50.005 – Programming Assignment 2

Secure File Transfer

Team Members:  
Ashlyn Goh Er Xuan 1002840 Cl02  
Wong Chi Seng 1002853 Cl02

# Instructions to Run

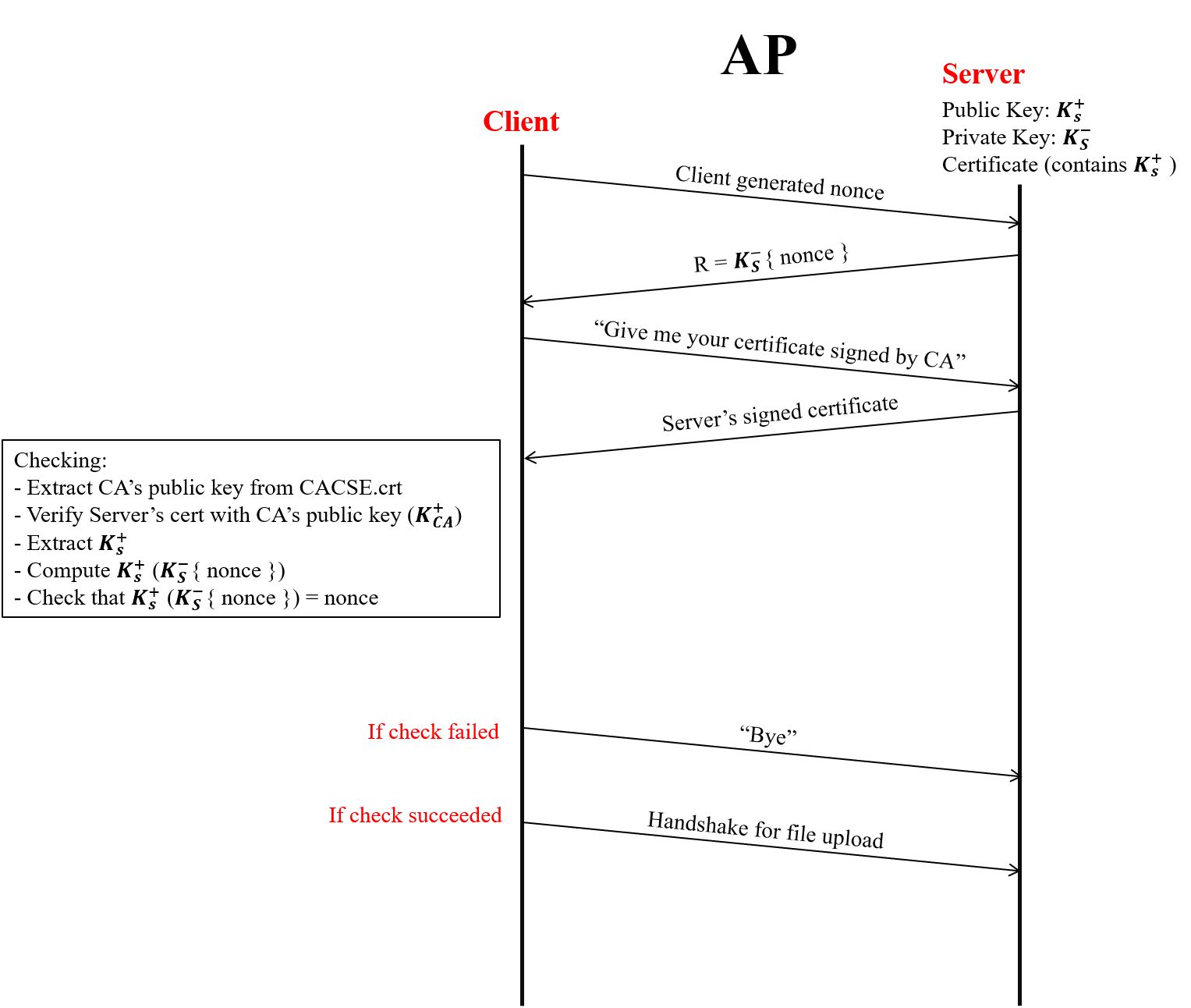
# Problem with Original Protocol

The problem with the original protocol is that it does not prevent a playback attack. Hence, an attacker can maliciously repeat a valid data transmission. In our case, the attacker can store information without authorisation and then retransmit it back to the client to trick the client into transferring the file.

To prevent the playback attack, we introduced a nonce into our protocol. The client generates a nonce and sends it to the server. On the other hand, the server must return the nonce that is encrypted with its private key back to the client. Thereafter, the client would check if the decrypted nonce (with server’s public key) matches the original nonce sent. More details are included in the specification diagram in the next section.

