CSS2C08

COMPUTER NETWORKS

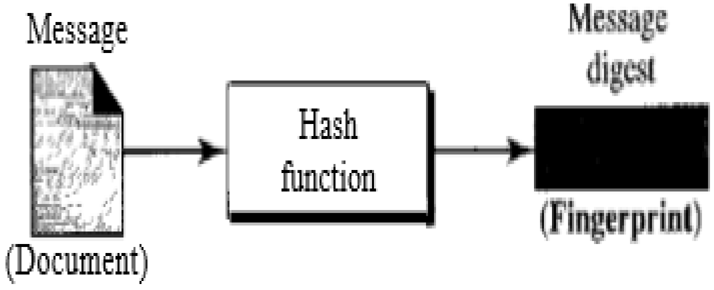
MODULE 5
Security in Networks

1. **Principles of cryptography**
2. Integrity
3. Authentication
4. Key distribution and certification
5. Firewalls
6. Attacks and counter measures

Integrity

- Message integrity means that the data must arrive at the receiver exactly as they were sent.
- Encryption and decryption provide secrecy, or confidentiality, but not integrity.
- **Document and Fingerprint**
  - One way to preserve the integrity of a document is through the use of a fingerprint.

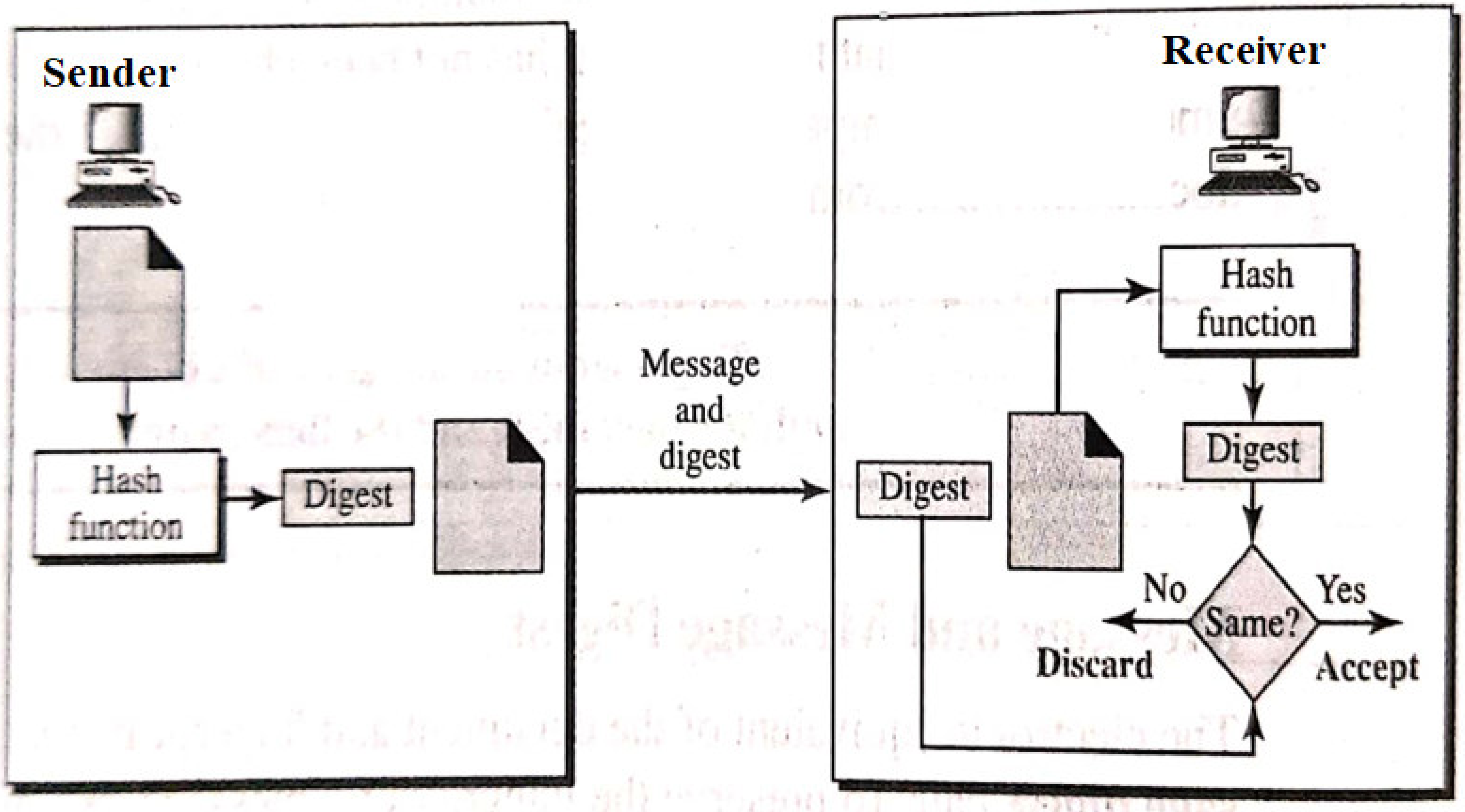
- **Message and Message Digest:**
  - ❖ The electronic equivalent of the document and fingerprint pair is the message and message digest pair.
  - ❖ To preserve the integrity of a message, the message is passed through an algorithm called a hash function. The hash function creates a compressed image of the message that can be used as a fingerprint.



