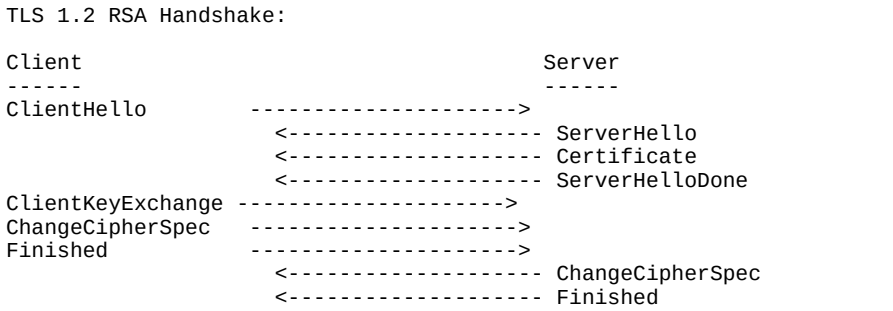
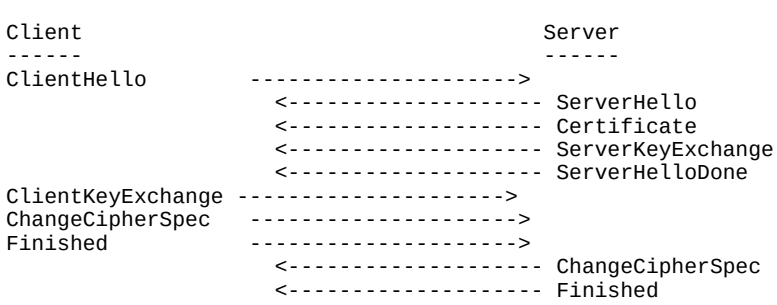
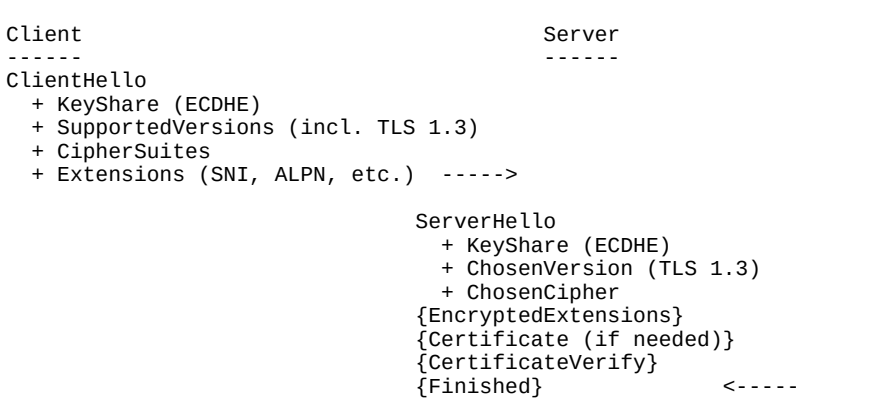
TLS Handshake Diagrams







Comparison: TLS 1.2 vs TLS 1.3

TLS 1.2 (RSA/ECDHE)	TLS 1.3 (ECDHE)
- Separate ClientKeyExchange	- ClientHello includes KeyShare
- Separate ServerKeyExchange	- ServerHello includes KeyShare
- ChangeCipherSpec messages	- No ChangeCipherSpec
- Handshake messages in cleartext	- Encrypted after ServerHello
- More roundtrips (2-RTT)	- Faster (1-RTT, 0-RTT possible)