

[What is HTTP(S)]  
↳ Secure?

\* Normal HTTP (Port 80)

↳ TCP handshake

↓  
Data send

↓  
Connection close

\* HTTPS (PORT 443)

↳ To encrypt and decrypt application data

↳ we need key (public, private)

↳ E.g RSA Algorithm

↳ TLS/SSL handshake

⇓  
Data send

⇓

Connection close

\* TLS/SSL are encryption protocol which uses some cryptography Algo like RSA or Diffie-Hellman.

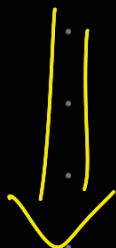
SSL → Secure Socket Layer

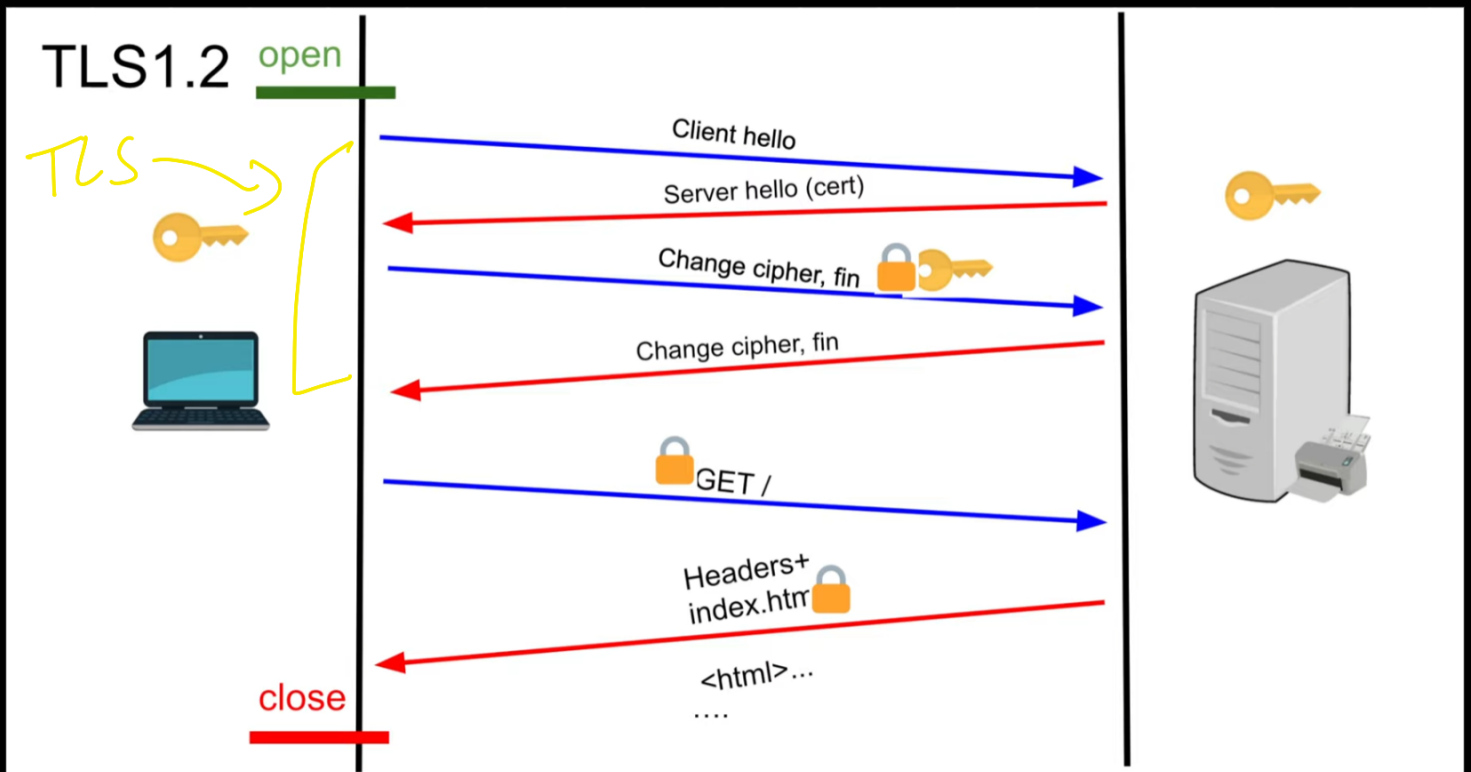


Replaced by TLS (Transport layer security)

TLS 1.2      TLS 1.3

\* HTTPS is slower than HTTP because of overhead of TLS





\* Algorithms that are used by TLS

AES      RSA      Diffie-Hellman