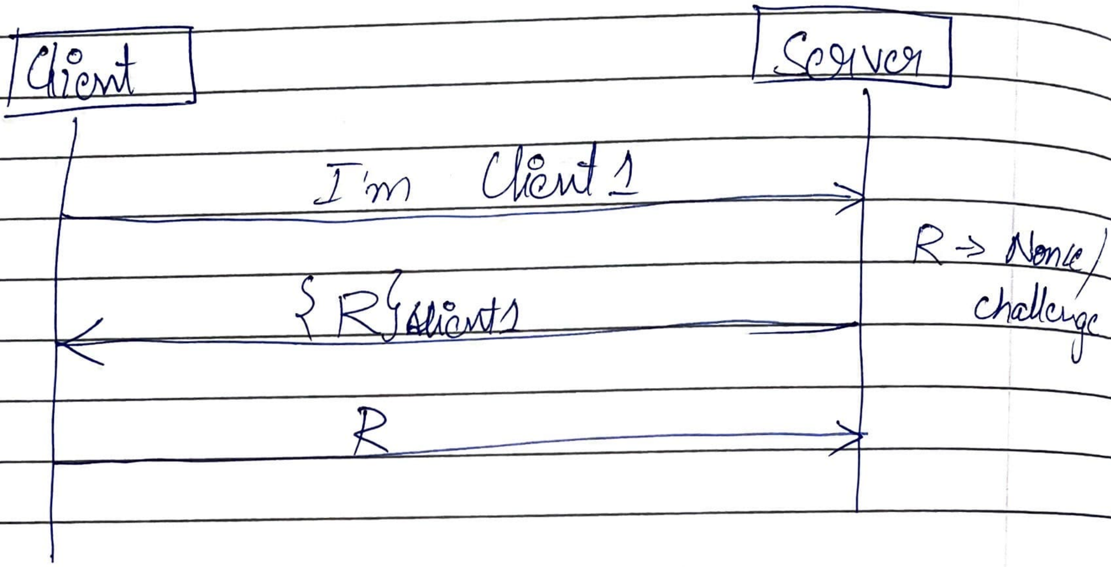
# Authentication

## Server - Client Authentication (9.6)



Its vulnerable to Man in the middle attack

## Integrity and Confidentiality

Client 1

$B_i = MD(K_{AB} \,||\, IV)$ IV -> 1st

$C_{i-1}$ -> from 2 to

$C_i = P_i \text{ XOR } B$

$(C_i \,||\, h(P_i))$ ith message

Client 2

$B_i = MD(K_{AB} \,||\, IV)$

$P_i = C_i \text{ XOR } B_i$

$h(P_i)$ -> for integrity check

# Key exchange

Server to Client 1 (After client 1 selects the client-2)

~~K1{~~ m = Client2

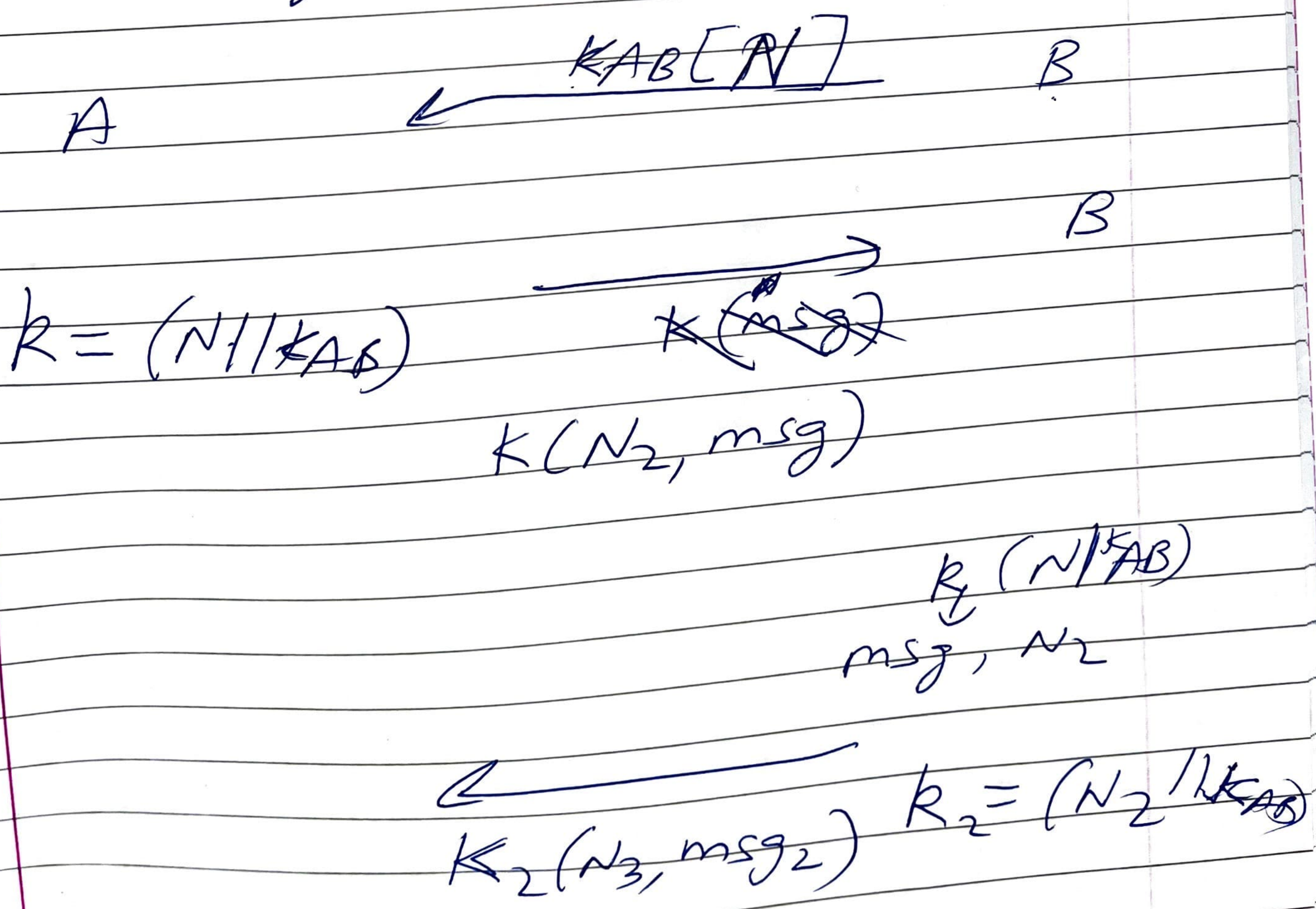
~~K1{ client1, client2,~~

Server to Client-1

K1{ Client-2, K12, IV, ticket}

ticket = K2{ ~~K12~~ Client 1, K12, IV}

## Replay Attack


KAB[~~N~~]
B
A
B
k = (N||KAB)
~~K(msg)~~
K(N2, msg)
k (N||KAB)
msg, N2
K2(N3, msg2)
K2 = (N2||KAB)