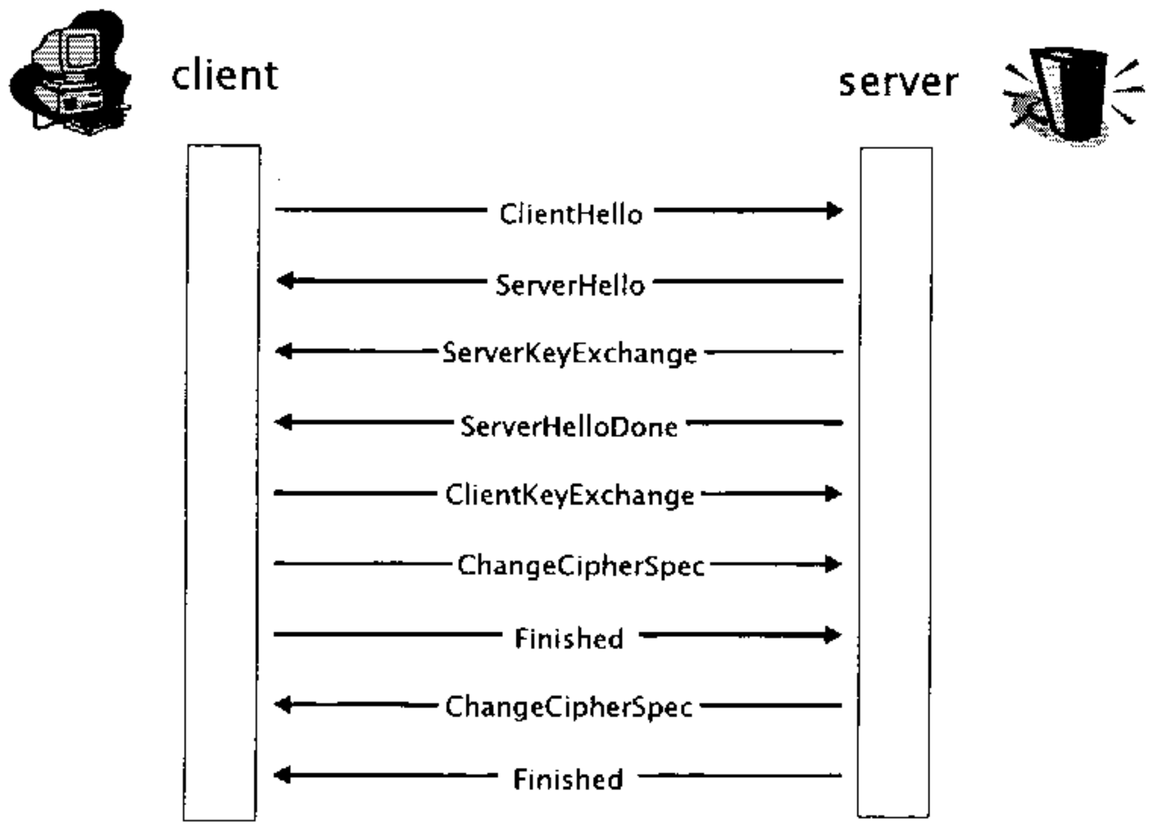
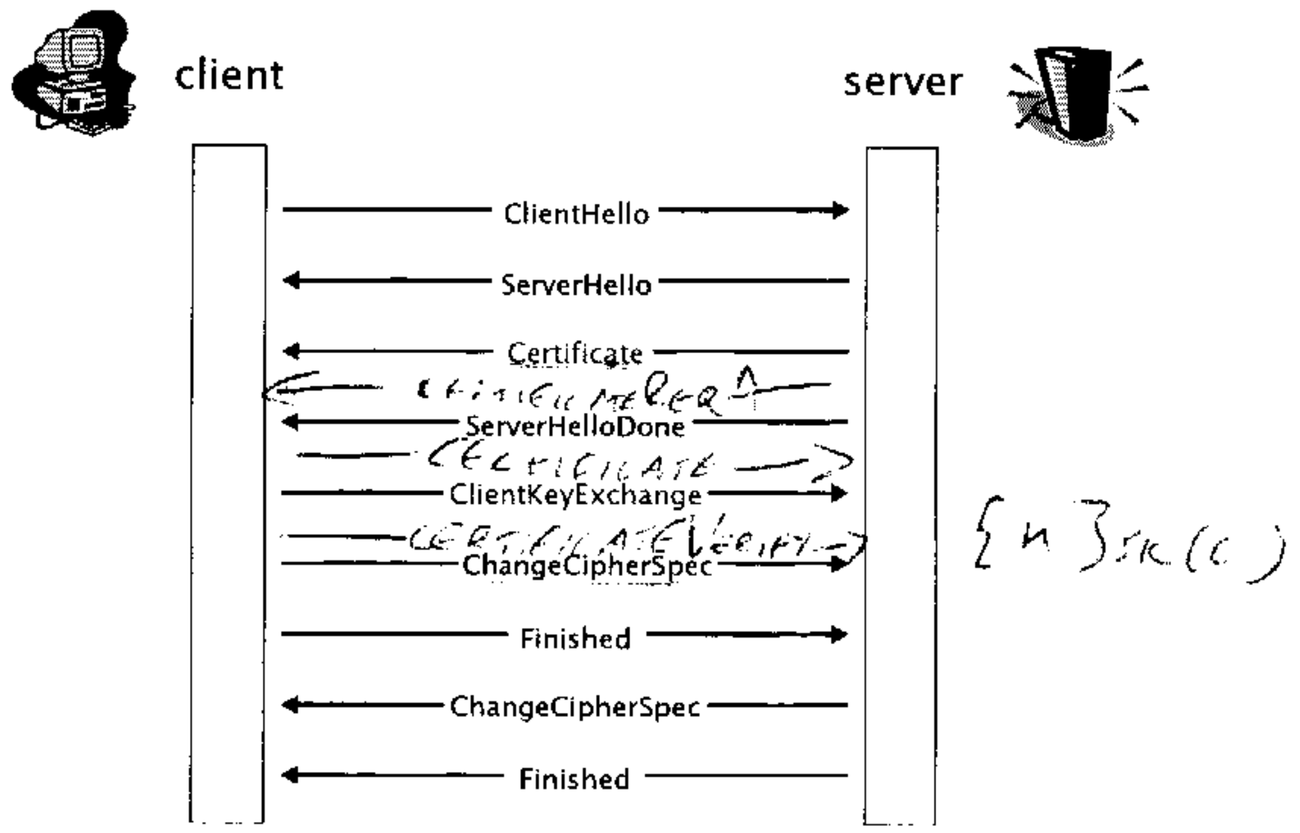
SSLMessage Exchange



Utility is limited by the lack of authenticated identities of the insider of the key. This problem is addressed, right?

Some Message Types

- *ClientHello* version, random number, session ID, supported cipher suites, compression methods
- *ServerHello* similar
- *ServerKeyExchange* server's public key
- *ClientKeyExchange* session key chosen by client, encrypted with server's public key
- *Finished* is encrypted with the session key and authenticated, and contains a hash of the preceding discussion — for final cross-checking



Some More Message Types

- *Certificate* server's X509 certificate; client is able to verify the certificate, and from it learns server's public key
- *ClientKeyExchange* session key chosen by client, encrypted with server's public key from certificate

ChangeCipherSpec: Stop public encryption, begin encryption with session key