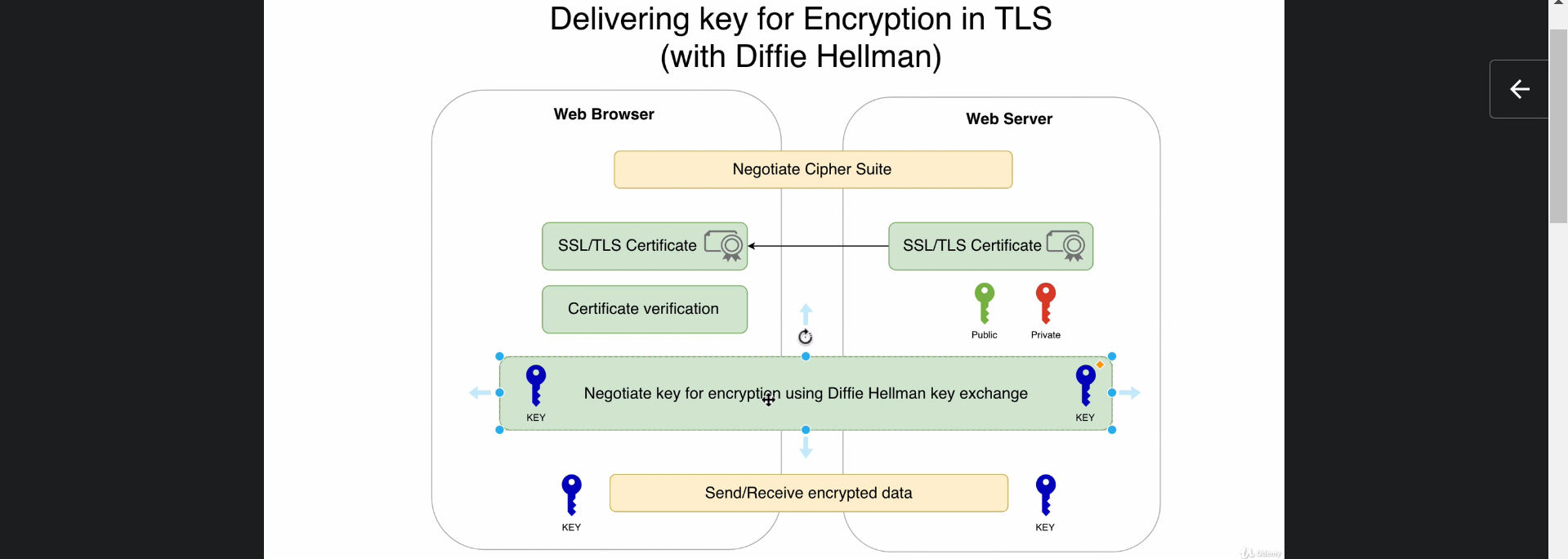
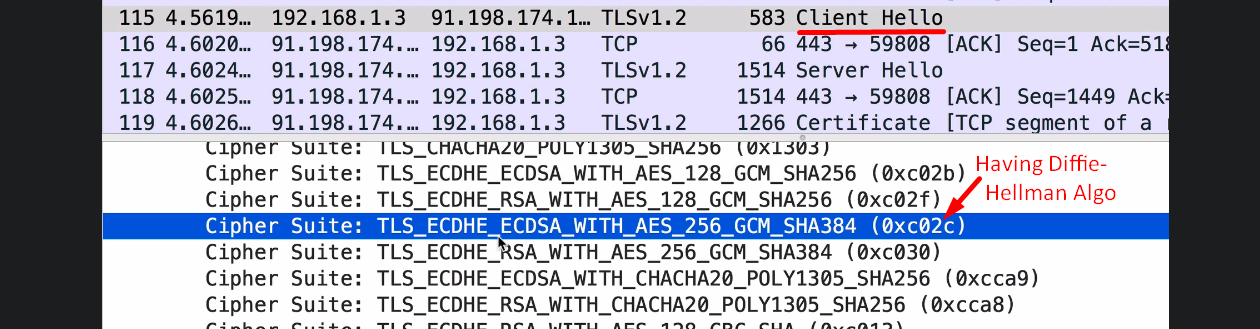
1. **Agenda:**
   1. Discuss about how Symmetric Key is exchanged with Diffie-Hellman Key Exchange Algo.
2. 
3. Suppose Browser and Webserver start negotiation of Cipher Suite and this time it chooses Cipher Suite with Diffie-Hellman Algo.
4. 
5. After certificate verification, the browser and server start negotiation of symmetric encryption key for traffic encryption.  
   In case of Diffie-Hellman key Exchange Algo is designed to generate symmetric key and exchange over unencrypted unsecure public network.
6. After key exchange, the encrypted traffic starts to flow back and forth and using the symmetric key, either of them can encrypt and decrypt data.
7. You may ask reasonable questions:
   1. What is Diffie-Hellman Algo?
   2. How it works?
   3. How a key is generated.
8. There are some issues with Diffie-Hellman algo and we will use a modified version.   
   We will discuss all this in respective lectures.