Authentication Basics

DR. VASUDHA ARORA

VASUDHA.ARORA@GDGU.ORG, VASUDHARORA6@GMAIL.COM

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

GD GOENKA UNIVERSITY, GURUGRAM

Authentication Basics

- Authentication is the process of validating the identity of a user or the integrity of a piece of data.
- There are three technologies that provide authentication
  - Message Digests / Message Authentication Codes
  - Digital Signatures
  - Public Key Infrastructure
- There are two types of user authentication:
  - Identity presented by a remote or application participating in a session
  - Sender’s identity is presented along with a message.

Security Attacks

- disclosure
- traffic analysis

} Confidentiality

- masquerade
- content modification
- sequence modification
- timing modification

} Authentication

- source repudiation
- destination repudiation

} Digital Signatures

Message Authentication functions

- message authentication is concerned with:
  - protecting the integrity of a message
  - validating identity of originator
  - non-repudiation of origin (dispute resolution)

- Any message Authentication or digital signature mechanisms have 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 the message.
  - This function is then used as a primitive in a higher level authentication protocol that enables a receiver to verify the authenticity of the message

Message Authentication functions

- Functions used to produce authenticator are grouped into three classes:
  - **Hash Functions:** A function that maps a message of any length into a fixed length hash value, which serves as the authenticator.
  - **Message Encryption:** The cipher text of entire message serves as its authenticator.
  - **Message Authenticated Code (MAC):** A function of the message and a secret key that produces a fixed-length value that serves as the authenticator

Message Encryption

- Message encryption by itself also provides a measure of authentication
- if symmetric encryption is used then:
  - receiver know sender must have created it
  - since only sender and receiver now key used
  - know content cannot of been altered
  - if message has suitable structure, redundancy or a checksum to detect any changes
- if public-key encryption is used:
  - encryption provides no confidence of sender
  - since anyone potentially knows public-key
  - however if
    - sender **signs** message using their private-key
    - then encrypts with recipients public key
    - have both secrecy and authentication
  - again need to recognize corrupted messages
  - but at cost of two public-key uses on message

