	BTL	Marks
	PART A			
1.	Define operating system.	1	1	2
2.	Define Kernal.	1	1	2
3.	Define system call.	1	1	2
4.	What is Boot strapping?	1	1	2
5.	Difference between Monolithic &Microlithic.	1	2	2
6.	What are the advantages of peer- to- peer systems over client -server systems?	1	1	2
7.	Write about fork () and exec () system call.	1	1	2
8.	List the various system call.	1	1	2
	PART B			
1.	Explain the various types of systems calls with an example for each?	1	4	16
2.	Explain about the services of Operating Systems.	1	4	16
3.	What is User Interface? And explain about types of User Interface.	1	4	16
4.	Explain the difference Operating Systems structures with neat sketch.	1	4	16

UNIT II

PROCESS MANAGEMENT

Process Concept – Process Scheduling – Operation on Processes, Inter-process Communication – Threads – Overview – Multithreading models – Threading issues; CPU Scheduling – Scheduling criteria, Scheduling algorithms; Process Synchronization – critical-section problem, Synchronization hardware, Mutex locks, Semaphores, Critical regions, Monitors; Deadlock – System model, Deadlock characterization, Methods for handling deadlocks, Deadlock prevention, Deadlock avoidance, Detection, Recovery

Q.No	Question	CO	BTL	Marks
	PART A			
1.	What is process?	2	1	2
2.	Sketch the process in memory.	2	1	2
3.	Sketch the process states.	2	1	2
4.	What is PCB?	2	1	2
5.	What is context switch?	2	1	2
6.	Write a C program forking separate process	2	1	2
7.	What is throughput?	2	1	2
8.	What is turnaround time?	2	1	2
	PART B			
1.	Explain about the process states with neat diagram.	2	4	16
2.	Explain about Process Control Block (PCB)?	2	4	16
3.	What is Inter Process Communication (IPC) and explain about the mechanism for communicate the process and its actions.	2	4	16
4.	Consider the FCFS, Non -pre-emptive SJF, Round Robin (RR) (quantum = 10 msec) scheduling algorithms. Illustrate the scheduling the Gantt chart, which algorithm will give the minimum average waiting time.	2	4	16

UNIT III

MEMORY MANAGEMENT AND FILE SYSTEMS

Main Memory – Background, Swapping, Contiguous Memory Allocation, Paging, Segmentation – Virtual Memory – Demand Paging, Page Replacement, Allocation, Thrashing; Allocating Kernel Memory. Mass Storage system - HDD Scheduling - File concept, Access methods, Directory Structure, Sharing and Protection; File System Structure, Directory implementation, Allocation Methods, Free Space Management

Q.No	Question	CO	BTL	Marks
	PART A			
1.	Difference between Address space and physical Address space.	3	2	2
2.	Define Swapping.	3	1	2
3.	Difference between Roll in and Roll out.	3	2	2
4.	What is fragmentation and its types?	3	1	2
5.	Difference between External and Internal fragmentation.	3	2	2
6.	What is Kernel Memory Allocation?	3	1	2
7.	What is HDD Scheduling?	3	1	2
8.	What is a File System?	3	1	2
	PART B			
1.	What is Demand Paging? Explain in detail.	3	4	16
2.	The page faults, hit ratio and miss ratio using FIFO, optimal page replacement and LRU schemes.	3	4	16
3.	Explain FIFO page replacement algorithm and optimal Page replacement Algorithm with an example and diagram.	3	4	16
4.	Explain File System Structure and Various File Allocation Methods	3	4	16

UNIT IV

SECURE SYSTEMS AND VERIFIABLE SECURITY GOALS

Security Goals – Trust and Threat Model – Access Control Fundamentals – Protection System – Reference Monitor – Secure Operating System Definition – Assessment Criteria – Information Flow – Information Flow Secrecy Models – Denning's Lattice Model – Bell LaPadula Model – Information Flow Integrity Models – Biba Integrity Model – Low-Water Mark Integrity – Clark Wilson Integrity

