



Empowerment Through Quality Technical Education
AJEENKYA DY PATIL SCHOOL OF ENGINEERING

Dr. D. Y. Patil Knowledge City, Charholi (Bk), Lohegaon, Pune – 412 105

Website: <https://dypsoe.in/>

LAB MANUAL

Laboratory Practice-II (310258)

TE (COMP) 2019 COURSE

Course Coordinator

Prof. Priti B. Rathod

Prof. Minal Toley

Dr. Phadtare Tushar

DEPARTMENT OF

COMPUTER ENGINEERING

Department of Computer Engineering

Vision: “To achieve excellence in technical and socio-economic fields”

Mission:

M1 : To develop excellent learning center through continuous up gradation in proximity with Academia . R&D centers and industries.

M2 : To pursue research of local and global relevance.

M3: To encourage students to consider "startups" as a career option through Entrepreneurship Development Cell.

M4: Uplift and groom the learners to emerge as committed professionals.

Program Educational Outcomes:

Our graduates will be able to,

PEO1: be globally competent having strong fundamentals, domain knowledge, updated with modern technology to provide the effective solutions for engineering problems.

PEO2: Work as a committed professional with strong professional ethics and values. sense of responsibilities. Understanding of legal. safety. health. societal. cultural and environmental issues.

PEO3: be committed and motivated graduates with research attitude lifelong learning, investigative approach and multidisciplinary thinking.

Program Specific Outcomes:

PSO1	Professional Skills -The ability to understand, analyze and develop computer programs in the areas related to algorithms, system software, multimedia, web design, big data analytics, and networking for efficient design of computer-based systems of varying complexities.
-------------	--

PSO2	Problem-Solving Skills- The ability to apply standard practices and strategies in software project development using open-ended programming environments to deliver a quality product for business success.
PSO3	Successful Career and Entrepreneurship- The ability to employ modern computer languages, environments and platforms in creating innovative career paths to be an entrepreneur and to have a zest for higher studies.

Table of Contents

Contents

1. Guidelines to manual usage	5
2. Laboratory Objective	10
3. Laboratory Equipment/Software.....	10
4. Laboratory Experiment list	11
4.1. Experiment No. 1	12
4.2. Experiment No. 2	17
4.3. Experiment No. 3	21
4.4. Experiment No. 4	23
4.5. Experiment No. 5	27
4.6. Experiment No. 6	31
4.7. Experiment No. 7	40
4.8. Experiment No. 8	46
4.9. Experiment No. 9	49
4.10. Experiment No. 10	60
4.11. Experiment No. 11	63
5. Appendix.....	Error! Bookmark not defined.

1. Guidelines to manual usage

This manual assumes that the facilitators are aware of collaborative learning methodologies.

This manual will provide a tool to facilitate the session on Digital Communication modules in collaborative learning environment.

The facilitator is expected to refer this manual before the session.

Icon of Graduate Attributes

K Applying Knowledge	A Problem Analysis	D Design & Development	I Investigation of problems
M Modern Tool Usage	E Engineer & Society	E Environment Sustainability	T Ethics
T Individual & Team work	O Communication	M Project Management & Finance	I Life-Long Learning

Disk Approach- Digital Blooms Taxonomy



- 1: Remembering / Knowledge**
- 2: Comprehension / Understanding**
- 3: Applying**
- 4: Analyzing**
- 5: Evaluating**
- 6: Creating / Design**

PO1	Engineering knowledge	Apply the knowledge of mathematics, science, Engineering fundamentals, and an Engineering specialization to the solution of complex Engineering problems.
------------	------------------------------	---

Program Outcomes:

PO2	Problem analysis	Identify, formulate, review research literature and analyze complex Engineering problems reaching substantiated conclusions using first principles of Mathematics, natural sciences and Engineering sciences.
PO3	Design / Development of Solutions	Design solutions for complex Engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and Environmental considerations.
PO4	Conduct Investigations of Complex Problems	Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
PO5	Modern Tool Usage	Create, select, and apply appropriate techniques, resources, and modern Engineering and IT tools including prediction and modeling to complex Engineering activities with an understanding of the limitations.
PO6	The Engineer and Society	Apply reasoning informed by the contextual knowledge to assess societal, health, Safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
PO7	Environment and Sustainability	Understand the impact of the professional Engineering solutions in societal and Environmental contexts, and demonstrate the knowledge of, and need for Sustainable development.
PO8	Ethics	Apply ethical principles and commit to professional ethics and responsibilities And norms of Engineering practice.
PO9	Individual and Team Work	Function effectively as an individual, and as a member or leader in diverse Teams, and in multidisciplinary settings.
PO10	Communication Skills	Communicate effectively on complex Engineering activities with the Engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make Effective presentations, and give and receive clear instructions.
PO11	Project Management and Finance	Demonstrate knowledge and understanding of Engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary Environments.
PO12	Life-long Learnin	Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological Change.

	g	
--	----------	--

Course Name: Laboratory Practice-II

Course Code: 310258

Course Outcomes

- **Artificial Intelligence**

CO1: Design a system using different informed search / uninformed search or heuristic approaches

CO2: Apply basic principles of AI in solutions that require problem solving, inference, perception, knowledge representation, and learning

CO3: Design and develop an interactive AI application

- **Information Security**

CO4: Use tools and techniques in the area of Information Security

CO5: Use the cryptographic techniques for problem solving

CO6: Design and develop security solution

CO to PO Mapping:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	2	-	2	-	3	-	-	2	2	2	1	2
CO2	1	-	2	2	3	2	-	2	2	2	1	2
CO3	1	-	2	2	3	2	-	2	2	2	2	2
CO4	1	-	2	-	3	-	-	2	2	2	2	2
CO5	1	-	2	-	3	-	-	2	2	2	2	2
CO6	1	-	2	-	3	-	-	2	2	2	2	2

CO to PSO Mapping:

	PSO1	PSO2	PSO3
CO1		2	
CO2		3	1
CO3	2	3	
CO4	2	2	
CO5	1	3	2
CO6	3		

1. Laboratory Objective

- To learn and apply various search strategies for AI
- To Formalize and implement constraints in search problems
- To understand the concepts of Information Security

2. Laboratory Equipment/Software

Operating System recommended: - 64-bit Windows OS and

Linux **Programming tools recommended:** -

Software:- C/C++/Java

Backend: MySQL /MongoDB/NodeJS

3. Laboratory Experiment list

Sr. No	Title
	Prerequisite practical assignments or installation (if any)
1	C/C++/Java
	Part I : Artificial Intelligence
	Group A All assignments are compulsory
1	Implement depth first search algorithm and Breadth First Search algorithm, Use an undirected graph and develop a recursive algorithm for searching all the vertices of a graph or tree data structure.
2	Implement A star Algorithm for any game search problem.
3	Implement Greedy search algorithm for any of the following application: I. Selection Sort II. Minimum Spanning Tree III. Single-Source Shortest Path Problem IV. Job Scheduling Problem V. Prim's Minimal Spanning Tree Algorithm VI. Kruskal's Minimal Spanning Tree Algorithm VII. Dijkstra's Minimal Spanning Tree Algorithm
	Group B
4	Implement a solution for a Constraint Satisfaction Problem using Branch and Bound and Backtracking for n-queens problem or a graph coloring problem.
5	Develop an elementary catboat for any suitable customer interaction application.
	Group C
6	Implement any one of the following Expert System I. Information management II. Hospitals and medical facilities III. Help desks management IV. Employee performance evaluation V. Stock market trading Airline scheduling and cargo schedules
	Part II : Elective II
	Information Security (Any five)
7	Write a Java/C/C++/Python program that contains a string (char pointer) with a value 'Hello World'. The program should AND or and XOR each character in this string with 127 and display the result.

8	Write a Java/C/C++/Python program to perform encryption and decryption using the method of Transposition technique.
9	Write a Java/C/C++/Python program to implement DES algorithm.
10	Write a Java/C/C++/Python program to implement AES Algorithm.
11	Write a Java/C/C++/Python program to implement RSA algorithm.
12	Implement the different Hellman Key Exchange mechanism using HTML and JavaScript. Consider the end user as one of the parties (Alice) and the JavaScript application as other party (bob).
13	Calculate the message digest of a text using the MD5 algorithm in JAVA.

Experiment No. 1

Title: - Implement depth first search algorithm and Breadth First Search algorithm

Objectives:-

1. Understand the implementation of depth first search algorithm
2. Understand the implementation of Breadth First Search algorithm

Problem Statement:-

Implement depth first search algorithm and Breadth First Search algorithm, Use an undirected graph and develop a recursive algorithm for searching all the vertices of a graph or tree data structure

Software and Hardware requirements:-

1. **Operating system:** Linux- Ubuntu 16.04 to 17.10, or Windows 7 to 10,
2. **RAM-** 2GB RAM (4GB preferable)
3. You have to install **Python3** or higher version

Theory-

1. Depth First Search

What do we do once have to solve a maze? We tend to take a route, keep going until we discover a dead end. When touching the dead end, we again come back and keep coming back till we see a path we didn't attempt before. Take that new route. Once more keep going until we discover a dead end. Take a come back again... This is exactly how Depth-First Search works.

The Depth-First Search is a recursive algorithm that uses the concept of backtracking. It involves thorough searches of all the nodes by going ahead if potential, else by backtracking. Here, the word backtrack means once you are moving forward and there are not any more nodes along the present path, you progress backward on an equivalent path to seek out nodes to

traverse. All the nodes are progressing to be visited on the current path until all the unvisited nodes are traversed after which subsequent paths are going to be selected.

DFS Algorithm

A standard Depth-First Search implementation puts every vertex of the graph into one in all 2 categories:

- 1) Visited 2) Not Visited.