BASIC USES OF MESSAGE ENCRYPTION

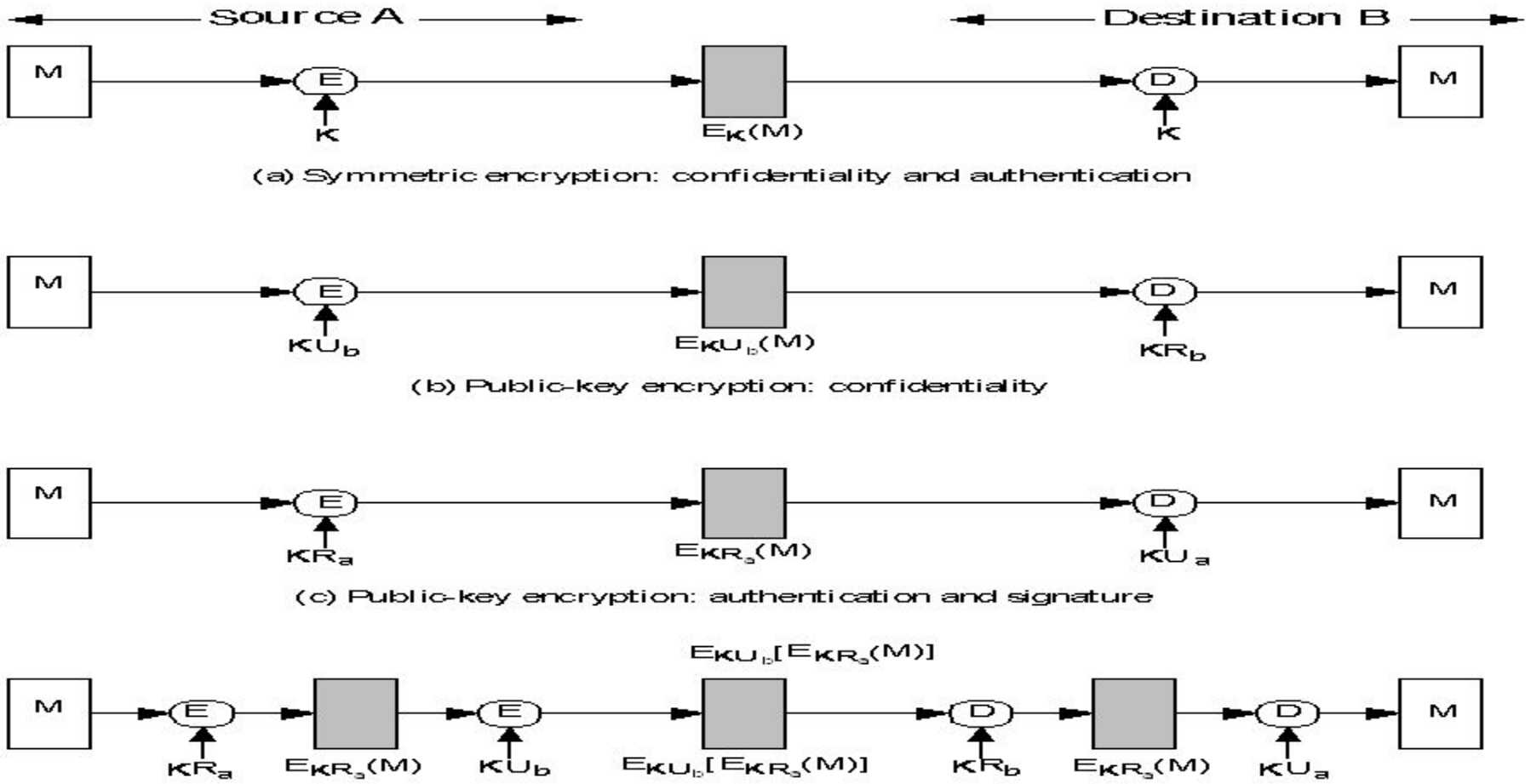
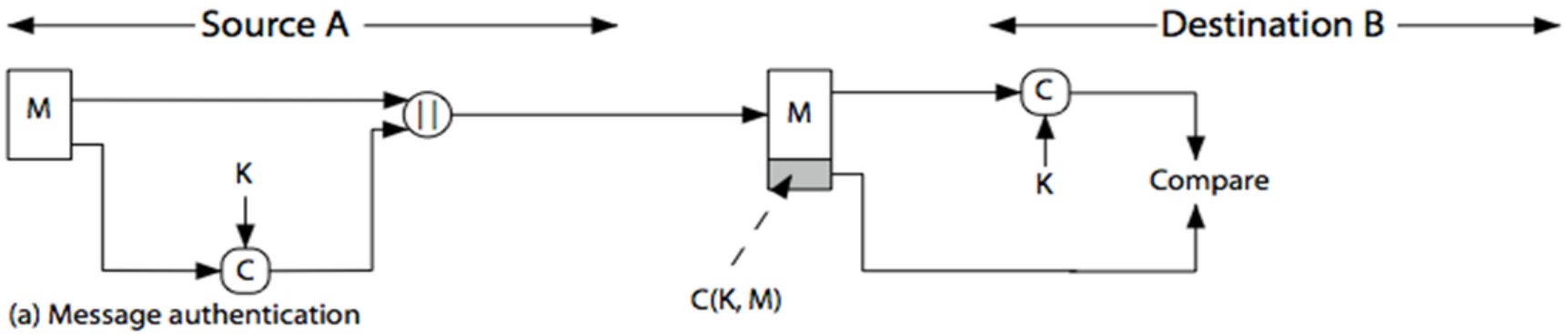


