Authentic Function

Authentication:-Verify the user's identity

A----->B

A send messge to B then it must be check to authenticate.

An authenticator must be there to authenticate the message.

Authenticator:-it is a value used to authenticate the message.

Authenticator function:-it is a function that is used to authenticate the message.

Authentication:-

1. It is one of the 5 principle of security.
2. Verifying the authenticity of the message is important.
3. An authenticator must be there to authenticate the message.

Types of Authentication(types of fn to produce authentication):

1.Message encryption:-cipher text act as a aunthenticator.

2.**MAC(Message authentication code):-** fixed length code

it have some authentication function and apply their on the plain text along with the key which produce a fixed length code called MAC.

C(M,K)=fixed length code(MAC){act as an Authnticator)(compressed data)

Here C=Authentication function, M-message,K-Key

3.**Hash function**:-hash value(message digest)

1. independent of key (key not used)

H(M)=fixed length code(hash code ‘h’) (message digest)

Here hash code act as an authenticator)

Message Digest is used to ensure the integrity of a message transmitted over an insecure channel (where the content of the message can be changed). The message is passed through a Cryptographic hash function. This function creates a compressed image of the message called **Digest**.

Authentication :-Authentication is the mechanism to identify the user or system or the entity. It ensures the identity of the person trying to access the information. The authentication is

mostly secured by using username and password. The authorized person whose identity is preregistered can prove his/her identity and can access the sensitive information.

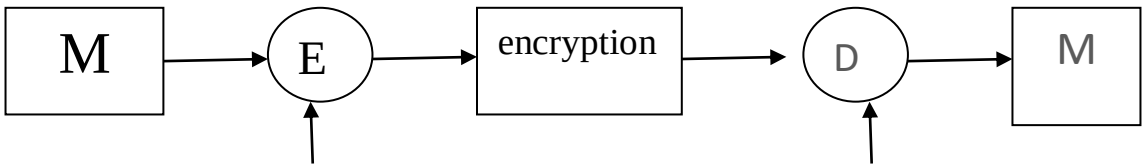
Confidentiality

The degree of confidentiality determines the secrecy of the information. The principle specifies that only the sender and receiver will be able to access the information shared between them. Confidentiality compromises if an unauthorized person is able to access a message.

For example, let us consider sender A wants to share some confidential information with receiver B and the information gets intercepted by the attacker C. Now the confidential information is in the hands of an intruder C.

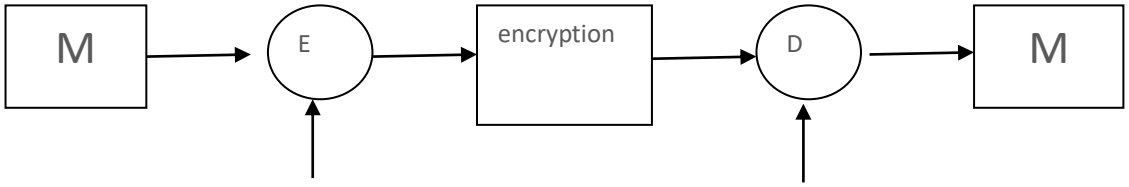
1.**Message encryption**:-cipher text is an authenticator

1. Symmetric encryption



Here Key K1 shared only between sender & Receiver.

1. For Asymmetric encryption(Confidentiality achieved but not authentication)



Sender $K_{publicB}$ Cipher text $K_{privateB}$ Receiver

Here public key is known to all.

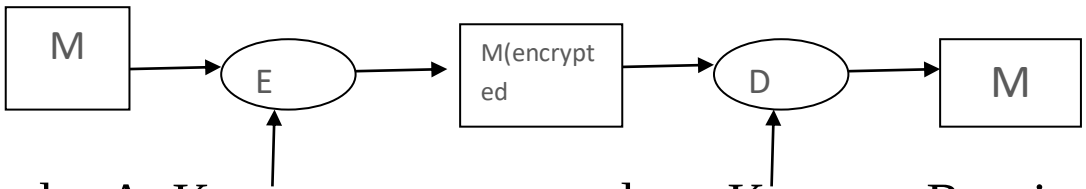
Not authentication because receiver don't know whose send the encrypted data.

Confidentiality achieved because only B(receiver) decrypt

The cipher text to plain text.

So In this Confidentiality achieved but not authentication(not authorize who sent).

