# Message Digest

(presentation by Bikal and Abanish)

# Message Digest

- It is a cryptographic hash function containing a string of digits created by a one way hashing formula.
- Message digests are designed to protect the integrity of a piece of data or media to detect changes and atternations to any part of message.
- Message digest ensures the integrity of document.
- The cryptographic hash function is a one way function,that is,a function which is practically in feasible to invert.

# Message digest version 4 (MD4)

- The MD4 function is a cryptographic algorithm that takes a message of arbitary length as input and produces a 128 bit message digest or hash value as output.
- Suppose a b-bit message as input and we need to find its message digest .It is assumed that the bits of the message are $m_0, m_1, \ldots\ldots, m_{b-1}$ .

# Step 1: Append padded bits

The message is padded so that its length is congurent to 448 ,modulo 512. A single 1 bit is append to the message and then 0 bits are appended so that the length in bits equals 448 modulo 512.

| | | |
|---|---|---|
| message | 100000 | |

(message length+padded bits)%512=448

# Step 2: Append length

A 64-bit representation of b is appended to the result of the previous step. The resulting message has a length that is an exact multiple of 512 bits.

| | | |
|---|---|---|
| message | 100000 | 64-bits |

(message length+padded bits+64 bits)%512=0

# Step 3: Initialize MD buffer

A 4-word buffer(A,B,C,D) is used to compute the message digest. Here each of A,B,C.D is a 32-bit register. These are initialized to the following values in hexa decimal,low-order byte first.

A: 01 23 45 67
B: 89 ab cd ef
C: fe dc ba 98
D: 76 54 32 10

# Step 4: Process message in 16-word blocks

It contains three passes(rounds) with 16 steps or operation each. We first define three auxiliary functions that each take as input three 32-bit words and produce as output one 32-bit word.

Pass 1: $F(X,Y,Z)=(X \wedge Y) \vee (\neg X \wedge Z)$ [step 0 to 15]
Pass 2: $G(X,Y,Z)=(X \wedge Y) \vee (X \wedge Z) \vee (Y \wedge Z)$ [step 16 to 31]
Pass 3: $H(X,Y,Z)=X \oplus Y \oplus Z$ [step 32 to 47]

# Step 5: Output

After all rounds have performed the buffer A,B,C,D contains the MD5 output starting with lower bit A and ending with higher bit D.

# Message digest version 5(MD5)

- The MD5-message digest algorithm is widely used cryptographic hash function producing a 128 bit(16-byte) hash value ,typically expressed in text format as a 32 digit hexadecimal number.
- MD5 was invented by Ron Rivest as an improvement version of MD4.

# Operations:

Step 1 to step 3: Same as MD4

Step4:

It contains 4 passes,with 16 steps or operation each. We first define four auxiliary functions that each take as input three 32-bit words and produce as output one 32-bit word.

# Operation

Pass 1: F(X,Y,Z)=(X^Y) ∨ (¬X^Z) [step 0 to step 15]
Pass 2: G(X,Y,Z)=(X^Z) ∨ (Y^¬Z) [step 16 to step 31]
Pass 3: H(X,Y,Z)=X⊕Y⊕Z [step 32 to step 47]
Pass 4: H(X,Y,Z)=Y⊕(X^¬Z)

# Step 5:output

After all rounds have performed the buffer A,B,C,D contains the MD5 output starting with lower bit A and ending with higher bit D.