**JWT :**

JWT (JSON Web Token) is a compact, URL-safe means of representing claims to be transferred between two parties. The claims in a JWT are encoded as a JSON object that is used as the payload of a JSON Web Signature (JWS) structure or as the plaintext of a JSON Web E

ncryption (JWE) structure, enabling the claims to be digitally signed or integrity protected with a Message Authentication Code (MAC) and/or encrypted.

**Key Concepts of JWT**

1. **Header**: Contains the type of token (JWT) and the signing algorithm being used (e.g., HMAC SHA256).
2. **Payload**: Contains the claims. Claims are statements about an entity (typically, the user) and additional data.
3. **Signature**: Used to verify the token was not altered. It is created by encoding the header and payload and signing it with a secret or a private key.