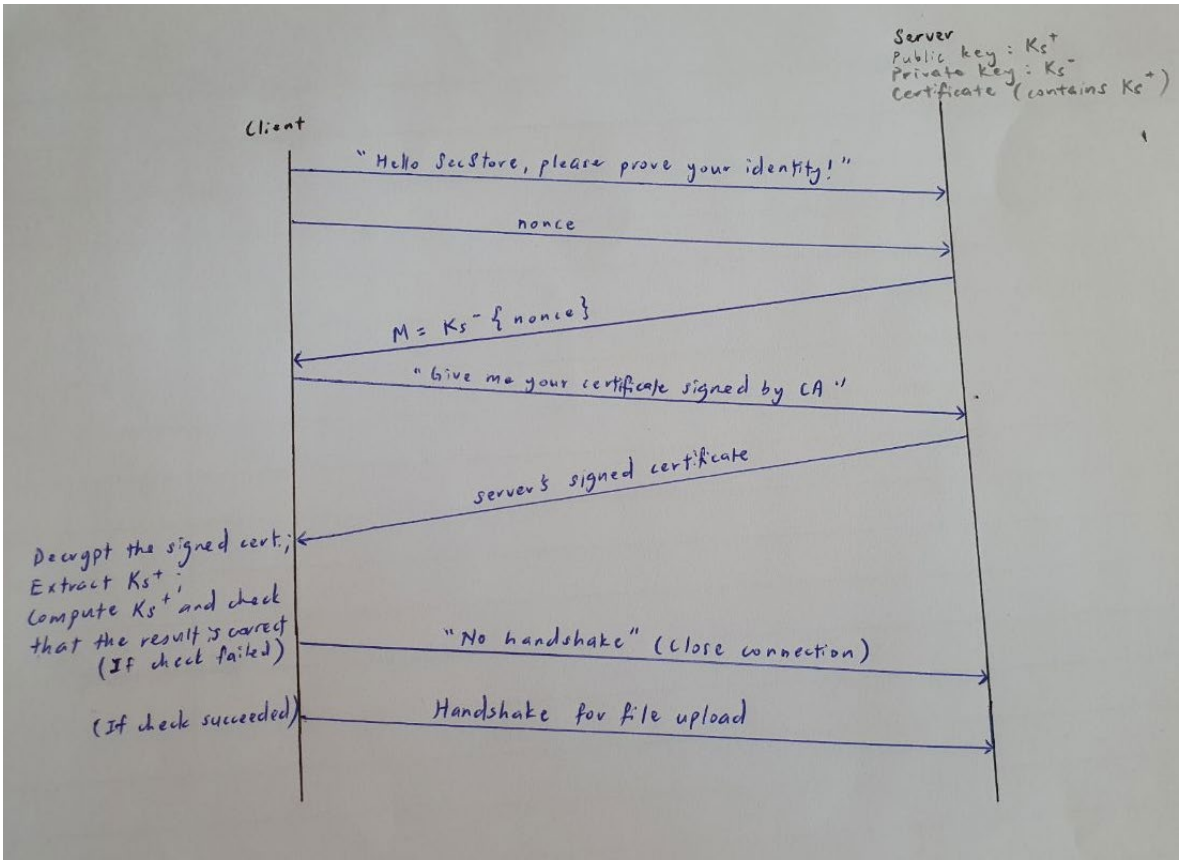
Names: Kwa Li Ying (1003833), Cheow Pak Leng Josiah (1003602)
Class: CI03

