ASSIGNMENT #:

Date: M T W T F S S

① What are cookies?

small piece of data stored on user's device,

Cookies are small text files stored in the user's browser. When you visit a website, the server can save data on your computer, Cookies help websites remember user and track their activities to provide a personalized experience.

Types of cookies:

① Session cookies, Session cookies are temporary cookies which are present as long as the user browser is open. session cookies are deleted once the browser is closed or inactive user session. it is used for maintaining the session of user on browser

② Persistent cookies

Permanent cookies, stored in user device for specific period (<6 months) use for long term tracking & remember user preference

③ first party cookies :- these are set by the website you currently visit, first party cookies are generally used to provide a good user experience, collecting the analytics data, remember language etc.

④ Third-party cookies

are set by domain that you are not visiting, third-party cookies are mostly use for cross site tracking & advertising purposes these

Page No. _____ Signature _____

Date:
M T W T F S S

Cookies collect data and serveads according to it.

Cookies used for ?

- User session
- Tracking
- Personalization.

JWT TOKEN :-

a secure way to send information b/w a client and a server it is mainly used in web application and APIs to verify user & prevent unauthorized access. JWT is Json data secured with a cryptographic signature.

→ Signing can be done with these methods

① HMAC (HASH BASED MESSAGE AUTHENTICATION)

② RSA or ECDSA (ASSYMETRIC CRYPTOGRAPHIC ALGORITHMS)

JWT Consist of Three Parts :-

① HEADER
② PAYLOAD
③ SIGNATURE

Date:

M	T	W	T	F	S	S

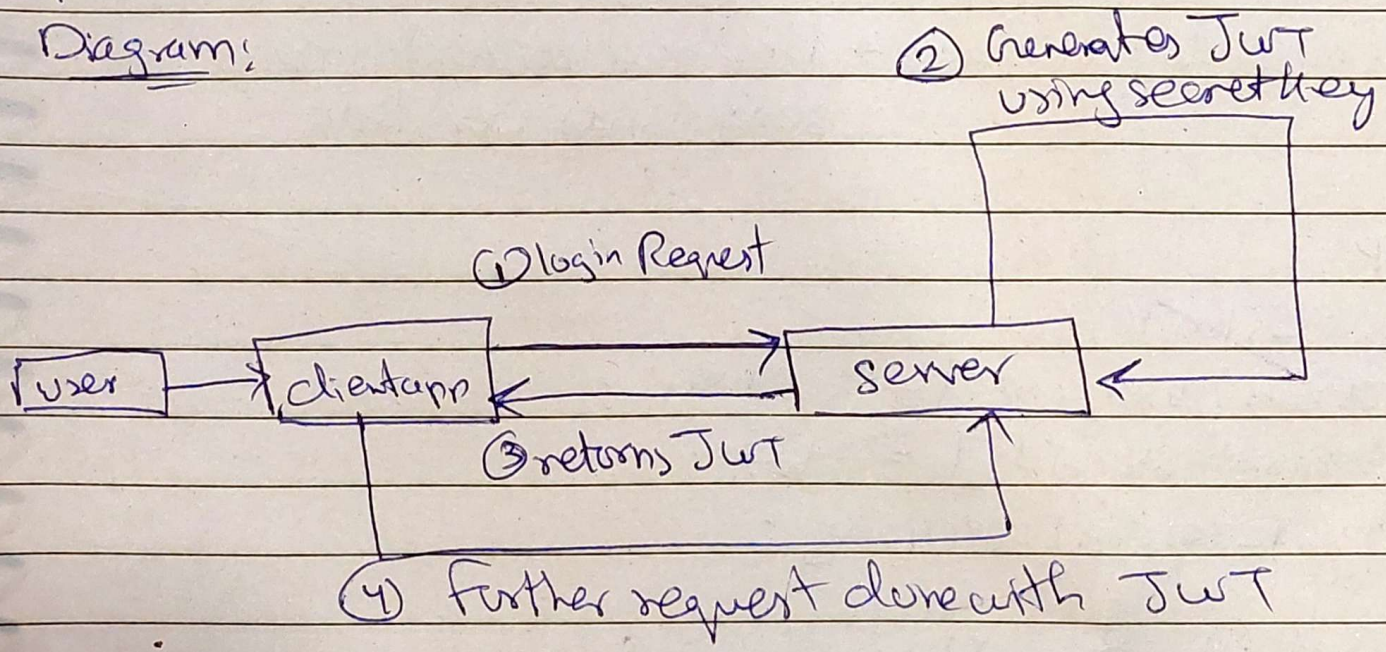
Header:- Contains metadata about token, also use for signing.

PAYLOAD:- Data beings transmitted

SIGNATURE:- Ensures the token's integrity and authenticity

after these three steps JWT Token generated by joining these three.

Diagram:



Signature

Date:

M	T	W	T	F	S	S

Sessions :-

Keeping user information safe on server while they Browse different pages of website. The user's browser only gets a small ID number.

How it works :-

① User visit website → Server Creates unique session ID

② Session ID saved in cookie → Browser stores only the ID

③ Data stored on server → All user info stays on server

④ User moves to another page → Browser sends session ID, server finds user data.

Code:

```
<? php
  session_start();
  $_session['username'] = "Ahsan";
  $_session['user_id'] = 123;
  echo $_session[username];

if(isset($_session['user_id'])){
        echo "You are logged in"; }
session_destroy();
?>
```

Date:

M	T	W	T	F	S	S

Sessions Vs Cookies

Sessions	Cookies
Data is stored on server	Data is stored on the client side (on the browser)
More secure as session data is not stored on client side.	Less secure as data is stored on the client side and can be change & stolen
Session usually expire when browser closed or in active user identified for a specific time	Cookies can have expiration date set to stay persistent across the browser sessions.