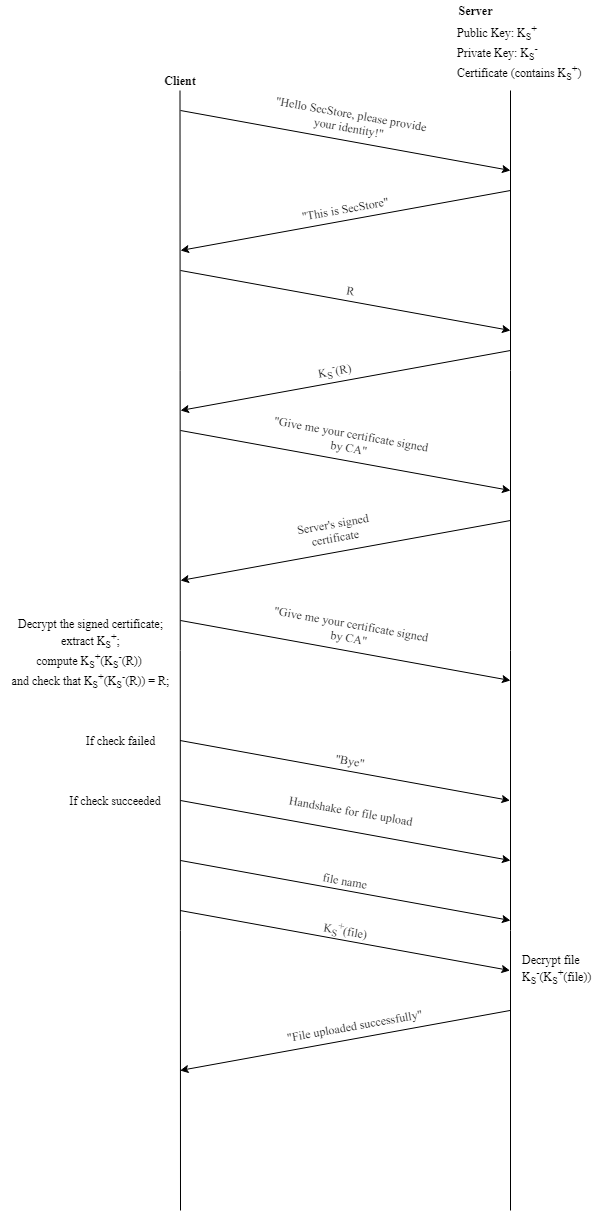
**CSE 50.005 (Spring 2018) Programming Assignment 2:**

