50.005 Computer System Engineering

PA 2 Submission Handout

Secure File Transfer

1. Authentication Fix

In the original AP protocol given, replay attack could occur if an attacker intercepts the 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 the server must return the nonce, encrypted with its private key. Since the nonce is freshly generated, the server's response must be instantaneous, therefore the client can guarantee that the server is the live server but not an imposter.

2. Specification Protocol

Attached at the end of this document

3. Data Throughput

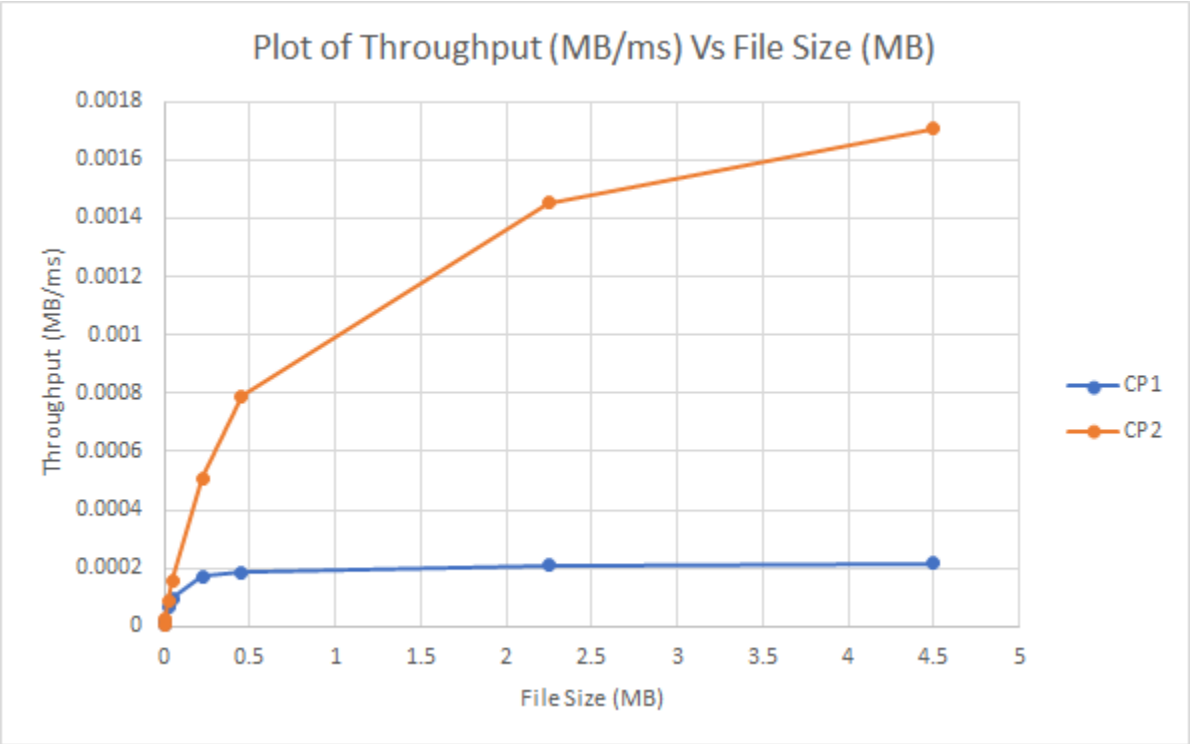
CP1 results

File Name	Size /MB	Time_1/ms	Time_2/ms	Time_3/ms	Average_time/ms	Throughput (MB/ms)
100.txt	0.005	248.4848	256.0258	244.6548	249.7218	2.00223E-05
200.txt	0.0009	275.8047	260.1836	273.2641	269.7508	3.33641E-06
500.txt	0.023	361.535	351.0554	339.4575	350.6826333	6.55864E-05
1000.txt	0.045	455.3293	450.4088	479.2137	461.6506	9.74763E-05
5000.txt	0.225	1303.6238	1272.2214	1352.4741	1309.439767	0.000171829