❖ The message and message digest can be unlinked (or sent) separately and, most importantly, the message digest needs to be kept secret.

❖ The message digest is either kept secret in a safe place or encrypted if we need to send it through a communications channel.

- **Creating and Checking the Digest**
  - The message digest is created at the sender site and is sent with the message to the receiver.
  - To check the integrity of a message, or document, the receiver creates the hash function again and compares the new message digest with the one received.
  - If both are the same, the receiver is sure that the original message has not been changed. Of course, we are assuming that the digest has been sent secretly.


Sender
Hash function
Digest
Message and digest
Receiver
Hash function
Digest
Digest
No
Same?
Yes
Discard
Accept

Hash Function Criteria

- To be eligible for a hash, a function needs to meet three criteria:
  - One-wayness
  - Resistance to weak collision
  - Resistance to strong collision

1. One-wayness

❖ A hash function must have one-wayness

❖ a message digest is created by a one-way hashing function.

❖ We must not be able to recreate the message from the digest.

❖ Sometimes it is difficult to make a hash function 100 percent one-way

❖ the criteria state that it must be extremely difficult or impossible to create the message if the message digest is given.

❖ This is similar to the document/fingerprint case. No one can make a document from a fingerprint.

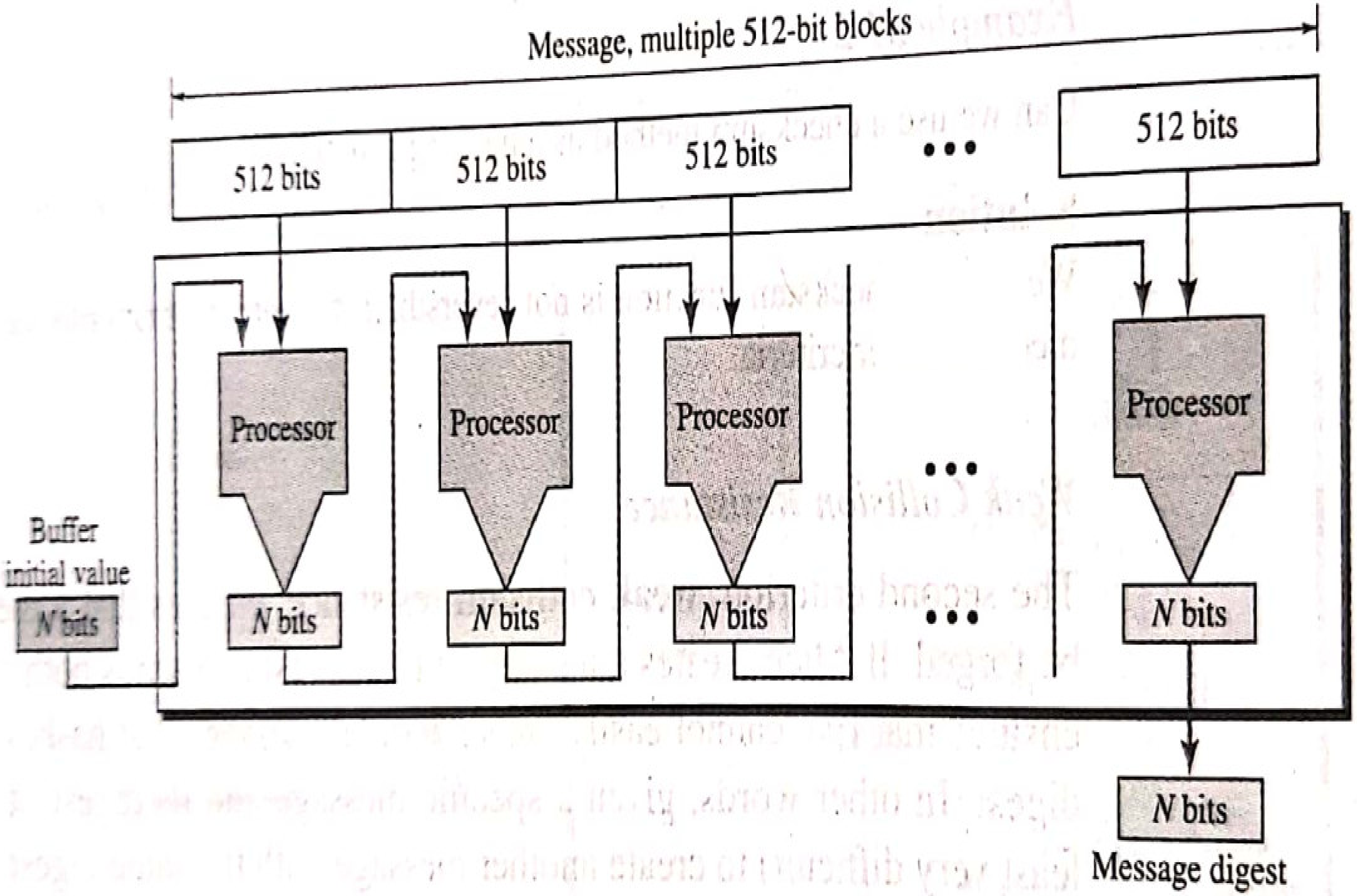
2. Weak Collision Resistance

- ❖The second criterion, weak collision resistance, ensures that a message cannot easily be forged.
- ❖Given a specific message and its digest, it is impossible (or at least very difficult) to create another message with the same digest. When two messages create the same digest, we say there is a collision.
- ❖In a week collision, given a message digest, it is very unlikely that someone can create a message with exactly the same digest.
- ❖A hash function must have weak collision resistance.

3. Strong Collision Resistance

- ❖The third criterion, strong collision resistance, ensures that we cannot find two messages that hash to the same digest.
- ❖This criterion is needed to ensure that , the sender of the message, cannot cause problems by forging a message.

- **Hash Algorithms: SHA-l:**
  - SHA-1 (Secure Hash Algorithm 1) is a revised version of SHA designed by the National Institute of Standards and Technology (NIST). It was published as a Federal Information Processing Standard (PIPS).
  - SHA-l hash algorithms create an N-bit message digest out of a message of 512-bit blocks.
  - SHA-l has a message digest of 160 bits (5 words of 32 bits).


Message, multiple 512-bit blocks
512 bits
512 bits
512 bits
512 bits
Processor
Processor
Processor
Processor
Buffer
initial value
N bits
N bits
N bits
N bits
N bits
N bits
Message digest

