50.005 CSE

Programming Assignment 2

Submission Handout

Jia Shuyi

1004576

Shoham Chakraborty

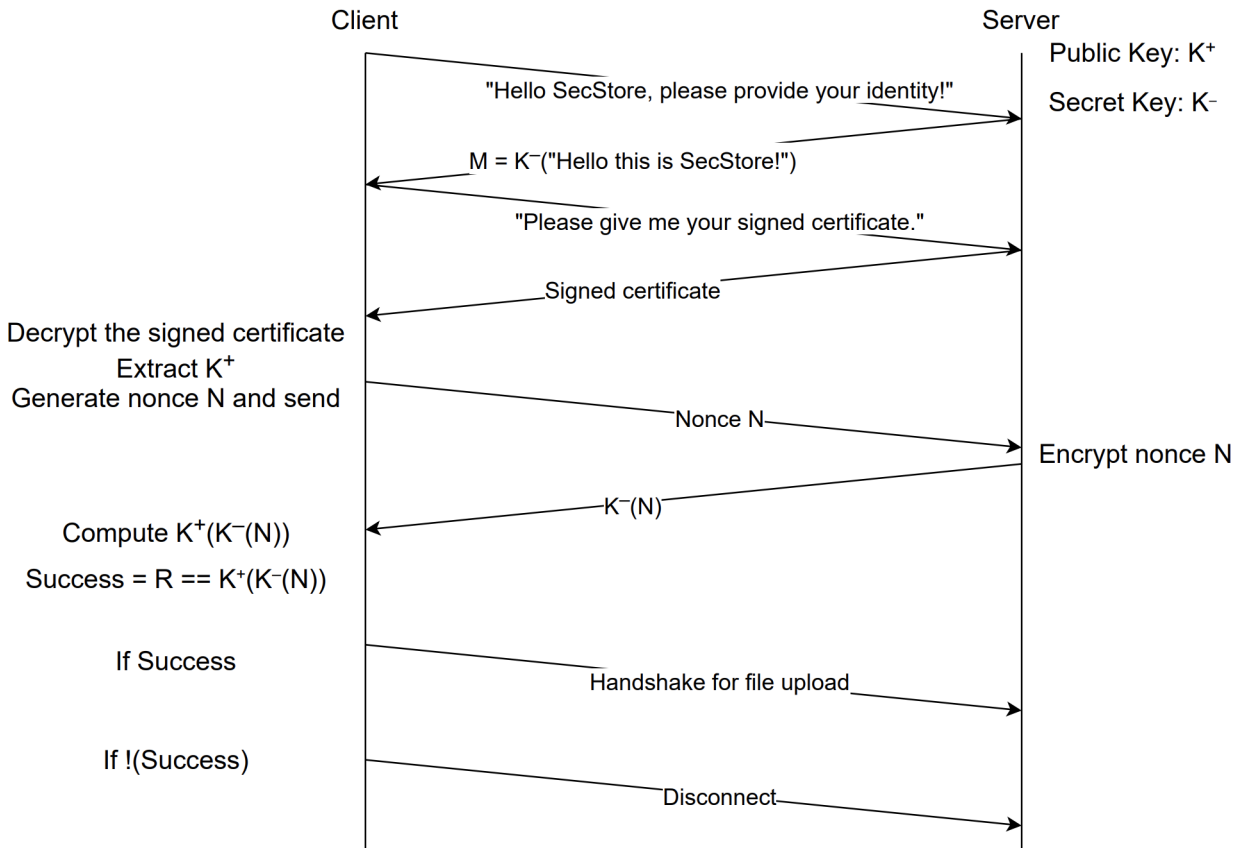
1004351

What is the problem with protocol presented in Figure 1?

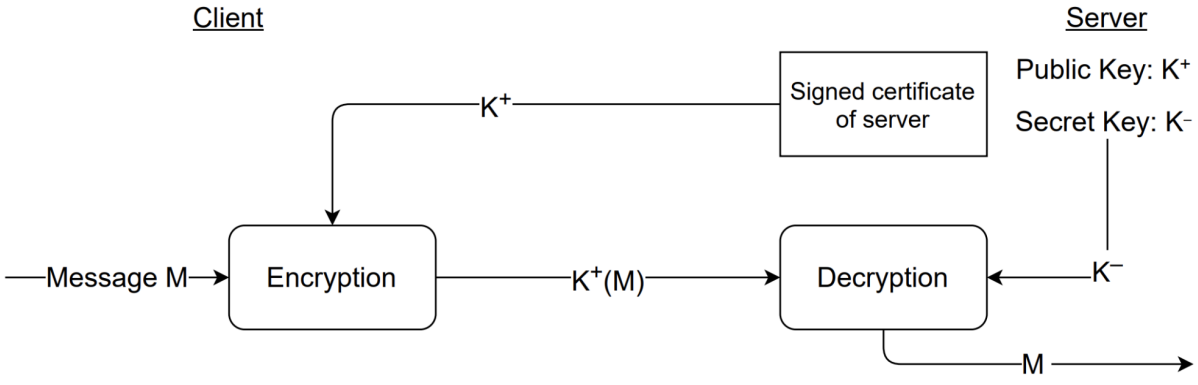
The protocol is susceptible to replay attack, wherein the attacker can intercept the server's signed certificate and re-transmit it, possibly as part of a spoofing attack, thereby getting authenticated when it is not the intended server.

We can fix it by using nonce. Such that before every transmission, we generate a nonce on the fly and pass it to the server for encryption. The server will encrypt the nonce using its private key and send it back to us (the client). We then decrypt the encrypted nonce using the server's public key and compare it to the original nonce. The server's authenticity is guaranteed when the decrypted nonce and the original are the same.