Q.No	Question	CO	BTL	Marks
	PART A			
1.	Write the disk scheduling?	4	1	2
2.	Write types of files with their extensions.	4	1	2
3.	List the various types of file structures.	4	1	2
4.	What is Kernal I/O subsystems?	4	1	2
5.	What is a Reference Monitor?	4	1	2
6.	What is a Secure Operating System?	4	1	2
7.	What are Assessment Criteria in Secure Systems?	4	1	2
8.	What is Information Flow in a Secure System	4	1	2
	PART B			
1.	Explain Contiguous allocation and linked allocation of disk space with an example.	4	4	16
2.	Following are the reference attempted tihard disks:67,22,78,34,21,78,99. Recommend a suitable disk scheduling algorithm among FIFO, SSTF, SCAN and LOOK after applying all. Provide statements that support your recommendation. (NOTE: Initial head position is 20.)	4	4	16
3.	Explain the Various Protection Mechanisms and the Role of the Reference Monitor in Secure Systems.	4	4	16
4.	Explain the Secure Operating System Definitions and their Importance in Security	4	4	16

UNIT V

SECURITY IN OPERATING SYSTEMS

UNIX Security – UNIX Protection System – UNIX Authorization – UNIX Security Analysis – UNIX Vulnerabilities – Windows Security – Windows Protection System – Windows Authorization – Windows Security Analysis – Windows Vulnerabilities – Address Space Layout Randomizations – Retrofitting Security into a Commercial Operating System – Introduction to Security Kernels

Q.No	Question	CO	BTL	Marks
	PART A			
1.	What is UNIX Security?	5	1	2
2.	What is the UNIX Protection System?	5	1	2
3.	What is UNIX Authorization?	5	1	2
4.	What is UNIX Security Analysis?	5	1	2
5.	What are UNIX Vulnerabilities?	5	1	2
6.	What is Windows Security?	5	1	2
7.	What is the Windows Protection System?	5	1	2
8.	What is Windows Authorization?	5	1	2
	PART B			
1.	Explain the UNIX Protection System and its Security Mechanisms.	5	4	16
2.	Explain the Concept of Address Space Layout Randomization (ASLR) and its Role	5	4	16
3.	What is a Security Kernel, and How Does it Contribute to Secure Operating Systems?	5	4	16
4.	Explain the Retrofitting of Security into Commercial Operating Systems.	5	4	16

-----END----

CB3491
CRYPTOGRAPHY AND CYBER SECURITY

UNIT I

INTRODUCTION TO SECURITY

Computer Security Concepts – The OSI Security Architecture – Security Attacks – Security Services and Mechanisms – A Model for Network Security – Classical encryption techniques: Substitution techniques, Transposition techniques, Steganography – Foundations of modern cryptography: Perfect security – Information Theory – Product Cryptosystem – Cryptanalysis.

Q.No	Question	CO	BTL	Marks
	PART **A**			
1.	Define confidentiality.	1	1	2
2.	Compare active and passive attack.	1	2	2
3.	Differentiate block cipher and stream cipher.	1	2	2
4.	What is the difference between Mono and polyalphabetic cipher?	1	1	2
5.	What is steganography?	1	1	2
6.	List out the problems of one-time pad.	1	1	2
7.	Find the given text “anna university” into cipher text using Rail fence technique.	1	2	2
8.	How substitution cipher is different from transposition cipher. Give example for each method.	1	1	2
	PART B			
1.	(i) Explain OSI security architecture model with neat diagram (ii) Describe the various security mechanism.	1 1	4 4	8 8
2.	(i) Describe the various security mechanism. (ii) Explain the cease cipher and monoalphabetic cipher.	1 1	4 4	8 8
3.	Describe (i) Playfair Cipher (ii) Rail fence Cipher (iii) Vignere Cipher.	1	4	16
4.	Discuss the rules to be followed in Playfair method. Encrypt the word “Network security” with the keyword “crypto” using Playfair method.	1	4	16

UNIT II

SYMMETRIC CIPHERS

Number theory – Algebraic Structures – Modular Arithmetic – Euclid's algorithm – Congruence and matrices – Group, Rings, Fields, Finite Fields
SYMMETRIC KEY CIPHERS: SDES – Block Ciphers – DES, Strength of DES – Differential and linear cryptanalysis – Block cipher design principles – Block cipher mode of operation – Evaluation criteria for AES – Pseudorandom Number Generators – RC4 – Key distribution.

