both hash value are same then it's Assure the message authentication has been verify.

Properties of Hash function.

1- H can be apply to block of data of any size.

2- H produce a fixed length output known as hash value or hash code.

3- H(M) is relatively easy to calculate For any given msg.

4- For any given value h it is very difficult to fined msg x such that $H(x) = h$ and this known as "one way property"

or any given block x it is computationally infeasible to find y such that.

$$H(x) = H(y).$$

it is known as (weak collision resistance).

6- it is computationally infeasible to find both x and y such away $H(x) = H(y)$ is known as (strong collision resistance)

مقاوم تصادم

مقاومة التصادم القوية

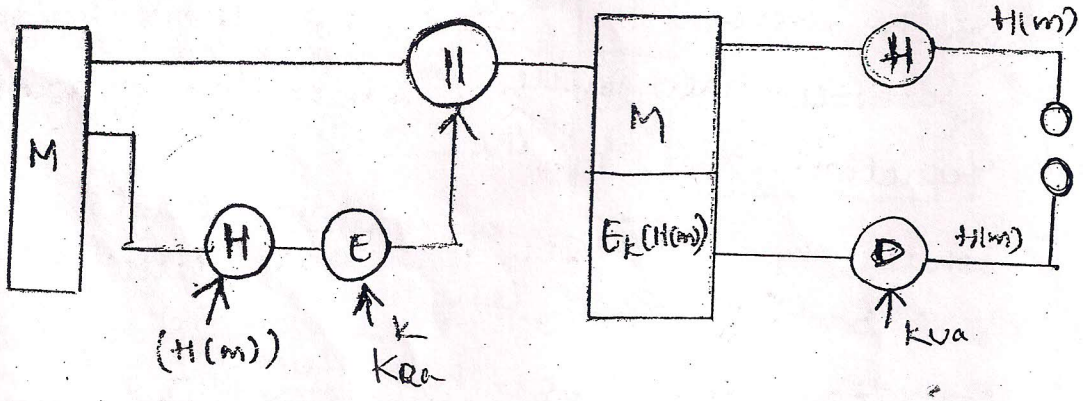
any given message H.

iv) For any given value h it is very difficult to find message x such that H(x) = h and this is known as one way property

v) For any given block x it is computationaly infeasible (means practically not possible) to find y such that H(x) = H(y) is known as weak collision resistance.

vi) It is computationally infeasible to find both x & y such that H(x) = H(y) is known as strong collision resistance.

* Uses of Hash function:



As shown in the diagram, Hash function is used as message authentication. Sender will generate the Hash value (H(m)) which is encrypted by using secret key K ~~and Hash value is encrypted by using secret key 'k'~~ which is combined with message.

At the receiver for the received message, Hash value is calculated which is compared with decrypted received Hash value.