1. What is DFS and BFS?
Ans: DFS (Depth-First Search) explores deeply into a branch before backtracking. BFS (Breadth-First Search) explores all nodes at the present depth before moving deeper.

2. What is recursive algorithm?
Ans: An algorithm that solves a problem by calling itself on smaller subproblems.

3. Explain DFS and BFS with an example.
Ans:

- DFS: A → B → D → backtrack → E
- BFS: A → B, C → D, E, F

*4. Explain A algorithm.**
Ans: A pathfinding algorithm that uses both actual cost and heuristic to find the shortest path efficiently.

*5. Formula of A?**
Ans: `f(n) = g(n) + h(n)` where `g(n)` is actual cost, and `h(n)` is heuristic estimate.

6. What is heuristic function?
Ans: A function that estimates the cost from the current node to the goal.

7. What is greedy search algorithm?
Ans: A search algorithm that picks the best option based on heuristic at each step.

8. Use of minimal spanning tree algorithm?
Ans: To connect all nodes in a graph with minimum total edge weight, used in network design.

9. Explain N-Queen problem with example.
Ans: Place N queens on an N×N chessboard such that no two attack each other.
Example for N=4: Queens at (1,2), (2,4), (3,1), (4,3).

10. Explain backtracking process.
Ans: Trial-and-error method where solutions are built incrementally, and wrong paths are discarded (backtracked).

11. What is chatbot?
Ans: AI software that interacts with users through text or voice like a human conversation.

12. Explain DES algorithm.
Ans: A symmetric-key block cipher using a 56-bit key and 16 rounds of encryption.

13. Explain AES algorithm.
Ans: Advanced symmetric-key encryption with 128/192/256-bit keys and multiple rounds (10, 12, 14).

14. Difference between AES and DES algorithm?
Ans: AES is more secure, faster, and uses longer keys than DES.

15. Explain RSA algorithm.
Ans: Asymmetric encryption using public and private keys for secure data transmission.

16. Explain Diffie Hellman algorithm.
Ans: A key exchange method that allows two parties to securely share a secret key over a public channel.

17. Explain MD5 algorithm.
Ans: A hash function that generates a 128-bit hash value; now considered cryptographically weak.

18. What is public key?
Ans: A key shared openly used to encrypt data or verify digital signatures.

19. What is private key?
Ans: A secret key used to decrypt data or generate digital signatures.

20. What is Asymmetric Key Cryptography?
Ans: Encryption using a pair of keys – public and private – for secure communication.

21. What is Symmetric Key Cryptography?
Ans: Encryption method where the same key is used for both encryption and decryption.

22. Difference between Asymmetric and Symmetric key cryptography?
Ans: Asymmetric uses two keys (public/private); Symmetric uses one shared key.

23. What is secret Key?
Ans: A key shared between sender and receiver in symmetric cryptography.

24. List of Asymmetric Key Cryptography algorithms?
Ans: RSA, Diffie-Hellman, ECC (Elliptic Curve Cryptography), DSA.

25. List of Symmetric Key Cryptography algorithms?
Ans: AES, DES, Triple DES, Blowfish, RC4, RC5.

26. What is Cryptography, Cryptanalysis?
Ans:

- Cryptography: The science of securing information.
- Cryptanalysis: The study of breaking or analyzing cryptographic systems.

27. What is Artificial Intelligence?
Ans: A branch of computer science that enables machines to mimic human intelligence.

28. Real world application of AI.
Ans: Self-driving cars, chatbots, recommendation systems, facial recognition.

29. What is CIA triad?
Ans: A model of security principles: **Confidentiality**, **Integrity**, and **Availability**.