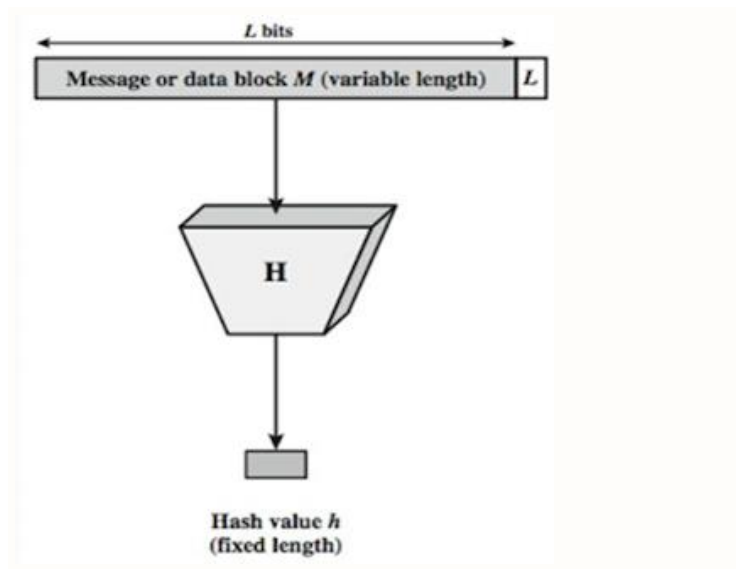


## Introduction of Hash Function

### Introductions

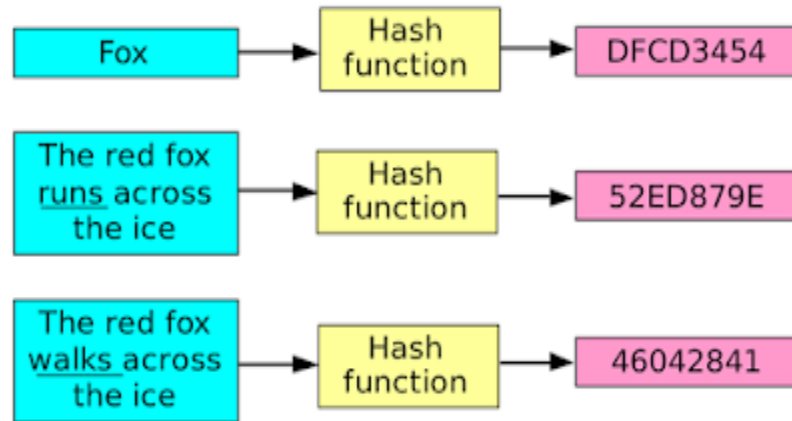
- In hash function  $H$  accepts a variable length block of input data called as 'M' and produces the fixed size hash value can be represented as

$$h = H(M).$$



**Figure: Block Diagram of hash function**

- When hash function provides security, this is called **cryptographic hash functions**.
- Hash function protects the **integrity** of the message. If encryption process is applying on message with hash function, it is also providing **authentication** and **confidentiality**.



- A hash function provides a property that has function applied on variable amount of data (M) and then it produces the fixed amount of output data.
- If any bit or bits changes in the data, then whole hash function output data will also change.
- Cryptographic hash function is **one-way function**, which is practically **infeasible to invert**. The most popular hashing algorithm is MD5 and SHA.

### Properties of hash Function

- ❖ **Compression:** As per compression properties, output of the hash function is much smaller than the size of input.
- ❖ **Pre-image resistance:** Pre-image resistance means difficult to find the input from given hash function output. i.e.,  $x = H(m)$ . So, if  $x$  is given, it is difficult to message  $m$ .

### Characteristics of hash Function

1. It is quick to calculate hash value (h) for any given message. i.e.,  **$x = H(m)$** .
2. Hash function (H) can be applied to **variable length of data block**.
3. A **small change** in a message should **change the hash value**.

