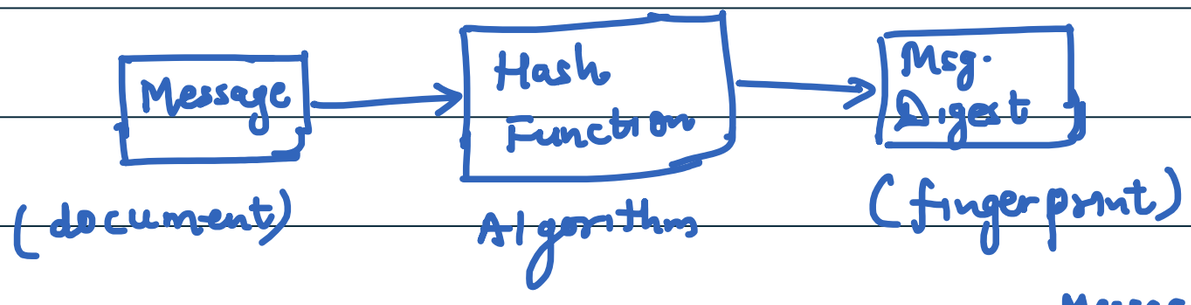
Authentication Function:

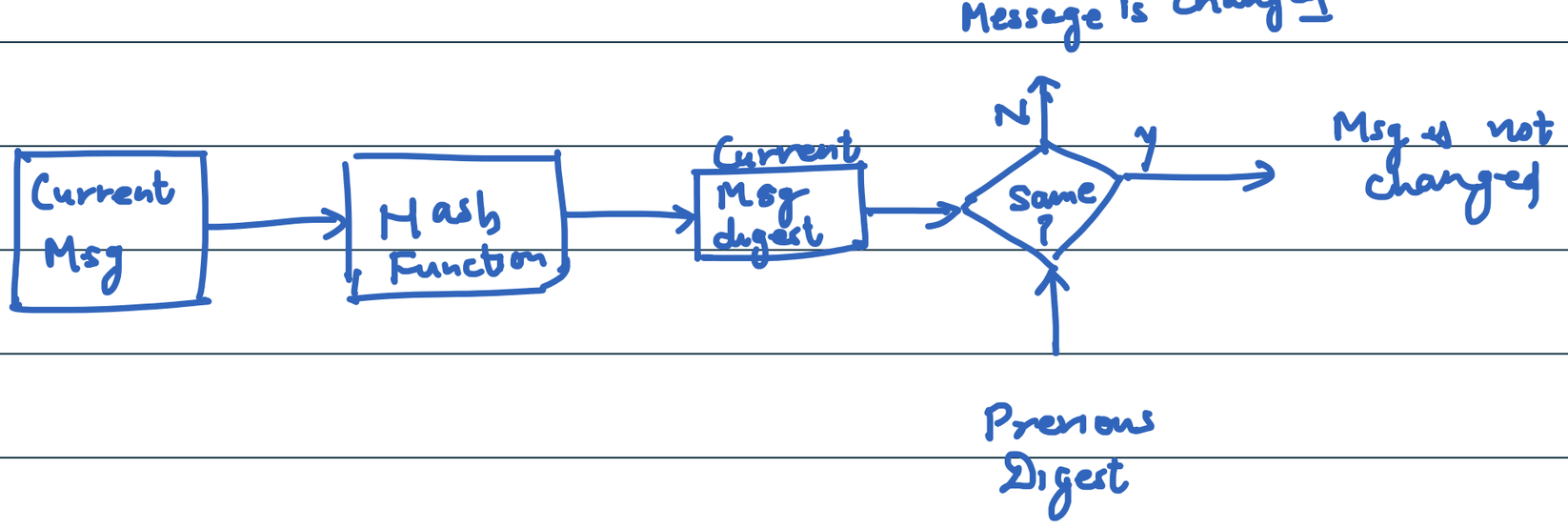
(1) Hash Function: This is a function that maps a msg of any length into a fixed length hash value, which serves as the authenticator

