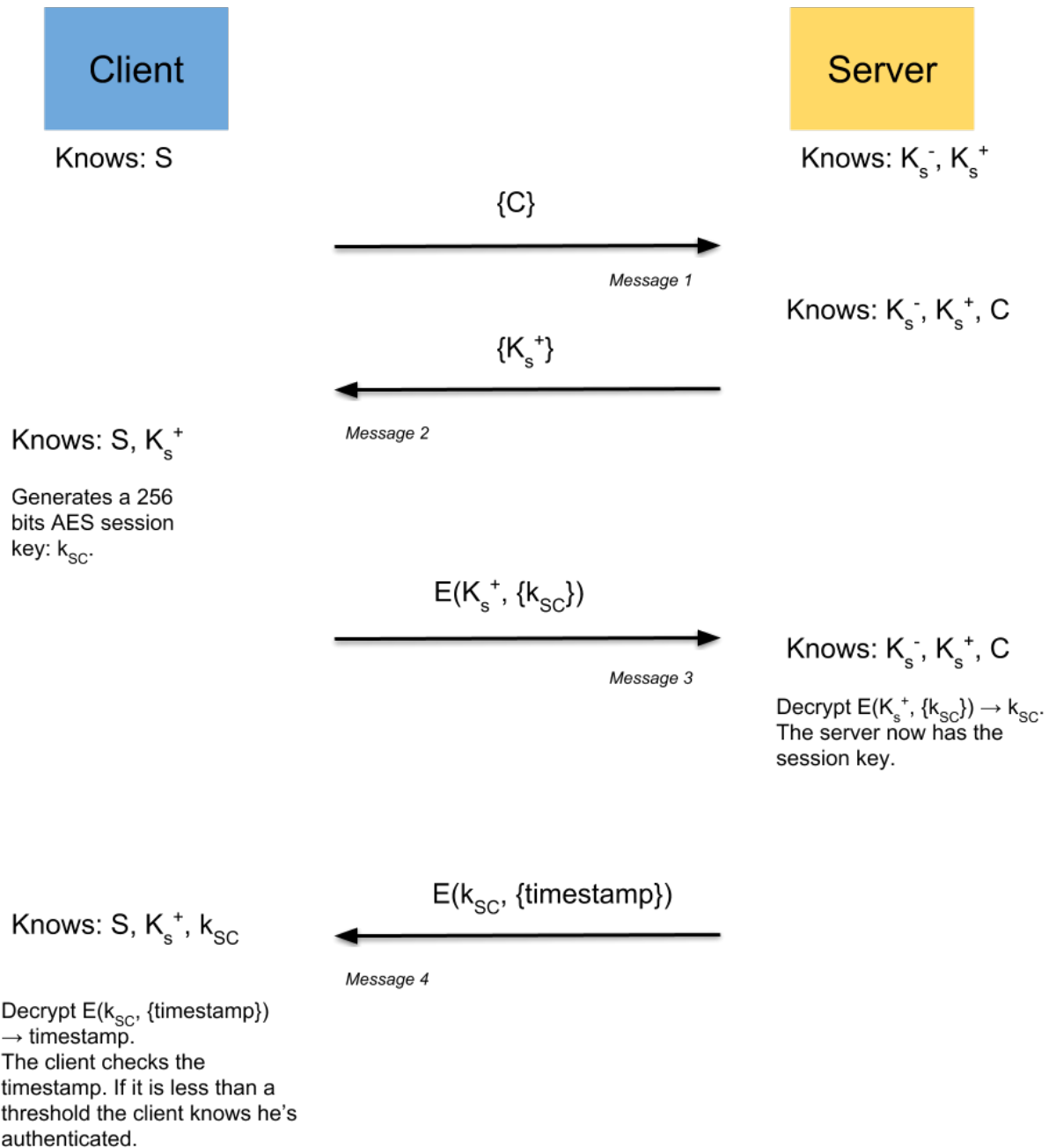


SSH Protocol (Implemented Version)



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.