Q.No	Question	CO	BTL	Marks
	PART A			
1.	What is symmetric key encryption? and its components.	2	1	2
2.	Give the 5 modes of operations of block cipher.	2	1	2
3.	Determine the GCD of (1970,1066) using Euclid's algorithm.	2	2	2
4.	Define field and ring in number theory.	2	1	2
5.	Define Abelian group.	2	1	2
6.	List the 4 different stages of AES.	2	1	2
7.	Difference between a block cipher and a stream cipher?	2	2	2
8.	What is the difference between diffusion and confusion?	2	1	2
	PART B			
1.	(i) Explain AES algorithm with all its round functions in detail. (ii)Explain triple DES and its algorithm.	2 2	4 4	8 8
2.	(i) Describe DES algorithm with neat diagram and the steps. (ii)Write notes about birthday attack.	2 2	4 4	8 8
3.	Solve GCD (98,56) using extended Euclidean algorithm also, write the algorithm.	2	6	16
4.	Explain about the RC4 algorithm with neat diagram?	2	4	16

UNIT III

ASYMMETRIC CRYPTOGRAPHY

MATHEMATICS OF ASYMMETRIC KEY CRYPTOGRAPHY: Primes – Primality Testing – Factorization – Euler's totient function, Fermat's and Euler's Theorem – Chinese Remainder Theorem – Exponentiation and logarithm.
ASYMMETRIC KEY CIPHERS: RSA cryptosystem – Key distribution – Key management – Diffie Hellman key exchange -– Elliptic curve arithmetic – Elliptic curve cryptography.

Q.No	Question	CO	BTL	Marks
	PART A			
1.	State Fermat's theorem.	3	1	2
2.	Check whether 1) 2 is a primitive root of mod 5 & 2) 4 is a primitive root of mod 5	3	2	2
3.	State Euler's theorem.	3	1	2
4.	Define discrete logarithm.	3	1	2
5.	What is the principal attraction of ECC, compared to RSA?	3	1	2
6.	Give the applications of the public key crypto system.	3	2	2
7.	For p = 11 and q = 19 and choose d = 17. Apply RSA algorithm where Cipher message = 80 and thus find the plain text.	3	2	2
8.	What is meet in the Middle Attack?	3	2	2
	PART B			
1.	(i) State and prove Fermat's theorem. (ii) State Chinese Remainder Theorem and find X for the given set of congruent equations using CRT (Dec 2020) X=1 (mod 5) X=2 (mod 7) X=3 (mod 9) X=4 (mod 11).	3 3	4 4	8 8
2.	(i) Explain RSA algorithm, perform encryption and decryption to the system with p=7, q=11, e=17, M=8. (ii) Explain public key cryptography and when it is preferred?	3 3	4 4	8 8
3.	Explain Diffie-Hellman key exchange algorithm in detail.	3	4	16
4.	Given prime number q=17, Primitive root a=6, private key of A, XA =5, message m=13, random number k=10. Perform encryption & decryption using El Gamal cryptosystem.	3	4	16

UNIT IV

INTEGRITY AND AUTHENTICATION ALGORITHMS

Authentication requirement – Authentication function – MAC – Hash function – Security of hash function: HMAC, CMAC – SHA – Digital signature and authentication protocols – DSS – Schnarr Digital Signature Scheme – El Gamal cryptosystem – Entity Authentication: Biometrics, Passwords, Challenge Response protocols – Authentication applications – Kerberos MUTUAL TRUST: Key management and distribution – Symmetric key distribution using symmetric and asymmetric encryption – Distribution of public keys – X.509 Certificates.