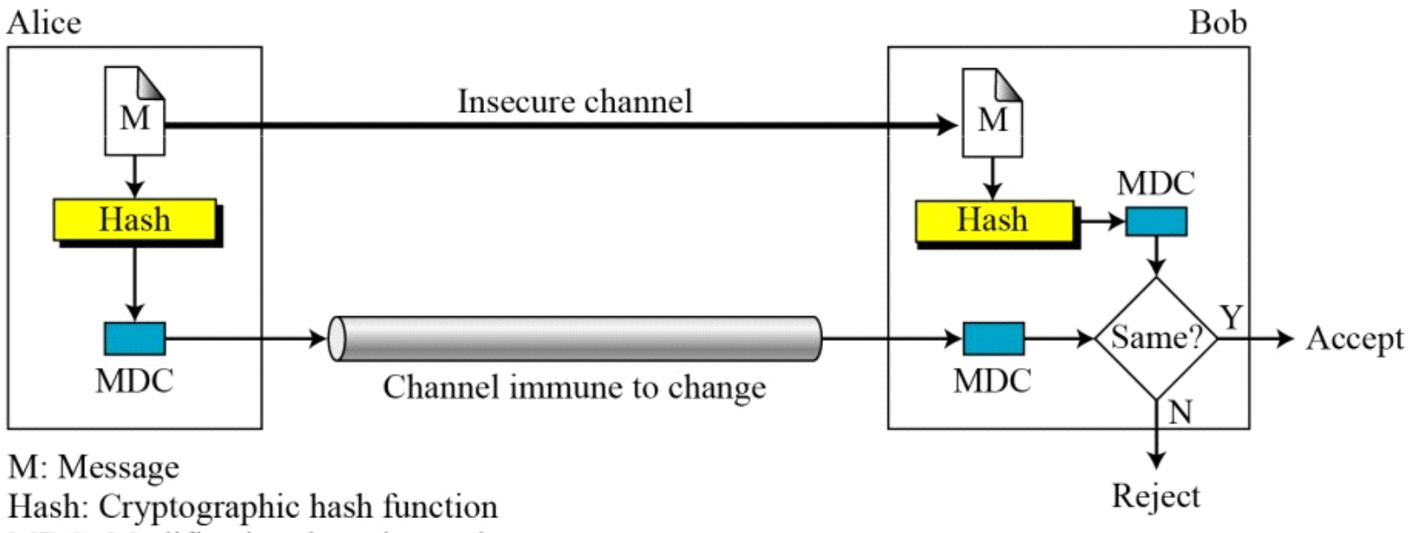
(2) Message Authentication Codes (MAC): A function of the msg and the secret key that produces a fixed length value that serves as authenticator.

(3) Message Encryption: Refer William Stalling.

Message and Message Digest pair the electronic equivalent of document and fingerprint pair.





