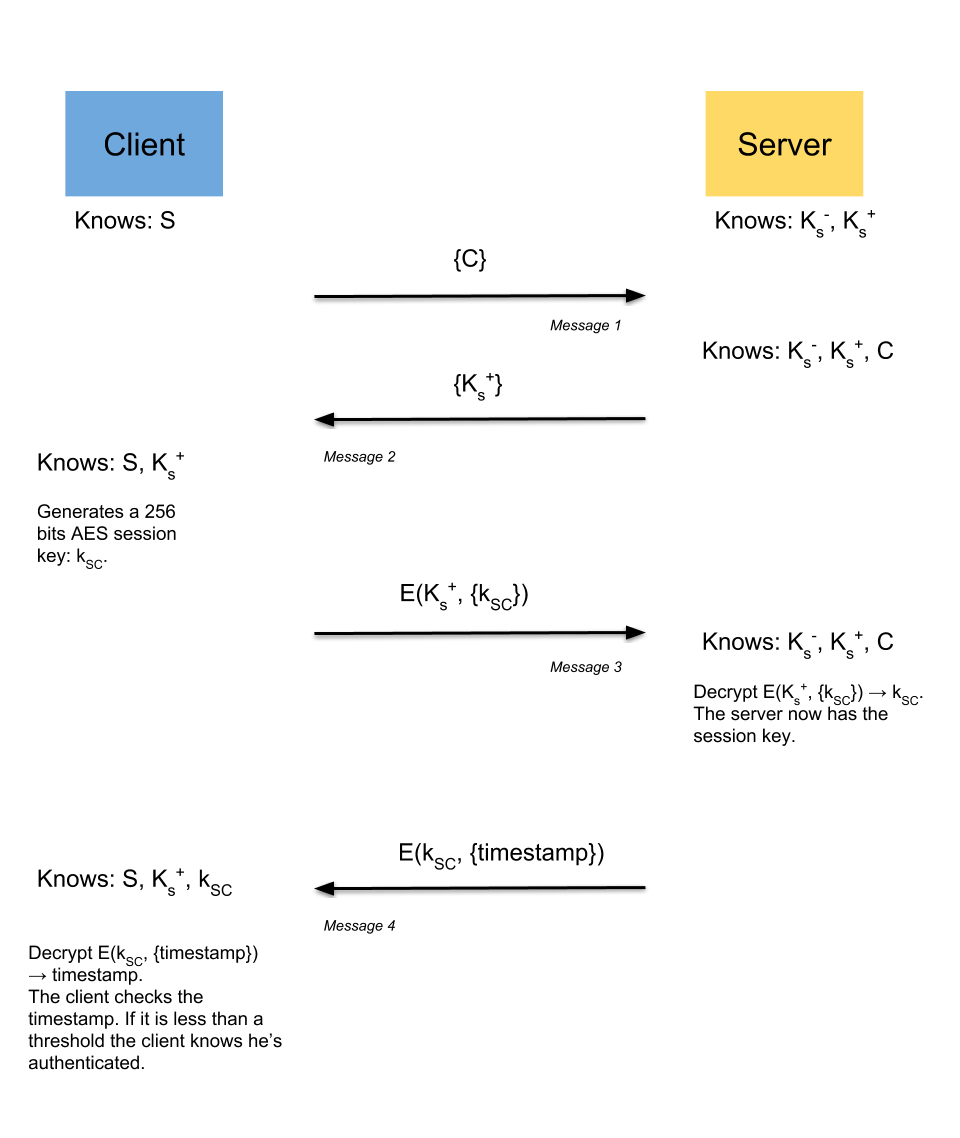