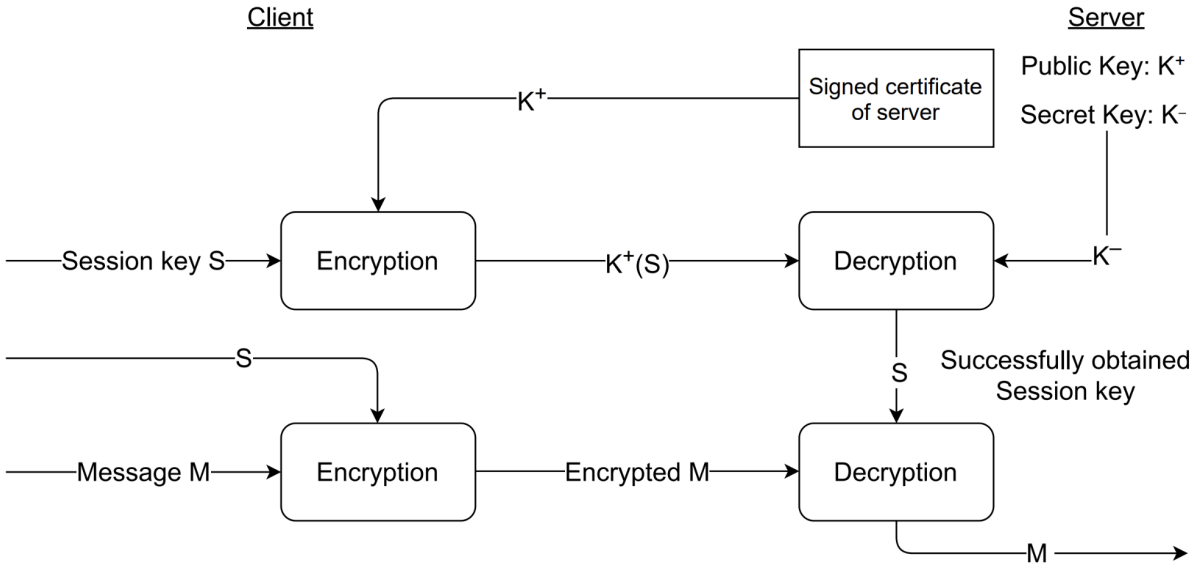
Specification Diagram: Authentication Protocol



Specification Diagram: CP1

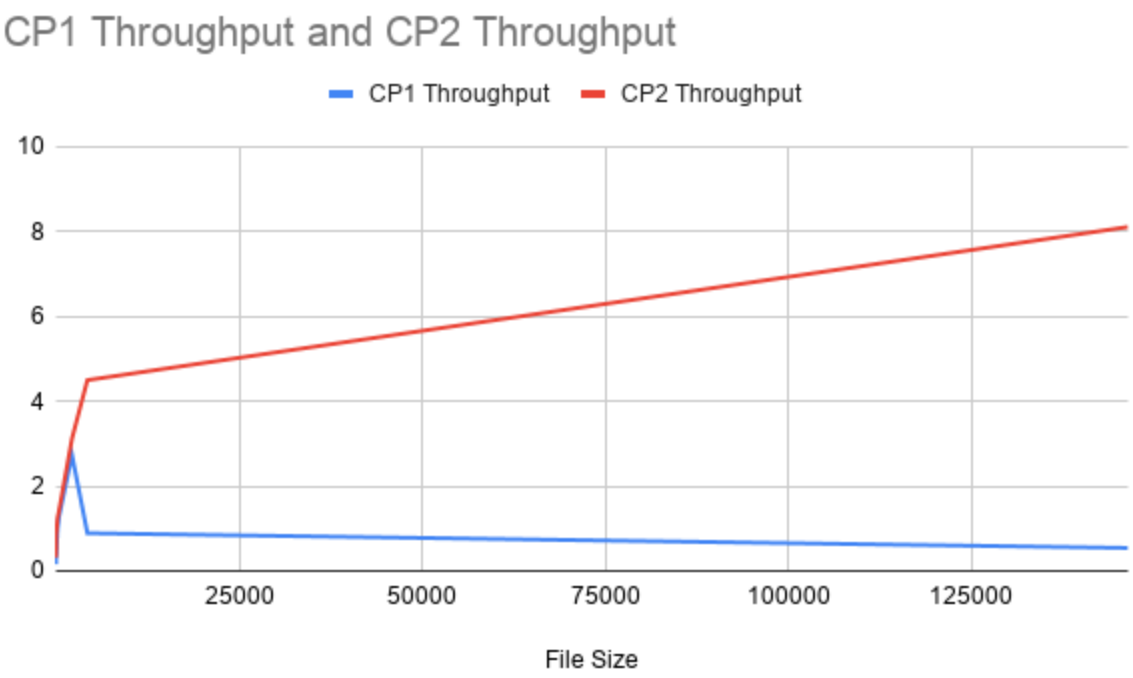


Specification Diagram: CP2



Data Throughput Visualisation

File Size	CP1 Time	CP2 Time	CP1 Throughput	CP2 Throughput
8.8	55.264395	18.287254	0.1592345307	0.4812094807
22	45.171712	69.546958	0.4870304672	0.3163330307
44	134.631333	52.114927	0.3268184235	0.8442878563
220	223.562107	177.061163	0.9840665887	1.2425085
440	340.074106	307.873908	1.293835644	1.42915651
2200	805.908518	704.792307	2.729838376	3.121486966
4300	4824.549172	955.909066	0.8912749869	4.498335828
146400	269292.2288	18057.46904	0.5436473256	8.107448484


CP1 Throughput and CP2 Throughput
CP1 Throughput
CP2 Throughput
10
8
6
4
2
0
25000
50000
75000
100000
125000
File Size