[What is HTTPS]

↳ 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~~ sent

⇓

Connection close

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

SSL → Secure Socket Layer

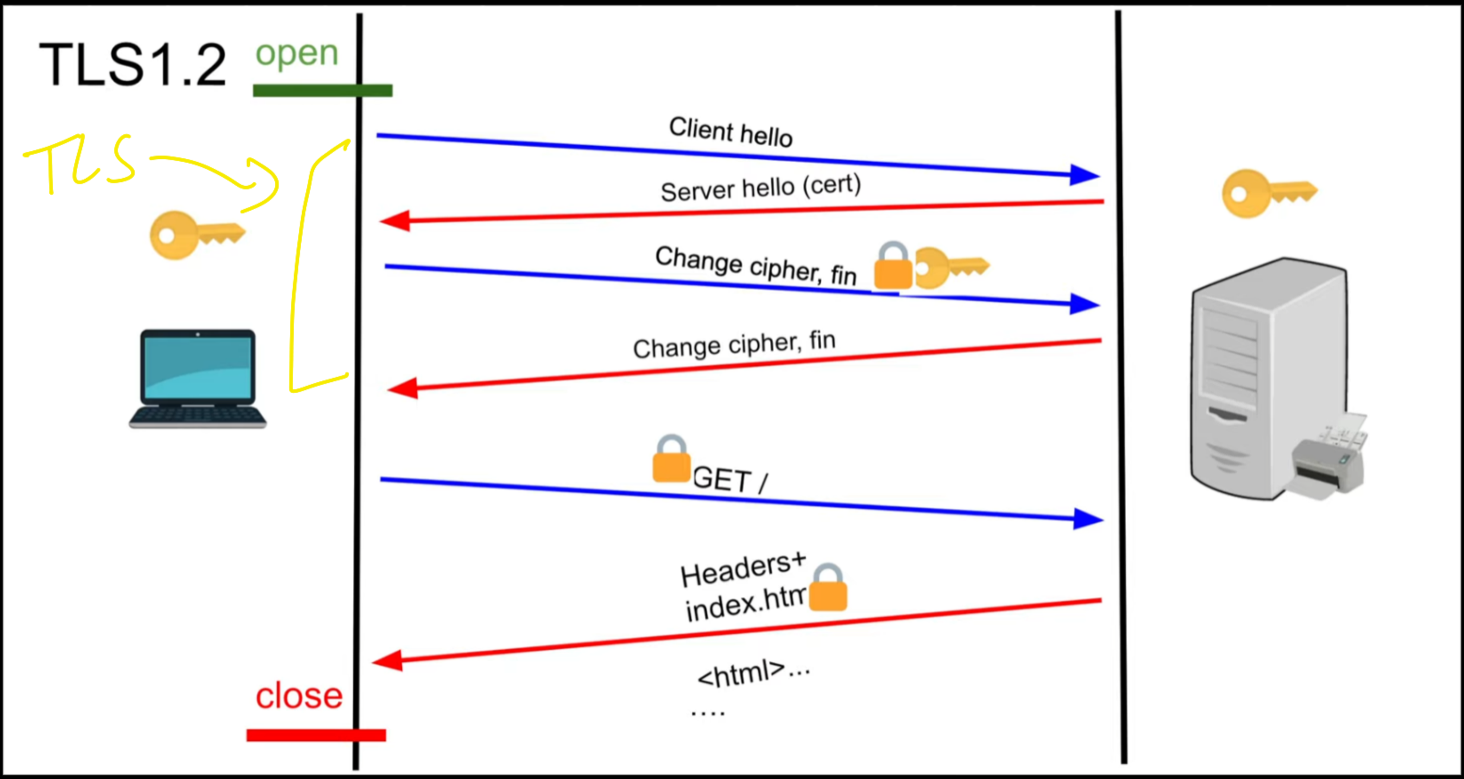
⇓

Replaced by TLS (Transport layer security)

TLS 1.2 TLS 1.3

* HTTPS is slower than HTTP because of overhead of TLS

⇓



TLS1.2

open

TLS

Client hello

Server hello (cert)

Change cipher, fin

Change cipher, fin

GET /

Headers+
index.htm

<html>...
....

close

* Algorithm that are used by TLS

AES RSA Deffi-hellman

Hashing Function → SHA256