**PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR**

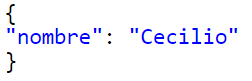
**FACULTAD DE INGENIERIA**

**ESCUELA DE SISTEMAS**

Manuel Alejandro Tinajero

SEMANA 7

El algoritmo criptográfico que vamos a utilizar**HS256**. Quiere decir que estamos usando un token JWT ( el más común) y un algoritmo de HASH muy concreto denominado HMAC que genera u**n hash con SHA256 utilizando una clave privada.**  La información que vamos a almacenar del proyecto es en nuestro caso únicamente el nombre del usuario.



1. El cliente se logea en el servidor y envía usuario y clave.
2. El sistema le valida y genera un token usando el algoritmo HMAC y la clave privada.
3. El cliente recibe el token.
4. El cliente solicita unos datos y pasa como identificador el token.
5. El servidor decodifica los bloques de base64 y usa su clave privada para comprobar el HASH. Si todo es correcto permite el acceso y envía la información solicitada al cliente.