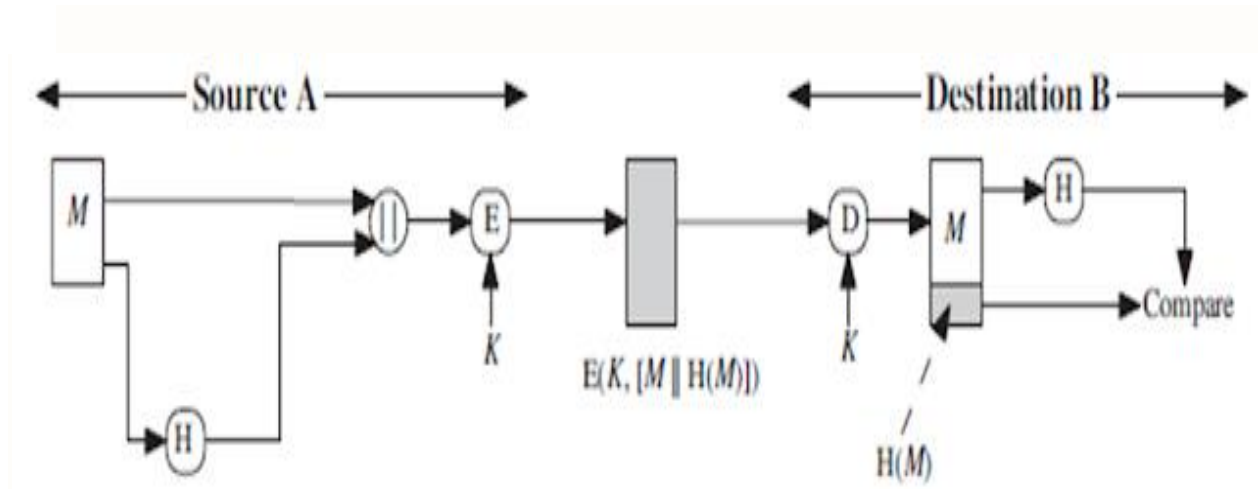
4. Hash function has **one-way property**; it is impossible to generate message from given hash value.
5. The hash function generates very different hash values for similar message.

### **Purpose of Hash Function**

- Purpose of a hash function is to ***verify the integrity of a message***.
- Message authentication is a mechanism or service used to ***achieve authentication***.
- Message authentication and hash function assure that data received are exactly as sent by sender. (i.e., contain no modification, insertion, deletion, or replay).
- In many cases, there is a requirement that the authentication mechanism assures that provide identity of the sender is valid.
- When a hash function is used to provide message authentication, the hash function value is often referred to as a ***message digest***.
- Since a hash is smaller representation of a larger data, it is also referred as a **message digest (MD)**.

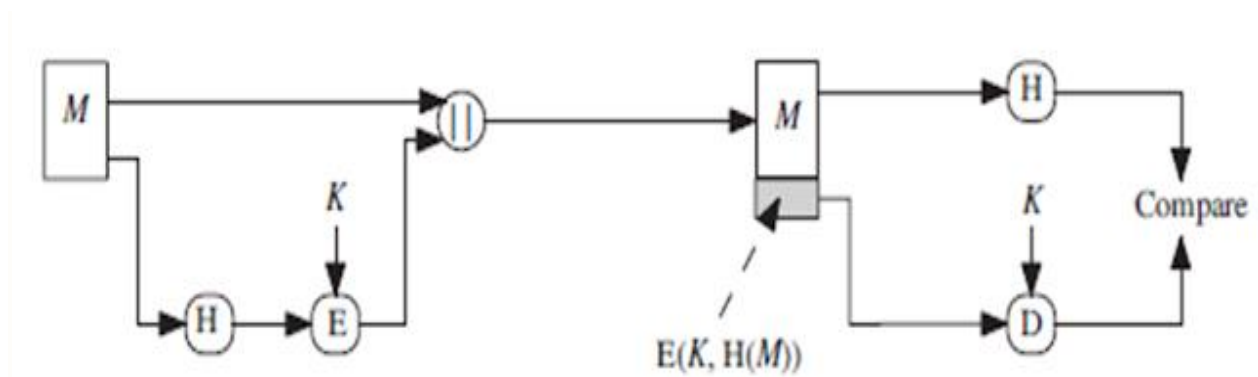
## Application of hash function Using Symmetric Key Cryptography

