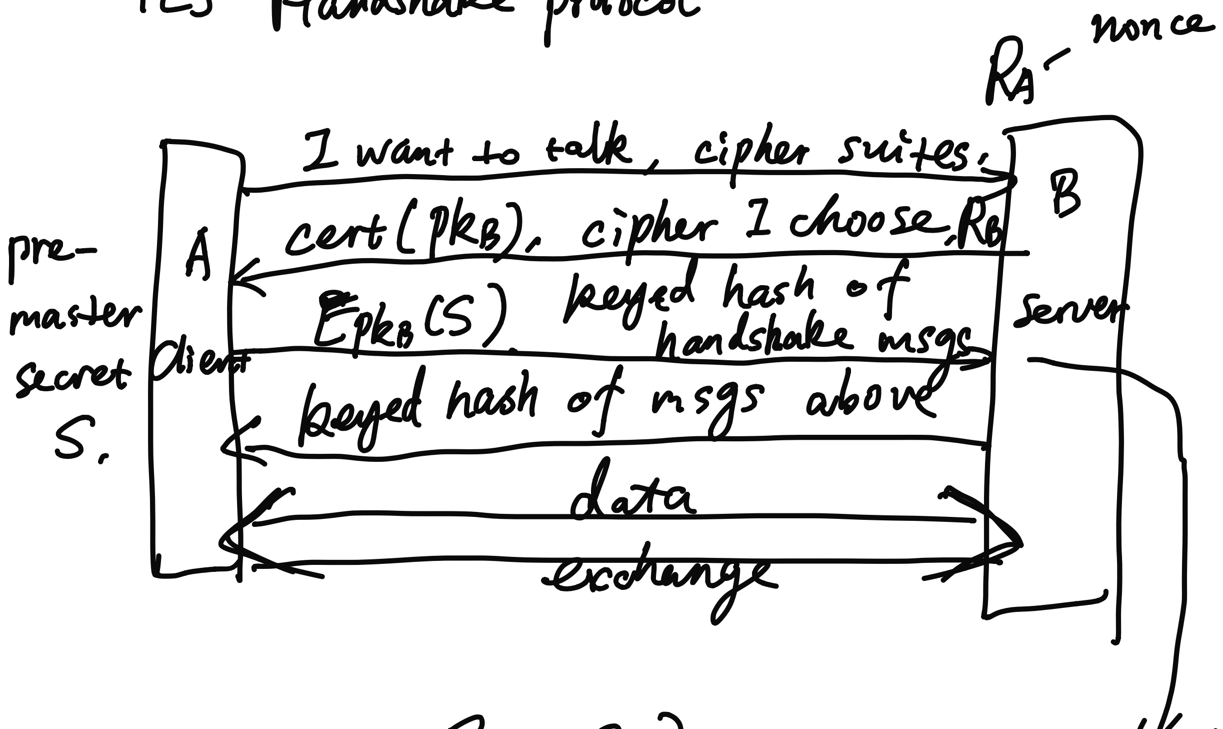
ECE 471/571 SSL / TLS

TLS Handshake protocol



R_A - nonce
I want to talk, cipher suites.
B
cert(pk_B), cipher I choose, R_B
pre-master secret S.
A
Client
$E_{pk_B}(S)$ keyed hash of handshake msgs
Server
keyed hash of msgs above
data exchange

$K = f(\underline{S}, \underline{R_A, R_B})$ $\underline{\underline{H(K, \text{handshake msg})}}$

(master key)

↳ compute 6 session keys

$$\left\{ \begin{array}{ll} \text{Encryption key} & . \times 2 \\ \text{Integrity protection} & . \\ \underline{\text{IV}} & . \end{array} \right.$$

prevent reflection attack.

$K' = f(K \| R_A \| R_B \| C_1)$

$$K'' = f(K \| R_A \| R_B \| C_2)$$

Session: e.g. opening a webpage

Connection: e.g. TCP connection for fetching data from a webpage

(short-lived).