# Hash Functions

- A hash function H accepts a variable-length block of data *M* as input and produces a fixed-size hash value
  - $h = \mathrm{H}(M)$
  - Principal object is data integrity
- Cryptographic hash function
  - An algorithm for which it is computationally infeasible to find either:

    (a) a data object that maps to a pre-specified hash result (the one-way property)

    (b) two data objects that map to the same hash result (the collision-free property)

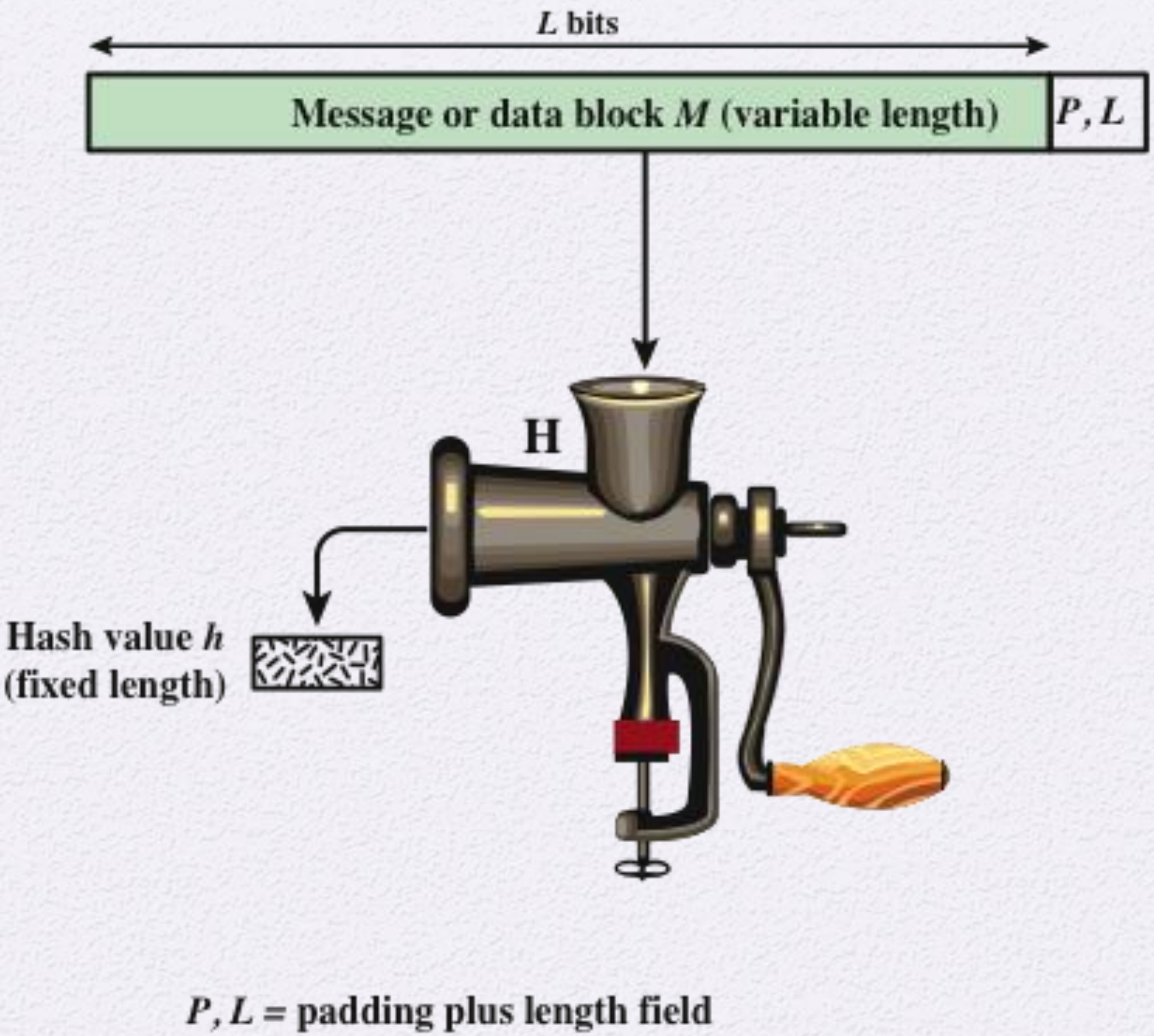
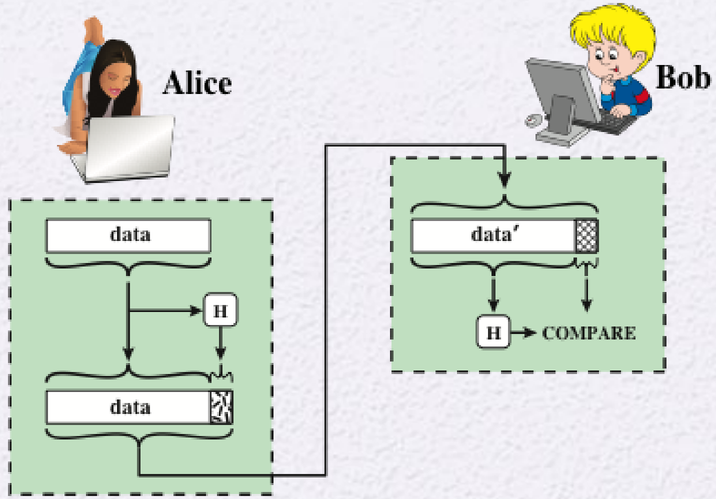
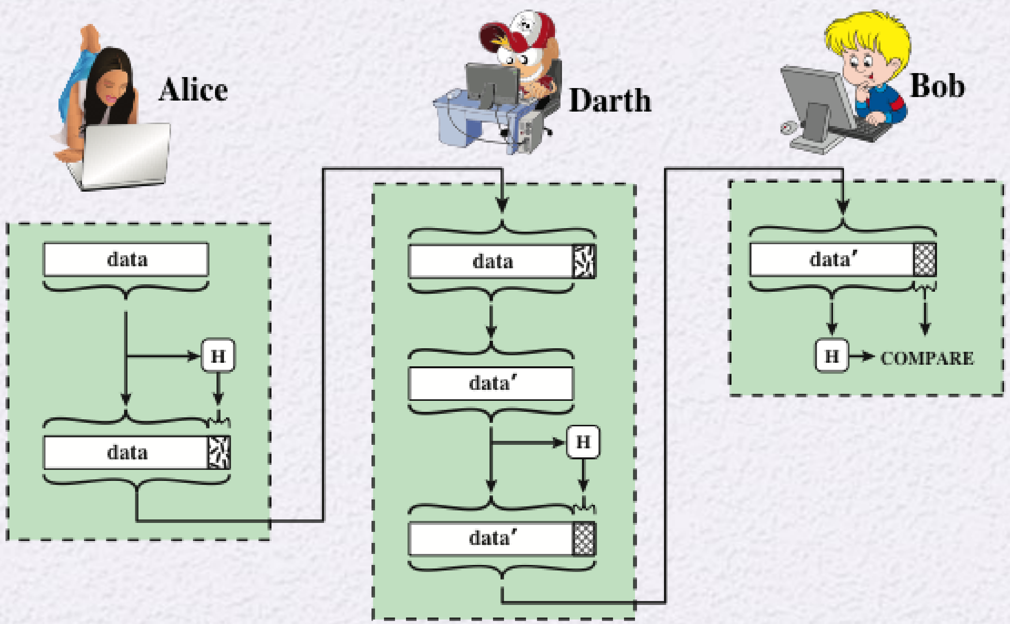



