1. Explain JWT in approx. with its benefis.

A JSON web token(JWT) is JSON Object which is used to securely transfer information over the web(between two parties). It can be used for an authentication system and can also be used for information exchange. The token is mainly composed of header, payload, signature. These three parts are separated by dots(.). JWT defines the structure of information we are sending from one party to the another, and it comes in two forms – Serialized, Deserialized. The Serialized approach is mainly used to transfer the data through the network with each request and response. While the deserialized approach is used to read and write data to the web token.

Benefits:

1. **More secure**: JWTs can use a public/private key pair in the form of an X.509 certificate for signing. A JWT can also be symmetrically signed by a shared secret using the HMAC algorithm. And while SAML tokens can use public/private key pairs like JWT, signing XML with XML Digital Signature without introducing obscure security holes is very difficult when compared to the simplicity of signing JSON.
2. **More common**: JSON parsers are common in most programming languages because they map directly to objects. Conversely, XML doesn't have a natural document-to-object mapping. This makes it easier to work with JWT than SAML assertions.
3. **Easier to process**: JWT is used at internet scale. This means that it is easier to process on user's devices, especially mobile
4. **Information Exchange:** JWTs are a good way of securely transmitting information between parties because they can be signed, which means you can be sure that the senders are who they say they are. Additionally, the structure of a JWT allows you to verify that the content hasn't been tampered with.