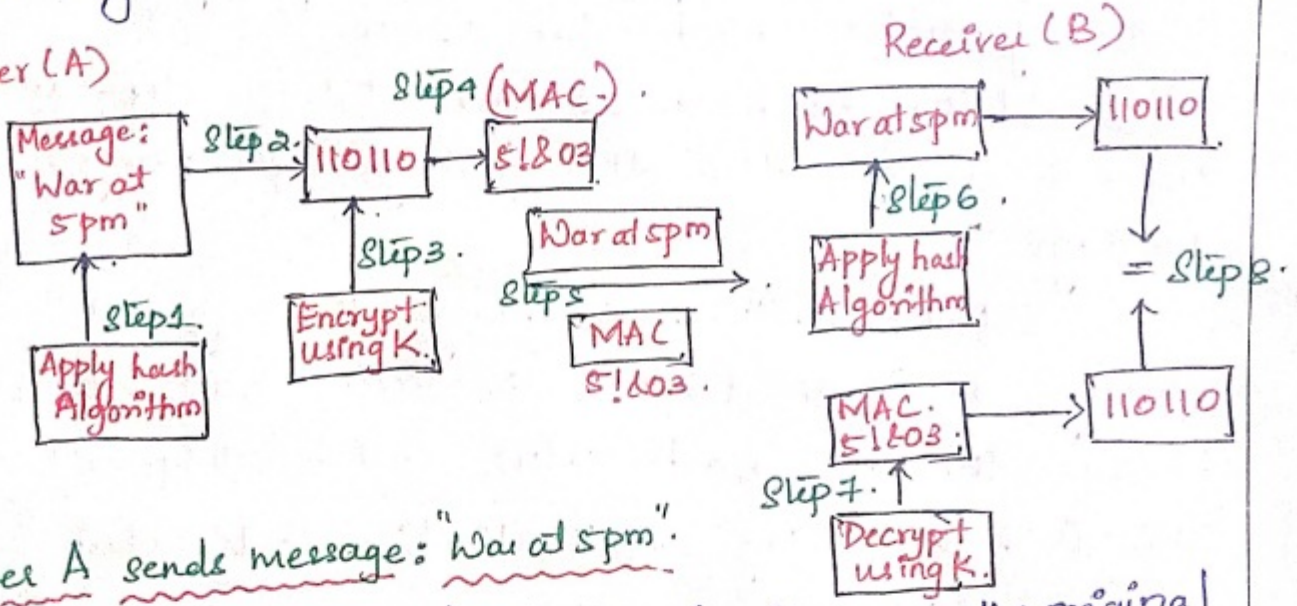
Semester : VI Subject : CSS Academic Year: 2023-2024

MESSAGE AUTHENTICATION CODE: (MAC)

* MAC supports integrity.
* Everyone can read the message, but cannot modify the message.
* Sender (A) and the Receiver (B) shares a symmetric secret key.



Sender A sends message: "War at 5pm".

Step 1: Sender will apply hash algorithm on the original message "War at 5pm".

Step 2: Consider that the output generated from step 1 is the hash value 110110

Step 3: Sender will encypt output generated in step 2 using the secret key.

Step 4: The encypted output generated is the MAC (ie) 5!&03.

Step 5: The sender will send the plain text message along with the MAC across network to the Receiver.

Semester : VI Subject : CSS Academic Year: 2023-2024

Receiver B checks integrity of message:

Step 5: The receiver receives both Message Authentication Code (MAC) and the original message.

Step 6: Receiver applies hash algorithm on the plain text and receives hash value 110110.

Step 7: The receiver decrypts MAC using symmetric key K and generates hash value 110110.

Step 8: If the hash value generated in step6 and step7 is similar then the message is the original message.

If the attacker has changed the original message as "WAR at 6pm", the receiver can identify because the two hash value will be different. This is how Message Authentication Code retains integrity of the message.