

## 9. Transport Layer Security: TLS 1.2 and 1.3

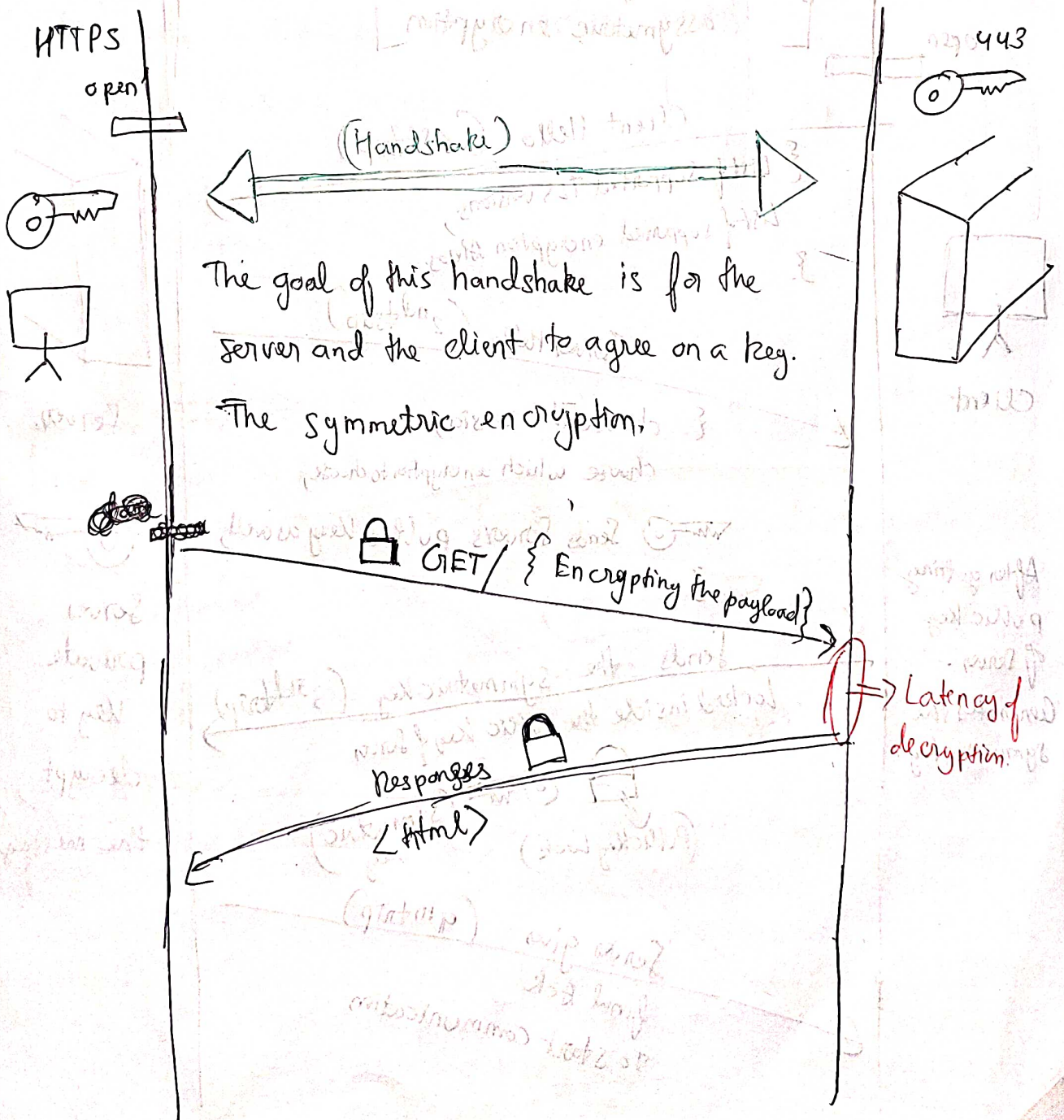
HTTP is a stateless protocol

TCP is stateful ~~state~~

Hence we can use UDP with HTTP as well

HTTPS

HTTPS is almost same as HTTP.

