**RSA** : En el intercambio de claves RSA, el servidor genera un par de claves: una clave pública y una clave privada. La clave pública se envía al cliente y se utiliza para cifrar una clave de sesión que se utiliza para cifrar los datos que se transmiten entre el cliente y el servidor. La clave privada se mantiene en secreto en el servidor y se utiliza para descifrar la clave de sesión cifrada.

La autenticación del servidor con RSA se realiza mediante la firma digital. El servidor genera una firma digital utilizando su clave privada y la envía al cliente junto con su certificado digital. El cliente utiliza la clave pública del servidor para verificar la firma digital y comprobar la autenticidad del servidor.

**AES:** AES es un algoritmo de cifrado de bloque que cifra los datos en bloques de 128 bits utilizando una clave simétrica compartida entre el cliente y el servidor. AES utiliza una de las tres longitudes de clave: 128 bits, 192 bits o 256 bits. Cuanto más larga sea la clave, más difícil será para un atacante descifrar los datos cifrados.

En SSL y TLS, el cliente y el servidor negocian un algoritmo de cifrado y una longitud de clave comunes que se utilizarán para cifrar los datos que se transmiten entre ellos. Después de la negociación, el cliente y el servidor utilizan la clave compartida para cifrar y descifrar los datos que se transmiten entre ellos.

**SHA:** En SSL y TLS, SHA se utiliza para generar un resumen o "hash" de los datos que se transmiten entre el cliente y el servidor. Este resumen se utiliza para verificar que los datos no han sido modificados durante la transmisión. SHA se utiliza en combinación con otros algoritmos de cifrado y técnicas criptográficas para proporcionar una seguridad sólida en la comunicación en línea.

**DSA:** DSA es un algoritmo de firma digital asimétrico que utiliza una clave privada y una clave pública. La clave privada se utiliza para firmar digitalmente los datos, mientras que la clave pública se utiliza para verificar la firma digital.

En SSL y TLS, DSA se utiliza junto con otros algoritmos criptográficos, como AES y SHA, para garantizar la seguridad de la comunicación en línea. El servidor utiliza DSA para firmar digitalmente su certificado, que se envía al cliente para su verificación.

**ECDHE** se basa en la criptografía de curva elíptica y es una versión mejorada del algoritmo de intercambio de claves Diffie-Hellman (DHE). En ECDHE, el servidor y el cliente generan de manera independiente una claves pública y privada de curva elíptica, que se utilizan para generar una clave de sesión compartida.

En SSL y TLS, la clave de sesión generada por ECDHE se utiliza para cifrar los datos que se transmiten entre el cliente y el servidor, proporcionando una comunicación segura y privada.

**ChaCha20** es un cifrado rápido y seguro que utiliza una clave simétrica compartida entre el cliente y el servidor para cifrar los datos. Se considera una alternativa segura y eficiente a otros algoritmos de cifrado simétrico, como AES. ChaCha20 también es resistente a los ataques de tiempo y a los ataques de canal lateral.

En SSL y TLS, ChaCha20 se utiliza junto con Poly1305, un algoritmo de autenticación de mensajes, para proporcionar seguridad en la comunicación en línea. ChaCha20-Poly1305 proporciona cifrado y autenticación de mensajes en una sola operación, lo que lo hace más eficiente que otras combinaciones de cifrado y autenticación de mensajes.

ChaCha20 se está convirtiendo cada vez más en un cifrado común en SSL y TLS, especialmente en aplicaciones de navegadores web y móviles.