4.What is JWT?

JWT is a compact, URL-safe token used to represent claims between two parties. It adheres to the RFC 7519 standard.

Structure of JWT:

- **Header**: Contains metadata, such as the type of token and the signing algorithm.
- **Payload**: Contains claims (user data or other information).
- **Signature**: Verifies the integrity of the token.

Example:

- **Encoded JWT**: Base64-encoded string with header, payload, and signature.
- **Decoded JWT**: A human-readable JSON object with user information.

Validation:

- Verify the signature to confirm the token's authenticity and integrity.
- Check the claims for permissions and expiration.

Additional Enhancements

- Include diagrams for each section for better understanding:
  - Symmetric and asymmetric encryption flow.

    - Process of signing and verifying digital signatures.
    - Structure of a JWT with Header, Payload, and Signature labeled.
- Highlight practical examples, such as how tokens are used in APIs for secure communication.