Figure 11.1 Basic Uses of Message Encryption

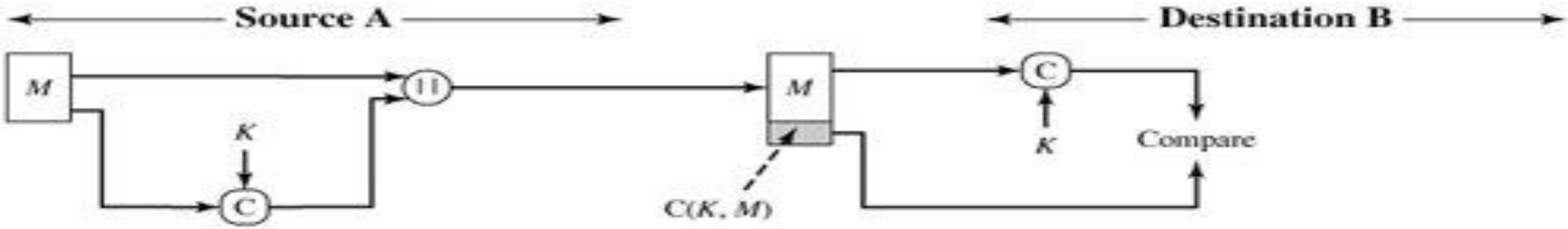
MAC-Message Authentication Codes

- A MAC function is similar to encryption, with only one difference, i.e., a MAC function need nod be reversible, as an encryption algorithm for decryption.
- For establishing MAC process, the sender and receiver share a symmetric key K.
- Essentially, a MAC is an encrypted checksum generated on the underlying message that is sent along with a message to ensure message authentication.

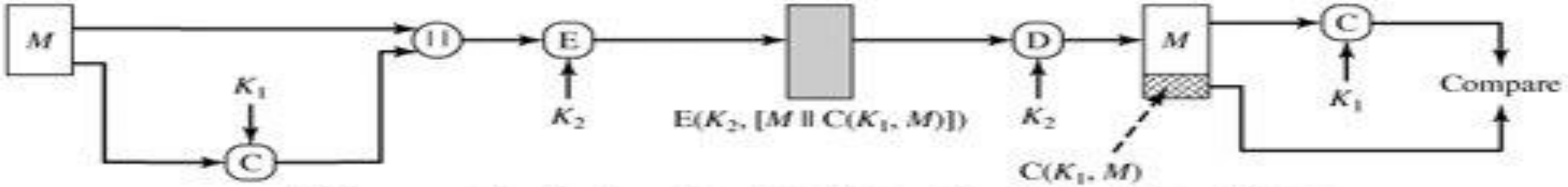


MAC-Message Authentication Codes

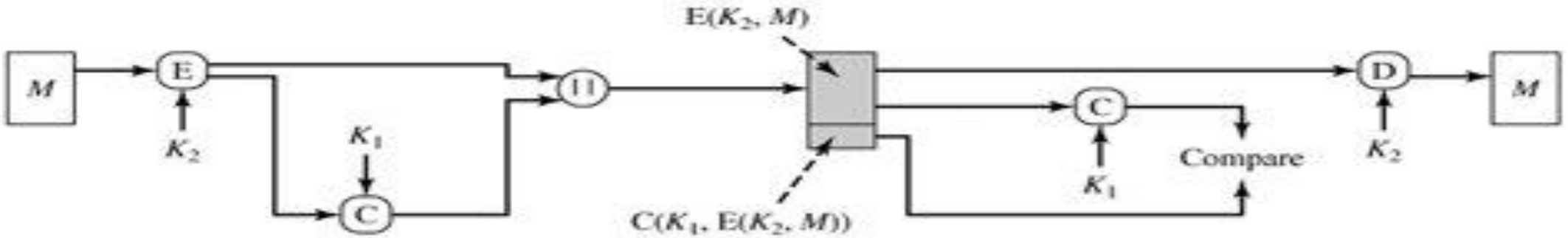
- The sender uses some publicly known MAC algorithm, inputs the message and the secret key K and produces a MAC value.
- Similar to hash, MAC function also compresses an arbitrary long input into a fixed length output. The major difference between hash and MAC is that MAC uses secret key during the compression.
- The sender forwards the message along with the MAC. Here, we assume that the message is sent in the clear, as we are concerned of providing message origin authentication, not confidentiality. If confidentiality is required then the message needs encryption.
- On receipt of the message and the MAC, the receiver feeds the received message and the shared secret key K into the MAC algorithm and re-computes the MAC value.
- The receiver now checks equality of freshly computed MAC with the MAC received from the sender. If they match, then the receiver accepts the message and assures himself that the message has been sent by the intended sender.
- If the computed MAC does not match the MAC sent by the sender, the receiver cannot determine whether it is the message that has been altered or it is the origin that has been falsified. As a bottom-line, a receiver safely assumes that the message is not the genuine.