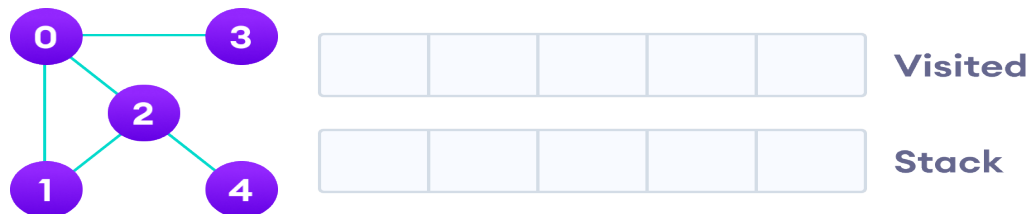
The only purpose of this algorithm is to visit all the vertex of the graph avoiding cycles.

The DSF algorithm follows as:

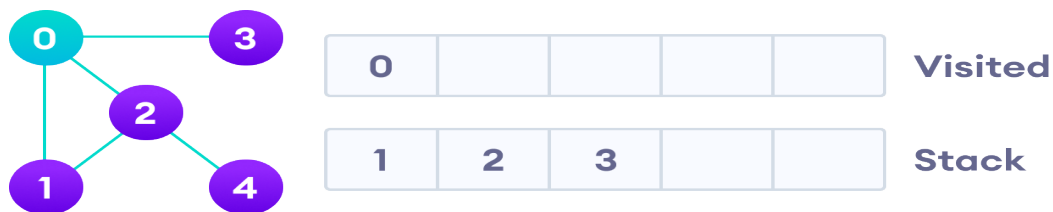
1. We will start by putting any one of the graph's vertex on top of the stack.
2. After that take the top item of the stack and add it to the visited list of the vertex.
3. Next, create a list of that adjacent node of the vertex. Add the ones which aren't in the visited list of vertexes to the top of the stack.
4. Lastly, keep repeating steps 2 and 3 until the stack is empty.

Depth First Search Example

Let's see how the Depth First Search algorithm works with an example. We use an undirected graph with 5 vertices.

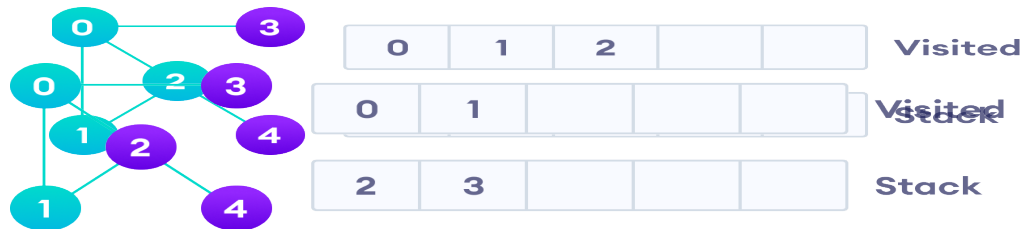


We start from vertex 0, the DFS algorithm starts by putting it in the Visited list and putting all its adjacent vertices in the stack.

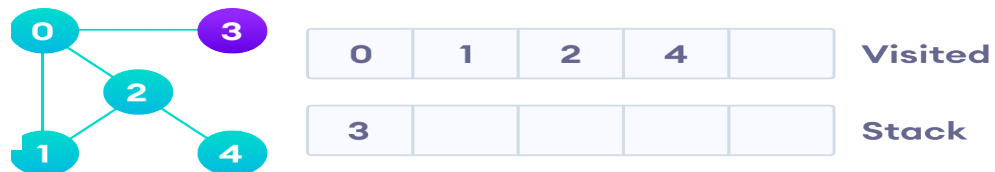


Next, we visit the element at the top of stack i.e. 1 and go to its adjacent nodes. Since 0 has already been visited, we visit 2 instead

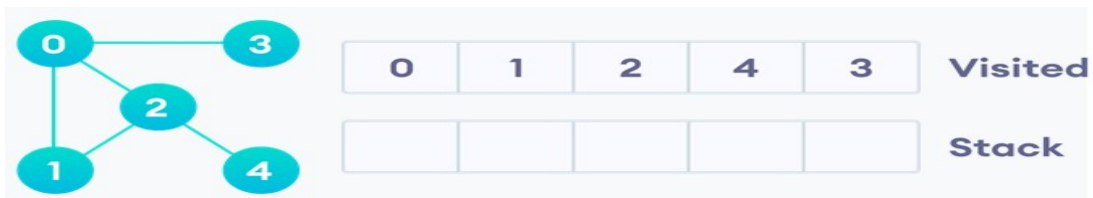
Vertex 2 has an unvisited adjacent vertex in 4, so we add that to the top of the stack and visit it.



Vertex 2 has an unvisited adjacent vertex in 4, so we add that to the top of the stack and visit it.



After we visit the last element 3, it doesn't have any unvisited adjacent nodes, so we have completed the Depth First Traversal of the graph.



After we visit the last element 3, it doesn't have any unvisited adjacent nodes, so we have completed the Depth First Traversal of the graph.

Application of DFS Algorithm

1. For finding the path
2. To test if the graph is bipartite

3. For finding the strongly connected components of a graph
4. For detecting cycles in a graph.

Breadth-First Search

Breadth-First Search (BFS) is an algorithm used for traversing graphs or trees.

Traversing means visiting each node of the graph. Breadth-First Search is a recursive algorithm to search all the vertices of a graph or a tree. BFS in python can be implemented by using data structures like a dictionary and lists. Breadth-First Search in tree and graph is almost the same. The only difference is that the graph may contain cycles, so we may traverse to the same node again.

BFS Algorithm

Breadth-first search is the process of traversing each node of the graph, a standard BFS algorithm traverses each vertex of the graph into two parts:

- 1) Visited
- 2) Not Visited.

So, the purpose of the algorithm is to visit all the vertex while avoiding cycles. BFS starts from a node, then it checks all the nodes at distance one from the beginning node, then it checks all the nodes at distance two, and so on. So as to recollect the nodes to be visited, BFS uses a queue.

The steps of the algorithm work as follow:

1. Start by putting any one of the graph's vertices at the back of the queue.
2. Now take the front item of the queue and add it to the visited list.
3. Create a list of that vertex's adjacent nodes. Add those which are not within the visited list to the rear of the queue.
4. Keep continuing steps two and three till the queue is empty.

Many times, a graph may contain two different disconnected parts and therefore to make sure that we have visited every vertex, we can also run the BFS algorithm at every node.

Explanation:

1. Create a graph.
2. Initialize a starting node.
3. Send the graph and initial node as parameters to the bfs function.
4. Mark the initial node as visited and push it into the queue.
5. Explore the initial node and add its neighbours to the queue and remove the initial node from the queue.
6. Check if the neighbours node of a neighbouring node is already visited.
7. If not, visit the neighbouring node neighbours and mark them as visited.
8. Repeat this process until all the nodes in a graph are visited and the queue becomes empty.

Advantages of BFS

1. It can be useful in order to find whether the graph has connected components or not.
2. It always finds or returns the shortest path if there is more than one path between two vertices.

Disadvantages of BFS

1. The execution time of this algorithm is very slow because the time complexity of this algorithm is exponential.
2. This algorithm is not useful when large graphs are used.

Conclusion

Depth-First Search and Breadth-First Search (BFS) are used to traverse the graph or tree. We implemented Depth-First Search and Breadth-First Search (BFS) in python for searching all the vertices of a graph or tree data structure.

Experiment No. 02

Title

Write a Java/C/C++/Python program to perform encryption and decryption using the method of Transposition technique.

Objective

Learn how to Perform Encryption and Decryption using method of transposition technique.

Problem Definition:

Perform Encryption and Decryption using method of transposition technique.

Outcome

After completion of this assignment students will be able to understand the Perform Encryption and Decryption using method of transposition technique.

Software Requirements:

Python 3

Hardware Requirements:

PC, 2GB RAM, 500 GB HDD

Theory

Transposition Techniques

1. Rail Fence Technique

In Rail fence cipher, techniques are essentially Transposition Ciphers and generated by rearrangement of characters in the plaintext. The characters of the plain text string are arranged in the form of a rail-fence as follows.

Given Plain text is - COMPUTER SECURITY TECHNOLOGY

Rail Fence Technique algorithm:

1. Write down the plain text message as a sequence of diagonals.
2. Read the plain text written in Step-1 as a sequence of rows. Example: plain text = COMPUTER SECURITY TECHNOLOGY is converted to cipher text with this help of Rail Fence Technique with dual slope.

Cipher Text is - CMUESCRTTCNLGOPTREUIYEHOOY

2. Columnar Transposition

Following are two types of Columnar Transposition

Simple Columnar Transposition

The columnar transposition cipher is a transposition cipher that follows a simple rule for mixing up the characters in the plaintext to form the cipher-text. It can be combined with other ciphers, such as a substitution cipher, the combination of which can be more difficult to break than either cipher on its own.

The cipher uses a columnar transposition to greatly improve its security.

Algorithm:

1. The message is written out in rows of a fixed length.
2. Read out again column by column according to given order or in random order.
3. According to order write cipher text.

Example

The key for the columnar transposition cipher is a keyword e.g. ORANGE. The row length that is used is the same as the length of the keyword.

To encrypt a below Plain Text - COMPUTER PROGRAMMING

O	R	A	N	G	E
C	O	M	P	U	T
E	R	P	R	O	G
R	A	M	M	I	N
G	L	E	X	X	M

In the above example, the plaintext has been padded so that it neatly fits in a rectangle. This is known as a regular columnar transposition. An irregular columnar transposition leaves these characters blank, though this makes decryption slightly more difficult. The columns are now reordered such that the letters in the key word are ordered alphabetically.

