Programming Assignment 2

Tee Zhi Yao | 1002845

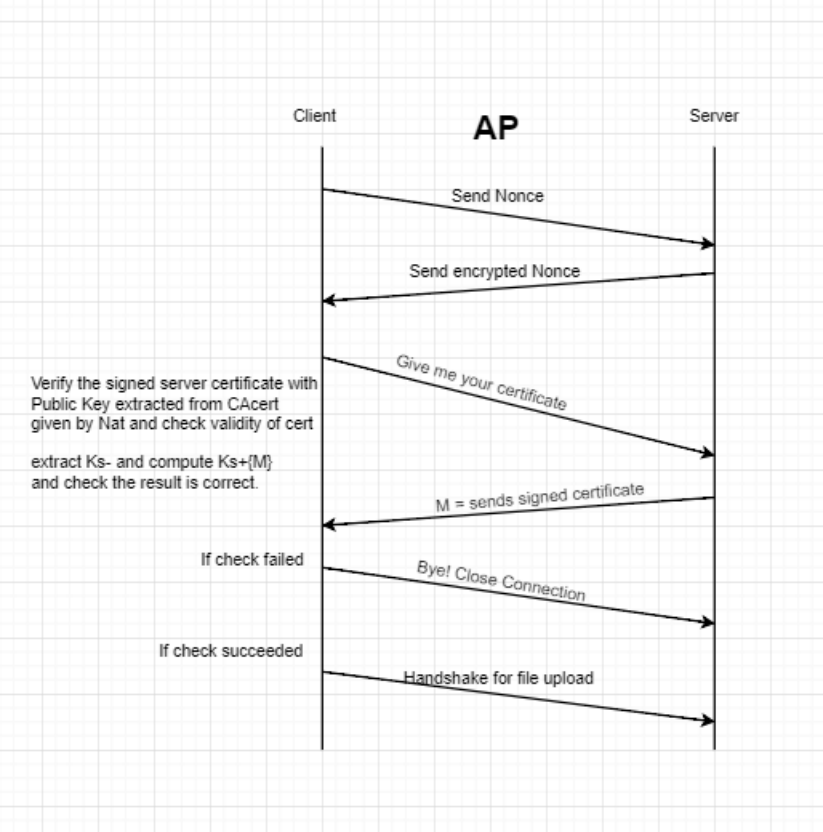
Sarthak Ganoorkar | 1002901

2) Clear and succinct instructions of how to run your programs.

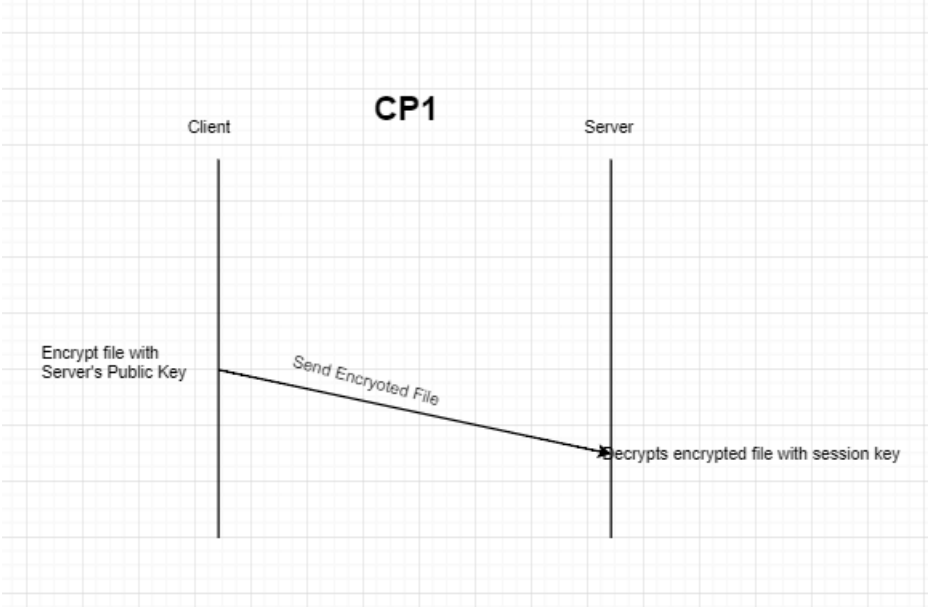
The instructions of how to run your programs are present in the README file

3) Specifications for the protocol AP, CP-1, and CP-2. Follow Fig.1 for the format of your specifications