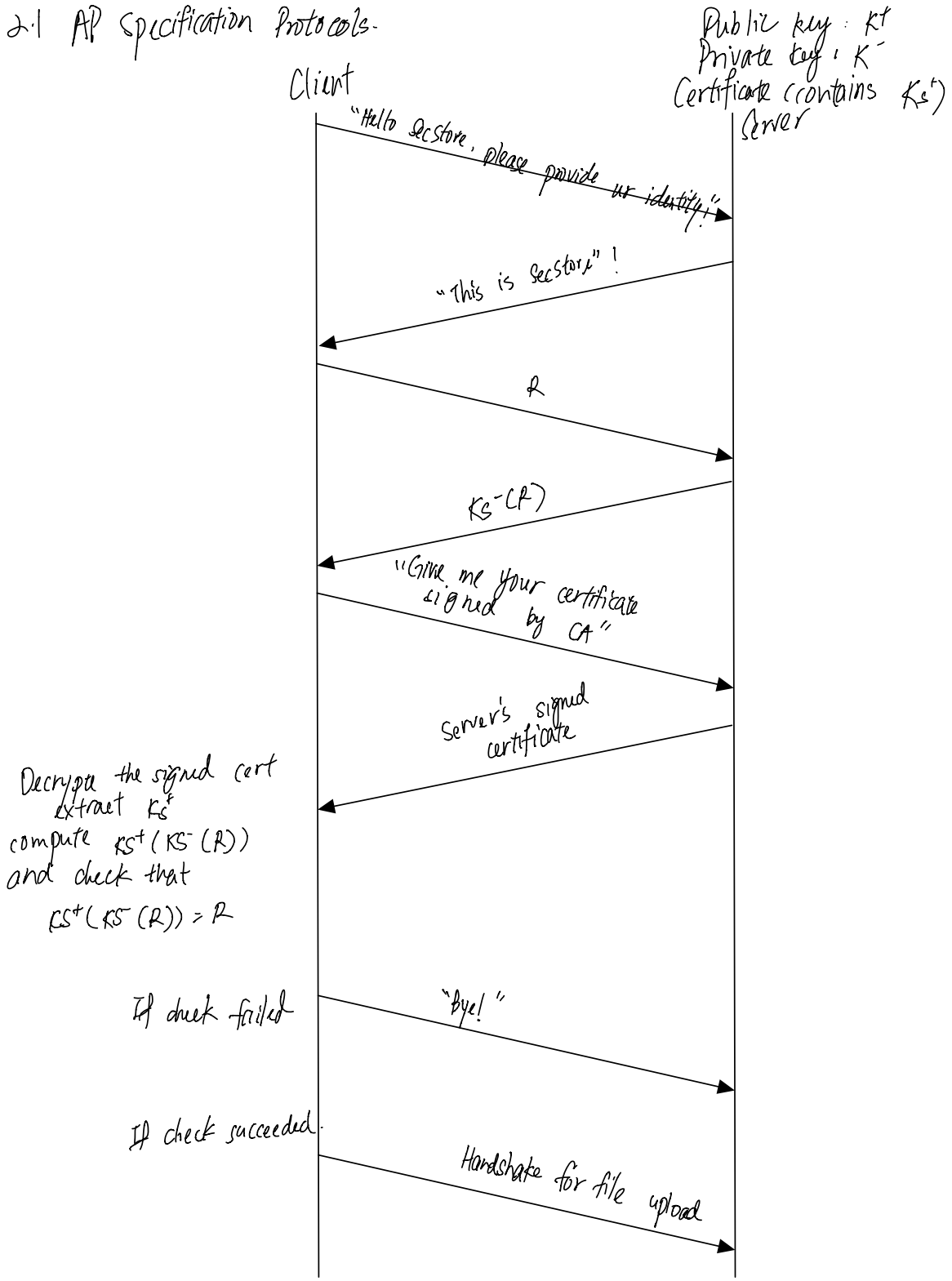
10000.txt	0.45	2459.2089	2492.9413	2334.8271	2428.992433	0.000185262
50000.txt	2.247	10766.9511	10670.3053	10675.1261	10704.1275	0.000209919
100000.txt	4.493	20479.7887	20659.9337	21379.1627	20839.62837	0.000215599

