

## Message authentication

- Verifying the user identity is Authentication.
- An authenticator must be there to authenticate the message.
- An authenticator is generated with the help of authentication function.
- An authenticator is a value use to authenticate a message
- authentication function is a function which is use to produce an authenticator and that authenticator is use to authenticate a message.
- "Message authentication is a procedure to verify that received messages come from the alleged source and have not been altered."
- "A digital signature is an authentication technique that also includes measures to counter repudiation by either source or destination."

## Types of authentication function or types of function to produce authenticator.

Three main classes of **Authentication Functions** used in cryptography:

### 1. Message Encryption

- The entire message is encrypted.
- The resulting ciphertext acts as an **authenticator**.
- Authentication comes inherently through confidentiality.

## 2. Message Authentication Code (MAC)

- We will have some authentication function and we apply them on the plain text along with the key which produces the fixed length code called as MAC.
- Uses a **secret key** and a **public function** of the message.
- Produces a **fixed-length value** (MAC) that authenticates the message.
- MAC will act as **authenticator**.

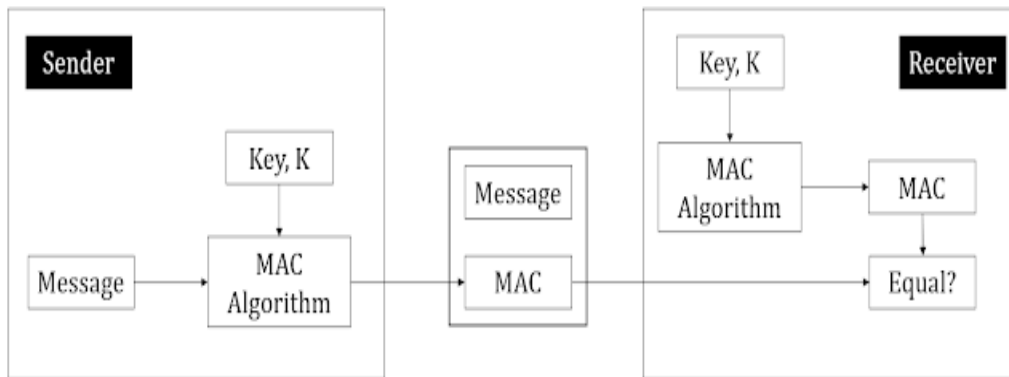
## 3. Hash Functions

- Public function that maps a message of **any length** to a **fixed-length hash value**.
- The hash value acts as the **authenticator**.
- Typically used without a key, so less secure unless combined with other techniques (e.g., HMAC).

## Introduction of MAC (Message Authentication Code)

### Introduction of MAC

- Message authentication is a mechanism or service used to verify the integrity of a message.
- Message authentication guarantees that the sender of the message is authentic.



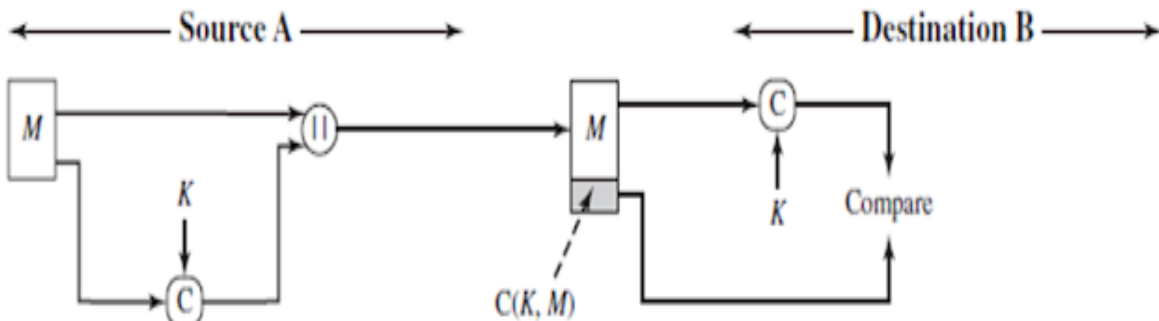
**Figure: Block Diagram of MAC**

- A MAC algorithm, sometimes called a **keyed hash function** accepts as input a secret key an arbitrary-length message to be authenticated, and outputs a MAC.
- MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers to detect any changes.
- The MAC is a small fixed-size block of data that is generated based on a message M of variable length using secret key K as follows.
- MAC is also called **cryptographic checksum**.