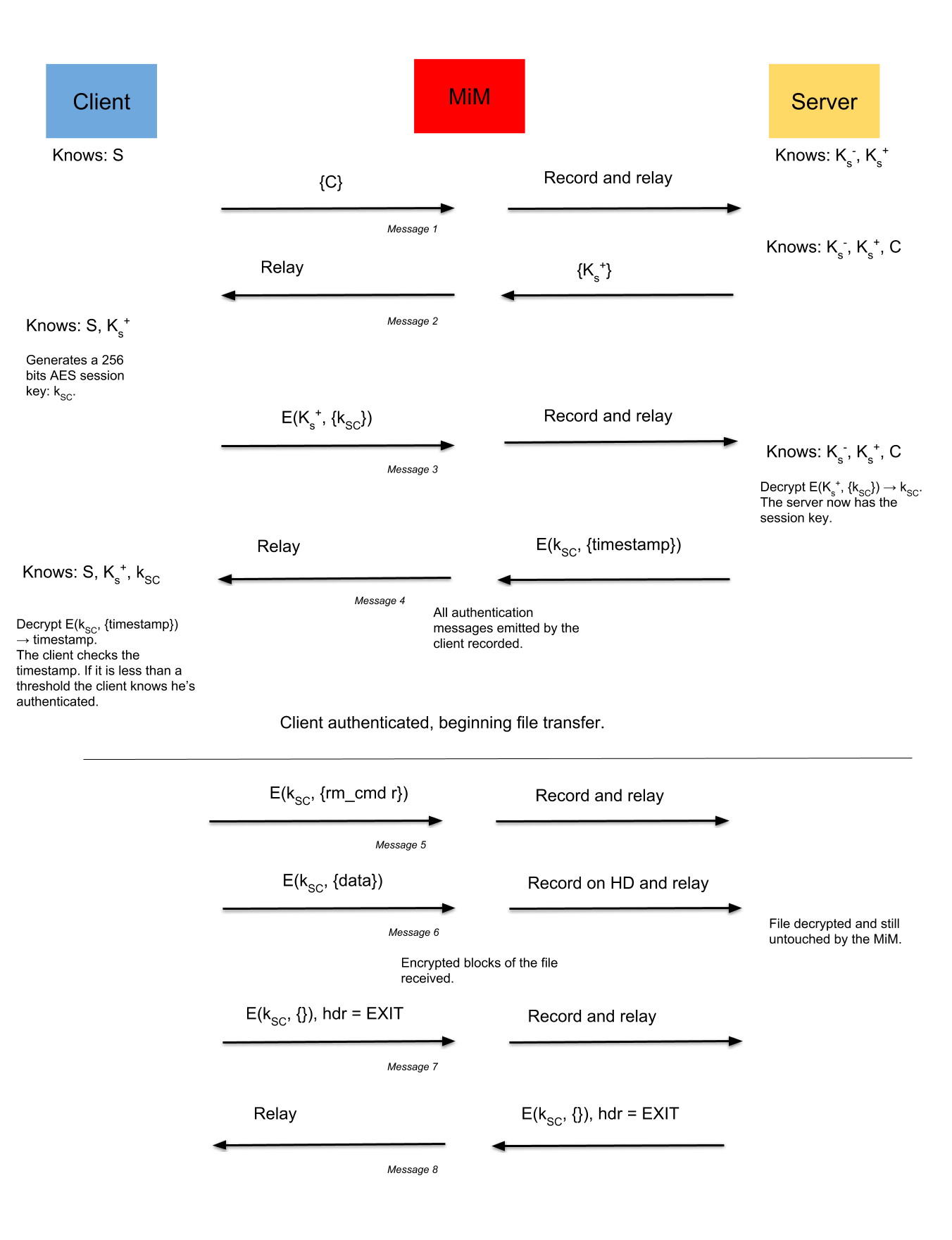
# SSH Protocol – Initial version