5	6	1	4	3	2
O	R	A	N	G	E
C	O	M	P	U	T
E	R	P	R	O	G
R	A	M	M	I	N
G	L	E	X	X	M

The Encrypted text or Cipher Text is: MPMET GNMUO IXPRM XCERG ORAL (Written in blocks of five)

3. Double Columnar Transposition

A single Columnar Transposition can be attacked by guessing possible column lengths by writing the message from columns (with the wrong order because the key is unknown) and then trying to get the possible message.

Therefore to make it stronger, a double transposition was used. This is simple columnar transposition technique applied twice. Here the same key can be used for both transpositions or two different keys can be used.

For Example – Plain Text: - WELCOME HOME Key:-PLAYER (with length 6) Round 1

1	2	3	4	5	6
W	E	L	C	O	M

E H O M E

Now read it with some random order of (4,6,1,2,5,3) = "CMMWEEHOELO" Round 2 now

"CMMWEEHOELO" this will be next cipher Text

1 2 3 4 5 6

C M M W E E

H O E L O

Again read with the order of (4,6,1,2,5,3) = "WLECHMOEOME"

Algorithm:-

1. Write the plain text message row-by-row in a rectangle of a predefined size
2. Read the message column-by-column in any random order.
3. The message thus obtained is cipher text message of round one
4. Repeat step 1 to 3 as many times as desired.

Conclusion

Thus we learn that how to Perform Encryption and Decryption using method of transposition technique.

Experiment No. 3

Title: - Implement A star Algorithm for any game search problem.

Objectives:-

1. Understand the implementation of A star Algorithm

Problem Statement:-

Implement A star Algorithm for any game search problem.

Software and Hardware requirements:-

1. **Operating system:** Linux- Ubuntu 16.04 to 17.10, or Windows 7 to 10,
2. **RAM-** 2GB RAM (4GB preferable)
3. You have to install **Python3** or higher version

Theory-

A* Search

A* search is the most commonly known form of best-first search. It uses heuristic function $h(n)$, and cost to reach the node n from the start state $g(n)$.

It has combined features of UCS and greedy best- first search, by which it solve the problem efficiently. A* search algorithm finds the shortest path through the search space using the heuristic function.

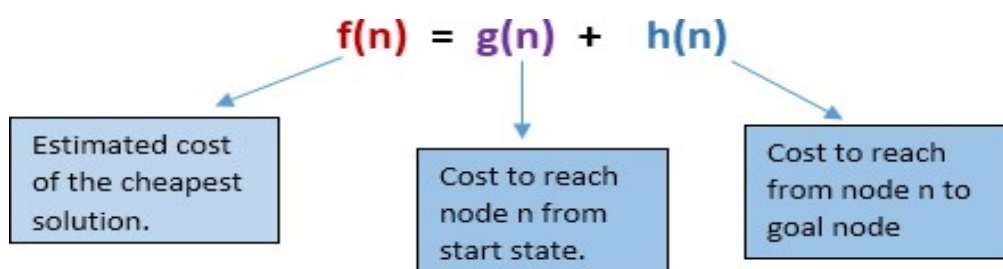
This search algorithm expands less search tree and provides optimal result faster. A* algorithm is similar to UCS except that it uses $g(n)+h(n)$ instead of $g(n)$.

In A* search algorithm, we use search heuristic as well as the cost to reach the node. Hence we can combine both costs as following, and this sum is called as a fitness number.

Algorithm of A* search:

Step1: Place the starting node in the OPEN list.

Step 2: Check if the OPEN list is empty or not, if the list is empty then return failure and stops.



Step 3: Select the node from the OPEN list which has the smallest value of evaluation function ($g+h$), if node n is goal node then return success and stop, otherwise

Step 4: Expand node n and generate all of its successors, and put n into the closed list. For each successor n' , check whether n' is already in the OPEN or CLOSED list, if not then compute evaluation function for n' and place into Open list.

Step 5: Else if node n' is already in OPEN and CLOSED, then it should be attached to the back pointer which reflects the lowest $g(n')$ value.

Step 6: Return to Step 2.

Advantages:

1. A* search algorithm is the best algorithm than other search algorithms.
2. A* search algorithm is optimal and complete.
3. This algorithm can solve very complex problems.

Disadvantages:

1. It does not always produce the shortest path as it mostly based on heuristics and approximation.
2. A* search algorithm has some complexity issues.
3. The main drawback of A* is memory requirement as it keeps all generated nodes in the memory, so it is not practical for various large-scale problems.

Conclusion

Implement A star Algorithm for any game search problem in python for searching path

Experiment No. 4

Title: - Implement Greedy search algorithm for Prim's Minimal Spanning Tree Algorithm

Objectives:-

1. Understand the concept of Greedy search algorithm.
2. Understand the implementation of Prim's Minimal Spanning Tree Algorithm

Problem Statement:-

Implement Greedy search algorithm for any of the following application:

- I. Selection Sort
- II. Minimum Spanning Tree
- III. Single-Source Shortest Path Problem
- IV. Job Scheduling Problem
- V. **Prim's Minimal Spanning Tree Algorithm**
- VI. Kruskal's Minimal Spanning Tree Algorithm
- VII. Dijkstra's Minimal Spanning Tree Algorithm

Software and Hardware requirements:-

4. **Operating system:** Linux- Ubuntu 16.04 to 17.10, or Windows 7 to 10,
5. **RAM-** 2GB RAM (4GB preferable)
6. You have to install **Python3** or higher version

Theory-

Minimum Spanning Tree?

As we all know, the graph which does not have edges pointing to any direction in a graph is called an undirected graph and the graph always has a path from a vertex to any other vertex. A spanning tree is a subgraph of the undirected connected graph where it includes all the nodes of the graph with the minimum possible number of edges.

Remember, the subgraph should contain each and every node of the original graph. If any node is missed out then it is not a spanning tree and also, the spanning tree doesn't contain

cycles. If the graph has n number of nodes, then the total number of spanning trees created from a complete graph is equal to $n^{(n-2)}$.

In a spanning tree, the edges may or may not have weights associated with them. Therefore, the spanning tree in which the sum of edges is minimum as possible then that spanning tree is called the minimum spanning tree. One graph can have multiple spanning-tree but it can have only one unique minimum spanning tree.

There are two different ways to find out the minimum spanning tree from the complete graph i.e Kruskal's algorithm and Prim's algorithm. Let us study prim's algorithm in detail below:

Prim's Algorithm?

Prim's algorithm is a minimum spanning tree algorithm which helps to find out the edges of the graph to form the tree including every node with the minimum sum of weights to form the minimum spanning tree.

Prim's algorithm starts with the single source node and later explore all the adjacent nodes of the source node with all the connecting edges. While we are exploring the graphs, we will choose the edges with the minimum weight and those which cannot cause the cycles in the graph.

Prim's Algorithm for Minimum Spanning Tree

Prim's algorithm basically follows the greedy algorithm approach to find the optimal solution. To find the minimum spanning tree using prim's algorithm, we will choose a source node and keep adding the edges with the lowest weight.

The algorithm is as given below:

- Initialize the algorithm by choosing the source vertex
- Find the minimum weight edge connected to the source node and another node and add it to the tree
- Keep repeating this process until we find the minimum spanning tree

Pseudocode

$T = \emptyset;$

$M = \{ 1 \};$

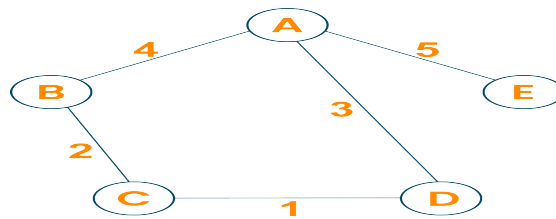
while ($M \neq N$)

let (m, n) be the lowest cost edge such that $m \in M$ and $n \in N - M$; $T = T \cup \{(m, n)\}$

$M = M \cup \{n\}$

Here we create two sets of nodes i.e M and M-N. M set contains the list of nodes that have been visited and the M-N set contains the nodes that haven't been visited. Later, we will move each node from M to M-N after each step by connecting the least weight edge.

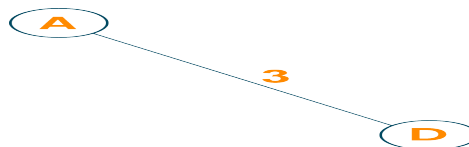
Example Let us consider the below-weighted graph



Later we will consider the source vertex to initialize the algorithm

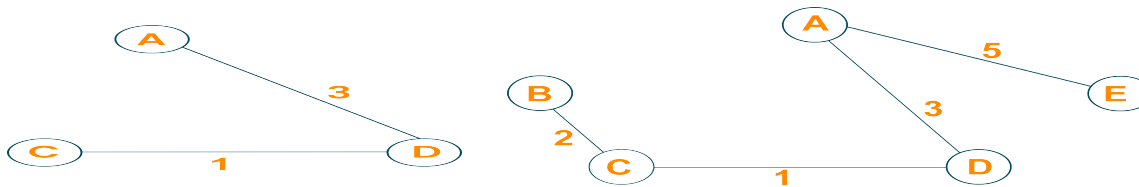


Now, we will choose the shortest weight edge from the source vertex and add it to finding the spanning tree.



Then, choose the next nearest node connected with the minimum edge and add it to the solution.
If there are multiple choices then choose anyone.

Continue the steps until all nodes are included and we find the minimum spanning tree.



Time Complexity:

The running time for prim's algorithm is $O(V \log V + E \log V)$ which is equal to $O(E \log V)$ because every insertion of a node in the solution takes logarithmic time. Here, E is

the number of edges and V is the number of vertices/nodes. However, we can improve the running time complexity to $O(E + \log V)$ of prim's algorithm using Fibonacci Heaps.