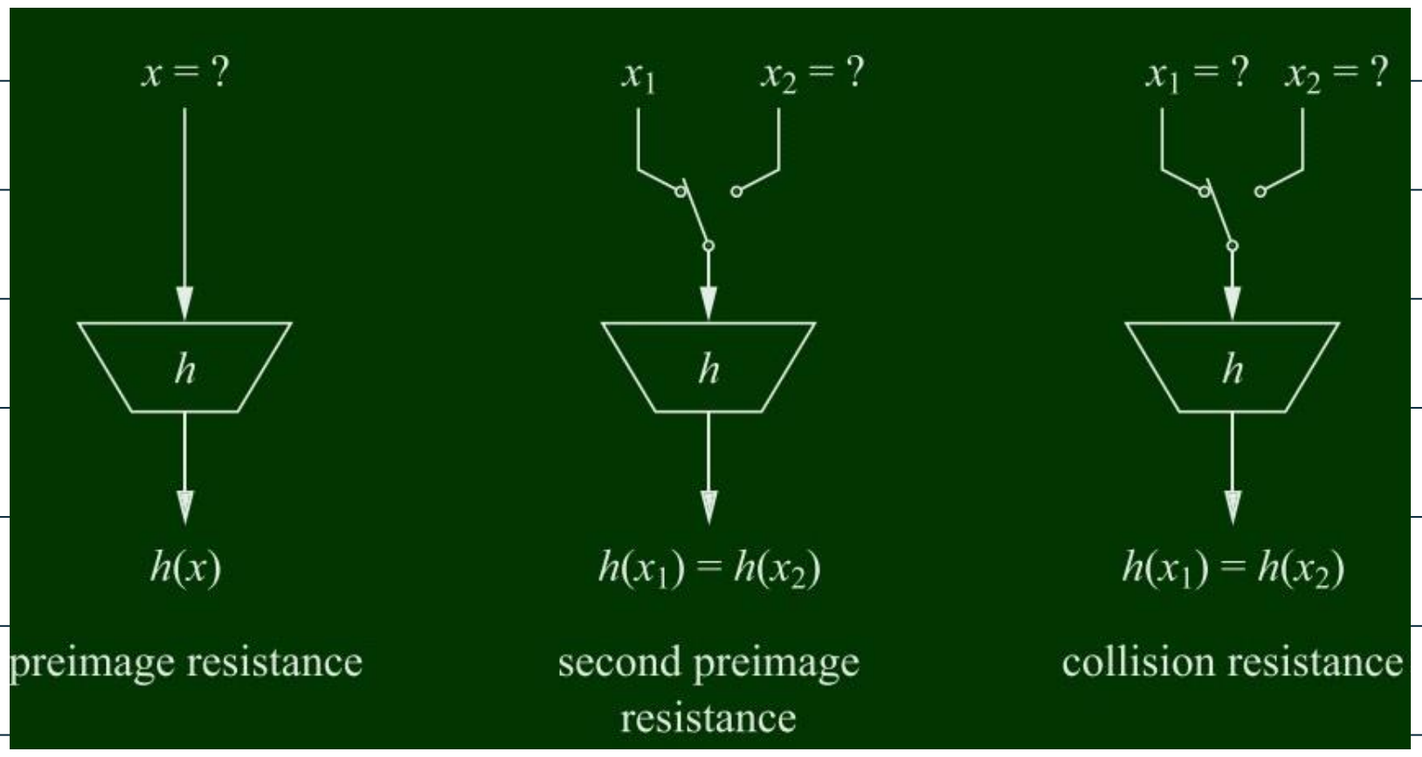


Cryptographic Hash Function Criteria

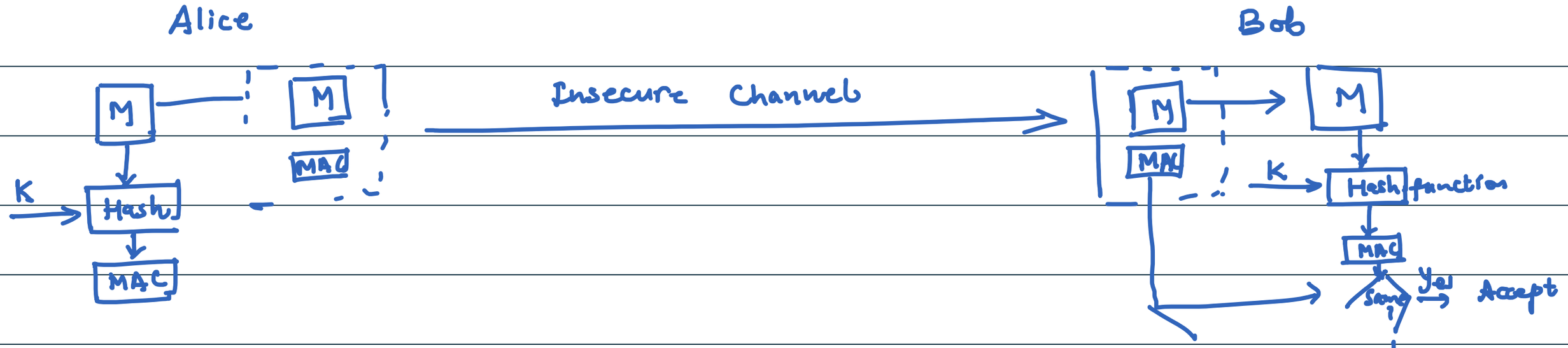
(1) Preimage Resistance (or Onewayness)

(2) Second Preimage Resistance (or weak collision res)

(3) Collision Resistance



Message Authentication Code (MAC) (Keyed Hash Function)

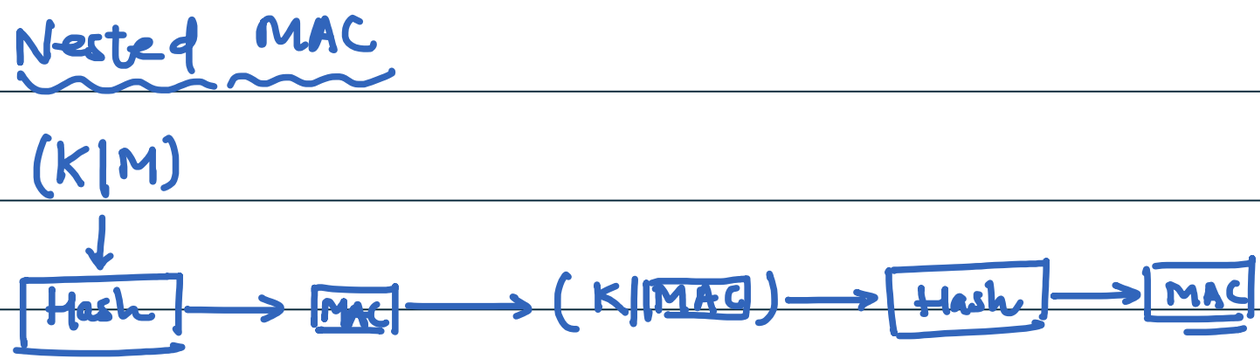


Security of MAC.

