JWT (JSON Web Tokens)

1) In simple terms, it is a way for **securely exchanging or transferring information in JSON format** between two parties.
2) The two parties are the client and the server.
3) JWT is most commonly used in authentication.
4) And the steps are as follows:
    a) When a user signs in, the server sends a JWT to the user.
    b) The token is now transmitted back to the server with every request to access a route or web page through the **Authorization** header.
    c) The server will next validate the JWT to see if the user is permitted to access the route or web page. If the JWT is validated, the server will grant the user access to the web page.
5) JWT is made up of three components:

a) Header

i) The header contains the **type of algorithm used to sign the JWT** as well as **the type of token** (in this case, JWT).
ii) Example of a header:

```
{
    "alg": "HS256",
    "typ": "JWT"
  }
```

b) Payload

i) The payload contains the user's information as well as additional information such as the expiry time, issuer, issued at (iat), subject (sub), and audience.
ii) The information provided by the user, along with the supplementary information, is referred to as **"claims".**
iii) This **information is used by the server** to determine if the user has **authorization** to do the **action requested.**
iv) Example of payload:

```
{
    "role": "Admin",
    "sub": "1234567890",
    "iat": 1516239022,
    "name": "John Doe"
     }
```

c) Signature

i) The signature is created when the header and payload parts of the JWT are hashed together. The signature is created using the same algorithm that is described in the header part of the JWT.

Question: I understand the purpose of the header and the payload, but what exactly is the purpose of the signature?