9. Transport Layer Security - TLS 1.2 and 1.3

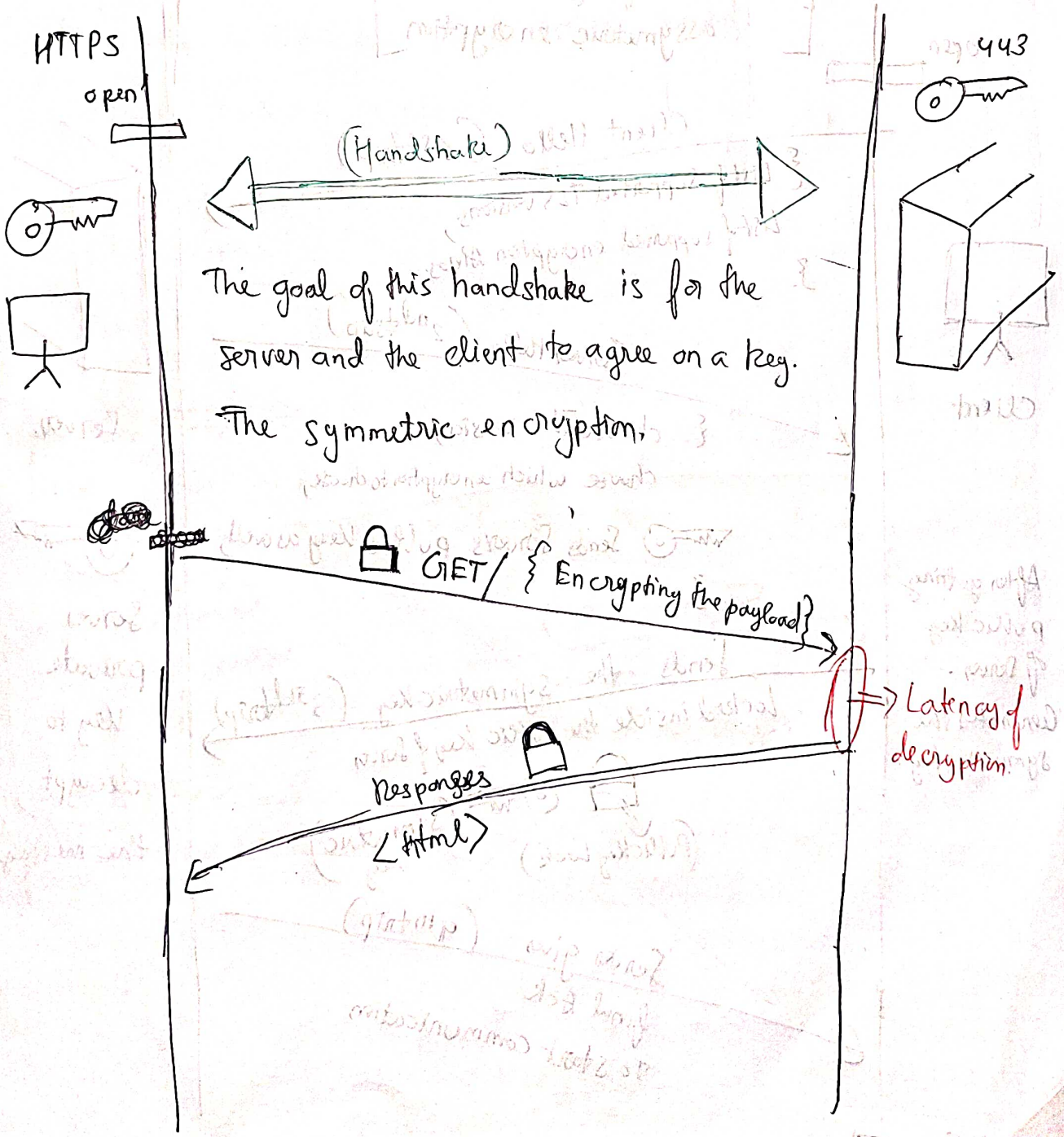
HTTP is a stateless protocol

TCP is stateful

Hence we can use UDP with HTTP as well

HTTPS

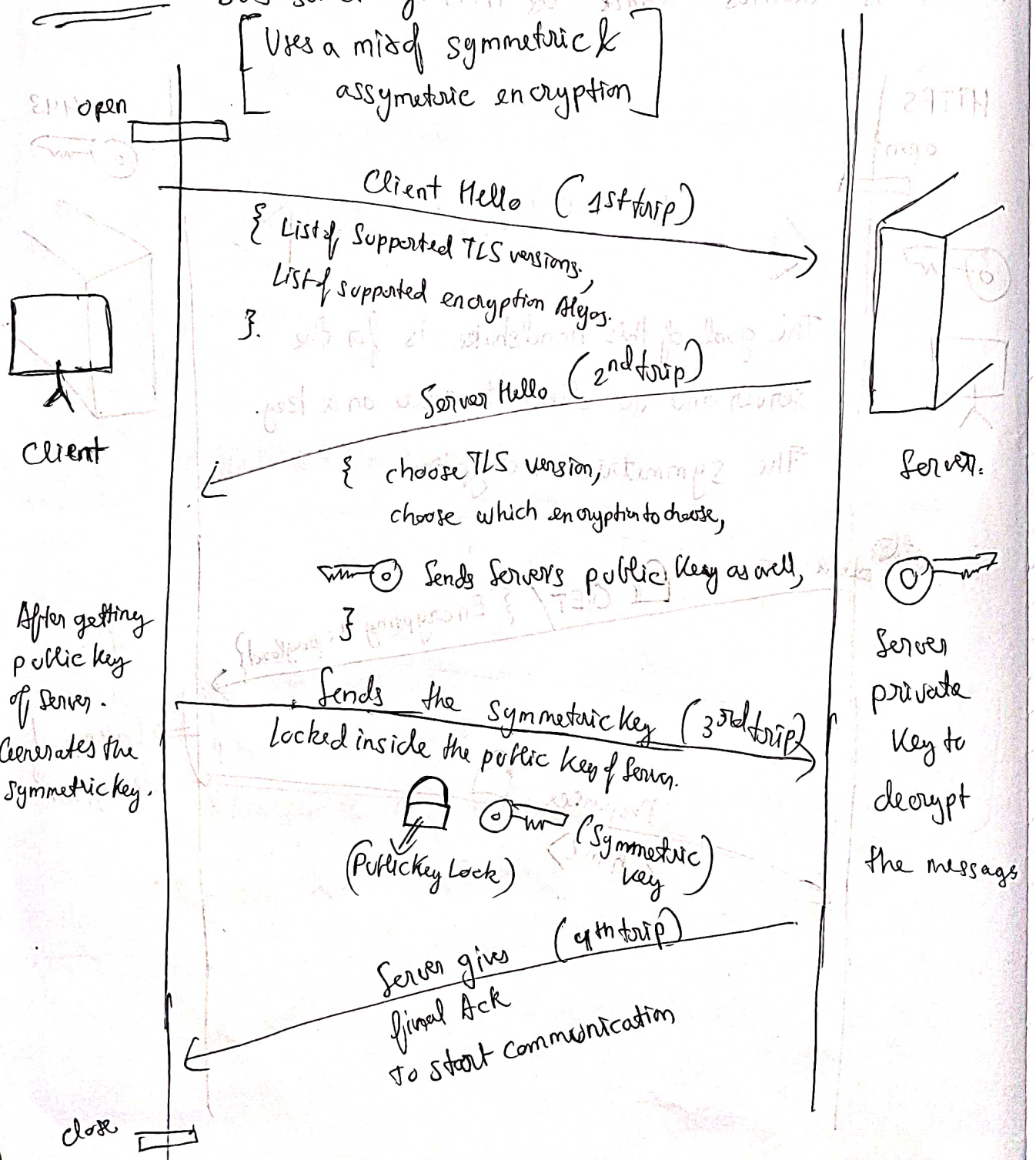
HTTPS is almost same as HTTP.



TLS 1.2 (Zoom into the handshake)

If you remember Asymmetric encryption. The message is sent by encrypting using public key of the server, by decrypted using the private key of the server.

TLS 1.2 Does something Similar.

