

M4:

A: ChangeCipherSpec:

B: Finished

NONE
MD5(M1 M2 M3A M3C)
SHA(M1 M2 M3A M3C)