MESSAGE AUTHENTICATION CODES

- Message authentication is a mechanism or service used to verify the integrity of a message. Message authentication assures that data received are exactly as sent by (i.e., contain no modification, insertion, deletion, or replay) and that the purported identity of the sender is valid.
- Symmetric encryption provides authentication among those who share the secret key.
- A message authentication code (MAC) is an algorithm that requires the use of a secret key. A MAC takes a variable-length message and a secret key as input and produces an authentication code. A recipient in possession of the secret key can generate an authentication code to verify the integrity of the message.
- One means of forming a MAC is to combine a cryptographic hash function in some fashion with a secret key.
- Another approach to constructing a MAC is to use a symmetric block cipher in such a way that it produces a fixed-length output for a variable length input.

MESSAGE AUTHENTICATION REQUIREMENTS

In the context of communications across a network, the following attacks can be identified.

- 1. Disclosure: Release of message contents to any person or process not possessing the appropriate cryptographic key.
- 2. Traffic analysis: Discovery of the pattern of traffic between parties. In a connection-oriented application, the frequency and duration of connections could be determined. In either a connection-oriented or connectionless environment, the number and length of messages between parties could be determined.
- 3. Masquerade: Insertion of messages into the network from a fraudulent source. This includes the creation of messages by an opponent that are purported to come from an authorized entity. Also included are fraudulent acknowledgments of message receipt or nonreceipt by someone other than the message recipient.
- 4. Content modification: Changes to the contents of a message, including insertion, deletion, transposition, and modification.
- 5. Sequence modification: Any modification to a sequence of messages between parties, including insertion, deletion, and reordering.
- 6. Timing modification: Delay or replay of messages. In a connection-oriented application, an entire session or sequence of messages could be a replay of some previous valid session, or individual messages in the sequence could be delayed or replayed. In a connectionless application, an individual message (e.g., datagram) could be delayed or replayed.
- 7. Source repudiation: Denial of transmission of message by source.

- 8. Destination repudiation: Denial of receipt of message by destination.
- Measures to deal with the first two attacks are in the realm of message confidentiality
- Measures to deal with items (3) through (6) in the foregoing list are generally regarded as message authentication.
- Mechanisms for dealing specifically with item (7) come under the heading of digital signatures.
- Generally, a digital signature technique will also counter some or all of the attacks listed under items (3) through (6).
- Dealing with item (8) may require a combination of the use of digital signatures and a protocol designed to counter this attack.

MESSAGE AUTHENTICATION FUNCTIONS

- Any message authentication or digital signature mechanism has two levels of functionality. At the lower level, there must be some sort of function that produces an authenticator: a value to be used to authenticate a message.
- This lower-level function is then used as a primitive in a higher-level authentication protocol that enables a receiver to verify the authenticity of a message.
- This section is concerned with the types of functions that may be used to produce an authenticator.
- These may be grouped into three classes.
    - Hash function: A function that maps a message of any length into a fixed length hash value, which serves as the authenticator
    - Message encryption: The ciphertext of the entire message serves as its authenticator

Message authentication code (MAC): A function of the message and a secret key that produces a fixed-length