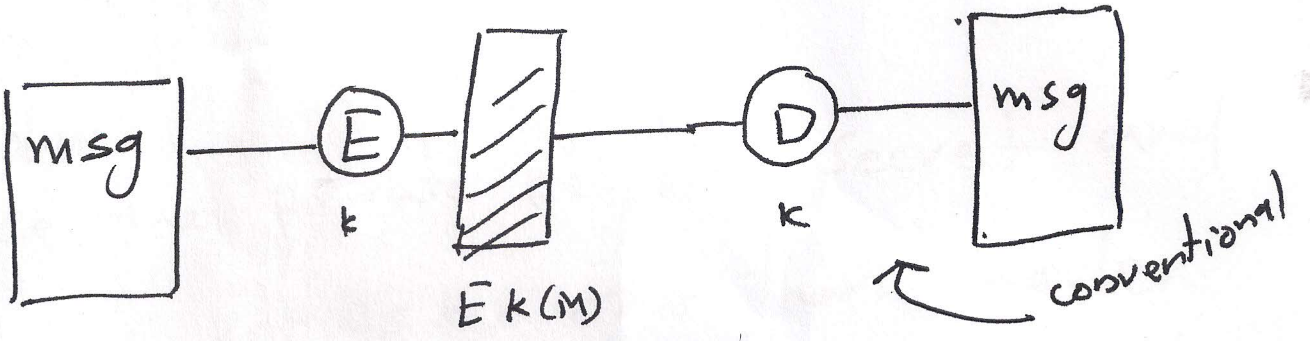
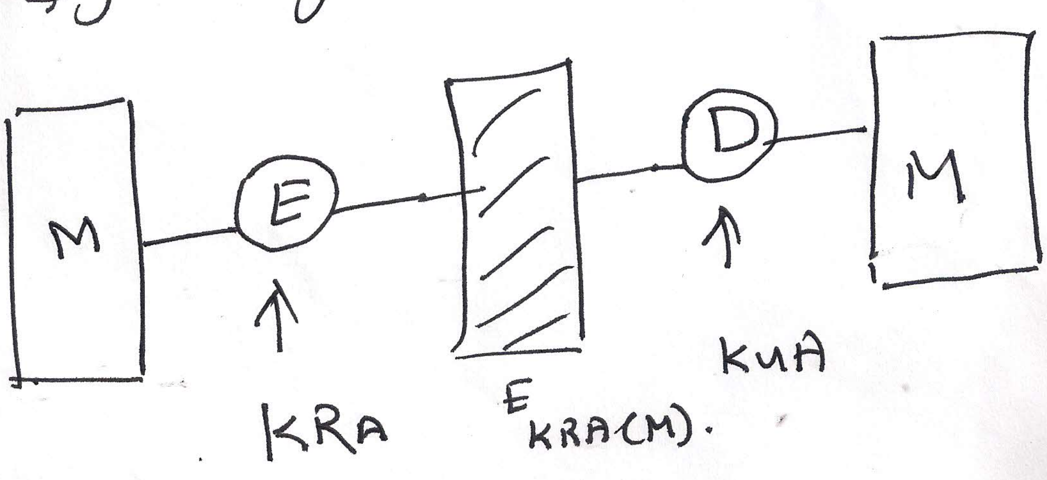
essage Encryption:



As shown in the diagram the secret key shared and the receiver can authenticate the sender by receiving Encrypted msg and nothing know, the secret key. the authentication can also be achieved by using secret k. Encryption

* By using public key Encryption.



shown in the diagram the msg is Encrypted with private key of Sender.

since the private key is secret and nobody knows the other than Sender. then we can achieve the authentication by using public key Encryption.

4

~~this~~

public key authenticity

ففي الرسالة تشفر بواسطة المفتاح السري الخاص لل Sender.

اما في عملية public key ~~secrecy~~ ~~att~~ secrecy الرسالة تشفر عن طريق

المفتاح العام لل receiver.

" hash Function "

a public function that maps a message of any length into a fixed length, hash value. which service as authentication.

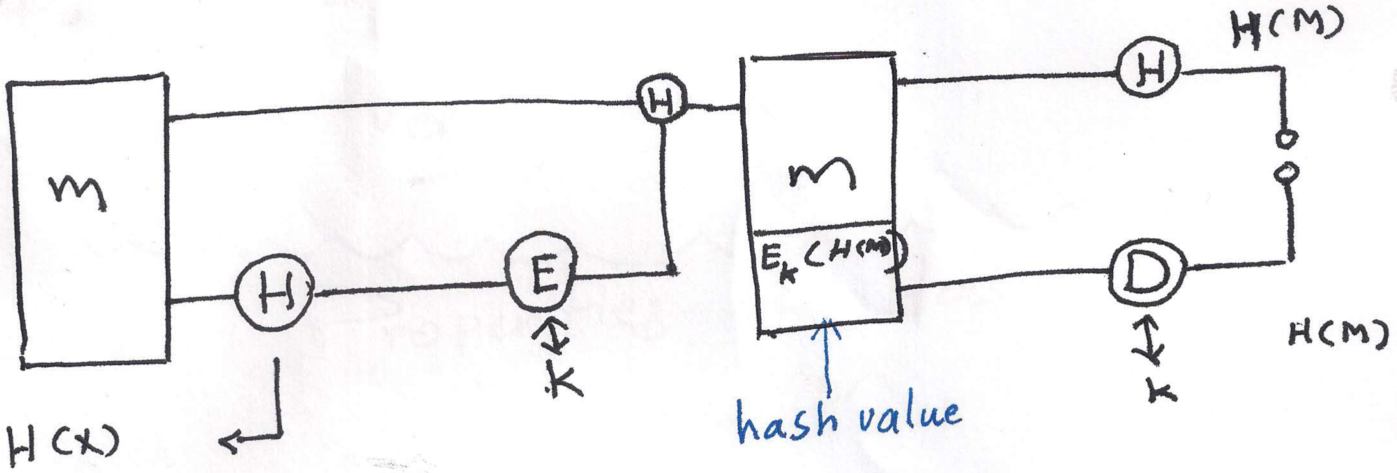
hash value is generated by function H in the form of.

$$\left[h = H(M) \right]$$

where $\underline{\underline{h}}$ is the msg of variable length.

$\underline{\underline{H(M)}}$ means afixed length of hash value.

" uses of hash function "



as shown in the diagram, hash function is used as amessage authentication.

→ Sender with generated hash value H(M) which is encrypted by using secret key (k) and hash value is combined with the msg.

→ at the receiver for the receive msg hash value is calculated which is compared with decrypted received hash value,