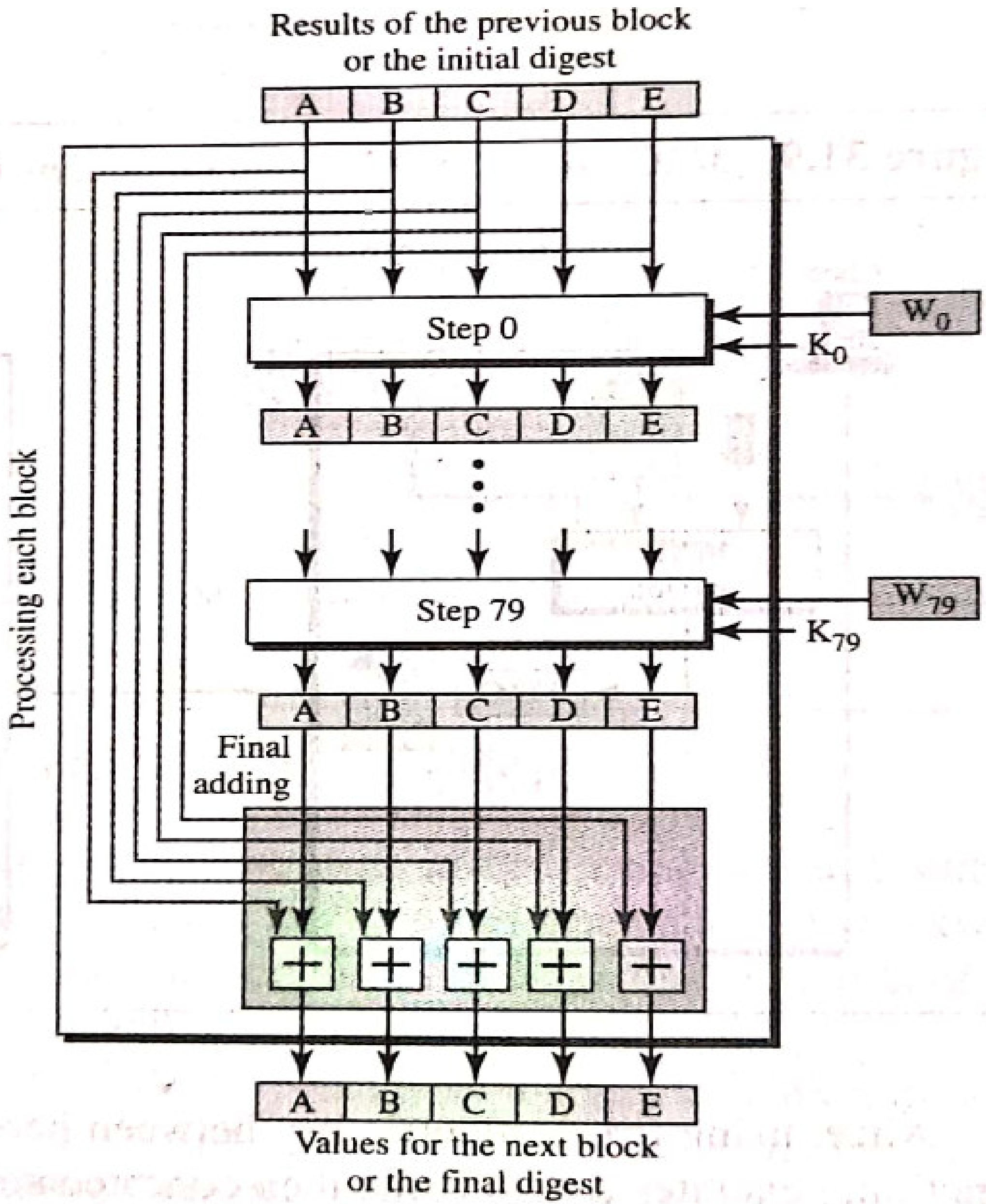
- A buffer of N bits is initialized to a predetermined value.
- The algorithm mangles this initial buffer with the first 512 bits of the message to create the first intermediate message digest of N bits.
- This digest is then mangled with the second 512-bit block to create the second intermediate digest.
- The (n - 1)th digest is mangled with the nth block to create the nth digest.
- If a block is not 512 bits, padding (0s) is added to make it so.
- When the last block is processed, the resulting digest is the message digest for the entire message.
- SHA-l has a message digest of 160 bits (5 words, each of 32 bits).

❖Word Expansion

Before processing, the block needs to be expanded. A block is made of 512 bits or 16 32-bit words, but we need 80 words in the processing phase. So the 16-word block needs to be expanded to 80 words, word 0 to word79.

❖Processing Each Block

There are 80 steps in block processing. In each step, one word from the expanded block and one 32-bit constant are mangled together and then operated on to create a new digest. At the beginning of processing, the values of digest words (A, B, C, D, and E) are saved into five temporary variables. At the end of the processing (after step 79), these values are added to the values created from step 79.


Results of the previous block
or the initial digest
A
B
C
D
E
Processing each block
Step 0
W_0
K_0
A
B
C
D
E
Step 79
W_{79}
K_{79}
A
B
C
D
E
Final
adding
+
+
+
+
+
A
B
C
D
E
Values for the next block
or the final digest