#1



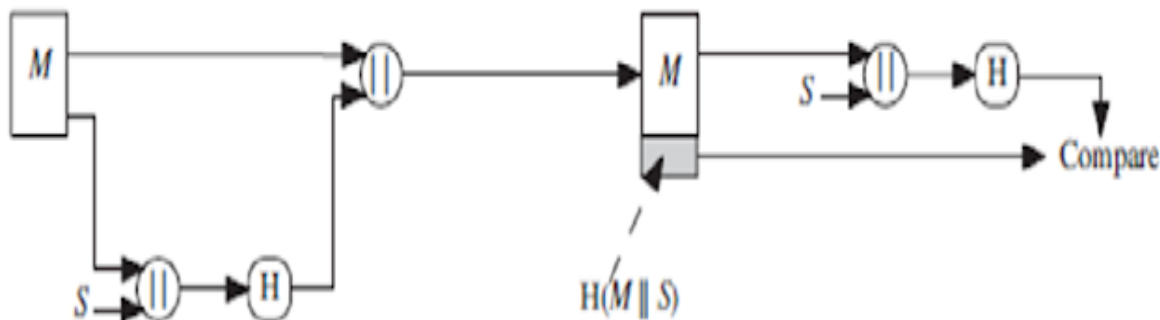
- In above figure, hash code is generating from message and then appended to message. The message plus concatenated hash code is encrypted using symmetric encryption.
- Because only A and B share the secret key( $K$ ), the message must have come from A and has not been altered.
- The hash code provides the structure or redundancy required to achieve authentication.
- Encryption is applied to the entire message plus hash code, confidentiality is also provided.

#2



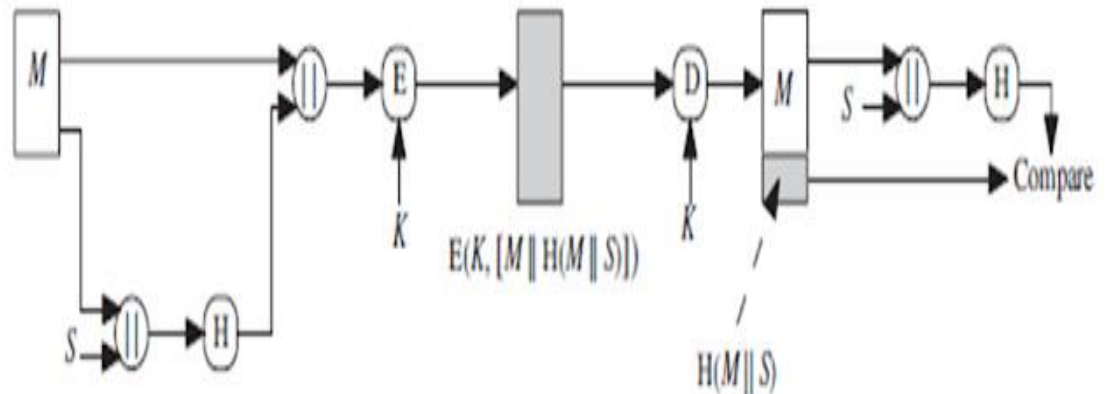
- In above figure, hash code is generated from given message. After generation of hash code, it is encrypted using secret key (K).
- Then encrypted hash code is append with original message and send to the receiver.
- It reduces the processing burden for those applications that do not require confidentiality.

#3



- It is possible to use a hash function but no encryption for message authentication.
- The technique assumes that the two communicating parties share a common secret value  $S$ .
- A compute the hash value over the concatenation of  $M$  and  $S$ , appends the resulting hash value to  $M$ .
- Because B possesses, it can recompute the hash value to verify. Because the secret value itself is not sent, an opponent cannot modify an intercepted message and cannot generate a false message.

