

M3: A: ClientKeyExchange:

RSA_Encrypt(
ServerPublicKey, PreMasterSecret)

B: ChangeCipherSpec:

NONE

C: Finished

MD5(M1 || M2 || M3A)

SHA(M1 || M2 || M3A)