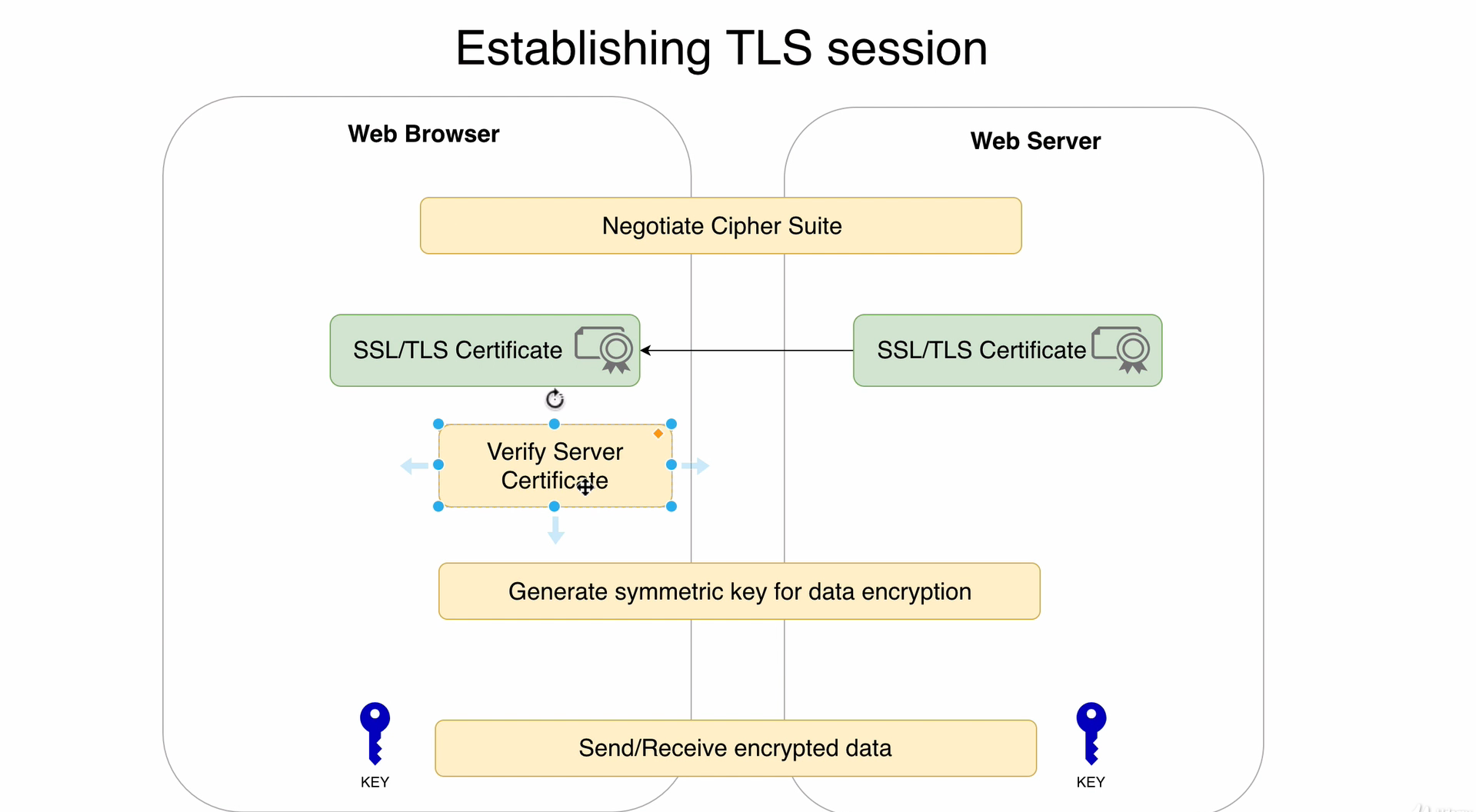
1. 
2. Let’s try to understand how TLS Session is established by the diagram.
3. Browser makes an connect request to server over **HTTPs**.
4. When **TCP Session** is established, we start establishing **TLS Session**.
5. TLS Session Establishment:
   1. First it sends the server a list of supported Cipher Suites.

Web Server selects one from the list. This step is called “**Negotiation of Cipher Suite”**.

* 1. Then webserver sends its certificate to web browser (All intermediate Certificates + End-User Certificate excluding Root Certificate assuming that root certificate is stored the client side in Root Certificate Store).
  2. Then Web Browser verifies the signature of the certificates in entire Chain of certificates. Like this.
     1. Verify Signature.
     2. Jatin: Verify the domain name. This is also equally important because if someone replace actual certificate with the fake one which can be verified successfully then domain name will help us here as signature process also involves the domain name by CA.
     3. Check the validity period.
     4. Verify whether the certificate was revoked or not (**optional**)
  3. Next step is to generate **Symmetric Key** for Data Encryption.   
     Sometimes, this key is generated on the browser side and after encryption by using the public key from the certificate is sent to the Webserver and   
     sometimes this key is generated by Diffie-Hellman Key Exchange Algorithm and in this case we don’t encrypt the key as this also is designed to generate same key both sides by unencrypted public connection.
  4. Once key is present, we can start sending data back and forth after encrypting the data using that **Symmetric Key**.  
       
     This is how secure session is set up.