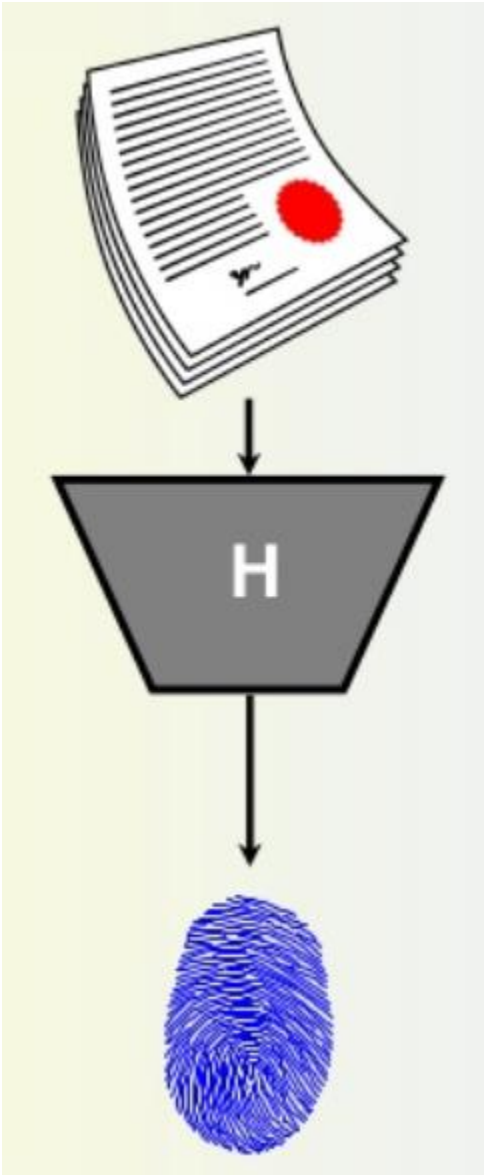
Cryptographic Hash and MAC



Outline

1. To introduce general ideas behind cryptographic hash functions
2. To discuss the Merkle-Damgard scheme as the basis for iterated hash functions
3. To distinguish between two categories of hash functions.
4. To discuss the structure of SHA-512.

Outline

- To define message integrity
- To define message authentication
- To define criteria for a cryptographic hash function
- To define the Random Oracle Model and its role in evaluating the security of cryptographic hash functions
- To distinguish between an MDC and a MAC
- To discuss some common MACs

Message Authentication Requirements

1. Disclosure
2. Traffic analysis
3. Masquerade
4. Content modification
5. Sequence modification
6. Timing modification
7. Source repudiation
8. Destination repudiation

Message Authentication Functions

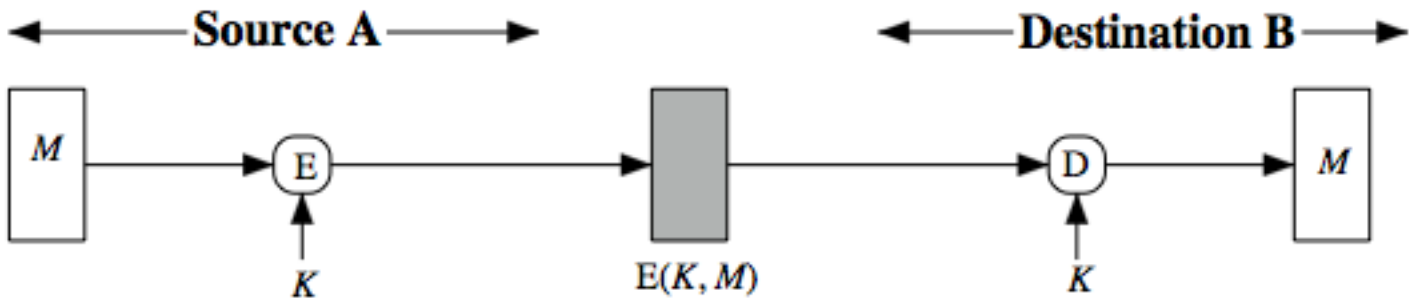
- **Hash function:** A function that maps a message of any length into a fixed length hash value, which serves as the authenticator

- **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

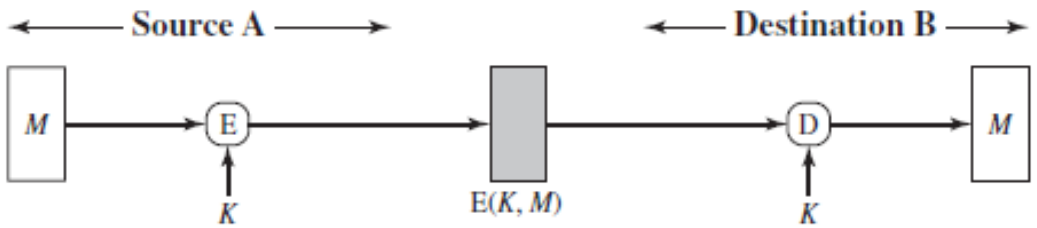
Symmetric Message Encryption

- encryption can also provides 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 have been altered
  - if message has suitable structure, redundancy or a checksum to detect any changes

