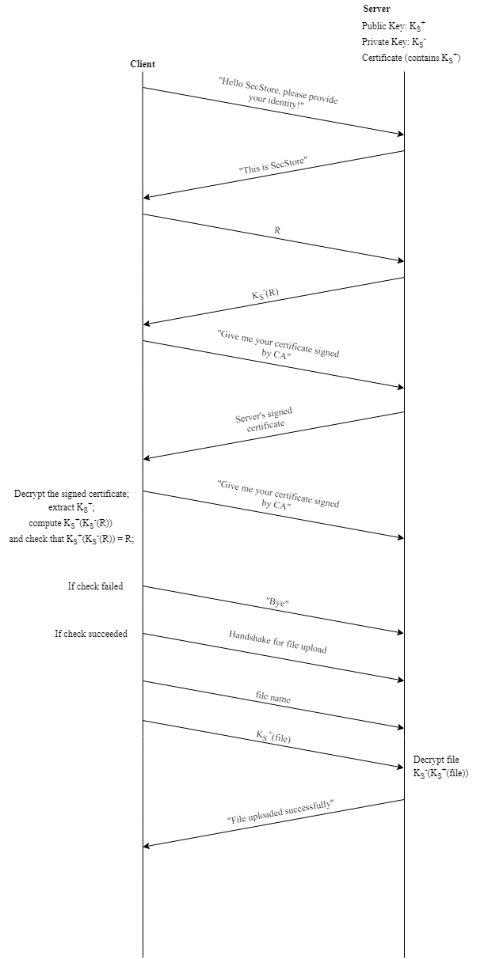
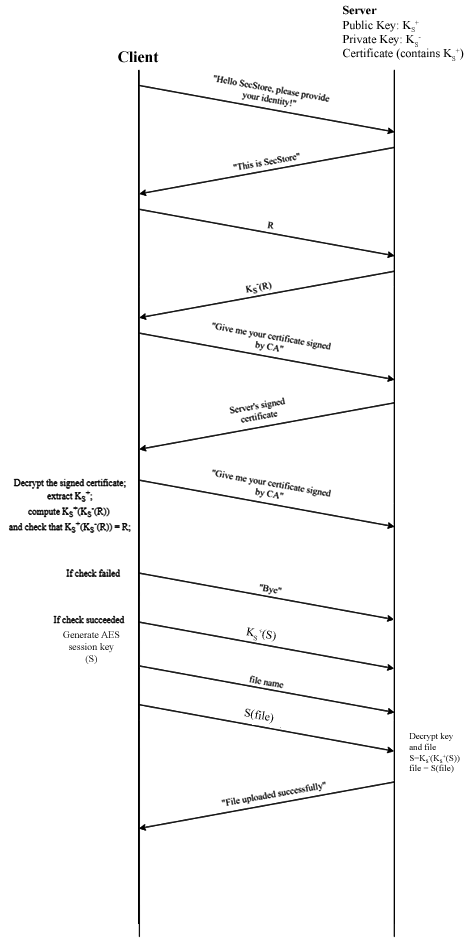
**PA2 Submission Report**

By Rahul Parthasarathy 1003718 and Sidharth Praveenkumar 1003647

**1)However, there’s one problem with the. What is the problem? Explain it in your handout for submission, and give a fix for the problem.**

Answer: The original AP Protocol given is highly vulnerable to a replay attack, such that any intermediate can access the encrypted message and spook the identity of the server by sending it to the client. To avoid this problem, we need to use a nonce that is generated at the time o running and then the server must return thus encrypted with it’s private key. Since this nonce was generated only at runtime, the client can guarantee the authenticity of the server.

**Specification Diagram (CP1 and CP2 respectively)**

****

**Throughput table and Plot**