$$\text{MAC} = C(K, M)$$

## Application of MAC

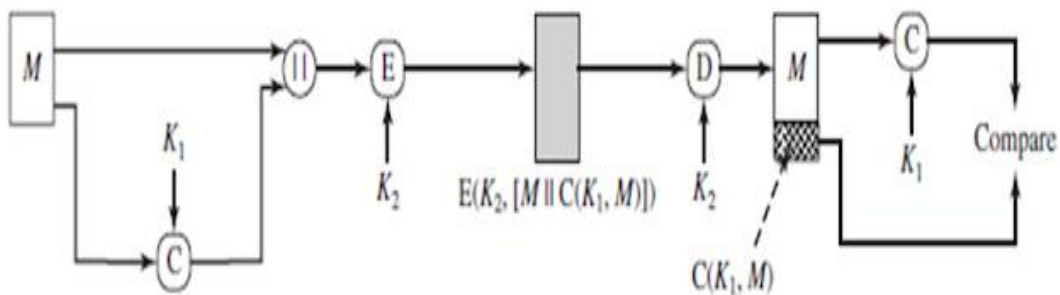
### #1 Message Authentication



**Figure: Message Authentication**

- Sender A want to send message to B via MAC, then the first condition is to share a secret key  $K$ .
- Sender A calculates the MAC from message  $M$  by applying  $K$ . Append MAC to the message  $M$ . A sends the original message  $M$  and the MAC to B.
- When B receives message, B also uses  $K$  to calculate own MAC over message  $M$ . B now compares MAC1 and MAC2.
- If both are same, B assures that message is not altered during transmission.
- If it is not matched, it means B can reject the message.

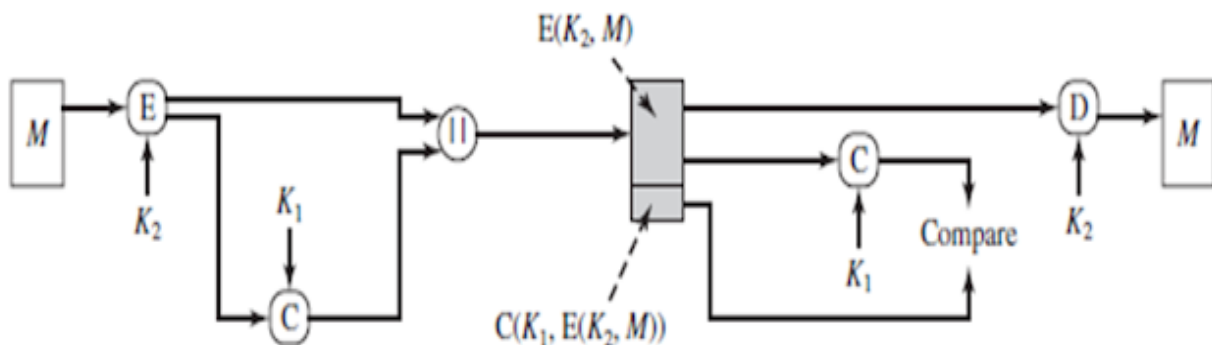
### #2 Message Authentication and Confidentiality; Authentication tied to plain text



**Figure: Message Authentication and Confidentiality**

- Sender A want to send message to B via MAC, then the first condition is to share a secret key  $K_1$ .
- Sender A calculates the MAC from message  $M$  by applying  $K_1$ . Append MAC to the message  $M$ . Encrypt message and appended MAC using key  $K_2$ .
- A sends the generate cipher text (Message + MAC) to B. When B receives cipher text, decrypt using key  $K_2$ .
- B also uses  $K_1$  to calculate own MAC over message  $M$ . B now compares MAC1 and MAC2.
- If both are same, B assures that message is not altered during transmission. If it is not matched, it means B can reject the message.

### #3 Message Authentication and Confidentiality; Authentication tied to cipher text



**Figure: Message Authentication and Confidentiality**

- Sender A want to send message to B via MAC, then the first condition is to share a secret key  $K_1$ .
- Sender A encrypt the message and generate cipher text using key  $K_2$ . Sender A calculates the MAC from cipher text by applying  $K_1$ . Then append MAC to cipher text.
- A send appended cipher text plus MAC to B. When B receives message, B also uses  $K_1$  to calculate own MAC over message  $M$ . Decrypt ciphertext using  $K_2$  and get original message.

- B now compares MAC1 and MAC2. If both are same, B assures that message is not altered during transmission.
- If it is not matched, it means B can reject the message.

### **Importance of MAC:**

- MAC ensures that only receiver can identify the original message. Even if attacker modifies the message M, but cannot modify MAC.
- In case of MAC is modified by attacker, receiver's calculations of MAC will differ from it. MAC cannot modify easily because MAC is encrypted by secret key K, but key is only known by sender and receiver only.
- MAC is one-way function. MAC provides data integrity and authentication both.
- Also apply encryption and achieve confidentiality.