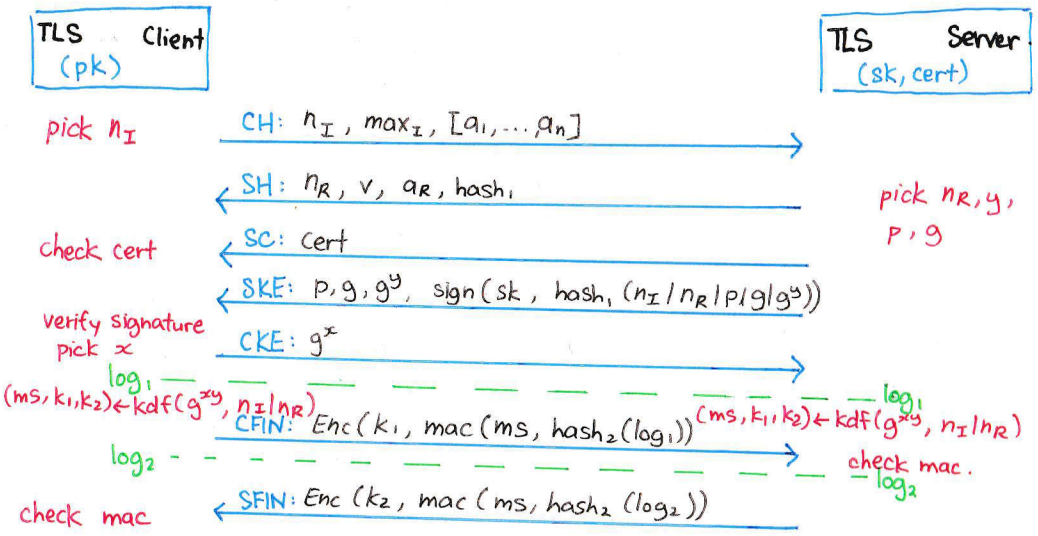
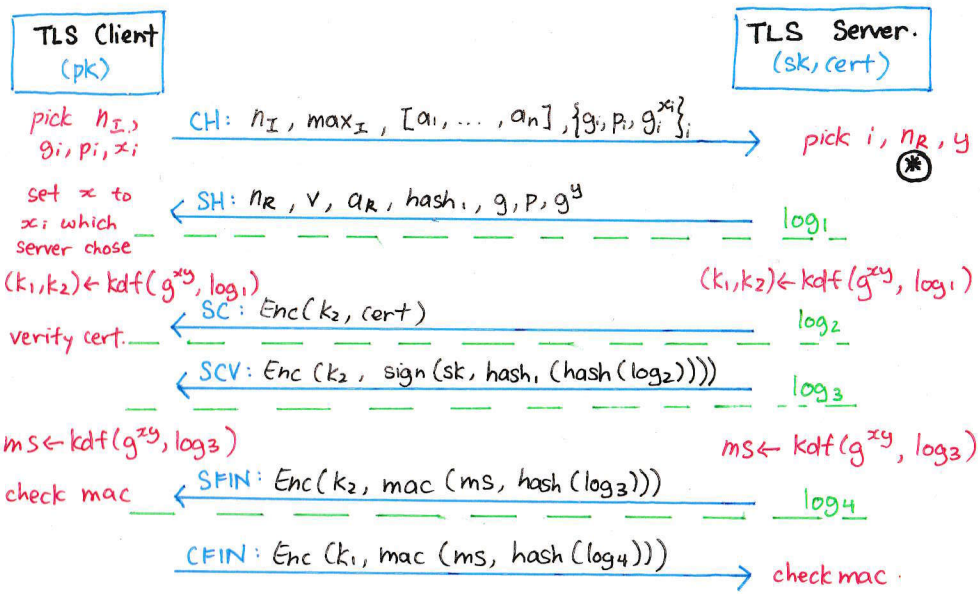
① TLS 1.0 - 1.2



Legend:

- n_I / n_R – Initiator (Client) / Receiver (Server) nonce.
- max_I – maximal TLS version supported by client.
- v – version number of protocol.
- pk/sk/cert – public / private signing keys, and certificate of server.
- $hash_1$ – hash function chosen by server.
- a_R / a_i – a tuple (mac, $hash_2$, kdf, enc, sign) defining algorithms that will be used/ can be used.
- p/g – modulus / generator of DH group that will be used.

② TLS 1.3



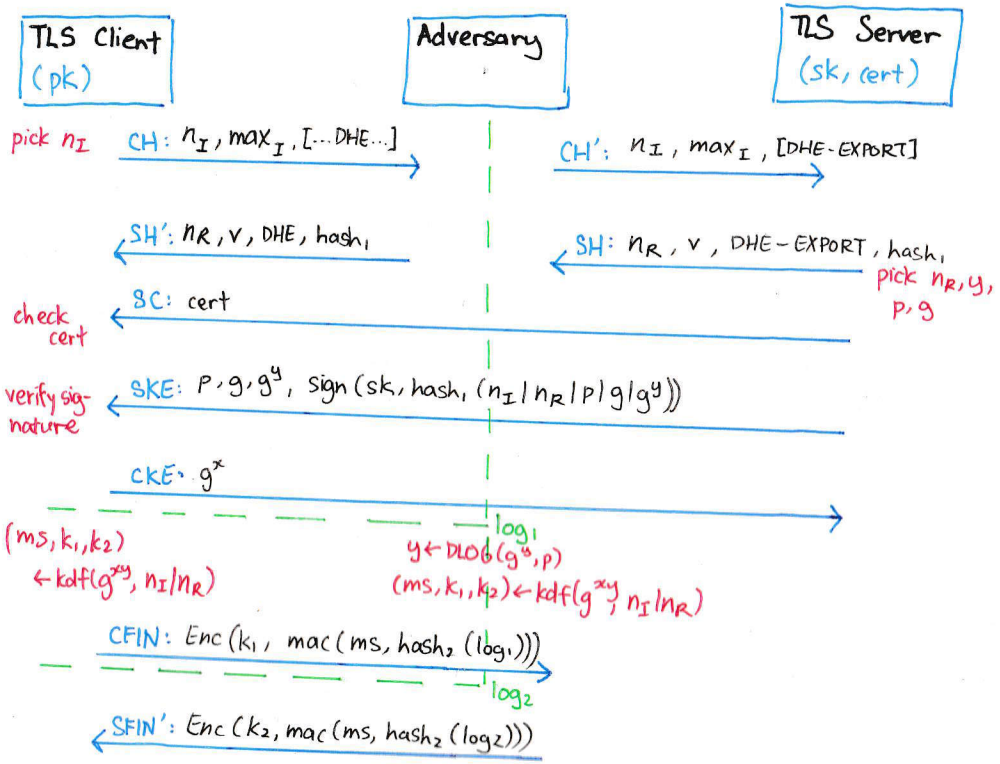
≈ "nonce hack"

pick n_R, then set $n_R \leftarrow v | n_R$.

Note:

The client follows protocol ① if v = 1.2, and ② if v = 1.3

③ LOGJAM (in TLS 1.2).



④ LOGJAM (in TLS 1.3)