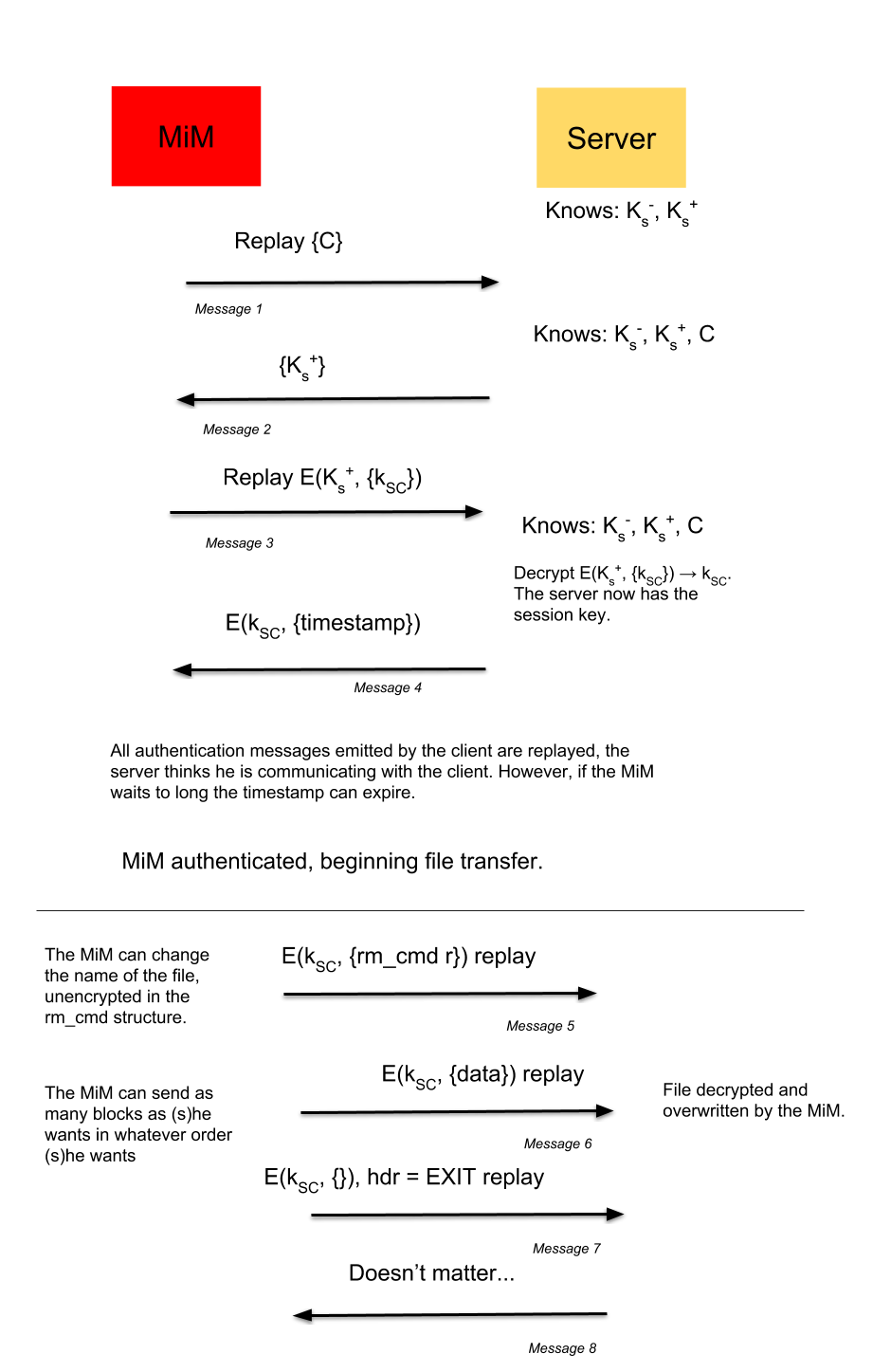


For message number four, the paper doesn’t specify the kind of confirmation the server should send. I chose to send a timestamp, I also hesitated to send the session key encrypted with the session key… The timestamp sounded like a better option.

