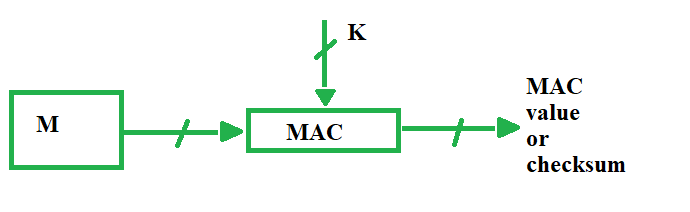
**MAC Verification**

Apart from intruders, the transfer of message between two people also faces other external problems like noise, which may alter the original message constructed by the sender. To ensure that the message is not altered there’s this cool method MAC.



MAC stands for Message Authentication Code. Here in MAC, sender and receiver share same key where sender generates a fixed size output called Cryptographic checksum or Message Authentication code and appends it to the original message. On receiver’s side, receiver also generates the code and compares it with what he/she received thus ensuring the originality of the message. These are components:

* Message
* Key
* MAC algorithm
* MAC value

There are different types of models Of Message Authentication Code (MAC) as following below:

1. **MAC without encryption –**  
   This model can provide authentication but not confidentiality as anyone can see the message.  
   Icon

   Description automatically generated
2. **Internal Error Code –**  
   In this model of MAC, sender encrypts the content before sending it through network for confidentiality. Thus this model provides confidentiality as well as authentication.

M' = MAC(M, k)

Icon

Description automatically generated

1. **External Error Code –**  
   For cases when there is an alteration in message, we decrypt it for waste, to overcome that problem, we opt for external error code. Here we first apply MAC on the encrypted message ‘c’ and compare it with received MAC value on the receiver’s side and then decrypt ‘c’ if they both are same, else we simply discard the content received. Thus it saves time.
2. c = E(M, k')

M' = MAC(c, k)

A picture containing diagram

Description automatically generated