Authentication

- Authentication is used by a server when the server needs to know exactly who is accessing their information or site.
- Authentication is used by a client when the client needs to know that the server is system it claims to be.
- In authentication, the user or computer has to prove its identity to the server or client.
- Usually, authentication by a server entails the use of a user name and password. Other ways to authenticate can be through cards, retina scans, voice recognition, and fingerprints.
- Authentication by a client usually involves the server giving a certificate to the client in which a trusted third party such as Verisign or Thawte states that the server belongs to the entity (such as a bank) that the client expects it to.
- Authentication does not determine what tasks the individual can do or what files the individual can see. Authentication merely identifies and verifies who the person or system is.

Message Authentication Code (MAC)

We will have some authentication function and we apply them on the plaintext along with the key which produced a fixed length code called MAC.

That is: **C (M,K) = FIXED LENGTH CODE (MAC)**

NOTE: C=AUTHENTICATION FUNCTION

M=MESSAGE

K=KEY

- Message authentication ensures that the message has been sent by a genuine identity and not by an imposter.

• The service used to provide message authentication is a **Message Authentication Code (MAC).**

• A MAC uses a keyed hash function that includes the symmetric key between the sender and receiver when creating the digest.

• Figure shows how a sender A uses a keyed hash function to authenticate his message and how the receiver B can verify the authenticity of the message.

• This system makes use of a symmetric key shared by A and B.

• A, using this symmetric key and a keyed hash function, generates a MAC.

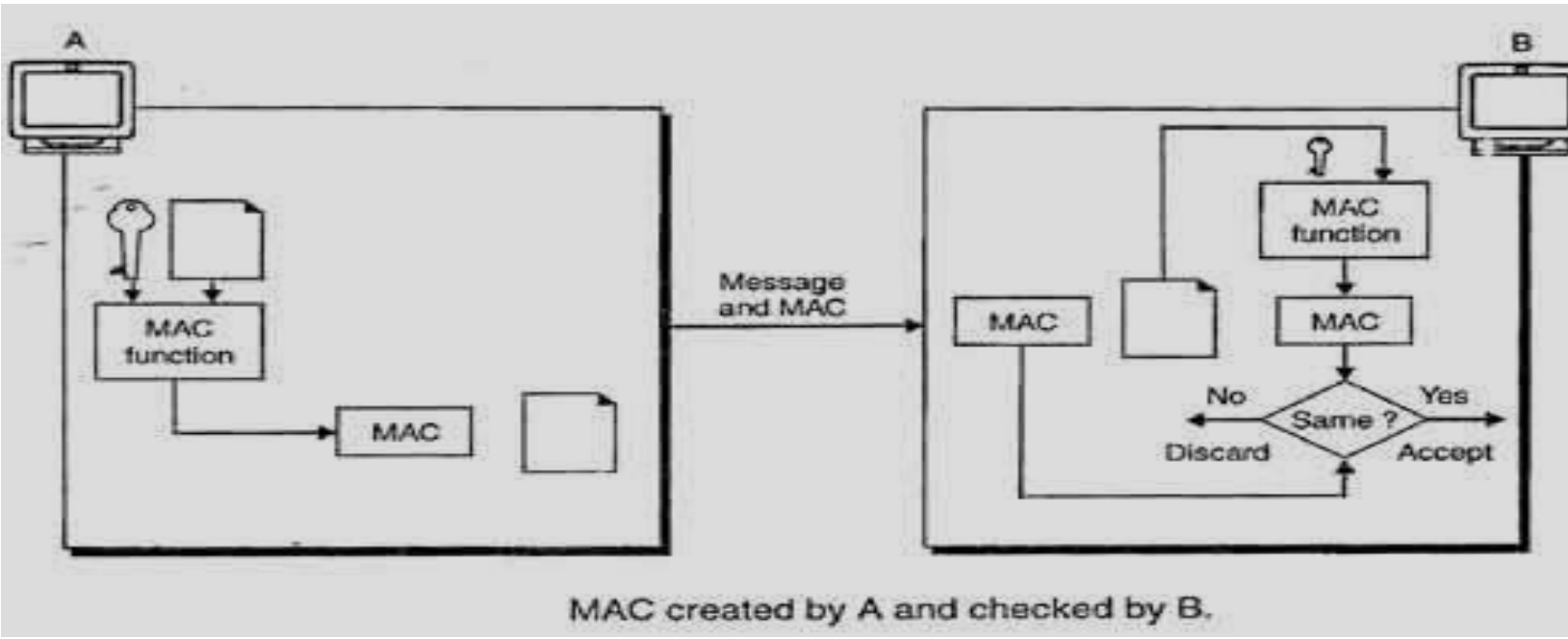
• A then sends this MAC along with the original message to B.

• B receives the message and the MAC and separates the message from the MAC.

• B then applies the same keyed hash function to the message using the same symmetric key to get a fresh MAC.

• B then compares the MAC sent by A with the newly generated MAC.

• If the two MACs are identical, it shows that the message has not been modified and the sender of the message is definitely A.



MAC created by A and checked by B.

TASK:

What are the requirements of authentication in cryptography?