Applications

- Prim's algorithm is used in network design
- It is used in network cycles and rail tracks connecting all the cities
- Prim's algorithm is used in laying cables of electrical wiring
- Prim's algorithm is used in irrigation channels and placing microwave towers
- It is used in cluster analysis
- Prim's algorithm is used in gaming development and cognitive science
- Pathfinding algorithms in artificial intelligence and traveling salesman problems make use of prim's algorithm.

Conclusion

As we studied, the minimum spanning tree has its own importance in the real world, it is important to learn the prim's algorithm which leads us to find the solution to many problems. When it comes to finding the minimum spanning tree for the dense graphs, prim's algorithm is the first choice

Experiment No. 5

Title: - Implement Branch and Bound and Backtracking for n-queens problem.

Objectives:-

1. Understand the concept and implementation of Branch and Bound for n-queens problem.
2. Understand the concept and implementation of Backtracking for n-queens problem.

Problem Statement:-

Implement a solution for a Constraint Satisfaction Problem using Branch and Bound and Backtracking for n-queens problem or a graph coloring problem.

Software and Hardware requirements:-

7. **Operating system:** Linux- Ubuntu 16.04 to 17.10, or Windows 7 to 10,
8. **RAM-** 2GB RAM (4GB preferable)
9. You have to install **Python3** or higher version

Theory-

The **N queens puzzle** is the problem of placing N chess queens on an $N \times N$ chessboard so that no two queens threaten each other. Thus, a solution requires that no two queens share the same row, column, or diagonal.

Backtracking Algorithm for N-Queen is already discussed [here](#). In backtracking solution we backtrack when we hit a dead end. **In Branch and Bound solution, after building a partial solution, we figure out that there is no point going any deeper as we are going to hit a dead end.**

“The idea is to place queens one by one in different columns, starting from the leftmost column. When we place a queen in a column, we check for clashes with already placed queens. In the current column, if we find a row for which there is no clash, we mark

this row and column as part of the solution. If we do not find such a row due to clashes, then we backtrack and return false.”

-			-				
-		-					
-	-						
×	-	-	-	-	-	-	-
-	-						
-		-					
-			-				
-				-			

-	-		-			-	
-	-	-			-		
-	-			-			
×	-	-	-	-	-	-	-
-	-	-					
-	-	-					
-	×	-	-	-	-	-	-
-	-	-	-	-	-		
-	-			-	-		

1. For the 1st Queen, there are total 8 possibilities as we can place 1st Queen in any row of first column. Let's place Queen 1 on row 3.
2. After placing 1st Queen, there are 7 possibilities left for the 2nd Queen. But wait, we don't really have 7 possibilities. We cannot place Queen 2 on rows 2, 3 or 4 as those cells are under attack from Queen 1. So, Queen 2 has only $8 - 3 = 5$ valid positions left.
3. After picking a position for Queen 2, Queen 3 has even fewer options as most of the cells in its column are under attack from the first 2 Queens.

We need to figure out an efficient way of keeping track of which cells are under attack. In previous solution we kept an 8-by-8 Boolean matrix and update it each time we placed a queen, but that required linear time to update as we need to check for safe cells.

Basically, we have to ensure 4 things:

1. No two queens share a column.
2. No two queens share a row.
3. No two queens share a top-right to left-bottom diagonal.
4. No two queens share a top-left to bottom-right diagonal.

Number 1 is automatic because of the way we store the solution. For number 2, 3 and 4, we can perform updates in $O(1)$ time. The idea is to keep **three Boolean arrays that tell us which rows and which diagonals are occupied**.

Lets do some pre-processing first. Let's create two $N \times N$ matrix one for / diagonal and other one for \ diagonal. Let's call them slashCode and backslashCode respectively. The trick is to fill them in such a way that two queens sharing a same /diagonal will have the same

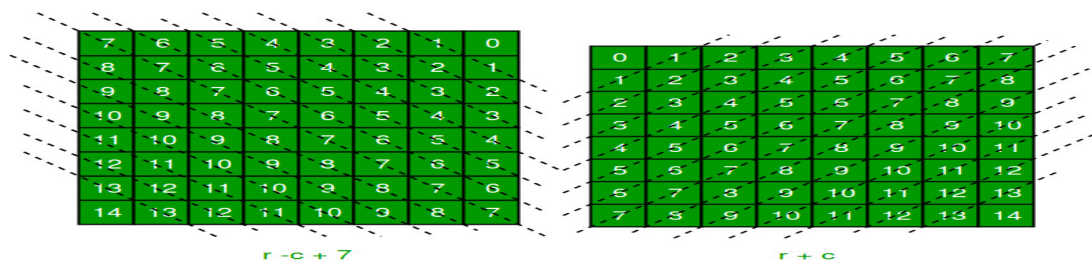
value in matrix slashCode, and if they share same diagonal, they will have the same value in backslashCode matrix.

For an N x N matrix, fill slashCode and backslashCode matrix using below formula

$$\text{slashCode}[\text{row}][\text{col}] = \text{row} + \text{col}$$

$$\text{backslashCode}[\text{row}][\text{col}] = \text{row} - \text{col} + (N-1)$$

Using above formula will result in below matrices



The 'N - 1' in the backslash code is there to ensure that the codes are never negative because we will be using the codes as indices in an array.

Now before we place queen i on row j , we first check whether row j is used (use an array to store row info). Then we check whether slash code ($j + i$) or backslash code ($j - i + 7$) are used (keep two arrays that will tell us which diagonals are occupied). If yes, then we have to try a different location for queen i . If not, then we mark the row and the two diagonals as used and recurse on queen $i + 1$. After the recursive call returns and before we try another position for queen i , we need to reset the row, slash code and backslash code as unused again

Backtracking:-

The N Queen is the problem of placing N chess queens on an $N \times N$ chessboard so that no two queens attack each other. For example, following is a solution for 4 Queen problem.

The expected output is a binary matrix which has 1s for the blocks where queens are placed.

For example, following is the output matrix for above 4 queen solution.

		Q	
			Q
Q			
		Q	

{ 0, 1, 0, 0 }

{ 0, 0, 0, 1 }

{ 1, 0, 0, 0 }

{ 0, 0, 1, 0}

Naive Algorithm

Generate all possible configurations of queens on board and print a configuration that satisfies the given constraints.

```
while there are untried configurations
{ generate the next configuration
  if queens don't attack in this configuration then
  { print this configuration;
  }
}
```

Backtracking Algorithm

The idea is to place queens one by one in different columns, starting from the leftmost column. When we place a queen in a column, we check for clashes with already placed queens. In the current column, if we find a row for which there is no clash, we mark this row and column as part of the solution. If we do not find such a row due to clashes then we backtrack and return false.

- 1) Start in the leftmost column
- 2) If all queens are placed return true
- 3) Try all rows in the current column.

Do following for every tried row.

- a) If the queen can be placed safely in this row then mark this [row, column] as part of the solution and recursively check if placing queen here leads to a solution.
 - b) If placing the queen in [row, column] leads to a solution then return true.
 - c) If placing queen doesn't lead to a solution then unmark this [row, column] (Backtrack) and go to step (a) to try other rows.
- 4) If all rows have been tried and nothing worked, return false to trigger backtracking.

Conclusion:- In these way we have implemented a solution for a Constraint Satisfaction Problem using Branch and Bound and Backtracking for n-queens problem.

Experiment No. 6

Title: - Develop an elementary catboat.

Objectives:-

1. Understand the concept of catboat.

Problem Statement:-

Develop an elementary catboat for any suitable customer interaction application.

Software and Hardware requirements:-

10. **Operating system:** Linux- Ubuntu 16.04 to 17.10, or Windows 7 to 10,
11. **RAM-** 2GB RAM (4GB preferable)
12. You have to install **Python3** or higher version or Turbo C++ or JDK.

Theory-

What is a chatbot?

A chatbot is a computer program designed to have a conversation with human beings over the internet. It's also known as conversational agents, which communicate and collaborate with human users, through text messaging, in order to accomplish a specific task. Basically, there are two types of chatbots. The one that uses Artificial Intelligence, and another one is based on multiple choice scripts.

Both types of chatbots aim to create a more personalized content experience for the users, whether that's while watching a video, reading articles or buying new shoes.

These Chatbots hold the promise of being the next generation of technology that people use to interact online with business enterprises. These Chatbots offer a lot of advantages, one of which is that, because Chatbots communicate using a natural language, users don't need to learn yet another new website interface, to get comfortable with the unavoidable quirks.

Chatbots are capable to interpret human speech, and decide which information is being sought. Artificial intelligence is getting smarter each day, and brands that are integrating

Chatbots with the artificial intelligence, can deliver one-to-one individualized experiences to consumers.

Why chatbot?

Chatbots can be useful in many aspects of the customer experience, including providing customer service, presenting product recommendations and engaging customers through targeted marketing campaigns. If a customer has an issue with a product, she can connect with a chatbot to explain the situation and the chatbot can input that information to provide a recommendation of how to fix the product. On the recommendation side, chatbots can be used

to share popular products with customers that they might find useful and can act as a sort of personal shopper or concierge service to find the perfect gift, meal or night out for a customer with just a few basic questions. Brands are also using chatbots to connect their customers with thought leaders and add personality to their products. In all cases, brands seem to be having great success and experiencing increased engagement and revenue.

Chatbots are easy to use and many customers prefer them over calling a representative on the phone because it tends to be faster and less invasive. They can also save money for companies and are easy to set up.

Chatbots are relatively new and most companies haven't implemented them yet, it's only natural that users are interested in them. Hence, people want to discover what chatbots can and cannot do.

The number of businesses using chatbots has grown exponentially. Chatbots have increased from 30,000 in 2016 to over 100,000 today. Every major company has announced their own chatbot and 60% of the youth population uses them daily.

These statistics prove that chatbots are the new-gen tech. No more waiting for the right time to incorporate them into your business. The time is now. By the year 2020, nearly 80% of businesses will have their own chatbot.