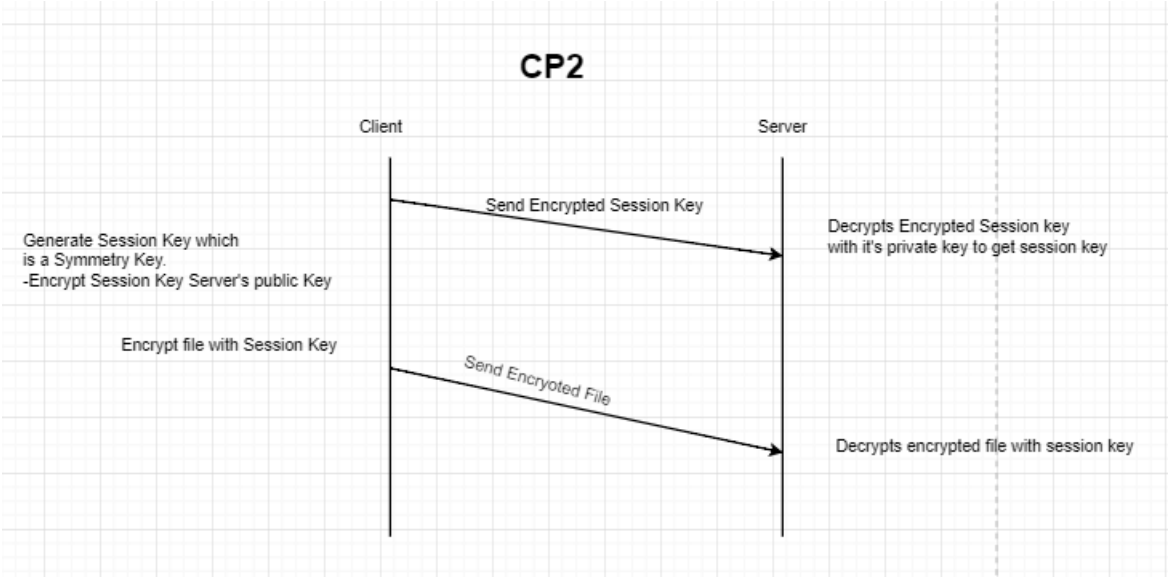
The diagram representing the Authentication protocol is as follows:



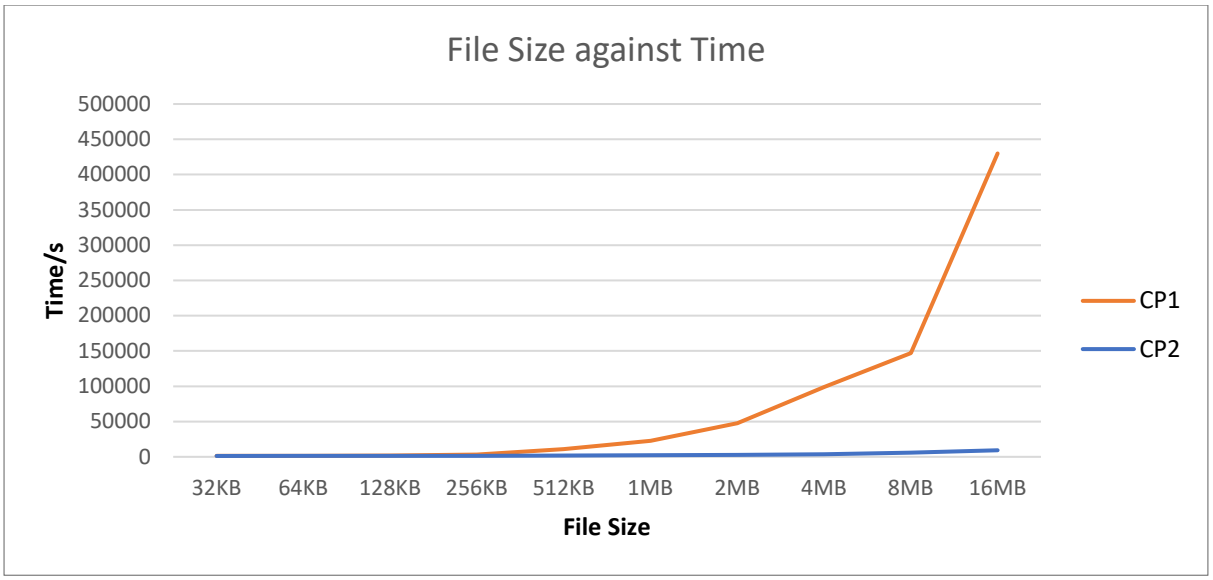
The diagram representing the CP-1 protocol:



The diagram representing the CP-2 protocol:



4) Plots of achieved data throughput of CP1 and CP2 against a range of file sizes.



We can see that the time taken to transfer the file over the network, the time taken for CP-1 has a much steeper gradient than CP -2.

CP – 1 uses RSA, which has intense mathematical calculations required during the encryption and decryption of data. Hence with large key sizes (for our case 2048 bits) it takes exponentially longer to handle the encryption and decryption of larger files.

$C = m^e \bmod n$

$M = c^d \bmod n$

CP-2 on the other hand isn't as dependent on mathematical calculations (related to the file size) hence the time taken for the file sizes does not vary as much.