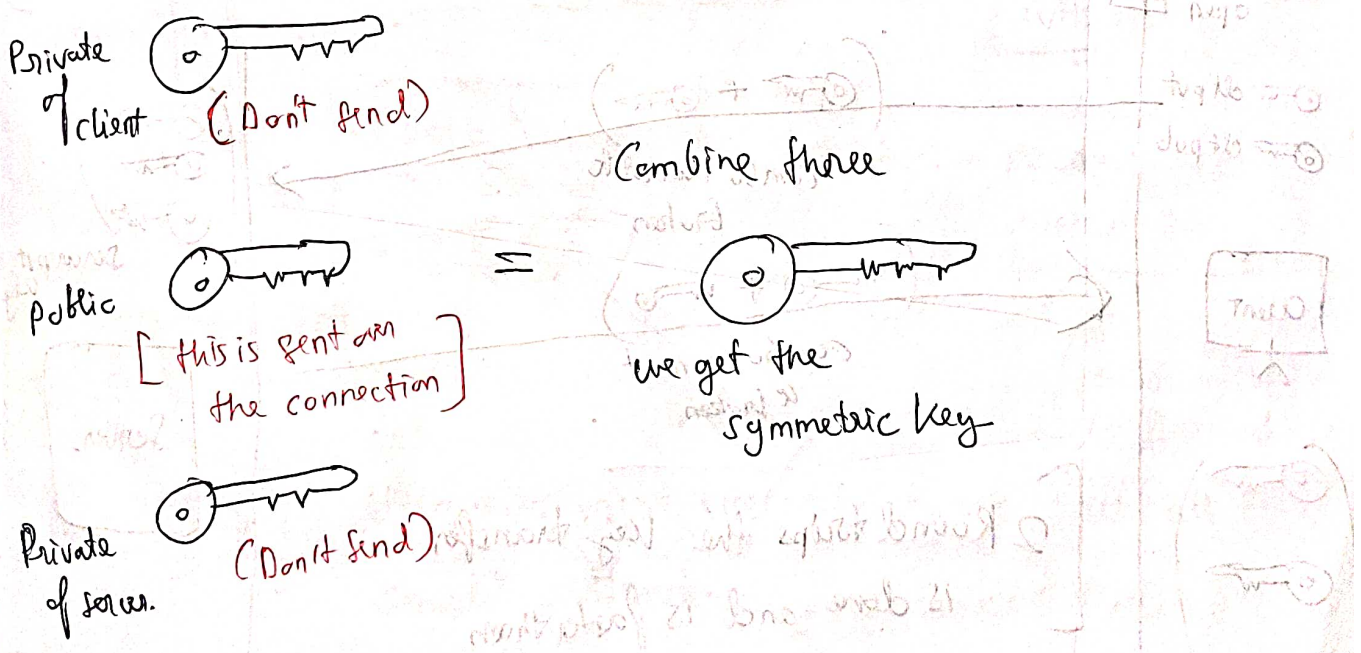


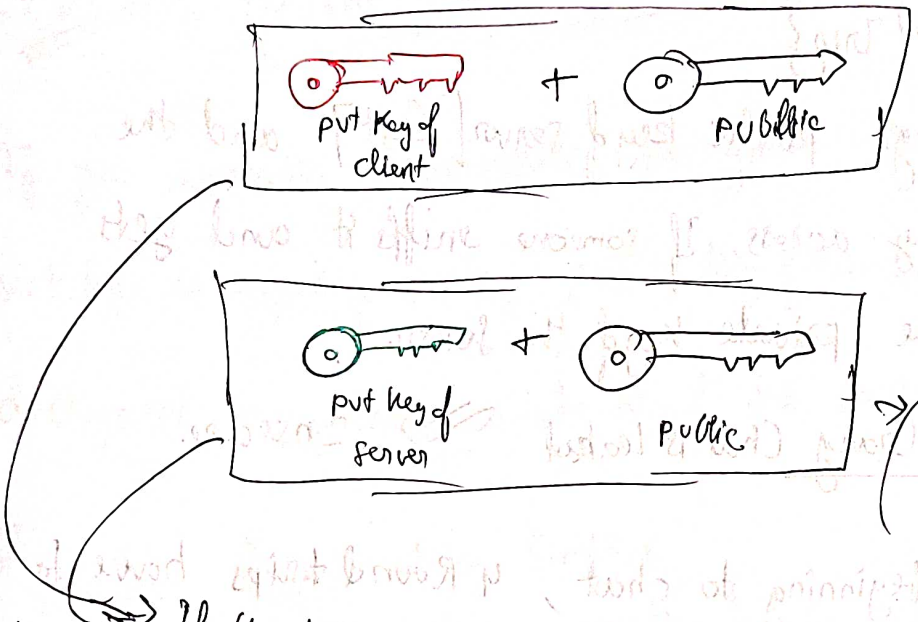
Problem with TLS 1.2

* {2nd trip and 3rd trip}
  You are sending public key of server [Cert] and the symmetric key across, If someone sniffs it and gets control over the private key of the server.
  Boom Boys Crang Chat is Leaked ⇒ Insecure.

* Before beginning to chat, 4 Round trips have to be made in order to start actual comms.
  Hence TLS 1.2 is slow.

Diffie Hellman





If the hacker even gets these, they cannot extract the RedKey [pvt key of client], GreenKey [pvt key of server] from the combination.

TLS 1-3