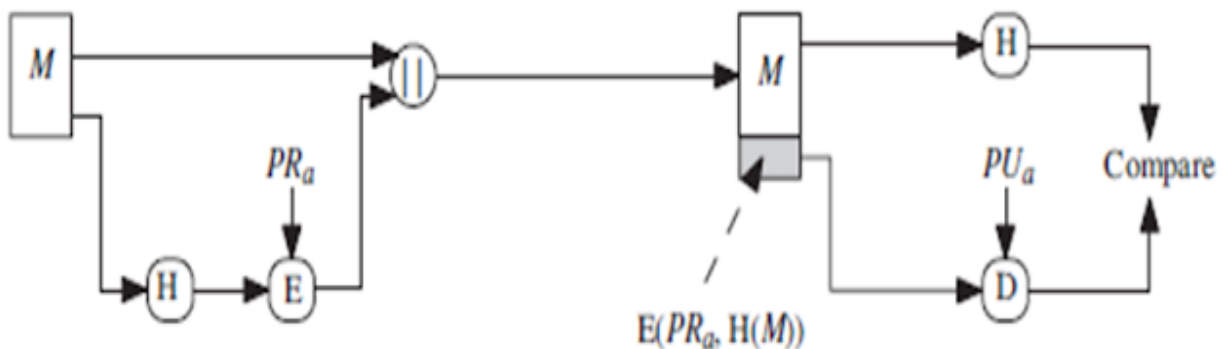
#4



- Confidentiality can be added to the approach of previous method by encrypting the entire message plus the hash code.
- When confidentiality is not required, method (2) has an advantage over methods (1) and (4), which encrypts the entire message, in that less computation is required.

## Application of hash function Using Asymmetric Key Cryptography

#1

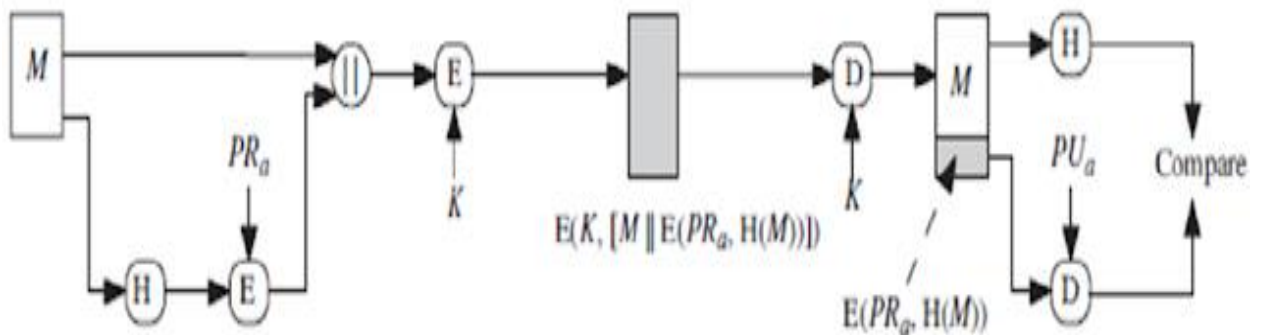


- Another important application, which is similar to the message authentication application, is the digital signature.
- Purpose of digital signature is verified sender's signature to achieve authentication. In the case of the digital signature, the

hash value of a message is encrypted with a user's private key  $PR_a$ .

- Anyone who knows the user's public key  $PU_a$  can verify the integrity of the message.
- It also provides a digital signature, because only the sender could have produced the encrypted hash code.

#2



- In above figure, hash code is encrypted using user's private key. Then encrypted hash code appended to the message.
- Now, message plus hash is encrypted using symmetric secret key ( $K$ ).
- Using above diagram, we can achieve **confidentiality** as well as **authentication**.
- Figure A and B both are **hash code based digital signature**.