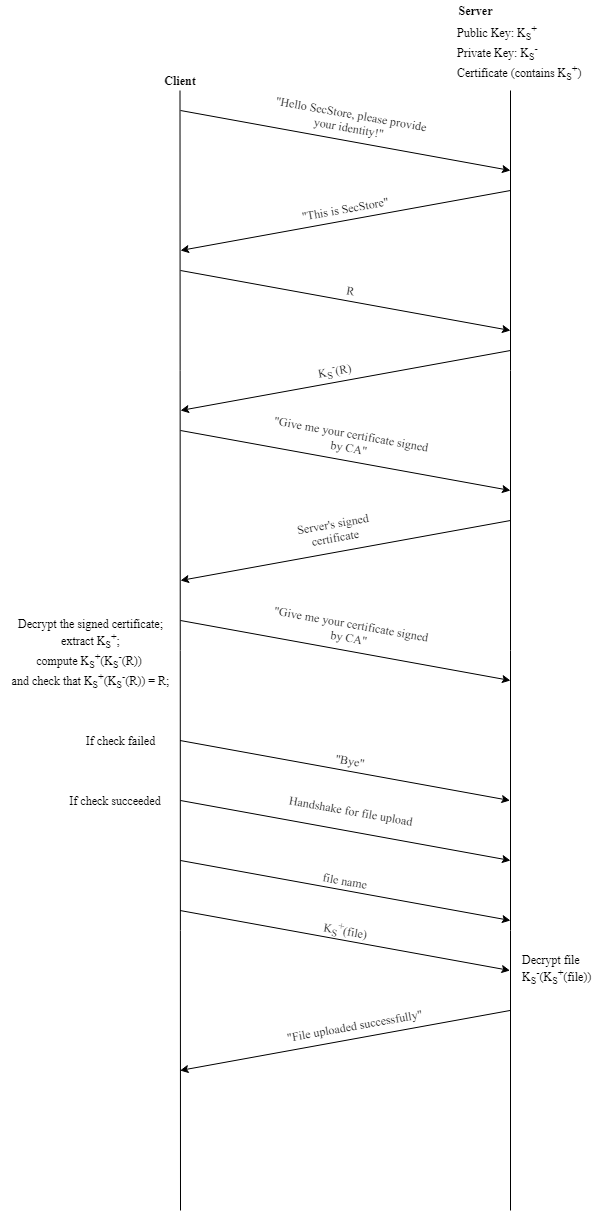
**Secure File Transfer**

1. **Authentication Fix**

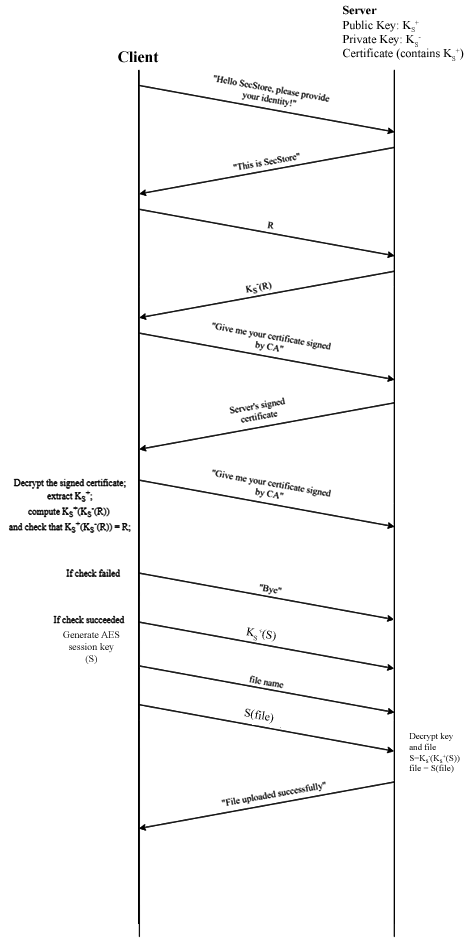
In the original AP protocol given, replay attack could occur if an adversary intercepts encrypted message M and retransmits it to the client, thereby fooling the client into believing that he is transferring the file to the actual server. To avoid replay attack, the client sends a freshly generated nonce, R, to the server, and server must return the nonce, encrypted with its private key. Since the nonce is fresh, the server’s response to it must be fresh as only the server knows how to generate response, the client can guarantee that the server is the live server and not an adversary.

1. **Protocol Specifications**

**2.1** **AP Specifications**

**2.2 CP-1 Specifications**

**2.3 CP-2 Specifications**

****

1. **Data Throughput**

**3.1 Data Throughput Plot**

**3.2 Data Throughput Table CP-1**

|  |  |  |  |
| --- | --- | --- | --- |
| **File Name** | **File Size (KB)** | **Time Taken (ms)** | **Throughput (Mbps)** |
| test3.txt | 39 | 611.83 | 0.063743197 |
| img.png | 135 | 1790.25 | 0.075408463 |
| rr.txt | 1981 | 19444.25 | 0.101881019 |
| audio.mp3 | 4216 | 37649.84 | 0.111979228 |

**3.4 Data Throughput Table CP-2**

|  |  |  |  |
| --- | --- | --- | --- |
| **File Name** | **File Size (KB)** | **Time Taken (ms)** | **Throughput (Mbps)** |
| test3.txt | 39 | 84.66 | 0.46066619 |
| img.png | 135 | 180.69 | 0.74713598 |
| rr.txt | 1981 | 622.48 | 3.18243156 |
| audio.mp3 | 4216 | 787.04 | 5.35677983 |

**Comments**

CP1 is slower as it uses RSA to encrypt the entire file, while CP2 uses AES to generate a session key such that the time taken is reduced. RSA is very computationally expensive by comparison with AES. It involves mathematics with very large numbers, whilst AES can be implemented with relatively simple bit operations. This can be seen in the plot.