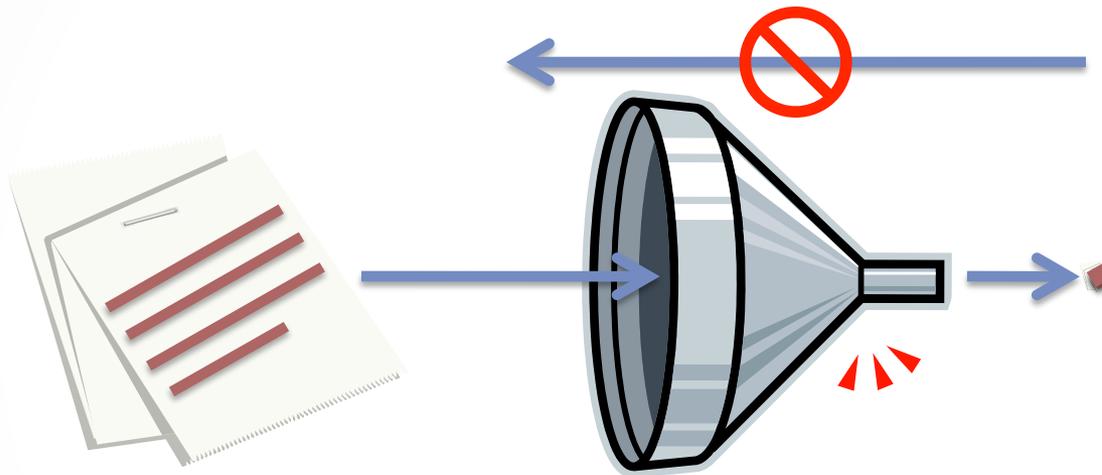# CS 465

# Cryptographic Hash Functions

# Message Digests



- Input to a hash function is called a pre-image

- Output of a hash function is a message digests, also known as hash codes or hash values
  - Sort of like a message fingerprint/footprint

- Hash functions are ONE-way
  - They cannot be inverted

# Properties of a Hash Function (H)

1. H can be applied to a block of data of any size
2. H produces a fixed-length output
3. $H(x)$ is relatively easy to compute for any given $x$
4. For any given value $h$, it is computationally infeasible to find $x$ such that $H(x) = h$

   **(one-way)**

5. For any given block $x$, it is computationally infeasible to find $y \neq x$ with $H(y) = H(x)$

   **(weak collision resistance)**

6. It is computationally infeasible to find any pair $(x, y)$ such that $H(x) = H(y)$

   **(strong collision resistance)**

# Attacks on Hash Functions

- ## First pre-image attack
  - Given a hash $h$, find a message $m$ such that $H(m) = h$
    - Think property #4

- ## Second pre-image attack
  - Given a message $m_1$, find a different message $m_2$ such that $H(m_2) = H(m_1)$
    - Cost: $2^n$ where n = # of digest bits
    - Think property #5

- ## Collisions
  - Two messages both hash to the same value
    - Birthday Attack
      - Given $n$-bit digest, birthday attack says that we'll find a match after $2^{n/2}$ attempts
    - Think property #6

253 people in a room
- Odds are good that one of them shares a birthday with you

23 people in a room
- Odds are good that two people share a birthday

# Useful Applications of Hashes

- Human-readable method to compare/verify data
  - File downloads
  - Testing/passing off Lab #1

- Chaining events together

- Digital signatures

- Fundamental building block of many secure protocols
  - Schneier (Secrets and Lies) – "They are probably the single most useful tool in a cryptographer's toolbox"

# SHA-1 Hash Function

- The following diagrams illustrates how SHA-1 is implemented

- SHA-1 is implemented using the Merkle-Damgård construction
  - See http://en.wikipedia.org/wiki/Merkle–Damgård_construction