**Figure 11.1 Cryptographic Hash Function; $h = H(M)$**




(a) Use of hash function to check data integrity

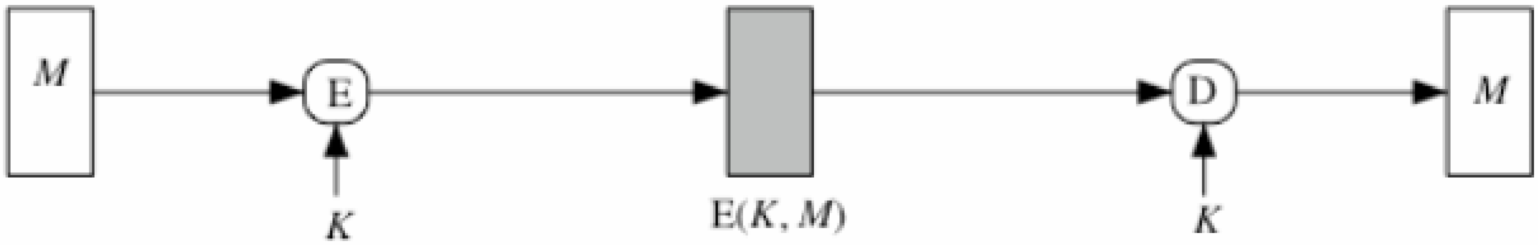



(b) Man-in-the-middle attack

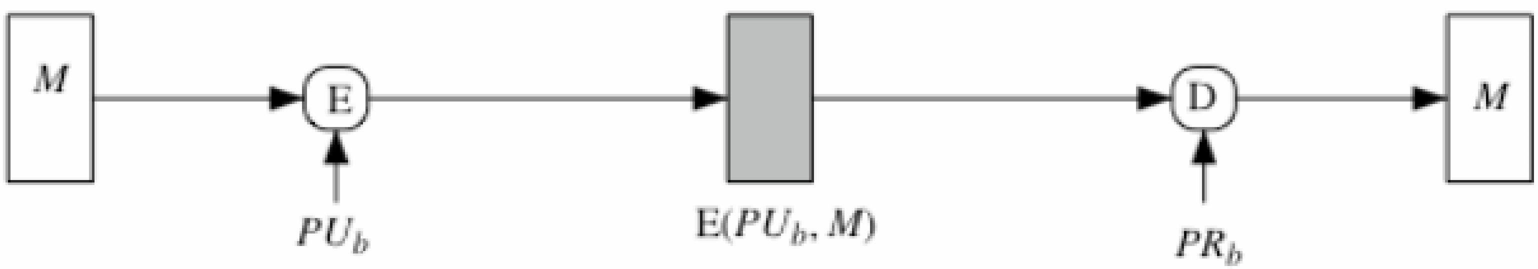
Figure 11.2 Attack Against Hash Function

- message authentication is concerned with:
  - protecting the integrity of a message validating
  - identity of originator
  - non-repudiation of origin (dispute resolution)
- three alternative functions used:
  - message encryption
  - message authentication code (MAC)
  - hash function

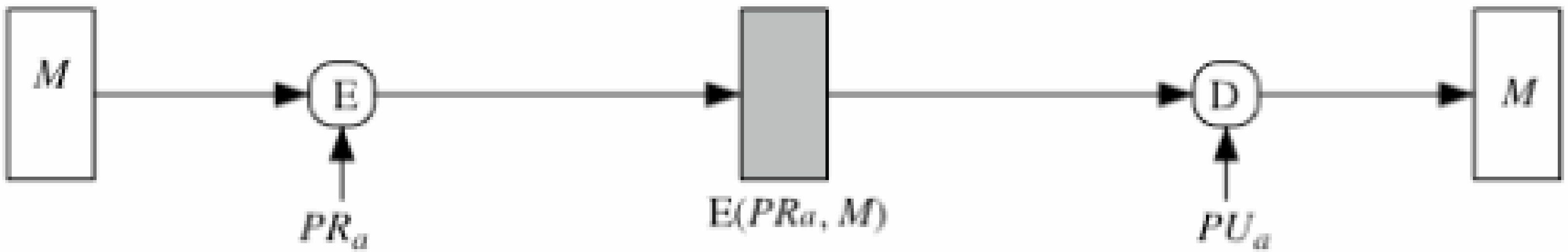
- Message authentication is a mechanism or service used to verify the integrity of a message.
- Message authentication assures that data received are exactly as sent (i.e., contain no modification, insertion, deletion, or replay).
- Identity of the sender is valid. When a hash function is used to provide message authentication, the hash function value is often referred to as a message digest .



