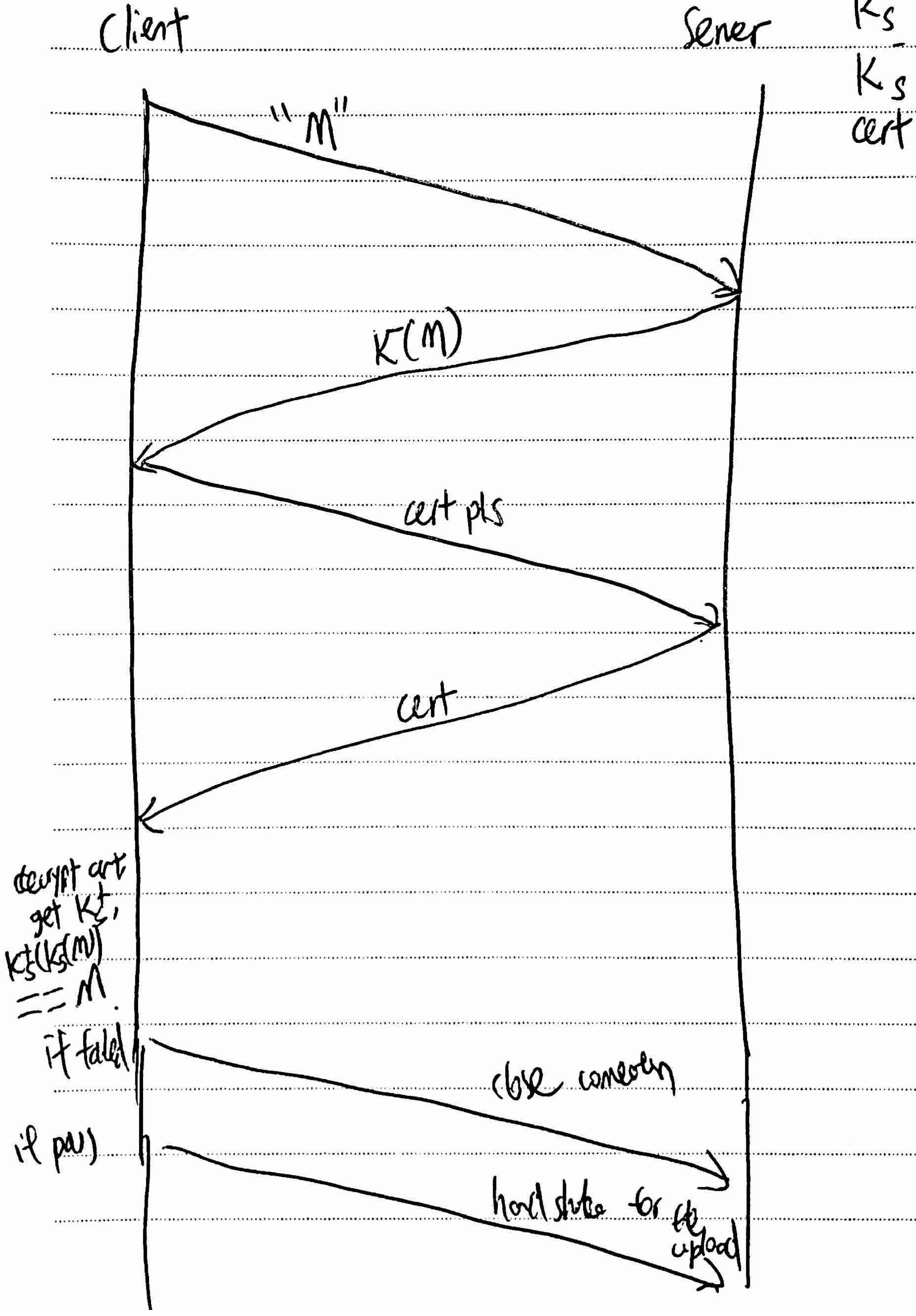
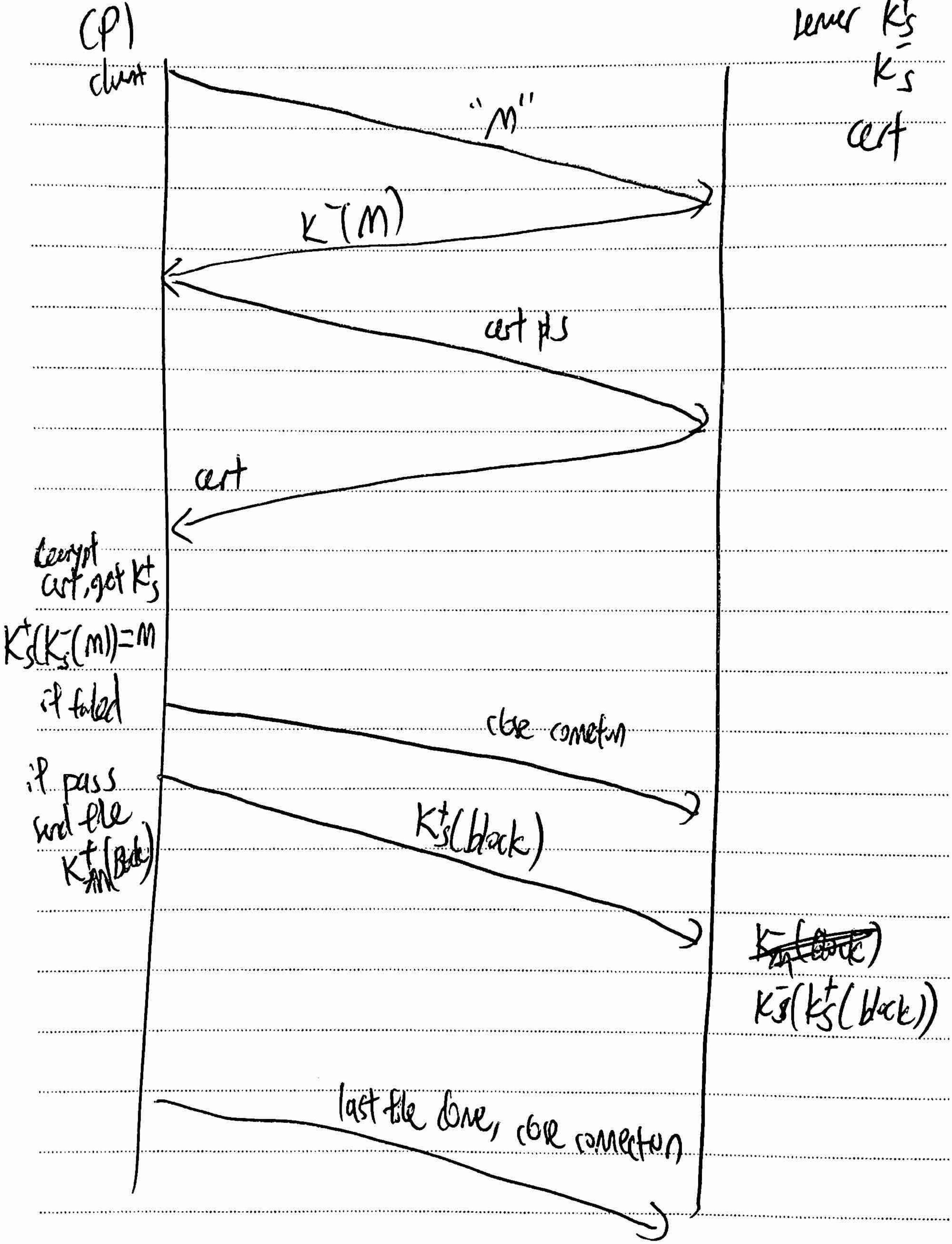
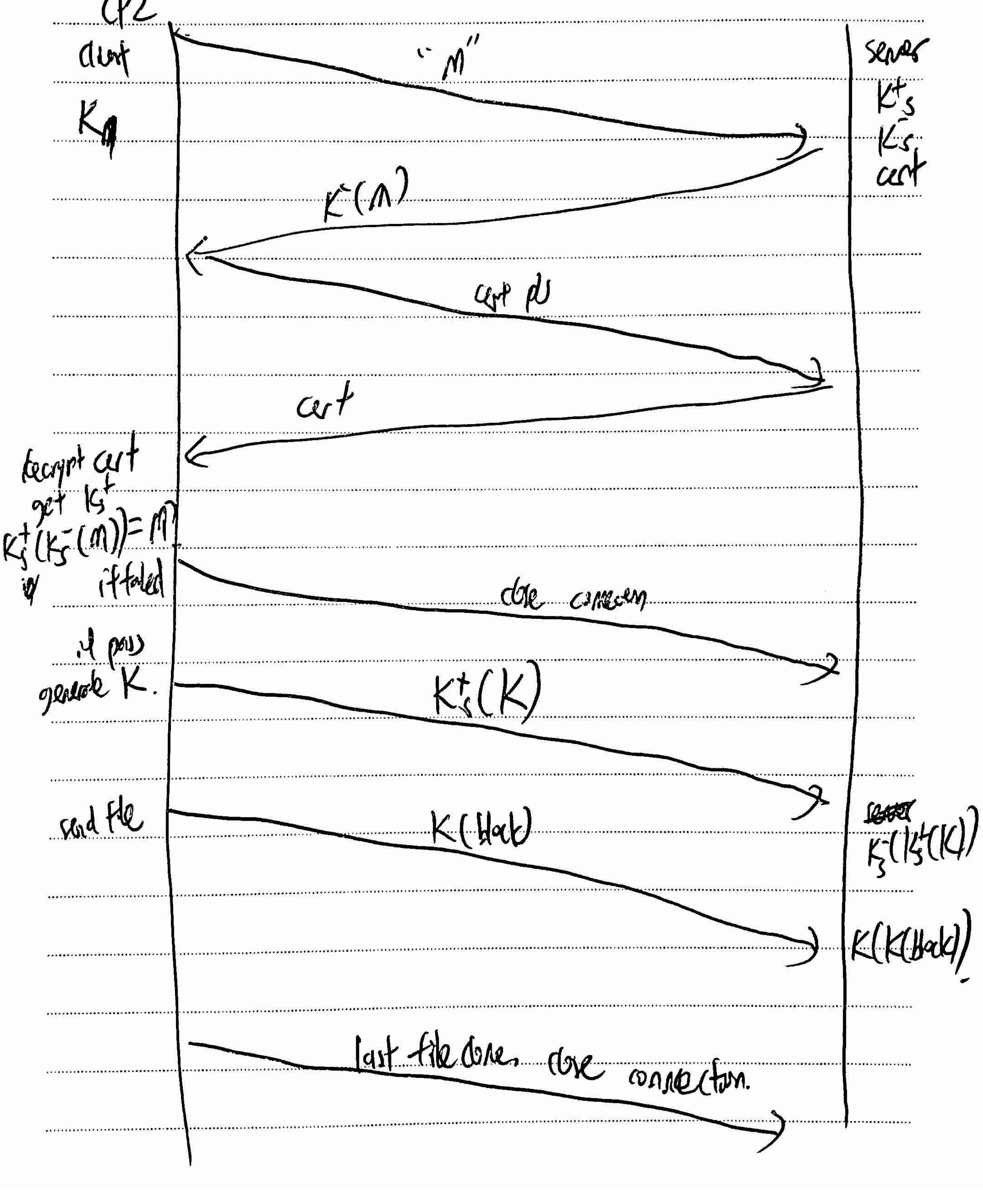
AP


Client
Sever
K_s^+
K_s^-
cert
"M"
K(M)
cert pls
cert
decrypt cert
get K_s^+,
$K_s^+(K_s^-(M))$
== M.
if failed
close conneciton
if pass
handshake for file upload



CP1
client
server K_S^+
K_S^-
cert
"M"
$K^-(M)$
cert pls
cert
decrypt cert, got K_S^+
$K_S^+(K_S^-(m))=M$
if failed
close conection
if pass
send file
K_{AN}^+(Block)
K_S^+(block)
~~K_{AN}^-(block)~~
$K_S^-(K_S^+(block))$
last file done, close connection


CP2
client
K_{p}
server
K_s^+
K_s^-
cert
"M"
$K^-(M)$
cert pls
cert
decrypt cert
get K_s^+
$K_s^+(K_s^-(M))=M?$
if failed
close connection
if pass
generate K.
$K_s^+(K)$
send file
K(block)
~~server~~
$K_s^-(K_s^+(K))$
K(K(block))
last file done, close connection.