answer in short about DES algorithm,AES Algorithm,RSA algorithm.Diffie-Hellman Key Exchange mechanism,MD5 algorithm,depth first search algorithm and Breadth First Search algorithm,A star Algorithm,Greedy search algorithm Selection Sort,Constraint Satisfaction Problem ,Backtracking for n-queens problem



Sure! Here's a short summary of each topic:

#### 1. DES Algorithm (Data Encryption Standard):

A symmetric-key block cipher that encrypts 64-bit blocks using a 56-bit key; now considered insecure due to small key size.

## 2. AES Algorithm (Advanced Encryption Standard):

A secure symmetric-key block cipher that supports 128-bit blocks and 128/192/256-bit keys; widely used for secure data encryption.

### 3. RSA Algorithm:

An asymmetric encryption algorithm using public and private keys; based on the difficulty of factoring large prime numbers.

## 4. Diffie-Hellman Key Exchange:

A mediod for two parties to securely share a secret key over an insecure channel without sharing the key directly.

#### 5. MD5 Algorithm (Message Digest 5):

A hashing algorithm that produces a 128-bit hash value; fast but vulnerable to collisions, not recommended for security.

## 6. Depth First Search (DFS):

A graph traversal algorithm that explores as far as possible along each branch before backtracking.

### 7. Breadth First Search (BFS):

A graph traversal algorithm that explores all neighbors at the current depth before moving to the next level.

## 8. A Algorithm:\*

A pathfinding algorithm using heuristics and cost to find the shortest path efficiently; combines features of BFS and greedy search.

## 9. Greedy Search Algorithm:

An algorithm that makes the locally optimal choice at each step, hoping to find a global optimum.

# 10. Selection Sort:

A simple sorting algorithm that repeatedly selects the smallest (or largest) element and moves it to the correct position.

## 11. Constraint Satisfaction Problem (CSP):

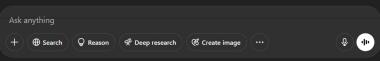
A problem where variables must be assigned values that satisfy specific constraints (e.g., Sudoku).

## 12. Backtracking for N-Queens Problem:

A recursive method to place N queens on an N×N chessboard so that no two queens attack each other, by trying and undoing placements.

Would you like a visual or code example for any of these?

ው ው ው ው ይ c v



ChatGPT can make mistakes. Check important info. See Cookie Preferences