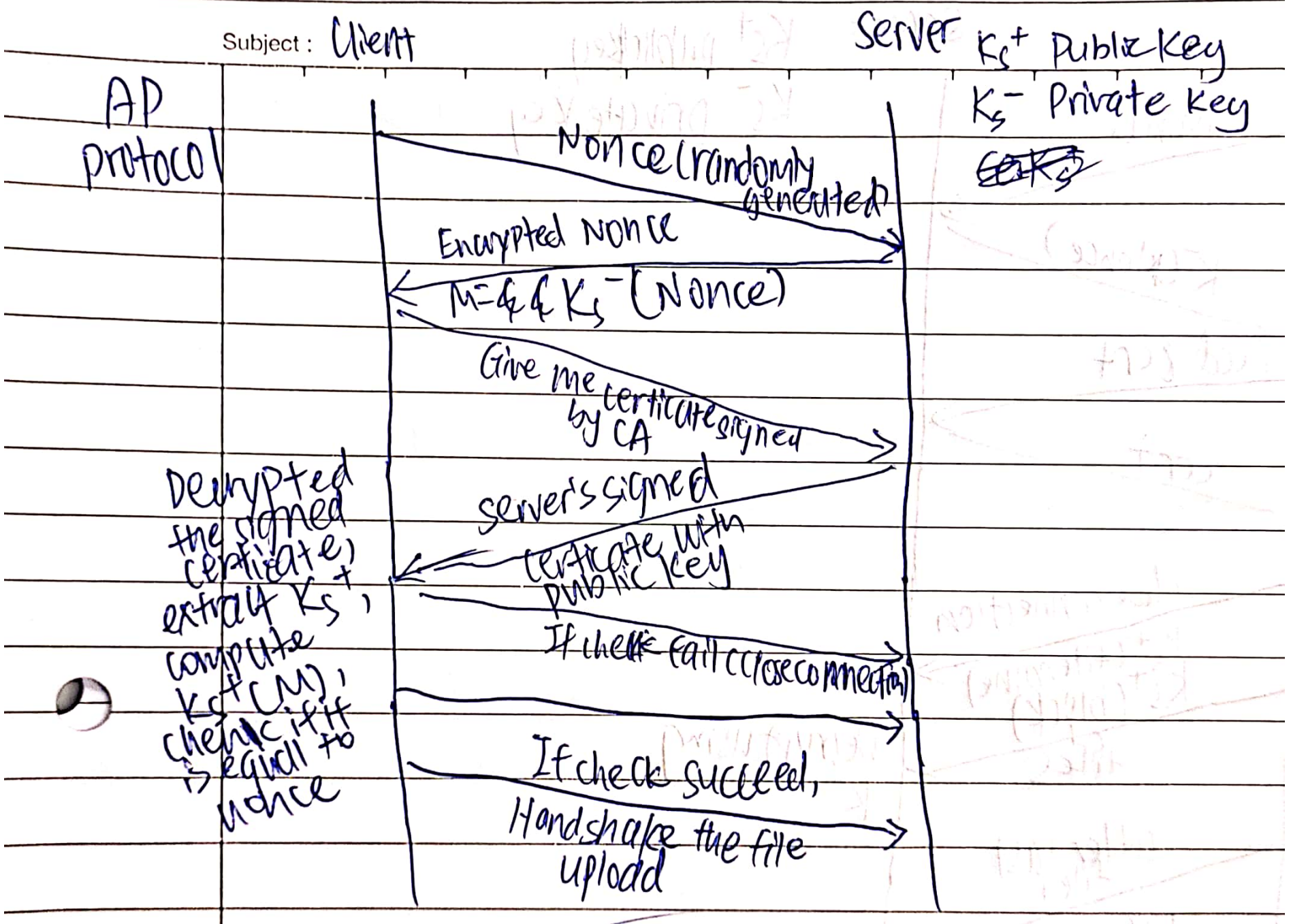
Submission Handout PA2

Subject :

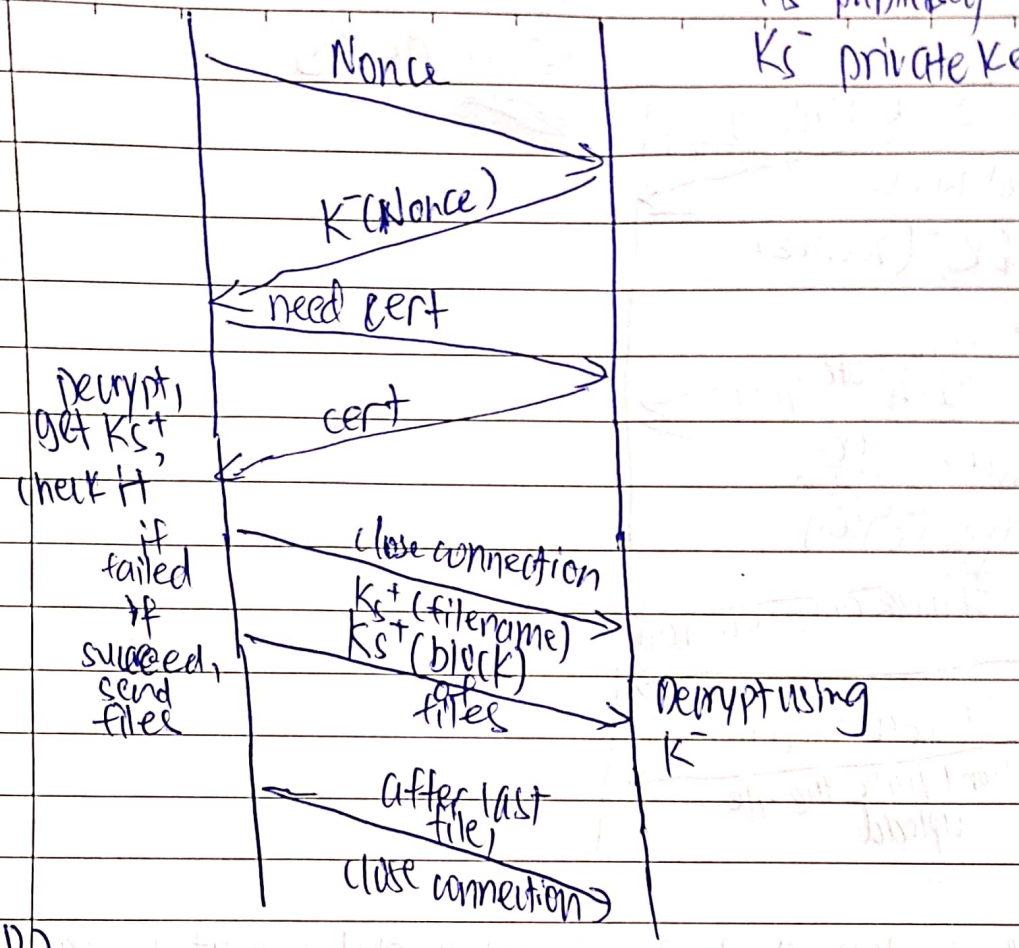


Security loophole of AP problem solved:

The loophole is that an intruder can record and send the encrypted message back to the client and act as the server, if the user always sends the same message/unencrypted message. A nonce ~~Generated~~ will ~~be~~ able to solved this ~~B~~ replay attack.

CP1 protocol

Subject : Client Server K_s^+ publickey K_s^- private key Date:



CP2 protocol