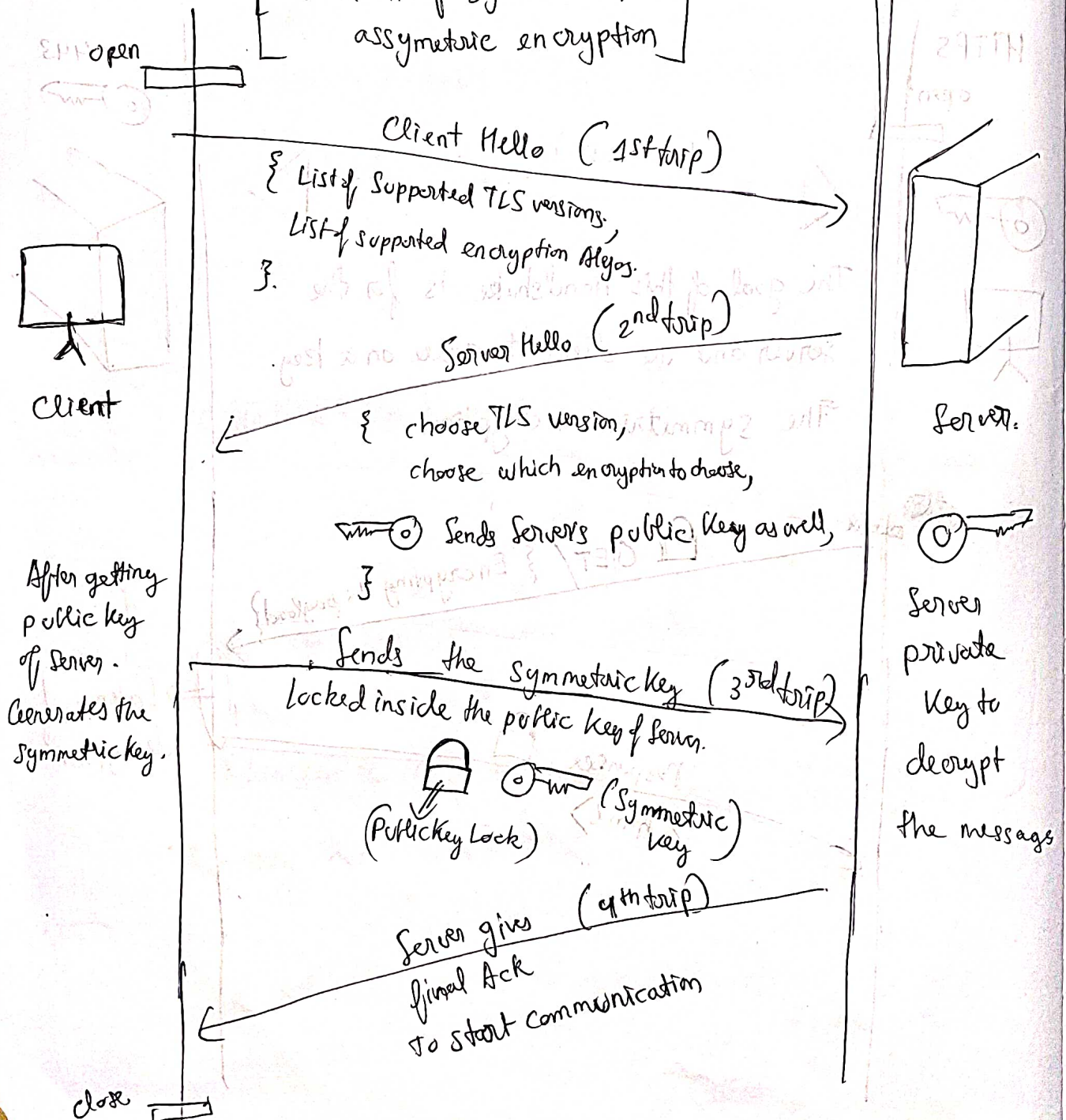


# TLS 1.2 (Zoom into the handshake)

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.

[ Uses a mix of symmetric & asymmetric encryption ]





## Problem with TLS 1.2

\* {2<sup>nd</sup> trip and 3<sup>rd</sup> 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 Grang Chat is leaked  $\Rightarrow$  Insecure.

\* Before ~~beginning~~ beginning to chat, 4 Round trips have to be made in order to start actual comms.

Hence TLS 1.2 is slow.

## Diffie Hellman

Private  
Client (Don't send)

Public  
[this is sent on the connection]

Private  
of server.  
(Don't send)

Combine these

we get the symmetric key

TLS

Handshake

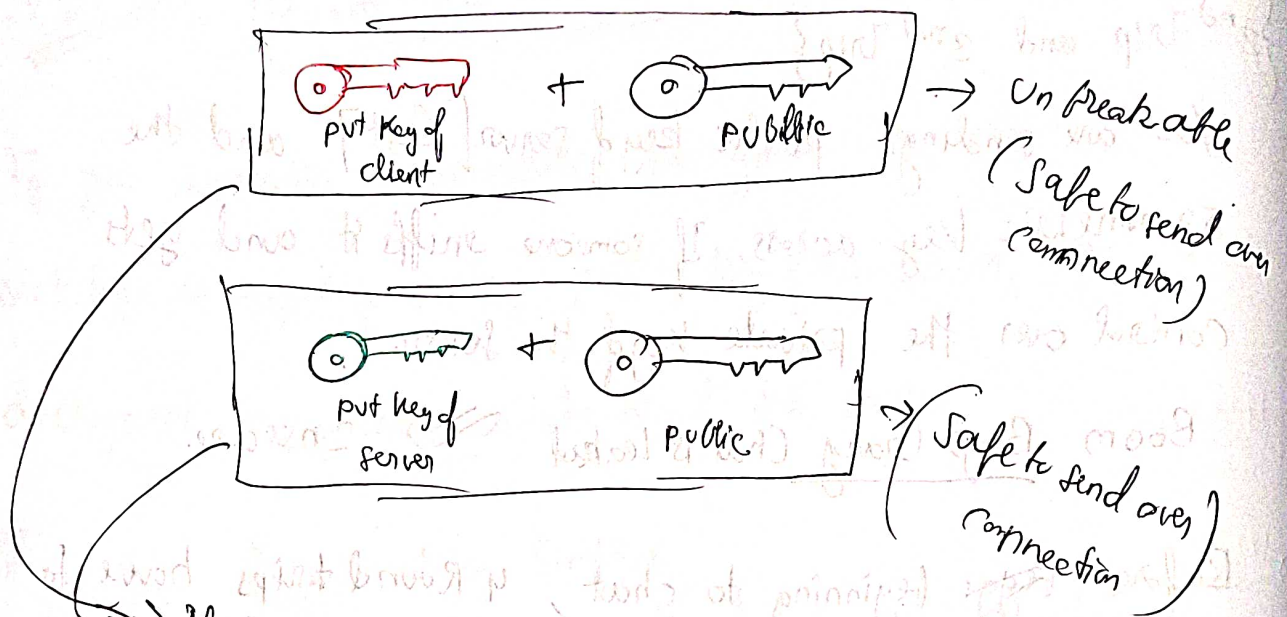
Key Exchange

Authentication

Key Confirmation

Finished

Secure Channel



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