Billions of people are already using chatbots, so it's time your business did too.

Benefits of chatbot?

1. Available 24*7:

I'm sure most of you have experienced listening to the boring music playing while you're kept on hold by a customer care agent. On an average people spend 7 minutes until they are assigned to an agent. Gone are the days of waiting for the next available operative. Bots are replacing live chat and other forms of contact such as emails and phone calls.

Since chat bots are basically virtual robots they never get tired and continue to obey your command. They will continue to operate every day throughout the year without requiring to take a break. This improves your customer satisfaction and helps you rank highly in your sector.

2. Handling Customers:

We humans are restricted to the number of things we can do at the same time. A study suggests that humans can only concentrate on 3–4 things at the same time. If it goes beyond that you are bound to meet errors.

Chatbots on the other hand can simultaneously have conversations with thousands of people. No matter what time of the day it is or how many people are contacting you, every single one of them will be answered instantly. Companies like Taco Bell and Domino's are already using chatbots to arrange delivery of parcels.

3. Helps you Save Money:

If you are a business owner you are bound have a lot of employees who need to be paid for the work they do. And these expenses just keep adding up as business grows. Chatbots are a one time investment which helps businesses reduce down on staff required.

You could integrate a customer support chatbot in your business to cater to simple queries of customers and pass on only the complex queries to customer support agents.

4. Provides 100% satisfaction to customers:

Humans react to others based on their mood and emotions. If a agent is having a good attitude or is in good mood he will most probably talk to customers in a good way. In contrary to this the customer will not be satisfied.

Whereas chatbots are bound by some rules and obey them as long as they're programmed to. They always treat a customer in the most polite and perfect way no matter how rough the person is. Also, in the travel and hospitality industry where travelers do not speak the same language, a bot can be trained to communicate in the language of the traveler.

5. Automation of repetitive work:

Lets be honest, no one likes doing the same work again and again over brief period of time. In the case of humans, such tasks are prone to errors. Chatbots now help automate tasks which are to be done frequently and at the right time.

Also, now there are numerous slack bots which automate repetitive tasks. This helps people save time and increase productivity. For example, there are new items bought from your eCommerce site or there is a bug reported then it sends a short summary to a slack channel.

6. Personal Assistant:

People could use Bots as a fashion advisor for clothing recommendations, or ask trading tips from a finance bot, suggest places to visit from a travel bot and so forth. This would help the users get a more personal touch from the chatbot. Also, the chatbot will remember all your choices and provide you with relevant choices the next time you visit it.

How chatbot can drive revenue for you?

Below we have compiled reasons why chatbots are important for your business and how can they help in increasing revenues:

a. Higher user customer engagement

Most businesses these days have a web presence. But with being on the internet, boundaries of day and night, availability and unavailability have changed, so have user expectations. This is probably the biggest reason to use them. Bots give the user an interactive experience. It makes customers feel they are working with someone to help resolve their issue. If done right, bots can help customers find what they are looking for and make them more likely to return.

Customer Engagement

- **Clearance Sale** : Notify users about on-going clearance sale of products relevant to the users at their nearest outlets.
- **Product Finder** : Enable consultative selling without the need of a call center
- **It offer Notification** : Notify users about offers, product launches on products/ services they've shown interest in, and products that's back in stock

b. Mobile-ready and immediate availability

Along with a web presence, it has also become increasingly important for brands to have a mobile presence - mobile apps, mobile-optimized websites. Considering how chat has been around on the mobile for ages, most chatbot implementations don't need you to work on tweaking their UI, they are ready to implement and so available to your customers immediately

You might argue that you have an app for that. Having an app for your brand is great, but having users discover that app, download it and use it to stay engaged is not an easy deal. Instead, implementing a chatbot - which works on the mobile browser or a messaging-app which the user regularly uses - makes it all the more reason for a customer to be engaged with the brand

c. It can drive sales

Chatbots can be intelligent. Depending on a user's preferences or purchases, it can send products to customers which are more likely to convert into sales. Or it can send coupons to

users for in-store purchases/discounts. Bots can also be used to link the user to your mCommerce site/app so they can buy the product directly from the convenience of their phones

Sell Intelligently

- **Product Recommendations:** Push proactive recommendations to users based on their preferences and search and order history.
- Enable order booking over chat.

d. Minimal cost - Maximum return

The best part about bots is they are cheap. Chatbot provide the necessary infrastructure and APIs for creating these bots. They require minimal maintenance and since it is automated, there is no labor-intensive work that goes in there.

e. Customer Service

- **Track Order :** Keep users up to date with order status. Schedule or reschedule delivery to a provided address or request to pick it up at any other Best Buy outlet.
- **Stock outs :** Notify users when desired product is available and place order over a chat.
- **Returns and Replacements:** No waiting time to reach customer care. Customers can instantly place request to replace or return an order.
- **Seek Reviews:** Reach out to users to seek reviews on the products recently bought

Application across Industries

According to a new survey, 80% of businesses want to integrate chatbots in their business model by 2020. So which industries can reap the greatest benefits by implementing consumer-facing chatbots? According to a chatbot, these major areas of direct-to-consumer engagement are prime:

Chatbots in Restaurant and Retail Industries

Famous restaurant chains like Burger King and Taco bell has introduced their Chatbots to stand out of competitors of the Industry as well as treat their customers quickly. Customers of these restaurants are greeted by the resident Chatbots, and are offered the menu options- like a counter order, the Buyer chooses their pickup location, pays, and gets told when they can head over to grab their food. Chatbots also works to accept table reservations, take special requests and go take the extra step to make the evening special for your guests.

Chatbots are not only good for the restaurant staff in reducing work and pain but can provide a better user experience for the customers.

Chatbots in Hospitality and Travel

For hoteliers, automation has been held up as a solution for all difficulties related to productivity issues, labour costs, a way to ensure consistently, streamlined production processes across the system. Accurate and immediate delivery of information to customers is a major factor in running a successful online Business, especially in the price sensitive and competitive Travel and Hospitality industry. Chatbots particularly have gotten a lot of attention from the hospitality industry in recent months.

Chatbots can help hotels in a number of areas, including time management, guest services and cost reduction. They can assist guests with elementary questions and requests. Thus, freeing up hotel staff to devote more of their time and attention to time-sensitive, critical, and complicated tasks. They are often more cost effective and faster than their human counterparts. They can be programmed to speak to guests in different languages, making it easier for the guests to speak in their local language to communicate.

Chatbots in Health Industry

Chatbots are a much better fit for patient engagement than Standalone apps. Through these Health-Bots, users can ask health related questions and receive immediate responses. These responses are either original or based on responses to similar questions in the database. The impersonal nature of a bot could act as a benefit in certain situations, where an actual Doctor is not needed.

Chatbots ease the access to healthcare and industry has favourable chances to serve their customers with personalised health tips. It can be a good example of the success of Chatbots and Service Industry combo.

Chatbots in E-Commerce

Mobile messengers- connected with Chatbots and the E-commerce business can open a new channel for selling the products online. E-commerce Shopping destination “Spring” was the early adopter. E-commerce future is where brands have their own Chatbots which can interact with their customers through their apps.

Chatbots in Fashion Industry

Chatbots, AI and Machine Learning pave a new domain of possibilities in the Fashion industry, from Data Analytics to Personal Chatbot Stylists. Fashion is such an industry where luxury goods can only be bought in a few physical boutiques and one to one customer service is essential. The Internet changed this dramatically, by giving the customers a seamless but a very impersonal experience of shopping. This particular problem can be solved by Chatbots. Customers can be treated personally with bots, which can exchange messages, give required suggestions and information. Famous fashion brands like Burberry, Tommy Hilfiger have recently launched Chatbots for the London and New York Fashion Week respectively. Sephora a famous cosmetics brand and H&M– a fashion clothing brand have also launched their Chatbots.

Chatbots in Finance

Chatbots have already stepped in Finance Industry. Chatbots can be programmed to assists the customers as Financial Advisor, Expense Saving Bot, Banking Bots, Tax bots, etc. Banks and Fintech have ample opportunities in developing bots for reducing their costs as well as human errors. Chatbots can work for customer’s convenience, managing multiple accounts, directly checking their bank balance and expenses on particular things. Further about Finance

and Chatbots have been discussed in our earlier blog: Chatbots as your Personal Finance Assistant.

Chatbots in Fitness Industry

Chat based health and fitness companies using Chatbot, to help their customers get personalised health and fitness tips. Tech based fitness companies can have a huge opportunity by developing their own Chatbots offering huge customer base with personalised services. Engage with your fans like never before with news, highlights, game-day info, roster and more.

Chatbots and Service Industry together have a wide range of opportunities and small to big all size of companies using chatbots to reduce their work and help their customers better.

Chatbots in Media

Big publisher or small agency, our suite of tools can help your audience chatbot experience rich and frictionless. Famous News and Media companies like The Wall Street Journal, CNN, Fox news, etc have launched their bots to help you receive the latest news on the go.

Conclusion

In this way we implemented an elementary catboat for any suitable customer interaction application.

Experiment No. 7

Title: - Implement Expert System.