CSE Programming Assignment 2 Report

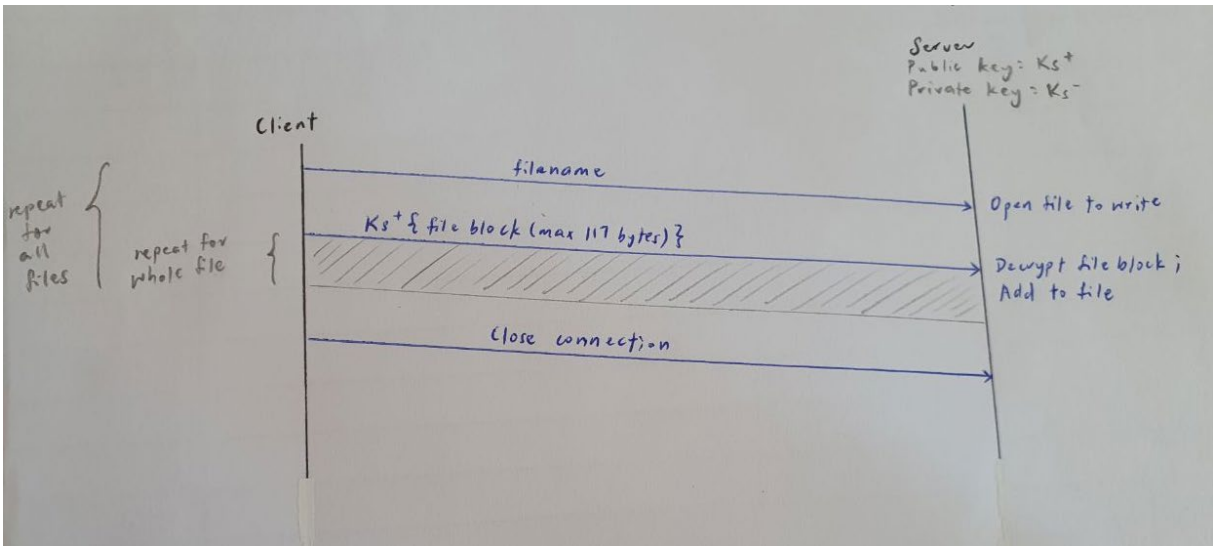
Specifications for the Protocols

AP

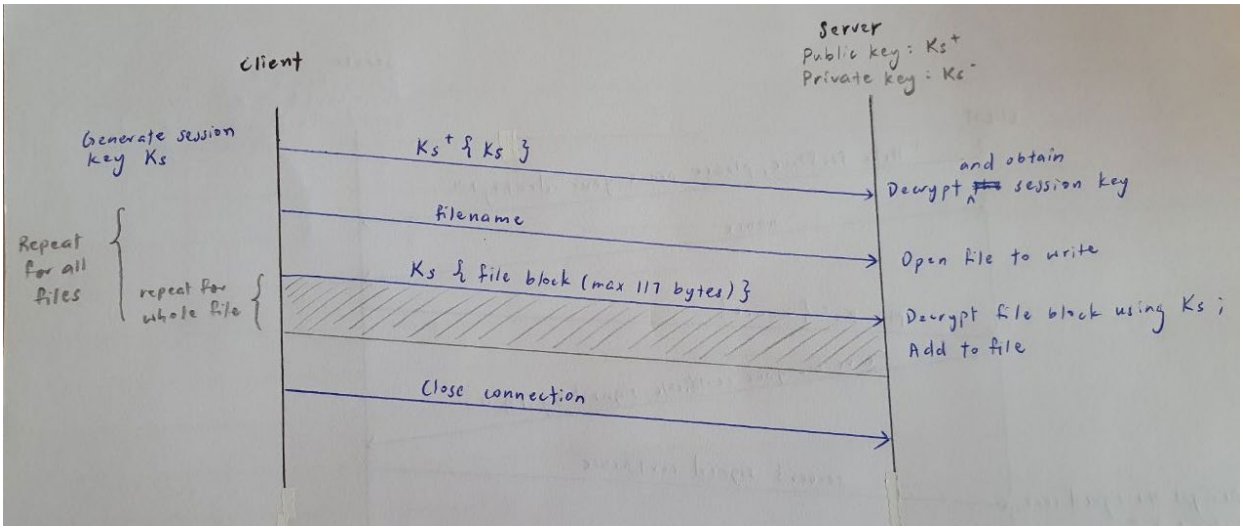


Names: Kwa Li Ying (1003833), Cheow Pak Leng Josiah (1003602)
Class: CI03

CP1



CP2



Names: Kwa Li Ying (1003833), Cheow Pak Leng Josiah (1003602)
Class: CI03

Answers to Questions

Fig. 1 below gives the basis of a possible protocol. 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.