(a) Message authentication



(b) Message authentication and confidentiality; authentication tied to plaintext



(c) Message authentication and confidentiality; authentication tied to ciphertext

Advantages of MAC

- Assuming only sender and receiver know the identity of the secret key and if the received MAC matches the calculated MAC then:
  - The receiver is assured that the message has not been altered.
  - The receiver is assured that the message is from the alleged sender.
  - If a message includes a sequence number then the receiver is assured of proper sequence because an attacker cannot successfully alter the sequence number.

Limitations of MAC

- **Establishment of Shared Secret:**
  - It can provide message authentication among pre-decided legitimate users who have shared key.
  - This requires establishment of shared secret prior to use of MAC.
- **Inability to Provide Non-Repudiation:**
  - Non-repudiation is the assurance that a message originator cannot deny any previously sent messages and commitments or actions.
  - MAC technique does not provide a non-repudiation service. If the sender and receiver get involved in a dispute over message origination, MACs cannot provide a proof that a message was indeed sent by the sender.
  - Though no third party can compute the MAC, still sender could deny having sent the message and claim that the receiver forged it, as it is impossible to determine which of the two parties computed the MAC.

why use a MAC?

- sometimes only authentication is needed
- sometimes need authentication to persist longer than the encryption (eg. archival use)

note that a MAC is not a digital signature

need the MAC to satisfy the following:

1. knowing a message and MAC, it is infeasible to find another message with same MAC
2. MACs should be uniformly distributed
3. MAC should depend equally on all bits of the message

MAC Properties

a MAC is a cryptographic checksum

$MAC = C_K(M)$

- condenses a variable-length message M
- using a secret key K
- to a fixed-sized authenticator

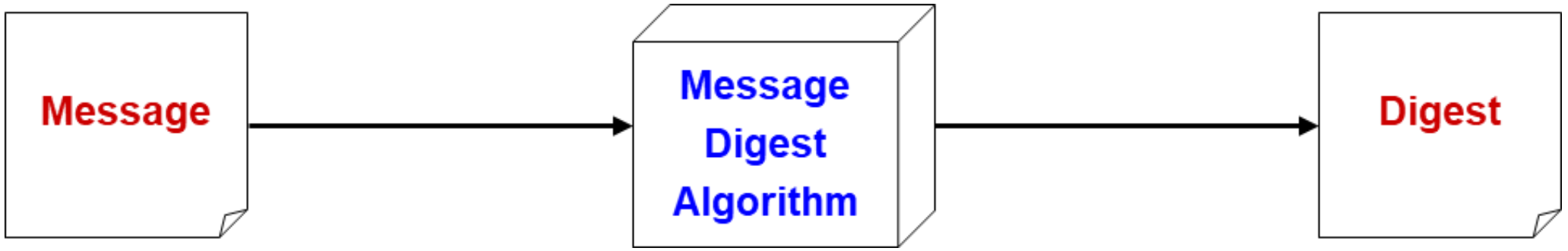
is a many-to-one function

- potentially many messages have same MAC
- but finding these needs to be very difficult

Message Digest/Hash

- A message digest is a fingerprint for a document
- Purpose of the message digest is to provide proof that data has not altered
- Process of generating a message digest from data is called hashing
- Hash functions are one way functions with following properties
  - Infeasible to reverse the function
  - Infeasible to construct two messages which hash to same digest
- Commonly used hash algorithms are
  - MD5 – 128 bit hashing algorithm by Ron Rivest of RSA
  - SHA & SHA-1 – 162 bit hashing algorithm developed by NIST

Idea of Message Digest/Hash



- The idea of message digests is based on the principle that it should not reveal or tell anything about the original message.
- The Message digest algorithms or hash functions are generally certain mathematical operations that are applied over a block of data to produce its hash or digest which is always smaller in size then the original message
- The major difference between hash and MAC is that MAC uses secret key during the compression. Hash functopns do not require any secret key.

Requirements of a Message Digest

1. Given a message, it should be very easy to find its corresponding message digest.
2. For a given message the message digest must always be same
3. Given a message digest, it should be very difficult to find the original message for which the digest was created.
4. Given two messages, if we calculate their message digests, the two message digests must be different. If two messages produce same message digests, it is called as collision, chances of two message digests being same are one in 2^{180} or 2^{160} , which is rarely possible in practice.
5. Even a small changes in two original messages can cause the message digests to differ vastly. The MD of two extremely similar messages are so different that they provide no clue at all that original messages were similar to each other.

Examples of message digests