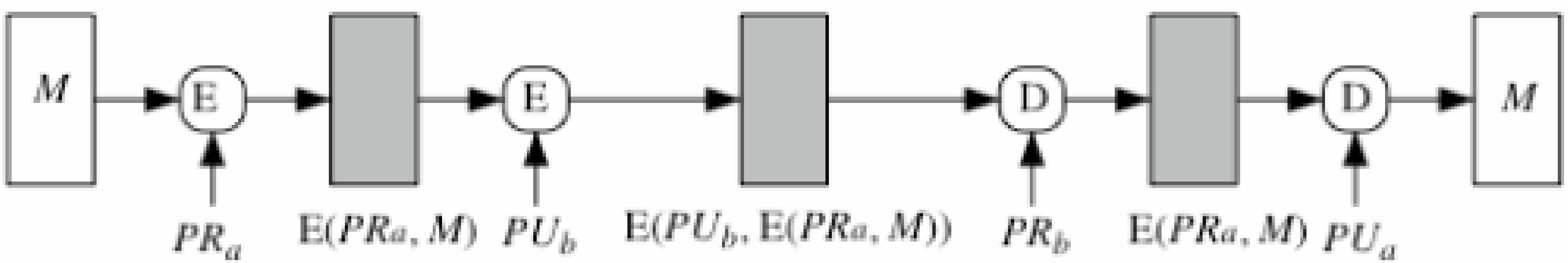

(a) Symmetric encryption: confidentiality and authentication




(b) Public-key encryption: confidentiality

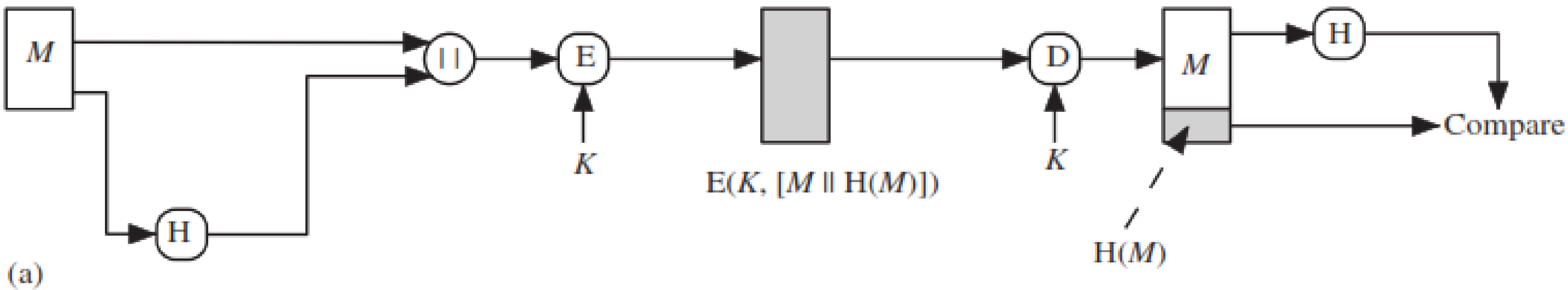



(c) Public-key encryption: authentication and signature

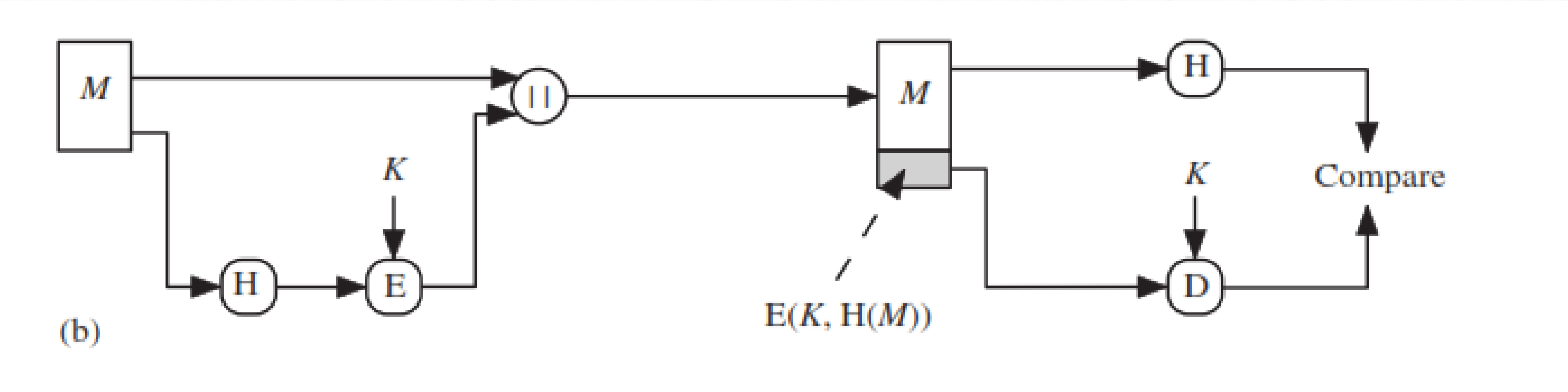



(d) Public-key encryption: confidentiality, authentication, and signature

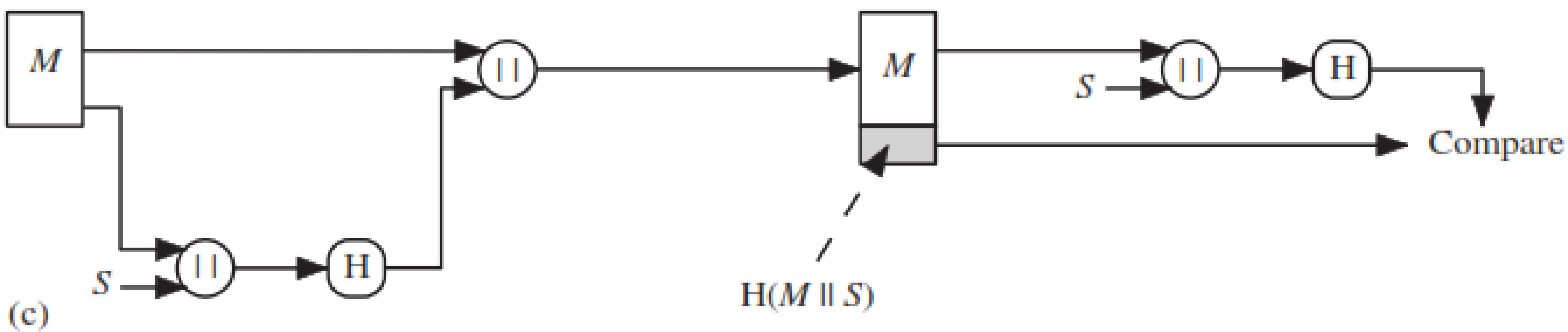
- The message plus concatenated hash code is encrypted using symmetric encryption. Because only A and B share the secret key, the message must have come from A and has not been altered.
- The hash code provides the structure or redundancy required to achieve authentication. Because encryption is  applied to the entire message plus hash code,  confidentiality is also provided


M
| |
E
K
E(K, [M || H(M)])
D
K
M
H
Compare
H
H(M)
(a)

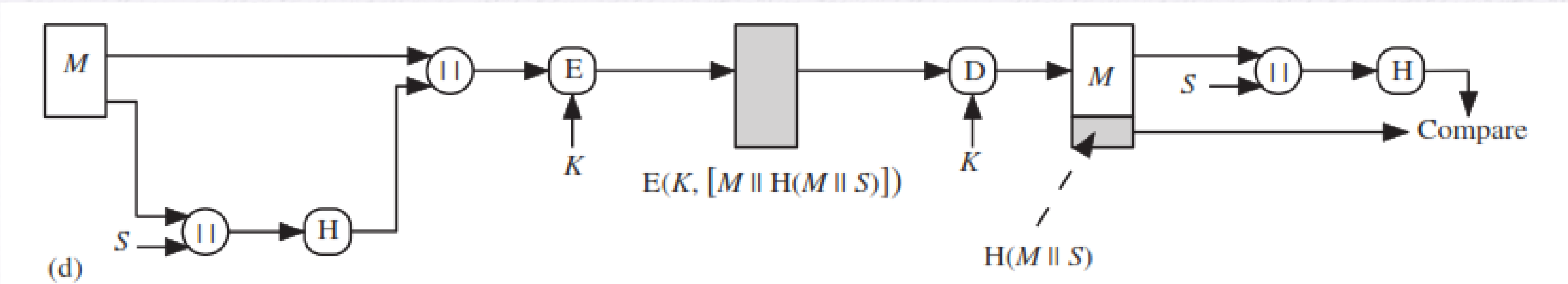
- Only the hash code is encrypted, using symmetric encryption. This reduces the processing burden for those applications that do not require confidentiality.


M
||
K
H
E
(b)
M
E(K, H(M))
H
K
Compare
D

It is possible to use a hash function but no encryption for message authentication. The technique assumes that the two communicating parties share a common secret value $S$. A computes the hash value over the concatenation of $M$ and $S$ and appends the resulting hash value to $M$. Because B possesses $S$, it can recompute the hash value to verify. Because the secret value itself is not sent, an opponent cannot modify an intercepted message and cannot generate a false message.


M
||
S
||
H
M
||
S
||
H
Compare
H(M || S)
(c)

- Confidentiality can be added to the approach of method (c) by encrypting the entire message plus the hash code.


M
S
H
E
K
E(K, [M || H(M || S)])
D
K
M
S
H
Compare
H(M || S)
(d)