Q.No	Question	CO	BTL	Marks
	PART A			
1.	What is digital signature?	4	1	2
2.	Compare MAC and hash function	4	2	2
3.	Specify the various types of authentication protocol	4	2	2
4.	What is digital signature?	4	1	2
5.	What is realm in Kerberos?	4	1	2
6.	How digital signatures differ from authenticator protocols?	4	1	2
7.	State Birthday Problem.	4	1	2
8.	Identify and write the requirements defined by Kerberos.	4	3	2
	PART B			
1.	(i) List out the advantages of MD5 and SHA algorithms. (ii) Write down the steps involved in (a) El Gamal digital signature scheme (iii) Schnorr digital signature scheme used for authenticating a person.	4 4	4 4	8 8
2.	(i) Explain El Gamal digital signature schemes. (ii) Explain the format of the X.509 certificate in detail.	4 4	4 4	8 8
3.	Explain Kerberos version 4 in detail.	4	4	16
4.	Explain PKI management model and its operations with help of a diagram.	4	4	16

UNIT V

CYBER CRIMES AND CYBER SECURITY

Cyber Crime and Information Security – classifications of Cyber Crimes – Tools and Methods – Password Cracking, Keyloggers, Spywares, SQL Injection – Network Access Control – Cloud Security – Web Security – Wireless Security.

Q.No	Question	CO	BTL	Marks
	PART A			
1.	Define Cybercrime.	5	1	2
2.	Define Information Security. List the need for information Security.	5	1	2
3.	Define Key loggers.	5	1	2
4.	What are the Types of SQL Injections?	5	1	2
5.	What is network access control? Advantages of Network Access Control?	5	1	2
6.	What is Cloud Security? What are the challenges of advanced Cloud Security?	5	1	2
7.	What are the security considerations in web security?	5	1	2
8.	Define Wireless Security.	5	1	2
	PART B			
1.	(i) Explain in detail about the classification of cybercrimes and wireless security. (ii) Explain about information security.	5 5	4 4	8 8
2.	(i) Explain in detail about the types of cyber-attacks. (ii) Write short notes on key-logger and explain in detail about types of Key-logger?	5 5	4 4	8 8
3.	Explain briefly about the spywares.	5	4	16
4.	Explain in detail about the SQL injection and its types.	5	4	16

----- END ----

GE3451
ENVIRONMENTAL SCIENCE AND SUSTAINABILITY

UNIT I

ENVIRONMENT, ECOSYSTEMS AND BIODIVERSITY

Definition, scope and importance of environment – need for public awareness. Eco-system and Energy flow– ecological succession. Types of biodiversity: genetic, species and ecosystem diversity– values of biodiversity, India as a mega-diversity nation – hot-spots of biodiversity – threats to biodiversity: habitat loss, poaching of wildlife, man-wildlife conflicts – endangered and endemic species of India – conservation of biodiversity: In-situ and ex-situ.

Q.No	Question	CO	BTL	Marks
	PART A			
1.	What is an ecosystem and what are the components of ecosystem?	1	1	2
2.	What are biotic and abiotic components of an ecosystem?	1	1	2
3.	What do you mean natural resources? Give examples.	1	1	2
4.	What are food chains and food webs and give its significance?	1	1	2
5.	Define Ecological succession.	1	1	2
6.	Differentiate between endangered and endemic species.	1	2	2
7.	Define primary succession and secondary succession.	1	1	2
8.	Define key stone species with suitable example.	1	1	2
	PART B			
1.	What is an ecosystem? Describe the structure and function of an ecosystem.	1	4	16
2.	Explain the values and threats to the biodiversity.	1	4	16
3.	"India is a mega diversity nation"– Explain. Brief biodiversity hotspots in India?	1	4	16
4.	Discuss the rules to be followed in Playfair method. Encrypt the word "Network security" with the keyword "crypto" using Playfair method.	1	4	16

UNIT II

ENVIRONMENTAL POLLUTION

Causes, Effects and Preventive measures of Water, Soil, Air and Noise Pollutions Solid, Hazardous and E-Waste management. Case studies on Occupational Health and Safety Management system (OHASMS). Environmental protection, Environmental protection acts.