Objectives:-

1. Understand the concept of Expert System

Problem Statement:-

Implement any one of the following Expert System

- I. Information management
- II. Hospitals and medical facilities
- III. Help desks management
- IV. Employee performance evaluation
- V. Stock market trading
- VI. Airline scheduling and cargo schedules

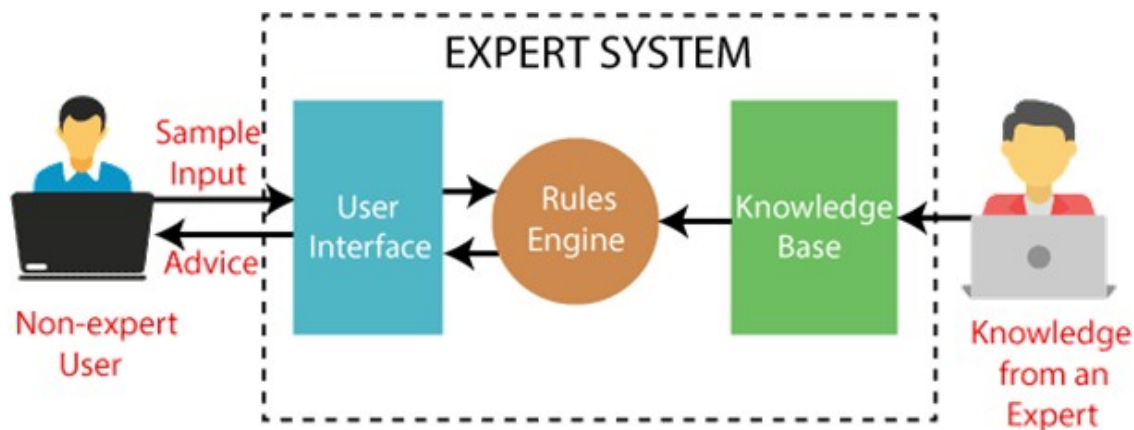
Software and Hardware requirements:-

2. **Operating system:** Linux- Ubuntu 16.04 to 17.10, or Windows 7 to 10,
3. **RAM-** 2GB RAM (4GB preferable)
4. You have to install **Python3** or higher version or Turbo C++ or JDK

Theory-

What is Expert System?

Expert System is an interactive and reliable computer-based decision-making system which uses both facts and heuristics to solve complex decision-making problems. It is considered at the highest level of human intelligence and expertise. The purpose of an expert system is to solve the most complex issues in a specific domain.



Expert Systems in Artificial Intelligence

The Expert System in AI can resolve many issues which generally would require a human expert. It is based on knowledge acquired from an expert. Artificial Intelligence and Expert Systems are capable of expressing and reasoning about some domain of knowledge. Expert systems were the predecessor of the current day artificial intelligence, deep learning and machine learning systems.

Examples of Expert Systems

Following are the Expert System Examples:

MYCIN: It was based on backward chaining and could identify various bacteria that could cause acute infections. It could also recommend drugs based on the patient's weight. It is one of the best Expert System Example.

DENDRAL: Expert system used for chemical analysis to predict molecular structure.

PXDES: An Example of Expert System used to predict the degree and type of lung cancer

CaDet: One of the best Expert System Example that can identify cancer at early stages

Characteristics of Expert System

The Highest Level of Expertise: The Expert system in AI offers the highest level of expertise. It provides efficiency, accuracy and imaginative problem-solving.

Right on Time Reaction: An Expert System in Artificial Intelligence interacts in a very reasonable period of time with the user. The total time must be less than the time taken by an expert to get the most accurate solution for the same problem.

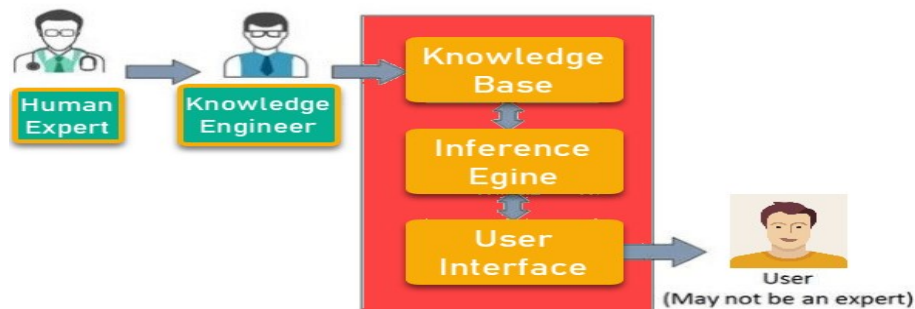
Good Reliability: The Expert system in AI needs to be reliable, and it must not make any a mistake.

Flexible: It is vital that it remains flexible as it the is possessed by an Expert system.

Effective Mechanism: Expert System in Artificial Intelligence must have an efficient mechanism to administer the compilation of the existing knowledge in it.

Capable of handling challenging decision & problems: An expert system is capable of handling challenging decision problems and delivering solutions.

Components of Expert System



The Expert System in AI consists of the following given components:

User Interface

The user interface is the most crucial part of the Expert System Software. This component takes the user's query in a readable form and passes it to the inference engine. After

that, it displays the results to the user. In other words, it's an interface that helps the user communicate with the expert system.

Inference Engine

The inference engine is the brain of the expert system. Inference engine contains rules to solve a specific problem. It refers the knowledge from the Knowledge Base. It selects facts and rules to apply when trying to answer the user's query. It provides reasoning about the information in the knowledge base. It also helps in deducting the problem to find the solution. This component is also helpful for formulating conclusions.

Knowledge Base

The knowledge base is a repository of facts. It stores all the knowledge about the problem domain. It is like a large container of knowledge which is obtained from different experts of a specific field.

Thus we can say that the success of the Expert System Software mainly depends on the highly accurate and precise knowledge.

Other Key terms used in Expert Systems

Facts and Rules

A fact is a small portion of important information. Facts on their own are of very limited use. The rules are essential to select and apply facts to a user problem.

Knowledge Acquisition

The term knowledge acquisition means how to get required domain knowledge by the expert system. The entire process starts by extracting knowledge from a human expert, converting the acquired knowledge into rules and injecting the developed rules into the knowledge base.

Advantages of Expert System

1. These systems are highly reproducible.

2. They can be used for risky places where the human presence is not safe.
3. Error possibilities are less if the KB contains correct knowledge.
4. The performance of these systems remains steady as it is not affected by emotions, tension, or fatigue.
5. They provide a very high speed to respond to a particular query.

Limitations of Expert System

1. The response of the expert system may get wrong if the knowledge base contains the wrong information.
2. Like a human being, it cannot produce a creative output for different scenarios.
3. Its maintenance and development costs are very high.
4. Knowledge acquisition for designing is much difficult.
5. For each domain, we require a specific ES, which is one of the big limitations.
6. It cannot learn from itself and hence requires manual updates.

Applications of Expert System

1. In designing and manufacturing domain

It can be broadly used for designing and manufacturing physical devices such as camera lenses and automobiles.

2. In the knowledge domain

These systems are primarily used for publishing the relevant knowledge to the users. The two popular ES used for this domain is an advisor and a tax advisor.

3. In the finance domain

In the finance industries, it is used to detect any type of possible fraud, suspicious activity, and advise bankers that if they should provide loans for business or not.

4. In the diagnosis and troubleshooting of devices

In medical diagnosis, the ES system is used, and it was the first area where these systems were used.

5. Planning and Scheduling

The expert systems can also be used for planning and scheduling some particular tasks for achieving the goal of that task.

Experiment No. 8

Title

Write a Java/C/C++/Python program that contains a string (char pointer) with a value 'HelloWorld'. The program should AND and XOR each character in this string with 127 and display the result.

Objectives

Implement AND, OR and XOR each character with 127

Outcome

Student should be able to see the result of AND, OR and XOR each character with 127.

Theory:

String

The string is the one-dimensional array of characters terminated by a null (0).

Each and every character in the array consumes one byte of memory, and the last character must always be 0.

The termination character (0) is used to identify where the string ends.

In C language string declaration can be done in two ways

1. By char array
2. By string literal

1. By char array

```
char ch[17]={'o','n','l','i','n','e','s','m','a','r','t','t','r','a','i','n','e','r','\0'};
```

As we know, array index starts from 0, so it will be represented as in the figure given below.

Index	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Character	o	n	l	i	n	e	s	m	a	r	t	t	r	a	i	n	e	r	\0

While declaring string, size is not mandatory. So we can write the above code as given below: `char ch[]={ 'o', 'n', 'l', 'i', 'n', 'e', 's', 'm', 'a', 'r', 't', 't', 'r', 'a', 'i', 'n', 'e', 'r', '\0' }`

2. By string literal

We can also define the string by the string literal in C language. For example:

```
char str[]="onlinesmarttrainer";
```

In such case, '\0' will be appended at the end of the string by the compiler.

AND Operation

There are two inputs and one output in binary AND operation.

The inputs and result to a binary AND operation can only be 0 or 1.

The binary AND operation will always produce a 1 output if both inputs are 1 and will produce a 0 output if both inputs are 0.

For two different inputs, the output will be 0.


Symbol	Truth Table		
	A	B	Q
	0	0	0
	0	1	0
	1	0	0
	1	1	1
Boolean Expression $Q = A \cdot B, A \text{ OR } B$			

Fig: AND Gate

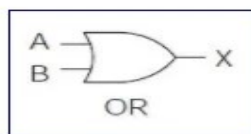
OR Operation

There are two inputs and one output in binary OR operation.

The inputs and result to a binary OR operation can only be 0 or 1.

The OR gate is a mostly used digital logic circuit. The output state of the OR gate will always be low when both of the inputs states is low.

Simply, if any input value in the OR gate is set to 1, then it will always return high-level output(1).



OR gate		
Input A	Input B	Output
0	0	0
1	0	1
0	1	1
1	1	1

Fig: OR Gate

XOR Operation

There are two inputs and one output in binary **XOR** (exclusive **OR**) operation.

It is similar to ADD operation which takes two inputs and produces one result i.e. one output.

The inputs and result to a binary **XOR** operation can only be 0 or 1.

The binary **XOR** operation will always produce a 1 output if either of its inputs is 1 and will produce a 0 output if both of its inputs are 0 or 1.