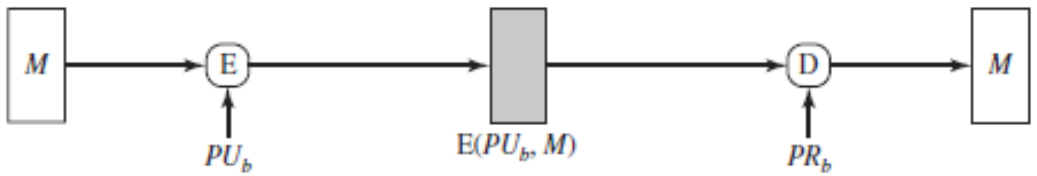


(a) Symmetric encryption: confidentiality and authentication

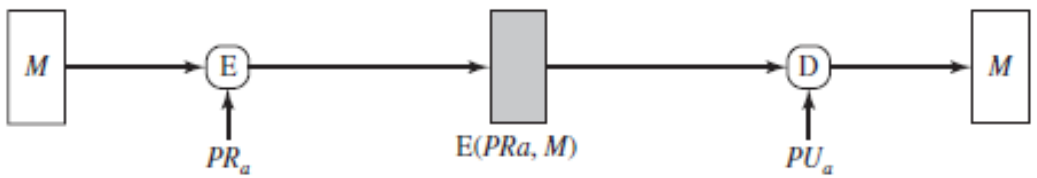
Message Encryption



(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

Figure 12.1 Basic Uses of Message Encryption

Message Integrity

The cryptography systems that we have studied so far provide secrecy, or confidentiality, but not integrity. However, there are occasions where we may not even need secrecy but instead must have integrity.

Topics:

1. Document and Fingerprint
2. Message and Message Digest
3. Difference
4. Checking Integrity
5. Cryptographic Hash Function Criteria

Document and Fingerprint

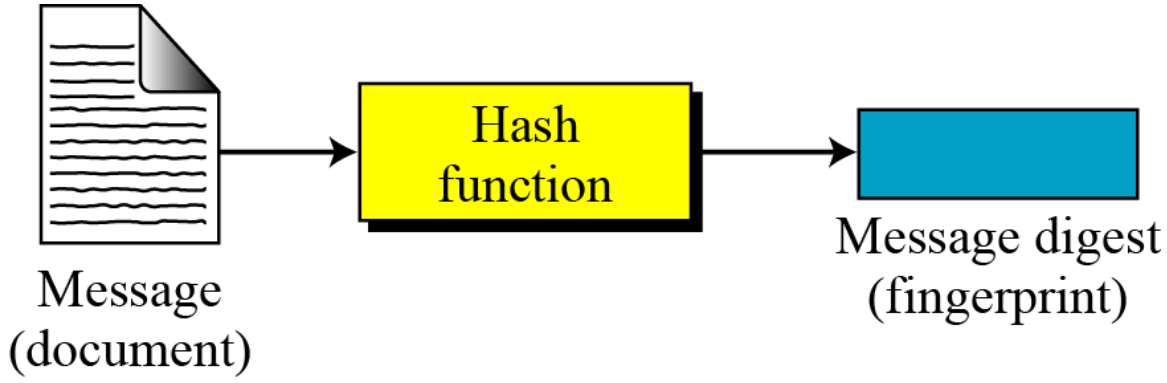
One way to preserve the integrity of a document is through the use of a fingerprint. If Alice needs to be sure that the contents of her document will not be changed, she can put her fingerprint at the bottom of the document.

Message and Message Digest

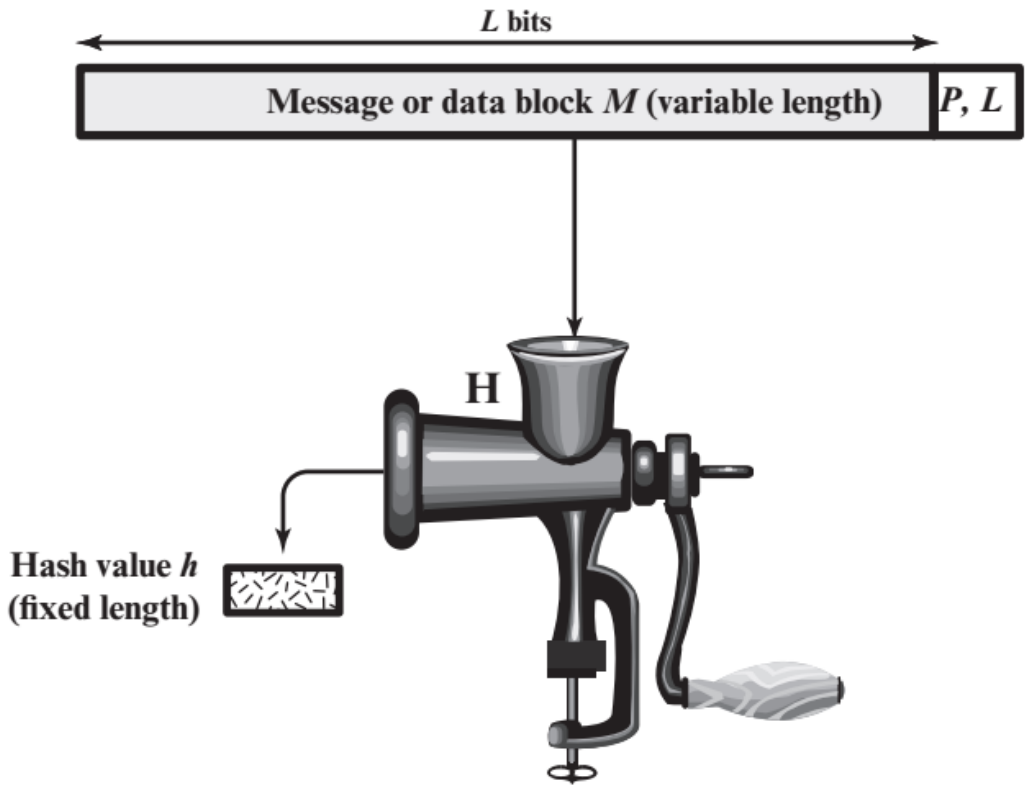
The electronic equivalent of the document and fingerprint pair is the message and digest pair.