Q.No	Question	CO	BTL	Marks
	PART A			
1.	Differentiate between primary and secondary air pollutants.	2	2	2
2.	Define photochemical smog.	2	1	2
3.	What are point and non-point sources of water pollution?	2	1	2
4.	Define e-waste management.	2	1	2
5.	Write the objectives of environmental acts.	2	1	2
6.	Define hazardous waste management.	2	1	2
7.	What are the effects of noise pollution?	2	1	2
8.	Write any two causes and sources of soil pollution.	2	1	2
	PART B			
1.	Describe the role of individual in the prevention of pollution. Explain the sources, effect and control methods of noise pollution.	2	4	16
2.	Demonstrate with a flow sheet and explain the steps involved in Solid waste management.	2	4	16
3.	What is OHASMS? Explain it with any one case study.	2	4	16
4.	Write about one of the industrial waste water treatments Techniques, support with a neat schematic diagram	2	4	16

UNIT III

RENEWABLE SOURCES OF ENERGY

Energy management and conservation, New Energy Sources: Need of new sources. Different types new energy sources. Applications of- Hydrogen energy, Ocean energy resources, Tidal energy conversion. Concept, origin and power plants of geothermal energy.

Q.No	Question	CO	BTL	Marks
	PART A			
1.	List the objectives of energy management.	3	1	2
2.	What is the significance of OTE?	3	1	2
3.	What is the important use of Artificial intelligence in energy sector?	3	1	2
4.	What is Bio-mass energy?	3	1	2
5.	Give any five applications of tidal energy conservation.	3	1	2
6.	Give some important applications of GTE.	3	1	2
7.	What is DESS? Mention its components.	3	1	2
8.	Mention the applications of hydrogen energy.	3	1	2
	PART B			
1.	Explain the applications of ocean energy and GTE.	3	4	16
2.	Explain the principle and various steps involved in the energy management.	3	4	16
3.	Explain detailed notes on new energy sources.	3	4	16
4.	Explain the origin, concept, advantages and disadvantages of Geo thermal energy.	3	4	16

UNIT IV

SUSTAINABILITY AND MANAGEMENT

Development, GDP, Sustainability- concept, needs and challenges-economic, social and aspects of sustainability-from unsustainability to sustainability-millennium development goals, and protocols-Sustainable Development Goals-targets, indicators and intervention areas Climate change Global, Regional and local environmental issues and possible solutions-case studies. Concept of Carbon Credit, Carbon Footprint. Environmental management in industry-A case study

Q.No	Question	CO	BTL	Marks
	PART A			
1.	What is GDP?	4	1	2
2.	Write any four millennium development goals.	4	1	2
3.	Define carbon credit.	4	1	2
4.	What are the sources of carbon foot print?	4	1	2
5.	Define environmental management.	4	1	2
6.	Mention any five important needs of sustainability.	4	1	2
7.	Write some advantages of carbon credits.	4	1	2
8.	Mention some effects of climate change.	4	1	2
	PART B			
1.	Brief notes on (i) Millennium Development Goals (ii) Sustainability protocols.	4	4	16
2.	What is environmental management? Explain the various steps of environmental management.	4	4	16
3.	Write notes on concept, goal and aim of sustainable development.	4	4	16
4.	What are the causes, effects and possible solutions of climate change? What is carbon credit? Explain the types and merits.	4	4	16

UNIT V

SUSTAINABILITY PRACTICES

Zero waste and R concept, Circular economy, ISO 14000 Series, Material Life cycle assessment, Environmental Impact Assessment. Sustainable habitat: Green buildings, green materials, Energy efficiency, Sustainable transports. Sustainable energy: Non-conventional Sources, Energy Cycles carbon cycle, emission and sequestration, Green Engineering: Sustainable urbanization Socioeconomical and technological change.

Q.No	Question	CO	BTL	Marks
	PART A			
1.	What is zero waste and R concept?	5	1	2
2.	Define circular economy.	5	1	2
3.	What are the key elements of ISO14000?	5	1	2
4.	Mention the objectives of EIA.	5	1	2
5.	What is green engineering?	5	1	2
6.	What is meant by energy cycles?	5	1	2
7.	What is sustainable urbanization?	5	1	2
8.	Define carbon sequestration.	5	1	2
	PART B			
1.	Explain the various steps to achieve zero waste? Mention advantages and disadvantages of zero waste.	5	4	16
2.	What is 3R concept? Determine the concept and advantages of R concept.	5	4	16
3.	(i)What are green materials? Explain important green building materials. (ii) What is sustainable transport? Discuss the key elements of sustainable transport.	5 5	4 4	8 8
4.	What is sustainable urbanization? Explain the rules to develop sustainable urban.	5	4	16

----- END ----