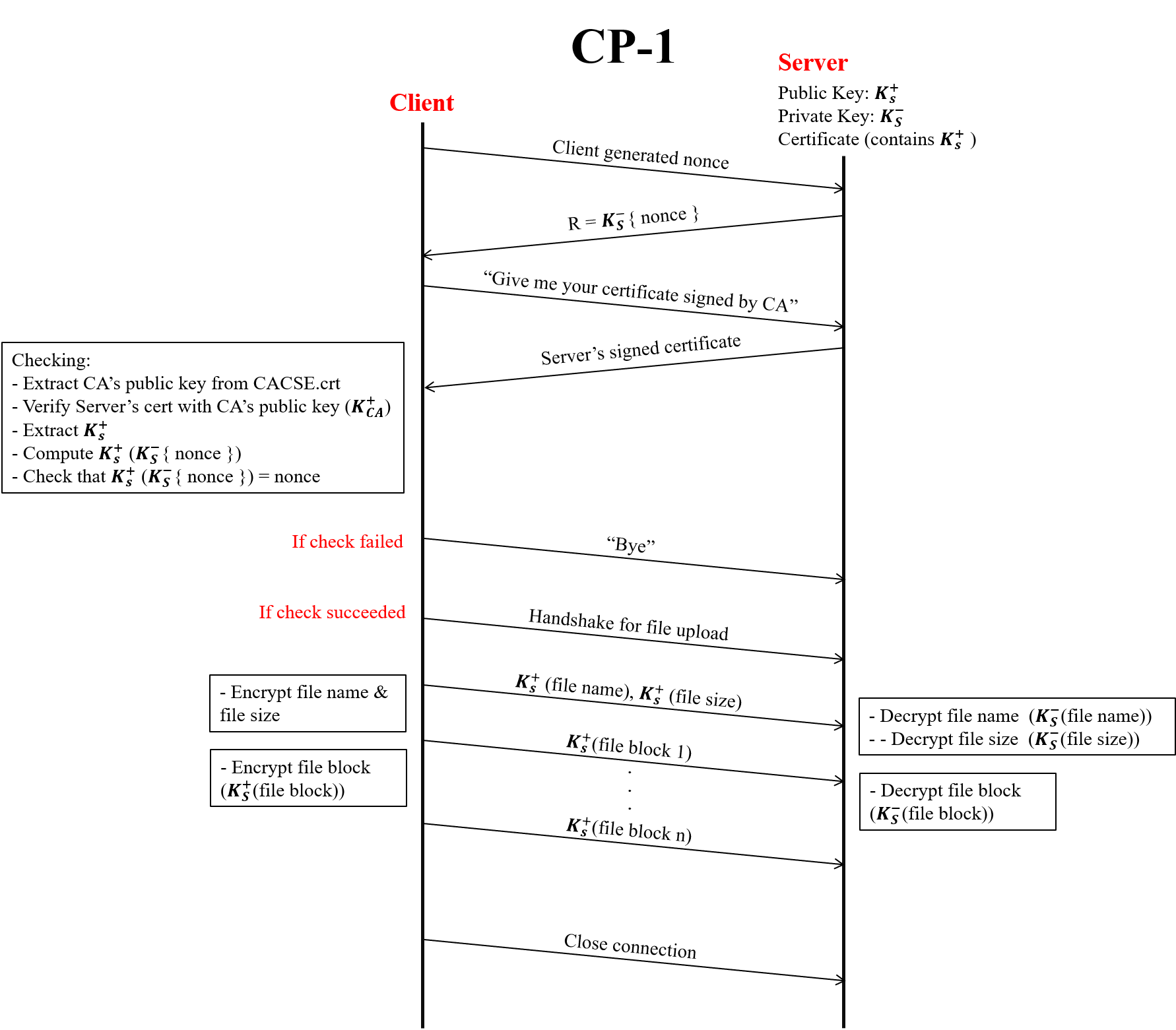
# Protocol Specifications

## AP Protocol



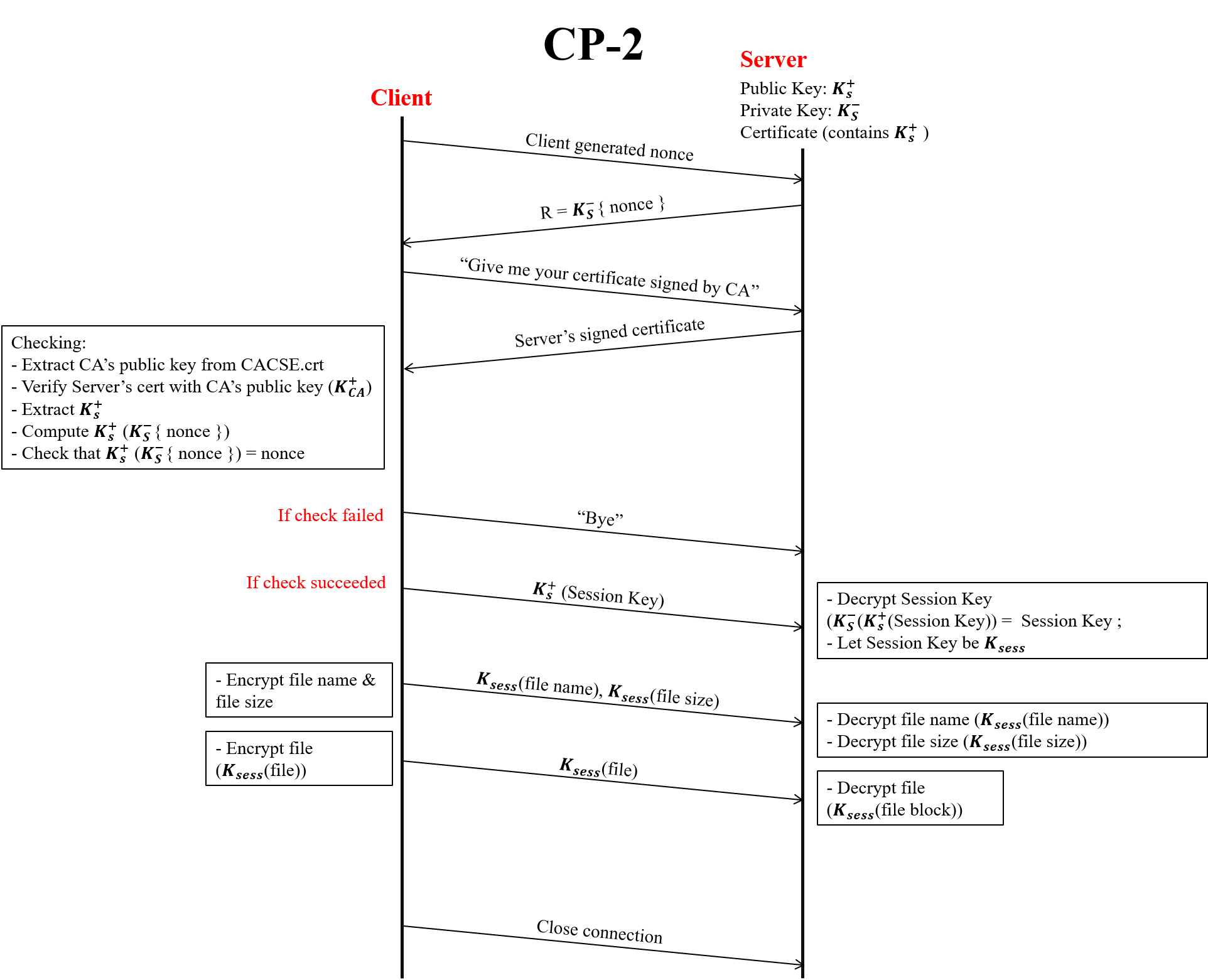
*Figure 1: Authentication Protocol Specification*

## CP-1 Protocol



*Figure 2: CP-1 Specification*

## CP-2 Protocol



*Figure 3: CP-2 Specification*

# Results

**Graphs**:

CP1:

|  |  |  |
| --- | --- | --- |
| **File size** | **Time Taken** | **Throughput** |
| 33kb |  |  |
| 66kb |  |  |
| 123kb |  |  |
| 232kb |  |  |
| 400kb |  |  |
| 1484kb |  |  |

CP2:

|  |  |  |
| --- | --- | --- |
| **File size** | **Time Taken** | **Throughput** |
| 33kb |  |  |
| 66kb |  |  |
| 123kb |  |  |
| 232kb |  |  |
| 400kb |  |  |
| 1484kb |  |  |

# Conclusion

For the confidentiality protocol (CP) 1, each file is being cut into blocks and encrypted separately with RSA encryption as compared to CP 2, where the whole file is being encrypted with AES encryption and sent over. The time taken to encrypt every block and subsequently decrypt it back into the file would contribute heavily to the difference in timings between the two protocols. From the graphs and the recordings, the timings and throughput seem to increase as the file size sent increases. We can also infer that the predicted behaviour is indeed true as the two protocols differ greatly in transfer timings and throughput for similar files.