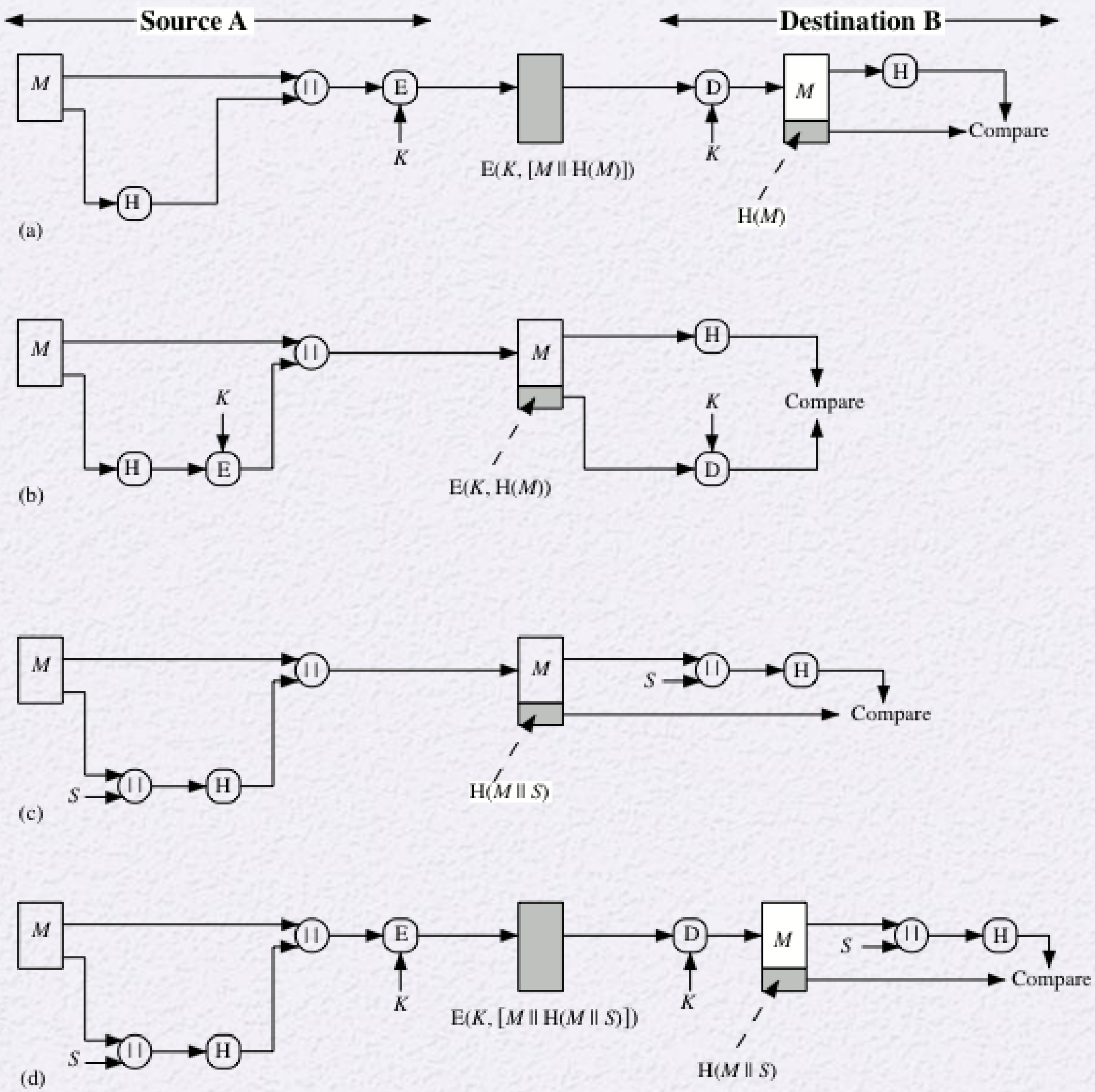



**Figure 11.3 Simplified Examples of the Use of a Hash Function for Message Authentication**

# Message Authentication Code (MAC)

- Also known as a *keyed hash function*
- Typically used between two parties that share a secret key to authenticate information exchanged between those parties

**Takes as input a secret key and a data block and produces a hash value (MAC) which is associated with the protected message**

- If the integrity of the message needs to be checked, the MAC function can be applied to the message and the result compared with the associated MAC value
- An attacker who alters the message will be unable to alter the associated MAC value without knowledge of the secret key

# Message Authentication Requirements

- Disclosure
  - Release of message contents to any person or process not possessing the appropriate cryptographic key
- Traffic analysis
  - Discovery of the pattern of traffic between parties
- Masquerade
  - Insertion of messages into the network from a fraudulent source
- Content modification
  - Changes to the contents of a message, including insertion, deletion, transposition, and modification
- Sequence modification
  - Any modification to a sequence of messages between parties, including insertion, deletion, and reordering
- Timing modification
  - Delay or replay of messages
- Source repudiation
  - Denial of transmission of message by source
- Destination repudiation
  - Denial of receipt of message by destination

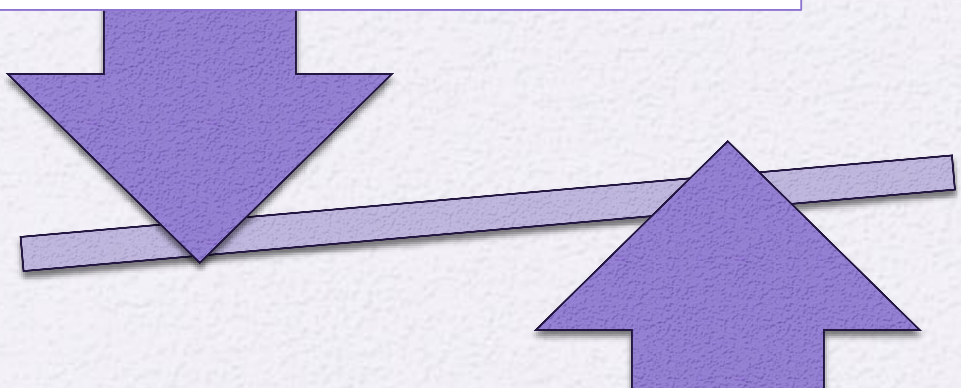
- message authentication is a procedure to verify that received messages come from the alleged source and have not been altered. Message authentication may also verify sequencing and timeliness. A digital signature is an authentication technique that also includes measures to counter repudiation by the source.

