

# Submission Handout PA2

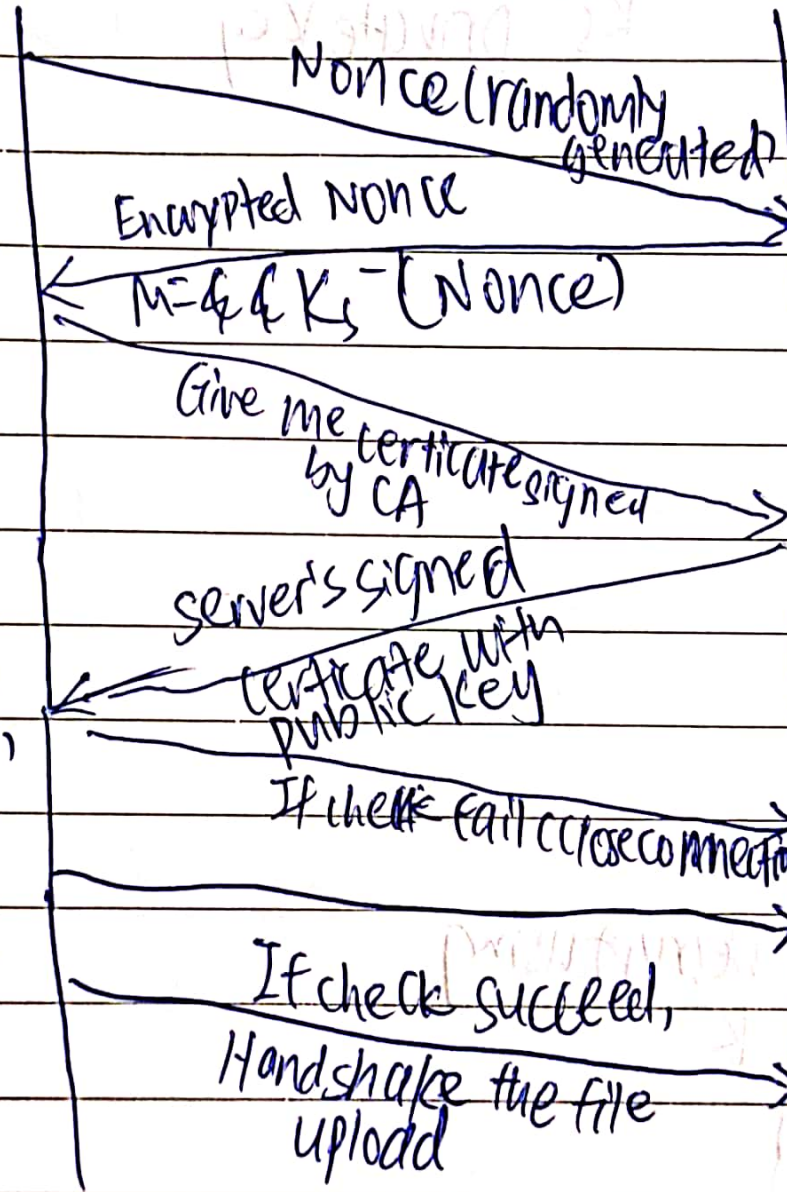
Subject: Client

Server

$K_s^+$  Public Key

$K_s^-$  Private Key

AP  
protocol



Decrypted the signed certificate, extract  $K_s^+$ , compute  $K_s^+(M)$ , check if it is equal to nonce

If check succeed,  
Handshake the file  
upload

Security loophole of AP problem solved:

The loophole is that an intruder can record and send the <sup>encrypted</sup> 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 solve this replay attack.

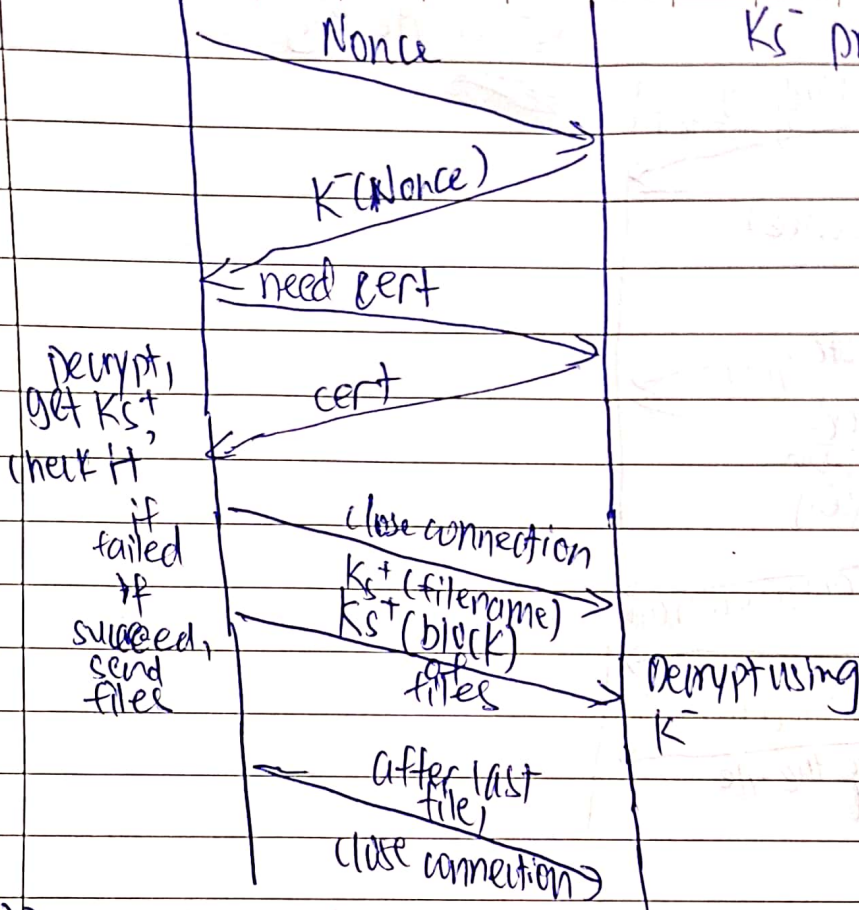
# CP1 protocol

Subject: Client

Server

$K_s^+$  public key  
 $K_s^-$  private key

Date:



## CP2 protocol

client

Server  $K_s^+$  public key

$K_s^-$  private key  
 $K$  session key  
Symmetry

