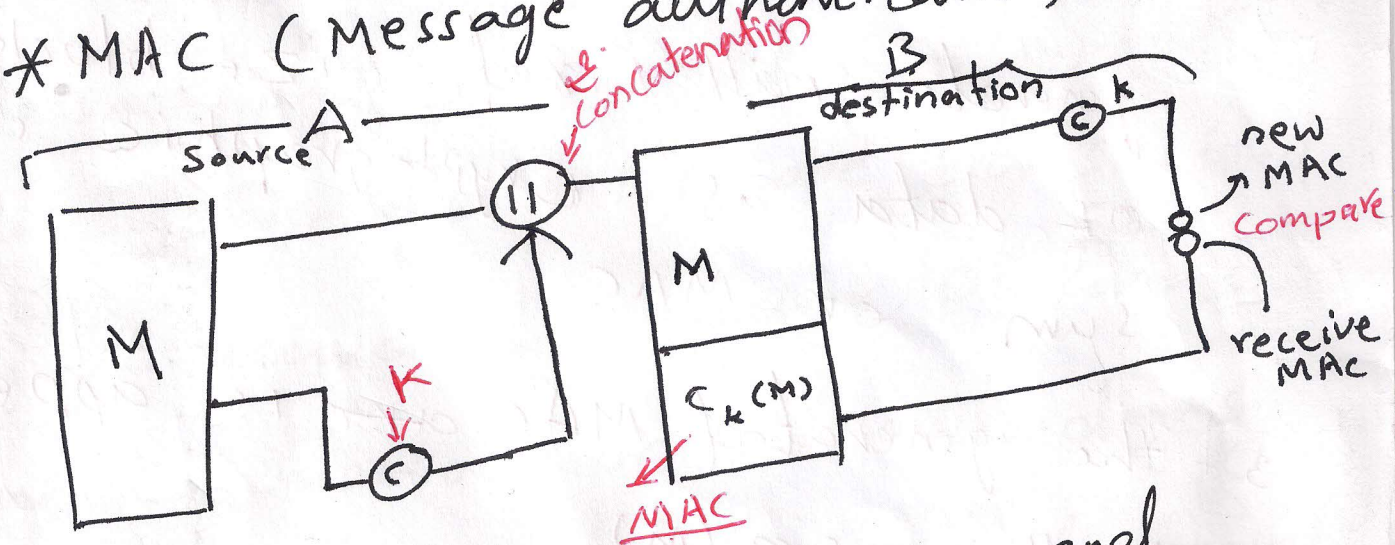
* Authentication Function :-

any message authentication involves the following Functions:-

1. Message Encryption.
2. Message authentication Code (MAC).
3. Hash Function.

(1) * MAC (Message authentication code).



→ apublic fun of the message and asecret key that produces fixed length value that Serves as authentication.

→ in this method the secret key is used to generates a small fixed sized block of data known as →

at the Sender.

1- * M: msg is sent from Sender

2- * M: entered the MAC Function (C) and use the secret key (K) to generate small fixed size block of data as Cryptographic check sum or MAC

3- the generated MAC ~~are~~ is appended to the msg (M)

4- the Msg plus MAC are transmitted to the destination.

from

yptographic checksum or message

authentication code) that is ~~appended~~

appended to the message.

→ As shown in the diagram ~~both A~~

and B

→ A want to send the msg to B.

→ A calculate the MAC as a function of message and secret key $C_K(m)$.

the message and MAC are transmitted to the receiver the receiver performs same calculation on the received msg by using same secret key and generates new MAC value.

the receiver mac is compared with the calculated MAC and if both are same the msg contain integrity check and it has not modified b in between.

at the destination.

step1:- the msg (M) and MAC are arrived at the destination.

step2:- the destination performs the same calculation on the received msg (M) using same secret key. (K) with (MAC) Fun to generate new MAC.

step3:- the destination obtained the MAC from the received msg (M).

step4:- the calculated (MAC) is compared with the received MAC.