# Message Authentication Functions

- Two levels of functionality:

**Lower level**

- There must be some sort of function that produces an authenticator



**Higher-level**

- Uses the lower-level function as a primitive in an authentication protocol that enables a receiver to verify the authenticity of a message

- 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 value that serves as the authenticator

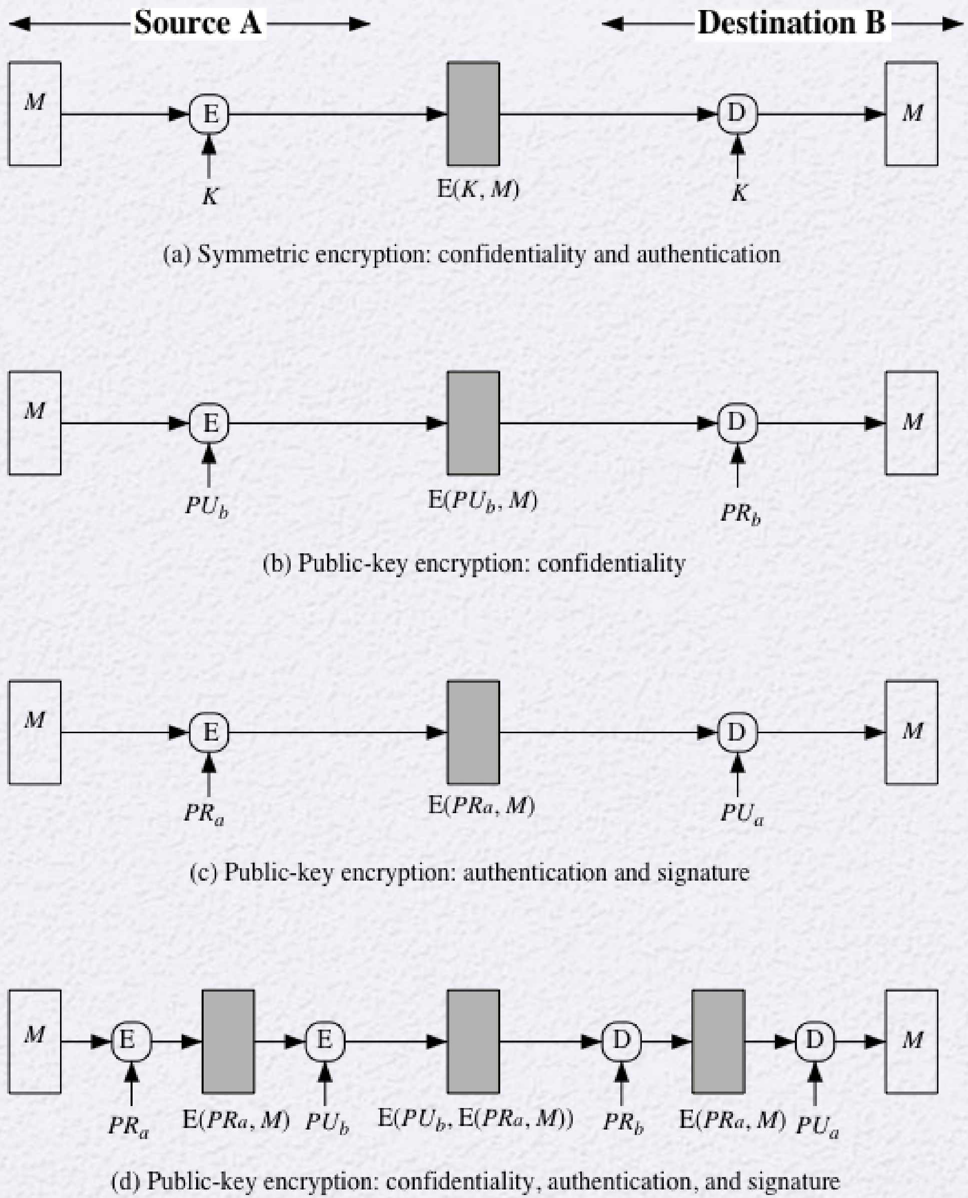



**Figure 12.1 Basic Uses of Message Encryption**

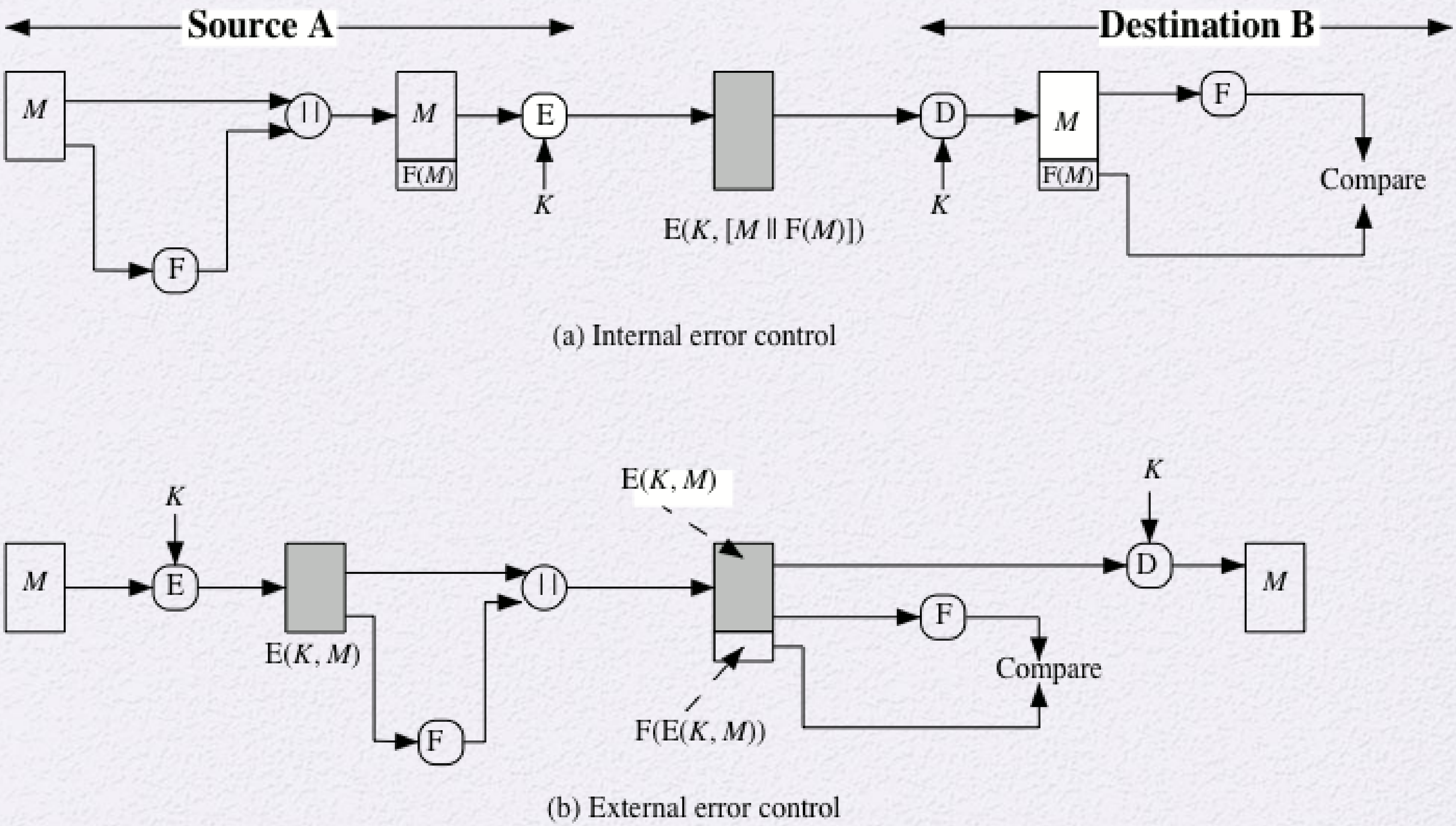