- It is important to understand the details of this implementation in order to understand the MAC attack that will be discussed in the MAC
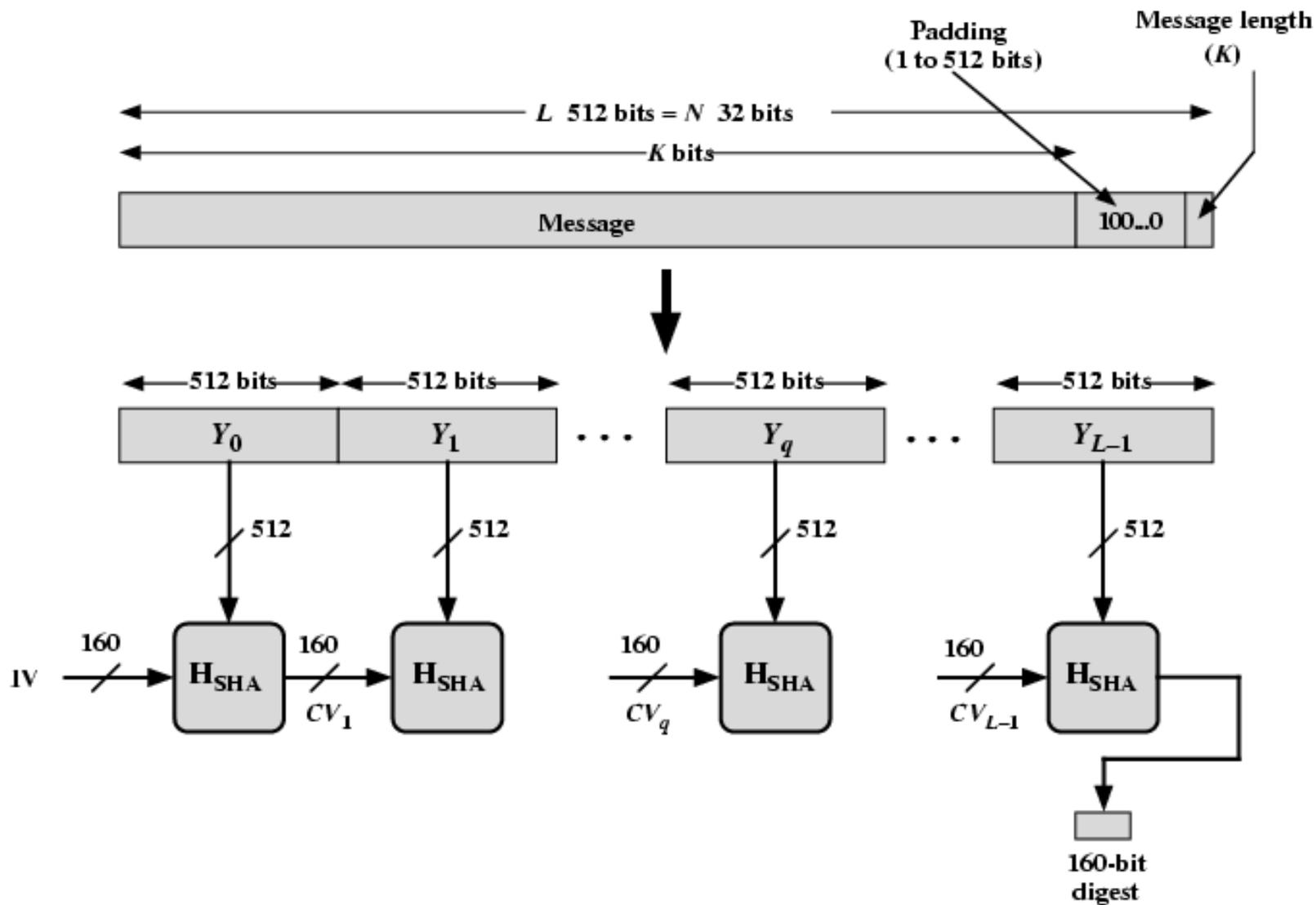
# Merkle-Damgård Construction
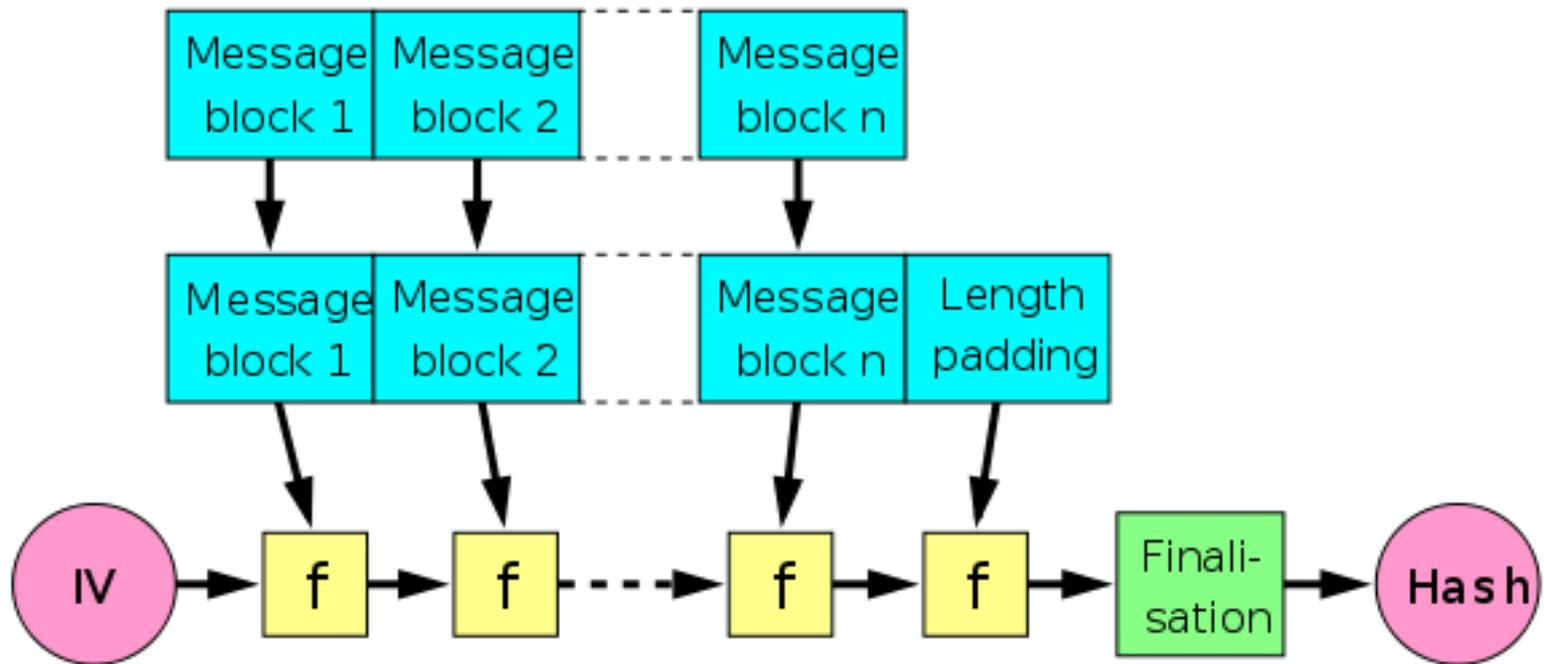
**Figure 3.4 Message Digest Generation Using SHA-1**