A hash function H accepts a variable-length block of data M as input and produces
a fixed-size hash value h = H(M).

Figure Message and digest



Cryptographic Hash Function



P, L = padding plus length field

Figure Cryptographic Hash Function; $h = \mathrm{H}(M)$

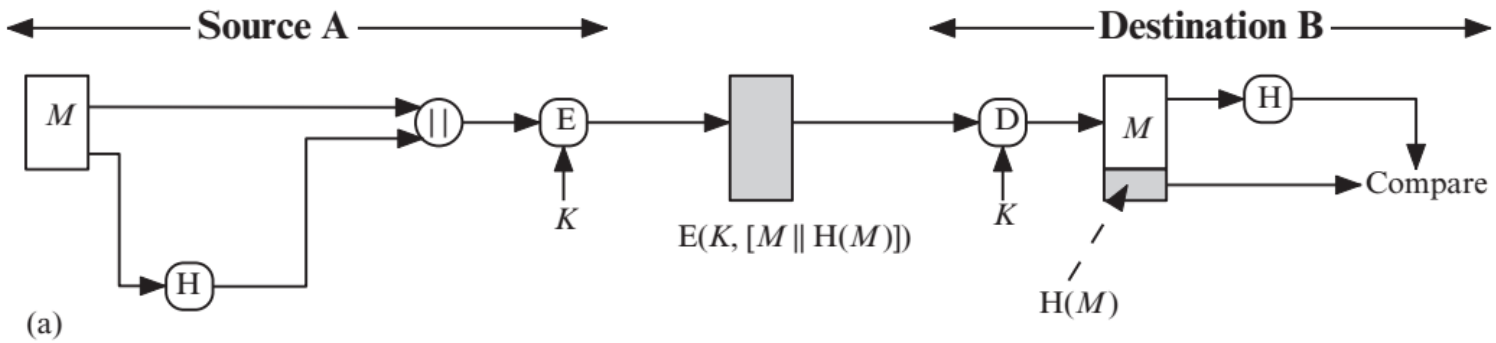
Application of Cryptographic Hash Function

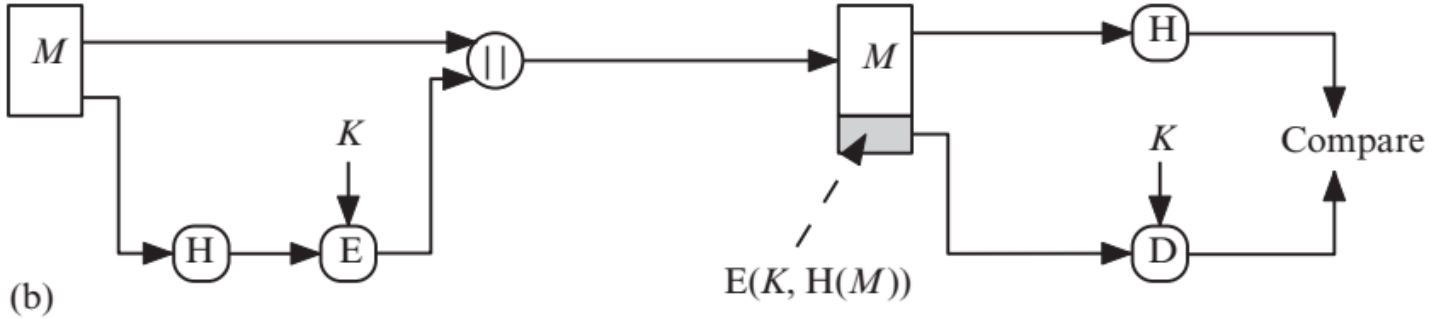
Message Authentication: Message authentication is a mechanism or service used to verify the integrity of a message.

When a hash function is used to provide message authentication, the hash function value is often referred to as a message digest.

Application of Cryptographic Hash Function

Figures illustrates a variety of ways in which a hash code can be used to provide message authentication, as follows.





Application of Cryptographic Hash Function