**Figure 12.2 Internal and External Error Control**

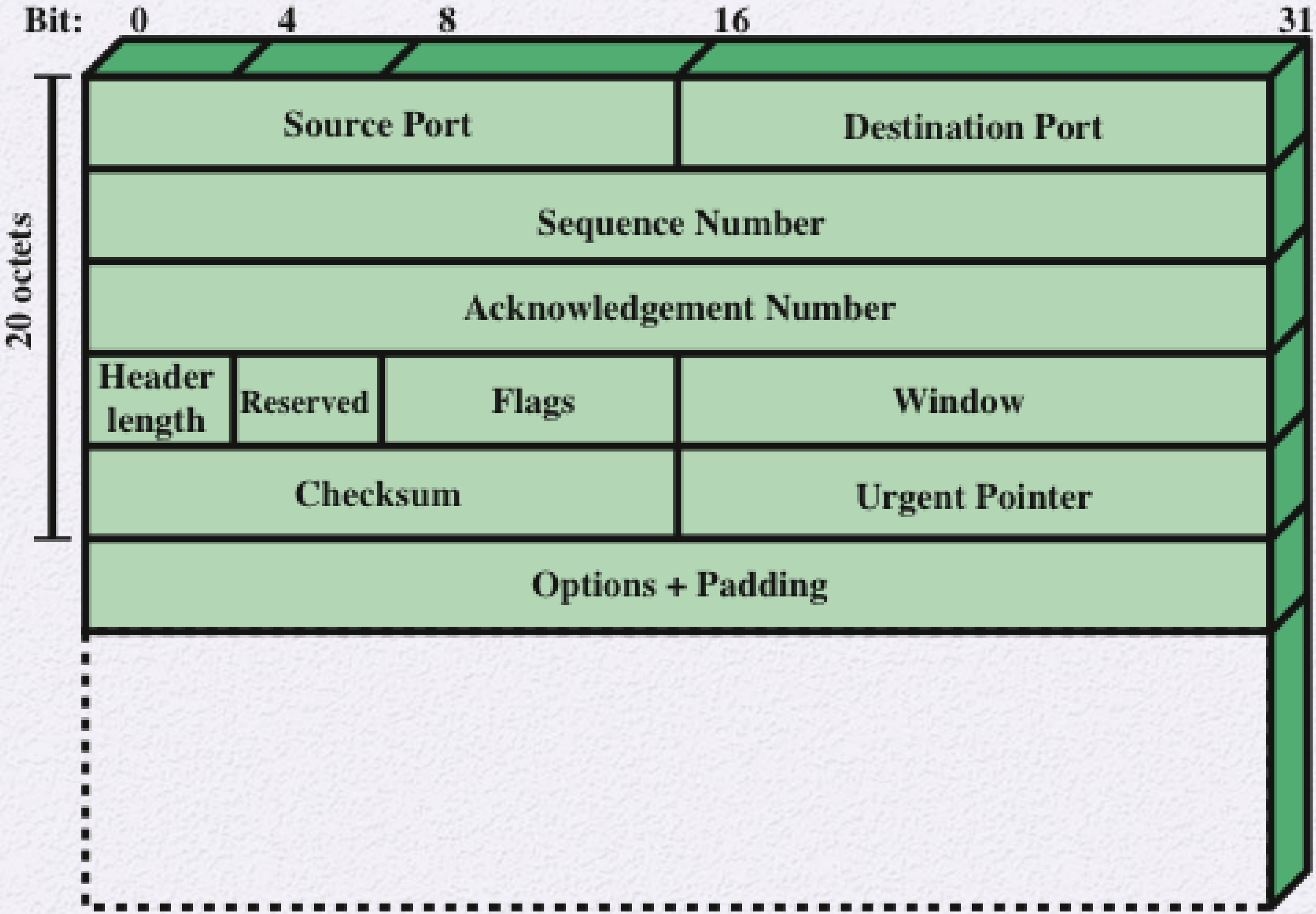



Figure 12.3 TCP Segment

# Public-Key Encryption

- The straightforward use of public-key encryption provides confidentiality but not authentication
- To provide both confidentiality and authentication, A can encrypt *M* first using its private key which provides the digital signature, and then using B's public key, which provides confidentiality
- Disadvantage is that the public-key algorithm must be exercised four times rather than two in each communication

