



Sahn Lam • Following

Coauthor of the Bestselling 'System Design Interview' Series | Cofounder at ByteByteGo

[Visit my website](#)

3h • 🌐

HTTPS Under the Hood

HTTPS is a secure way to share information on the internet. It encrypts data transfer between client and server.

But without common encryption key, how data is encrypted?

1 - Server Certificate Check

- Client and server exchange "HELLO" messages
- Server sends its certificate
- Client verifies it with a Certificate Authority

2 - Key Exchange

- Client extracts server's public key, creates a session key
- They agree on a cipher suite
- Client encrypts session key using server's public key
- Server decrypts it

3 - Encrypted Tunnel for data transmission

- Client and server both have a common key (session key)
- They use it to encrypt and decrypt data during transmission

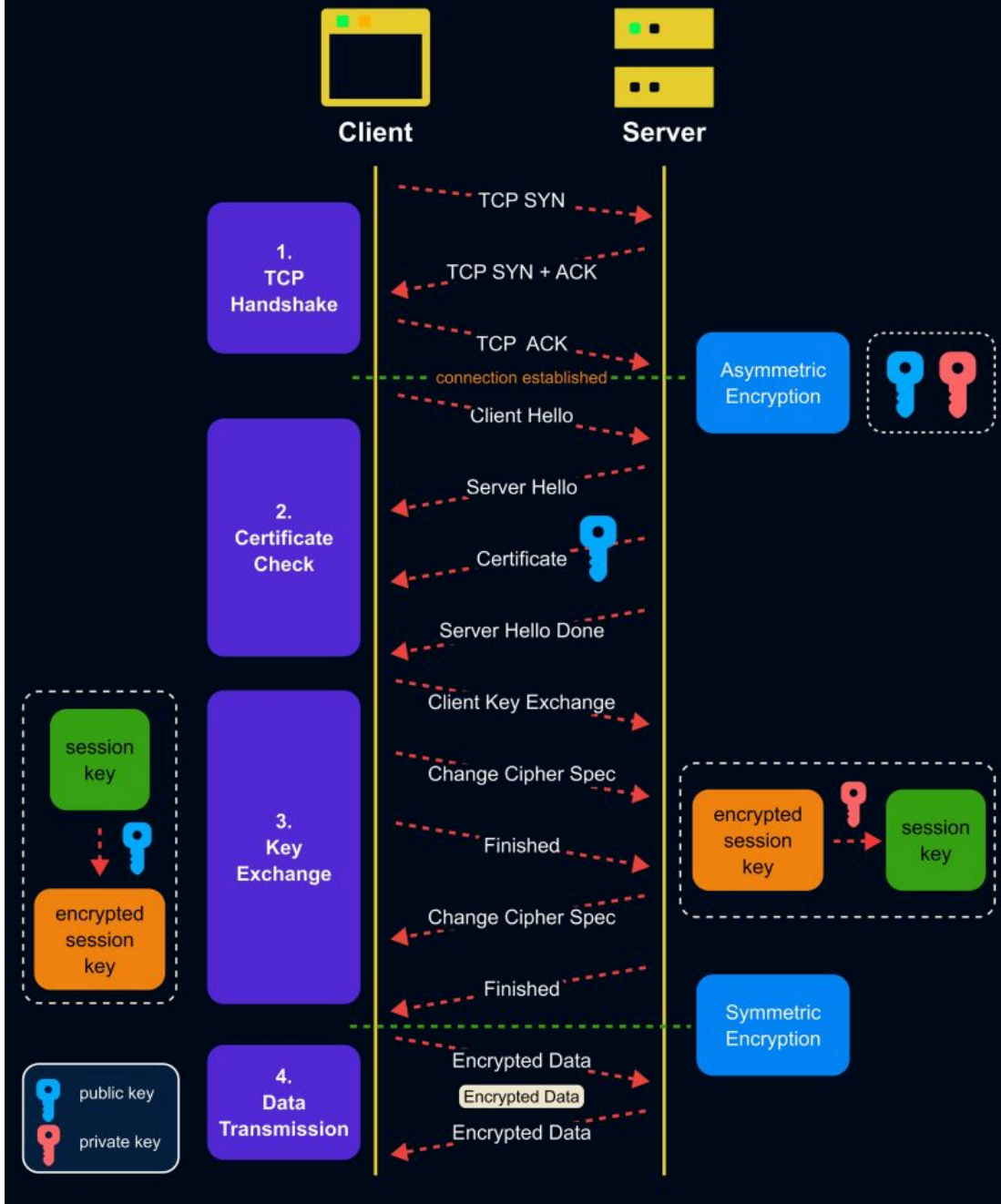
This creates a secure, encrypted tunnel for data transfer, protecting information from eavesdropping and tampering.

--

Subscribe to our weekly newsletter to get a Free System Design PDF (158 pages): <https://bit.ly/496keA7>

How does HTTPS Work?

ByteByteGo



 Shamsul H. Forhad and 189 others

5 comments 28 repos...