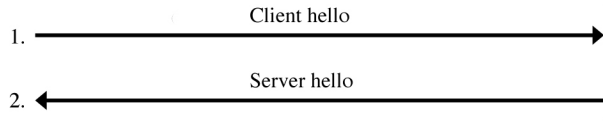


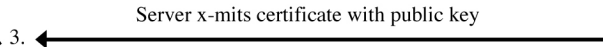
# SSL Handshake

CLIENT

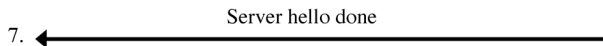
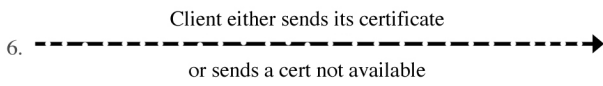
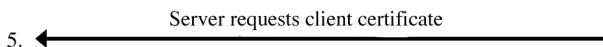
SERVER



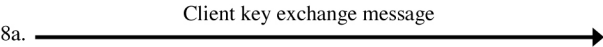
Establish connection and exchange operations parameters



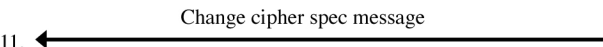
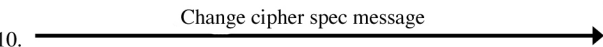
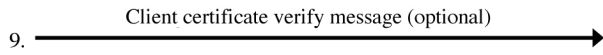
4. Client authenticates certificate with trusted authority



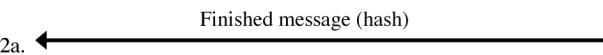
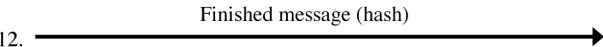
8. Client generates 48 bit premaster secret and encrypts it with server's public key



8b. Both client and server use premaster secret to generate symmetrical session key



Agreement on symmetrical and session key



Hashes of conversation up to this point calculated by server/client if equal

→ "SYMMETRICAL CRYPTOGRAPHY MODE" ←