# MAC

- An alternative authentication technique involves the use of a secret key to generate
- a small fixed-size block of data, known as a **cryptographic checksum or MAC, that is**
- appended to the message. This technique assumes that two communicating parties,
- say A and B, share a common secret key *K*.

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

where

$M$ = input message
C – MAC function
$K$ = shared secret key
MAC = message authentication code

- The message plus MAC are transmitted to the intended recipient. The recipient performs the same calculation on the received message, using the same secret key, to generate a new MAC. The received MAC is compared to the calculated MAC.

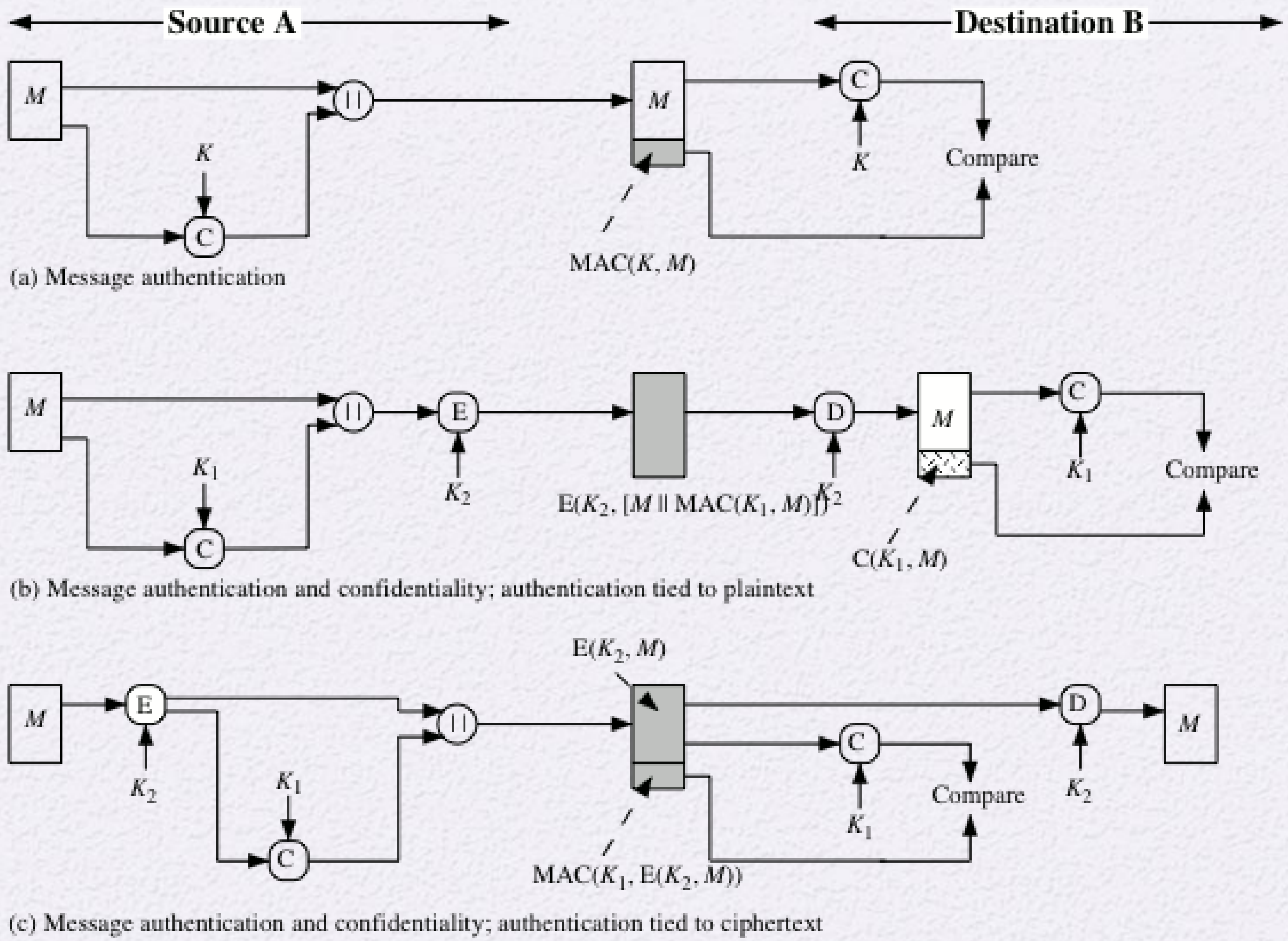



**Figure 12.4 Basic Uses of Message Authentication Code (MAC)**

# Requirements for MACs

Taking into account the types of attacks, the MAC needs to satisfy the following:

The first requirement deals with message replacement attacks, in which an opponent is able to construct a new message to match a given MAC, even though the opponent does not know and does not learn the key

The second requirement deals with the need to thwart a brute-force attack based on chosen plaintext

The final requirement dictates that the authentication algorithm should not be weaker with respect to certain parts or bits of the message than others