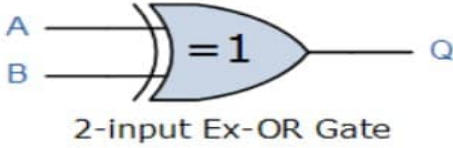
Symbol	Truth Table		
 <p>2-input Ex-OR Gate</p>	A	B	Q
	0	0	0
	0	1	1
	1	0	1
	1	1	0
Boolean Expression $Q = A \text{ XOR } B$			

Fig: XOR Gate

Algorithm:

1. Start
2. Take the input 'hello world' which is assigned to variable 'str'
3. Perform AND operation between the string and 127.
4. Perform OR operation between the string and 127
5. Perform XOR operation between the string and 127
6. Then print the result
7. Stop.

Conclusion:

Thus we have studied AND, OR and XOR gate operation on string to identify the encryption process.

Experiment No. 9

Aim:

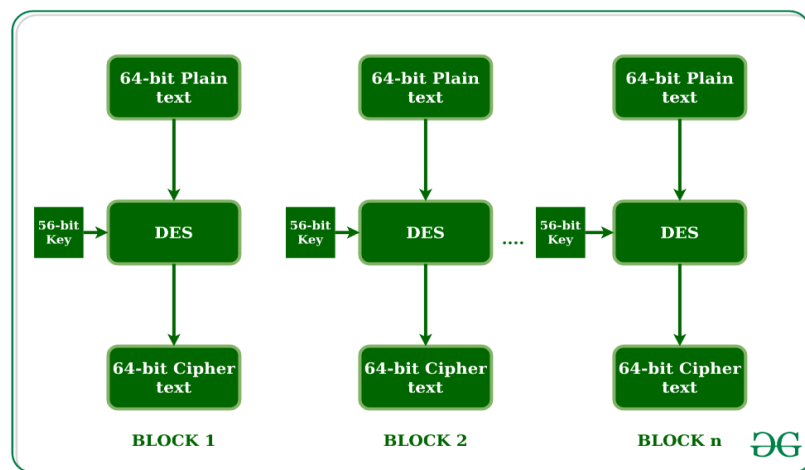
Write a Java/C/C++/Python program to implement DES algorithm.

Theory:

The Data Encryption Standard (DES) is the classic among the symmetric block cipher algorithm. DES was developed in the 1970's as a US-government standard for protecting non-classified information and was published as Federal Information Processing Standard.

Data encryption standard (DES) has been found vulnerable against very powerful attacks and therefore, the popularity of DES has been found slightly on the decline.

DES is a block cipher and encrypts data in blocks of size of 64 bits each, which means 64 bits of plain text goes as the input to DES, which produces 64 bits of ciphertext. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits. The basic idea is shown in the figure.



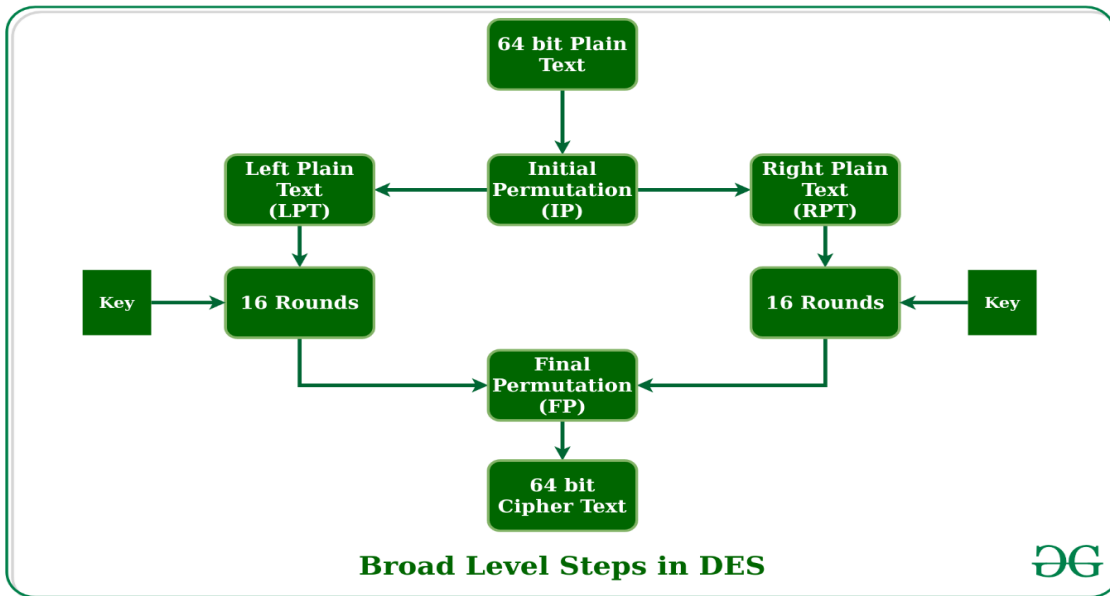
We have mentioned that DES uses a 56-bit key. Actually, the initial key consists of 64 bits. However, before the DES process even starts, every 8th bit of the key is discarded to produce a 56-bit key. That is bit positions 8, 16, 24, 32, 40, 48, 56, and 64 are discarded.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64

Figure - discarding of every 8th bit of original key

Thus, the discarding of every 8th bit of the key produces a 56-bit key from the original 64-bit key.

DES is based on the two fundamental attributes of cryptography: substitution (also called confusion) and transposition (also called diffusion). DES consists of 16 steps, each of which is called a round. Each round performs the steps of substitution and transposition.



Steps:-

1. 64-Bit plain text block is handed over to an Initial Permutation (IP) function
2. Initial Permutation (IP) is performed on plain text
3. IP produces two halves of permuted block
 Left plain text (LPT) and Right plain text (RPT)
4. Each LPT and RPT goes through 16 rounds of encryption process, each with its own key.
5. In the end LPT and RPT are rejoined and final Permutation (FP) is performed on combined block
6. The result is 64 bit cipher text.

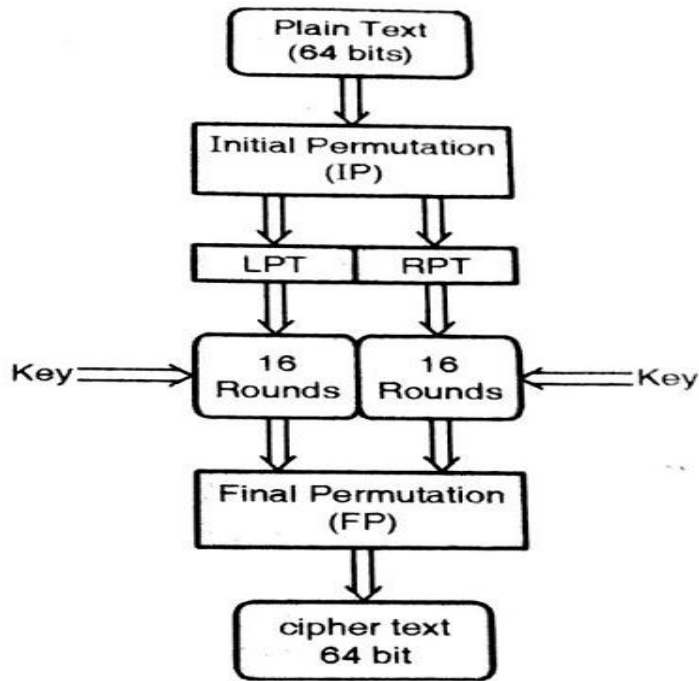


Fig: - Steps in DES

Initial Permutation (IP)

As we have noted, the initial permutation (IP) happens only once and it appens before the first round. It suggests how the transposition in IP should proceed, as shown infigure.

For example, it says that the IP replaces the first bit of the original plain text block with the 58th bit of the original plain text, the second bit with the 50th bit of the original plain text block, and so on.

This is nothing but jugglery of bit positions of the original plain text block. the same rule applies to all the other bit positions shown in the figure.

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	33	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Figure - Initial permutation table

As we have noted after IP is done, the resulting 64-bit permuted text block is divided into two half blocks. Each half-block consists of 32 bits, and each of the 16 rounds, in turn, consists of the broad level steps outlined in the figure.

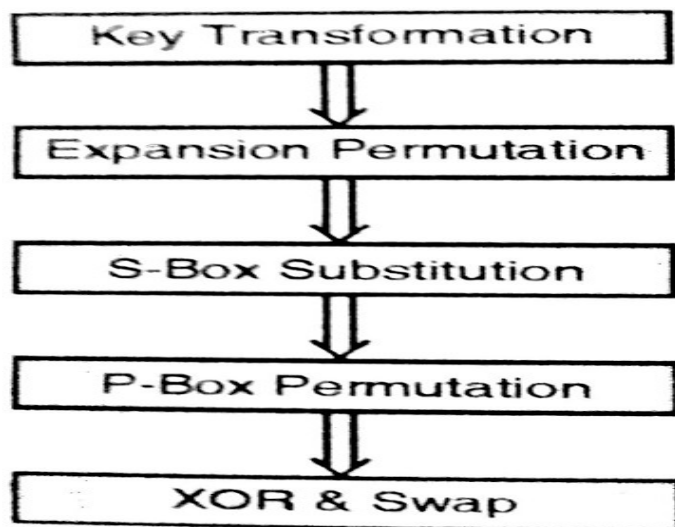


Fig: -Rounds in DES

Step-1: Key transformation –

We have noted initial 64-bit key is transformed into a 56-bit key by discarding every 8th bit of the initial key. Thus, for each a 56-bit key is available. From this 56-bit key, a different 48-bit Sub Key is generated during each round using a process called key transformation.

For this, the 56-bit key is divided into two halves, each of 28 bits. These halves are circularly shifted left by one or two positions, depending on the round.

For example, if the round numbers 1, 2, 9, or 16 the shift is done by only position for other rounds, the circular shift is done by two positions. The number of key bits shifted per round is shown in the figure.

Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
#key bits shifted	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Figure - number of key bits shifted per round

After an appropriate shift, 48 of the 56 bits are selected. for selecting 48 of the 56 bits the table is shown in the figure given below. For instance, after the shift, bit number 14 moves on the first position, bit number 17 moves on the second position, and so on. If we observe the table carefully, we will realize that it contains only 48-bit positions. Bit number 18 is discarded (we will not find it in the table), like 7 others, to reduce a 56-bit key to a 48-bitkey. Since the key transformation process involves permutation as well as a selection of a 48-bit subset of the original 56-bit key it is called Compression Permutation.

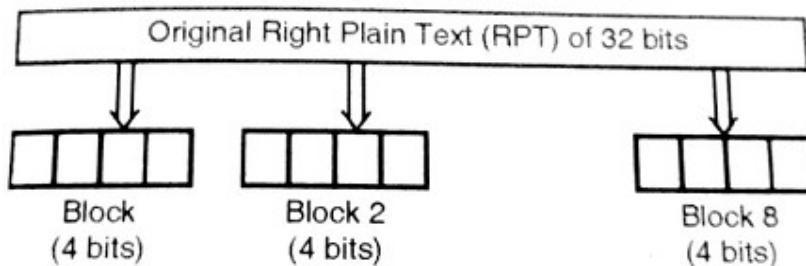
14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Figure - compression permutation

Because of this compression permutation technique, a different subset of key bits is used in each round. That makes DES not easy to crack.

Expansion Permutation

During Expansion permutation the RPT is expanded from 32 bits to 48 bits. The 32-bit RPT is divided into 8 blocks, with each block consisting of 4-bits.



Each 4-bits block of the previous step is then expanded to a corresponding 6-bit block. Per 4-bit block, 2 more bits are added. They are the repeated 1st and 4th bits of the 4-bit block.

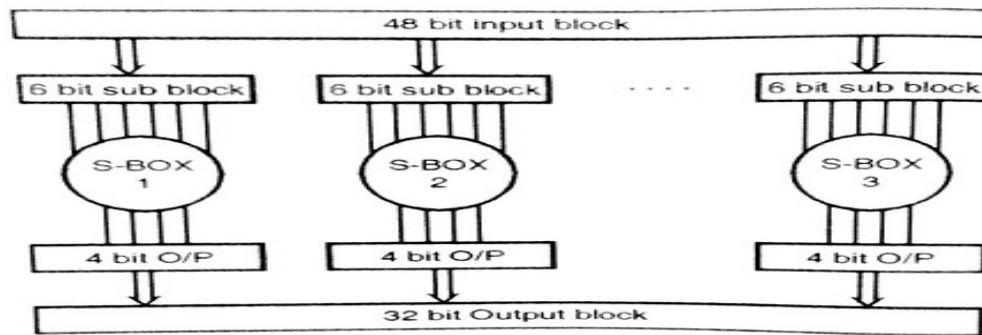
The 2nd and 3rd bits are written as they were in the input.

The 48 bit key is XORed with the 48-bit RPT and the resulting output is given to the next step.

S-box substitution

It accepts the 48-bits input from the XOR operation involving the compressed key and expanded RPT and produces 32-bit output using the substitution techniques.

Each of the 8 S-boxes has a 6-bit input and a 4-bit output as shown below.



P-box permutation

The output of S-box consists of 32 bits. These 32 bits are permuted using a P-box. It involves simple permutation.

For eg., a 16 in the first block indicates that the bit at position 16 of the original input moves to bit at position 1 in the output and a 10 in the block number 16 indicates that the bit at the position 10 of the original input moves to bit at position 16 in the output.

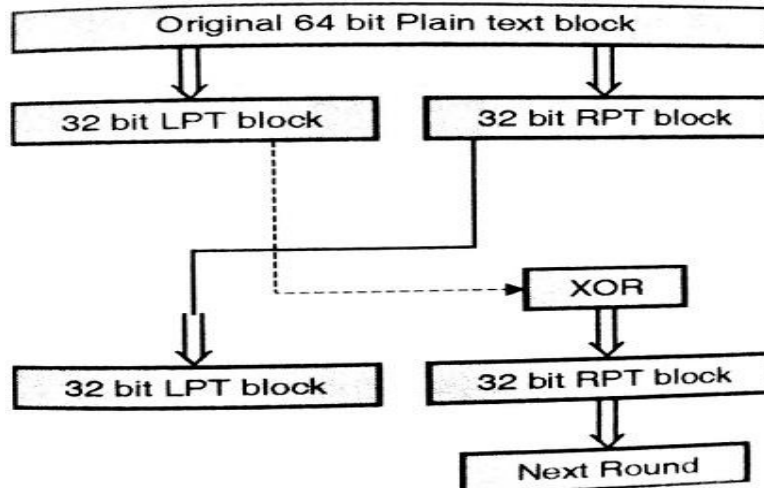
16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

XOR and swap

The LPT of the initial 64-bit plain text block is XORed with the output produced by P-box permutation.

The result of this XOR operation becomes the new RPT.

The old right half (RPT) becomes the new left half, in the process of swapping.



Final Permutation

At the end of 16 rounds, the Final Permutation is performed only once (simple transposition).

The output of Final Permutation is the 64 bit encryption block

Conclusion:

Thus we have studied encryption and decryption using DES algorithm

Experiment No. 10

Aim:

Write a Java/C/C++/Python program to implement RSA algorithm

Theory:

RSA (Rivest–Shamir–Adleman) algorithm is asymmetric cryptography algorithm. The acronym "RSA" comes from the surnames of Ron Rivest, Adi Shamir and Leonard Adleman, who publicly described the algorithm in 1977. Asymmetric actually means that it works on two different keys i.e. Public Key and Private **Key**. As the name describes that the Public Key is given to everyone and Private key is kept private.

An example of asymmetric cryptography :

1. A client (for example browser) sends its public key to the server and requests for some data.
2. The server encrypts the data using client's public key and sends the encrypted data.
3. Client receives this data and decrypts it.

Since this is asymmetric, nobody else except browser can decrypt the data even if a third party has public key of browser.

The idea! The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So, if somebody can factorize the large number, the private key is compromised. Therefore, encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024-bit keys could be broken in the near future. But till now it seems to be an infeasible task.

Let us learn the mechanism behind RSA algorithm :

Generating Public Key :

1. Select two prime no's. Suppose **P = 53 and Q = 59.**
2. Now First part of the Public key : **n = P*Q = 3127.**
3. We also need a small exponent say **e :**
4. But e Must be
5.
 - a. An integer.
 - b. Not be a factor of n.
 - c. **1 < e < $\Phi(n)$** [$\Phi(n)$ is discussed below],
 - d. Let us now consider it to be equal to 3.
6. Our Public Key is made of n and e
 - a. >> **Generating Private Key :**
7. We need to calculate $\Phi(n)$:
8. Such that **$\Phi(n) = (P-1)(Q-1)$**
9. so, $\Phi(n) = 3016$
10. Now calculate Private Key, **d :**
11. **$d = (k*\Phi(n) + 1) / e$** for some integer k
12. For k = 2, value of d is 2011.
 - a. Now we are ready with our – Public Key (n = 3127 and e = 3) and Private Key(d = 2011)
 - b. Now we will encrypt **“HI”** :
13. Convert letters to numbers : H = 8 and I = 9
14. Thus **Encrypted Data c = $89^e \bmod n$.**
15. Thus our Encrypted Data comes out to be 1394
16. Now we will decrypt **1394 :**

17. **Decrypted Data = $c^d \bmod n$.**
18. Thus our Encrypted Data comes out to be 89
19. **8 = H and I = 9 i.e. "HI".**

Conclusion:

Thus we have studied RSA (Rivest–Shamir–Adleman) algorithm, a asymmetric cryptography algorithm.

Experiment No. 11

Aim: Write a program to implement the Diffie-Hellman Key Exchange mechanism using HTML and JavaScript. Consider the end user as one of the parties (Alice) and the JavaScript application as other party (bob).

Theory:

Diffie-Hellman algorithm:

The Diffie-Hellman algorithm is being used to establish a shared secret that can be used for secret communications while exchanging data over a public network using the elliptic curve to generate points and get the secret key using the parameters.

- For the sake of simplicity and practical implementation of the algorithm, we will consider only 4 variables, one prime P and G (a primitive root of P) and two private values a and b .
- P and G are both publicly available numbers. Users (say Alice and Bob) pick private values a and b and they generate a key and exchange it publicly. The opposite person receives the key and that generates a secret key, after which they have the same secret key to encrypt.

Step-by-Step explanation is as follows:

Alice	Bob
Public Keys available = P, G	Public Keys available = P, G
Private Key Selected = a	Private Key Selected = b
Key generated =	Key generated =
Exchange of generated keys takes place	
Key received = y	key received = x
Generated Secret Key =	Generated Secret Key =

Alice	Bob
Algebraically, it can be shown that	
Users now have a symmetric secret key to encrypt	

Example:

Step 1: Alice and Bob get public numbers $P = 23$, $G = 9$

Step 2: Alice selected a private key $a = 4$ and

Bob selected a private key $b = 3$

Step 3: Alice and Bob compute public values

Alice: $x = (9^4 \bmod 23) = (6561 \bmod 23) = 6$

Bob: $y = (9^3 \bmod 23) = (729 \bmod 23) = 16$

Step 4: Alice and Bob exchange public numbers

Step 5: Alice receives public key $y = 16$ and

Bob receives public key $x = 6$

Step 6: Alice and Bob compute symmetric keys

Alice: $k_a = y^a \bmod p = 65536 \bmod 23 = 9$

Bob: $k_b = x^b \bmod p = 216 \bmod 23 = 9$

Step 7: 9 is the shared secret.

Conclusion:

Thus we have studied Diffie-Hellman Key Exchange mechanism using HTML and JavaScript

5. Appendix