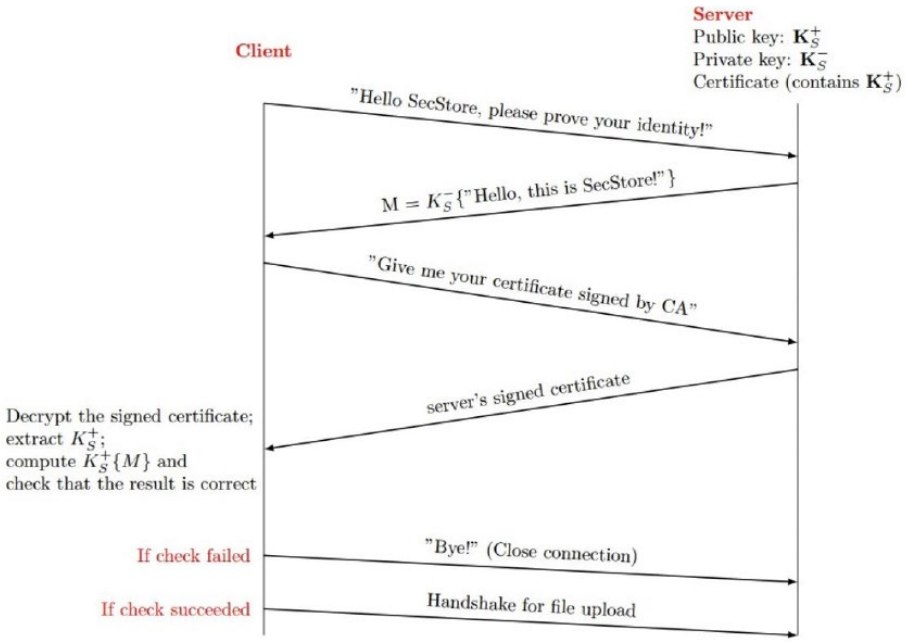


Fig. 1: Basis of Authentication Protocol

In Fig. 1, the encrypted message M is the encryption of "Hello, this is SecStore!" using the server's public key. It is not an encryption of the nonce ("Hello, SecStore, please prove your identity!") that the client sent to the server.

When the client later decrypts M, it has no basis of comparison as the plaintext is not the same as the original nonce. While the message is clearly in response to the client's nonce as illustrated in English in Fig. 1, this would not be the case when messages are in the form of byte arrays in the code. Therefore, it is essential that the message used by the server for encryption to produce M should be the exact same nonce that the client initially sends the server.

Also, the original message (nonce) should be a randomly generated byte array for one-time use only. This is so that any malicious user would not be able to impersonate the client by sending the client's default message (or any previous message) to B. The one-time-use nonce prevents the playback attack from happening.

Names: Kwa Li Ying (1003833), Cheow Pak Leng Josiah (1003602)
Class: CI03

Plots of Achieved Data Throughput against a Range of File Sizes

File Name	File Size (KB)	Time taken for CP1 (ms)	Time taken for CP2 (ms)
100.txt	4.49	1207.6072	1155.4009
200.txt	8.98	1246.5232	1149.8207
500.txt	22.4	1523.9174	1191.338
1000.txt	44.9	1489.082	1342.0158
5000.txt	224	2088.0655	1875.952
10000.txt	449	2847.3517	2542.8919
50000.txt	219000	5790.6511	4999.6383
100000.txt	438000	16885.0158	8278.6066