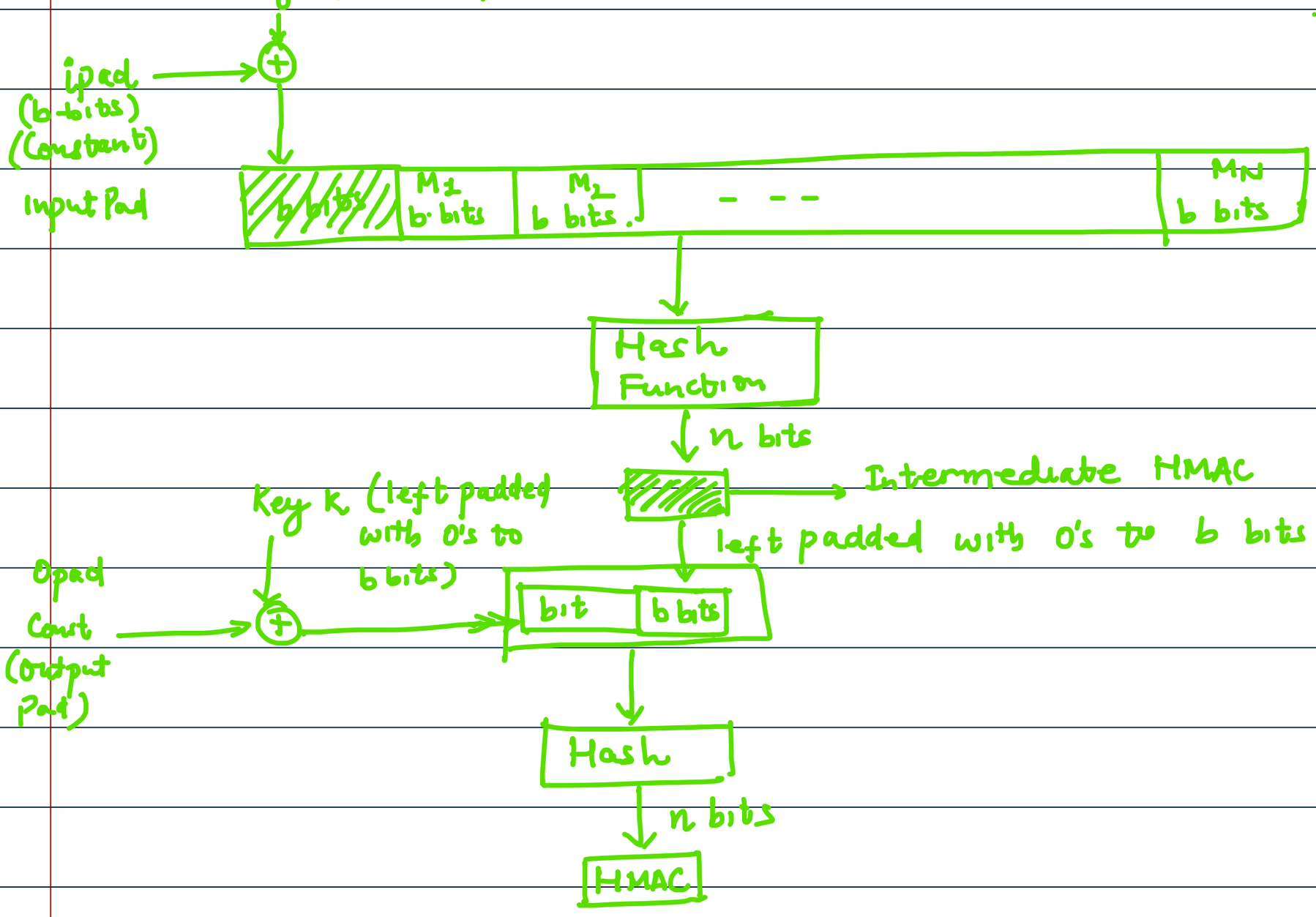
1. Brute Force.
2. Preimage Attack.
3. Given some pairs of msgs and their MACs Eve can manipulate them to come up with a new message and its MAC.

Note The security of the MAC depends on the security of the underlying Hash Algorithm

Nested MAC



HMAC (Hashed MAC)



Note: HMAC is a popular MAC used in many practical procols such as TLS.