2. Asymmetric encryption(Authentication achieved but not confidentiality)



Sender A $K_{privateA}$ encrypted $K_{publicA}$ Receiver B

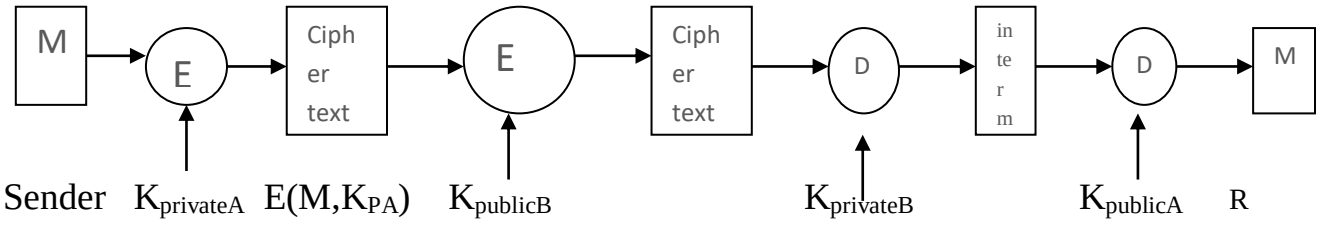
When used private key of A is used then but decrypt by public key so anyone can decrypt so not confidentiality.

Authentication achieved because any receiver who match with private key only they decrypt the message.

So Confidentiality not achieved because any one can decrypt.but authentication achieved.

4.Symmetric encryption(both Authentication & Confidentiality):-

In this two time encryption and two time decryption.



Authentication achieve because at last decryption public key of A used so it know encrypt by private key of A.

Confidentiality achieved because private key of B decrypt only .only it decrypt

So in this confidentiality and authentication achieved.

2.MAC(message Authentication Code):-

1.In this use a secret key to generate a small fixed size blocks of data called MAC .

2. it is then appended with the message.

3. the communicating parties will share a secret common key (which will be used to create the MAC).

Let A-sender

B-Receiver

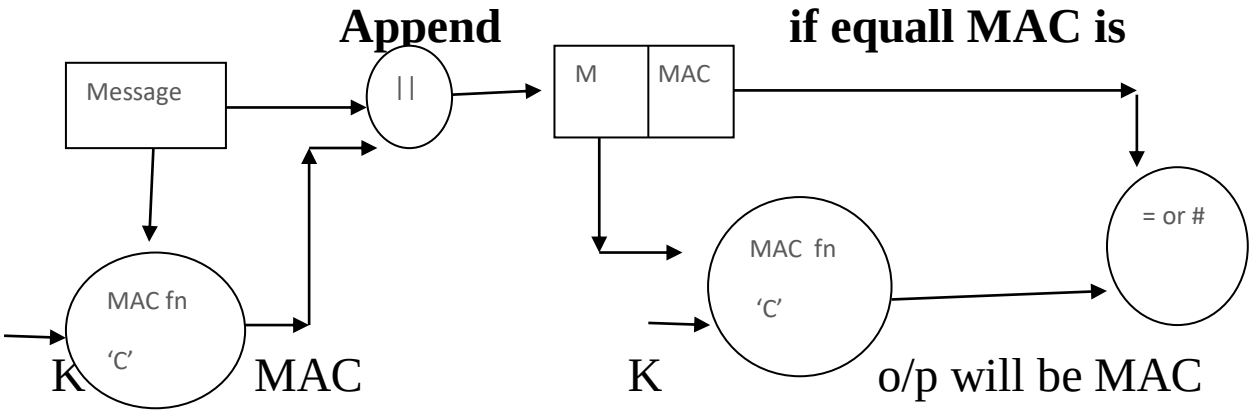
If input is 1MB then compress into 1kB(fixed size data)

When A sends a message to B:-it calculate the MAC as a function of the message and the key.

M=C(K,M) {here C-hash fn, M-i/p message,

K-shared secret key)