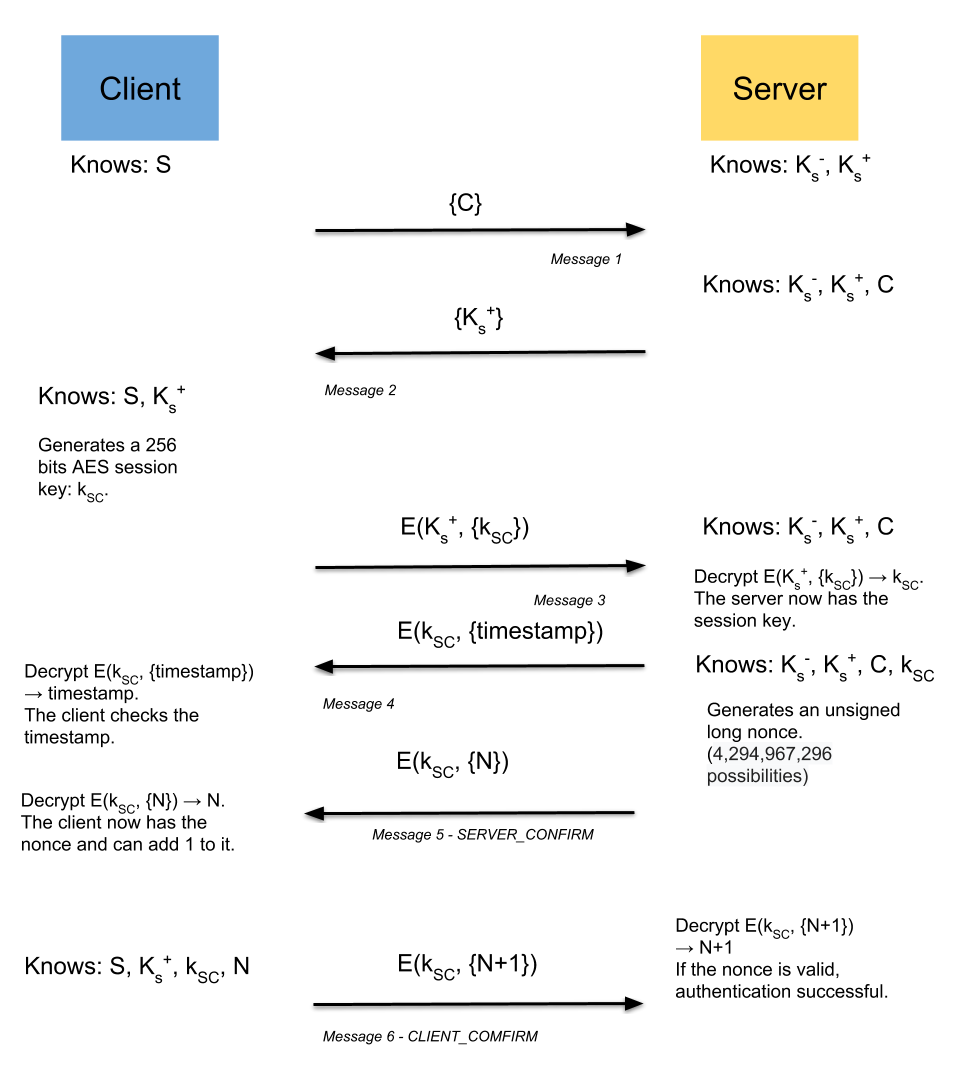
# MiM Record and replay – Recording phase



# MiM Record and replay – Replay phase



# SSH Protocol – Replay resistant version



This version counters the replay authentication because of the nonce. An adversary won’t be able to replay message 6 because the nonce N is unique.

However, this doesn’t solve the integrity issues. An adversary forwarding (not replaying) all the messages during the authentication can still modify the file sent by the client. The adversary records the file sent by the client, modifies the order of the blocks or the number of blocks sent and sent it to the server. The server doesn’t check for the integrity. There should be a global file HMAC in addition of the tag check during the decryption.