CP2 results

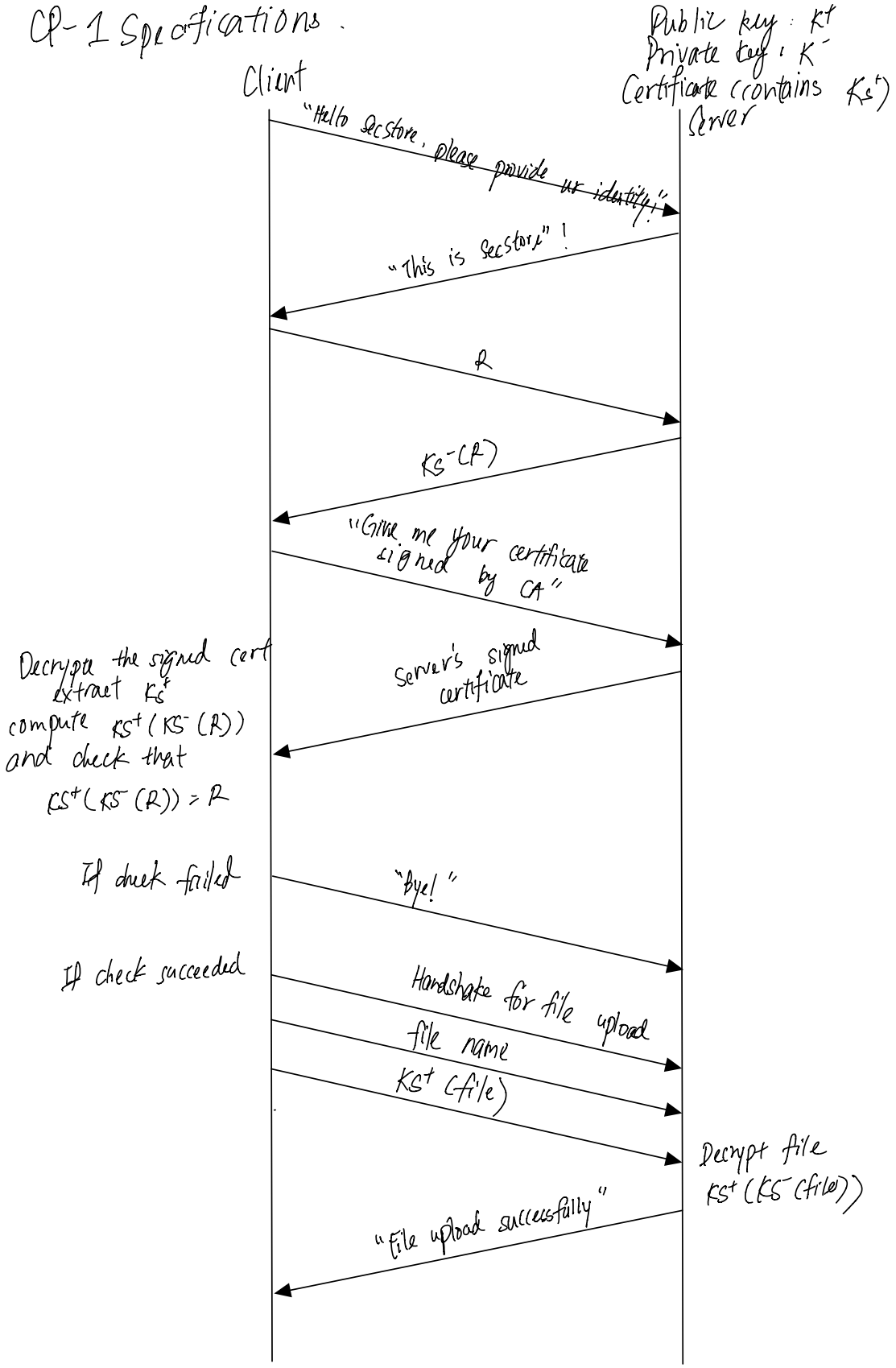
File Name	Size /MB	Time_1/ms	Time_2/ms	Time_3/ms	Average_time/ms	Throughput (MB/ms)
100.txt	0.005	217.3183	214.6213	223.9562	218.6319333	2.28695E-05
200.txt	0.0009	244.0004	234.3546	240.4375	239.5975	3.7563E-06
500.txt	0.023	256.3984	251.3153	254.8705	254.1947333	9.04818E-05
1000.txt	0.045	284.2049	283.9283	280.2452	282.7928	0.000159127
5000.txt	0.225	453.8183	433.4854	436.1485	441.1507333	0.00051003
10000.txt	0.45	577.2968	554.7669	578.3317	570.1318	0.000789291
50000.txt	2.247	1541.1569	1528.4487	1573.2293	1547.611633	0.001451915
100000.txt	4.493	2577.8941	2661.749	2665.9694	2635.204167	0.001704991


Plot of Throughput (MB/ms) Vs File Size (MB)
Throughput (MB/ms)
0.0018
0.0016
0.0014
0.0012
0.001
0.0008
0.0006
0.0004
0.0002
0
0
0.5
1
1.5
2
2.5
3
3.5
4
4.5
5
File Size (MB)
CP1
CP2

2.1 AP specification Protocols.



2.2 CP-1 Specifications.



2.3 - CP-2 Specifications