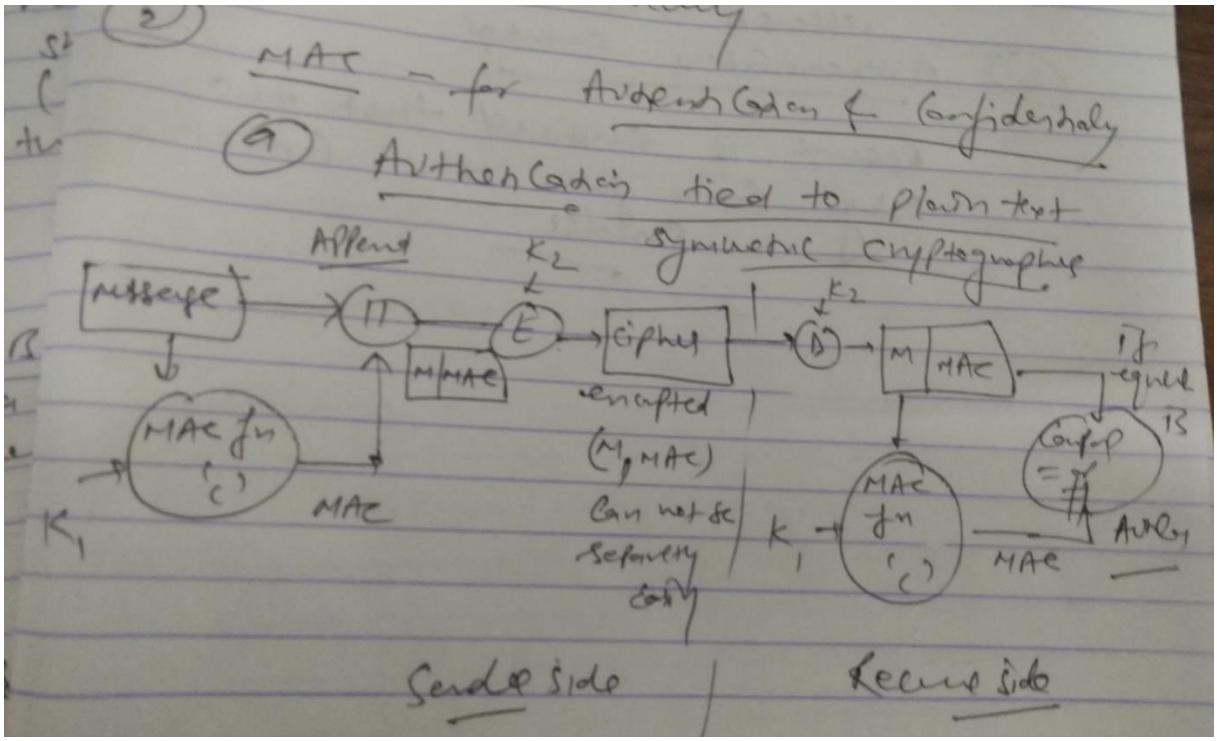
1.MAC for Authentication:-



If both Mac are equall then authentication.

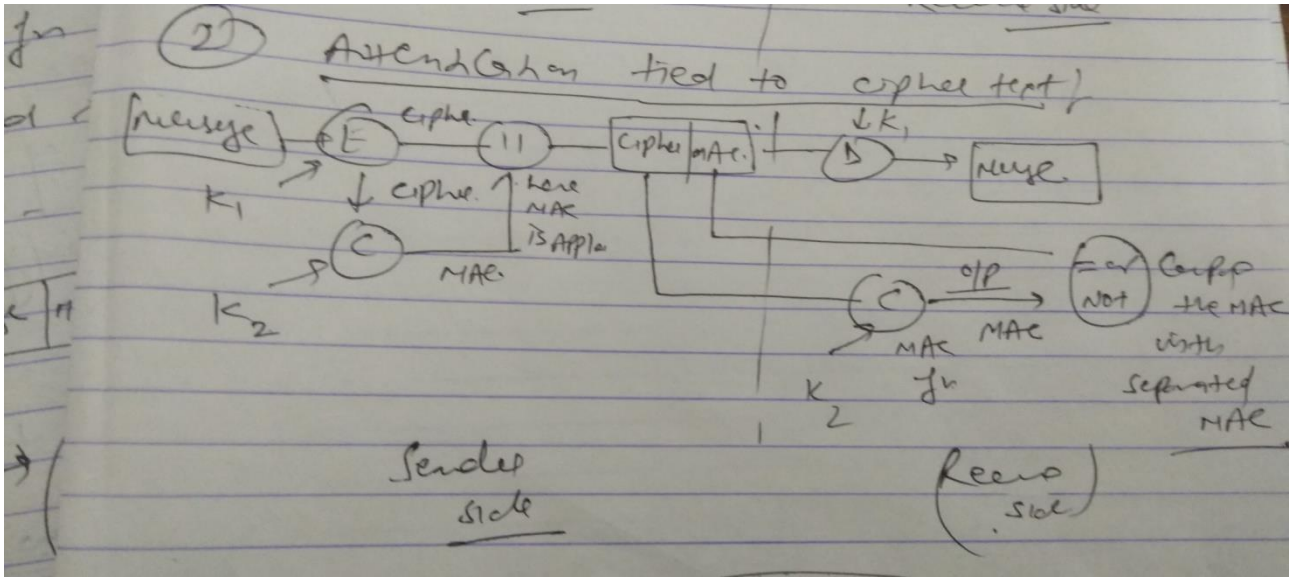
1. In this separate the message and the MAC.
2. only authentication.
3. No confidentiality because If third party come in between then he can get so no security.

1. MAC –for Authentication & Confidentiality
   (A) Authentication tied to plain text



Message is append with MAC so it is called tied with plain text

(B) Authentication tied to cipher text :-



Significance of MAC:-

1.Ensure that Receiver known whether the message has been altered or not

2.Authentication ensured (Receiver is ensured that the message come from the correct sender).