Semester : VI Subject : CSS Academic Year: 2023 2024

MD5 ALGORITHM :

- It uses an input bit of 512 bits blocks.
- It generates output of 128 bits message digests

How MD5 Works ?

Step1 : Padding

Step2 : Append Length

Step3 : Divide the input. into 512 bit blocks.

Step4 : Initialize chaining variables.

Step5 : Process Blocks (3 steps).

Step1 : Padding.

- The aim of this step is to make the length of the original message equal to a value which is 64 bits less than the exact multiple of 512 bits

Example :-

$512 \times 1 = 512 - 64 = 448$

$512 \times 2 = 1024 - 64 = 960$

$512 \times 3 = 1536 - 64 = 1472$

$512 \times 4 = 2048 - 64 = 1984$

If i/p. bits are 1000 then add 472 which is the exact multiple of 512 less than 64 bits.

(eg) $1000 + 472 = 1472$.

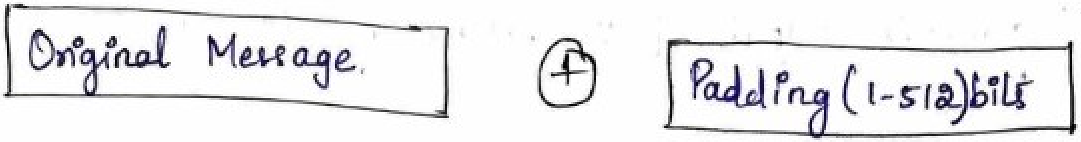
(eg) $500 + 460 = 960$.

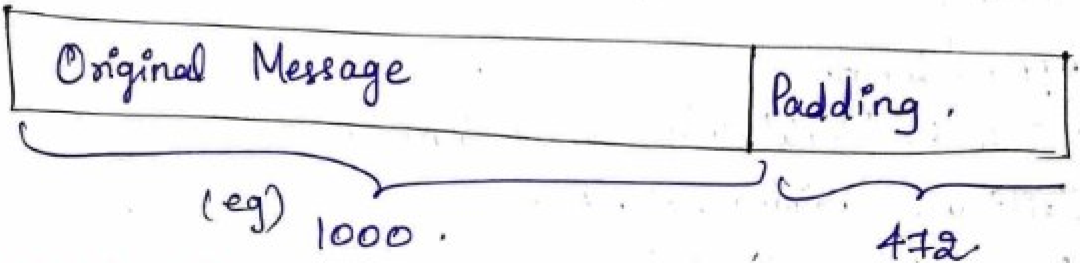
(eg) $448 + 512 = 960$.

448 is already a ~~multiple of 512~~ b 64 bits less than the multiple of 512 bits. But still padding has to be done.

Semester : VI Subject : CSS Academic Year: 2023-2024

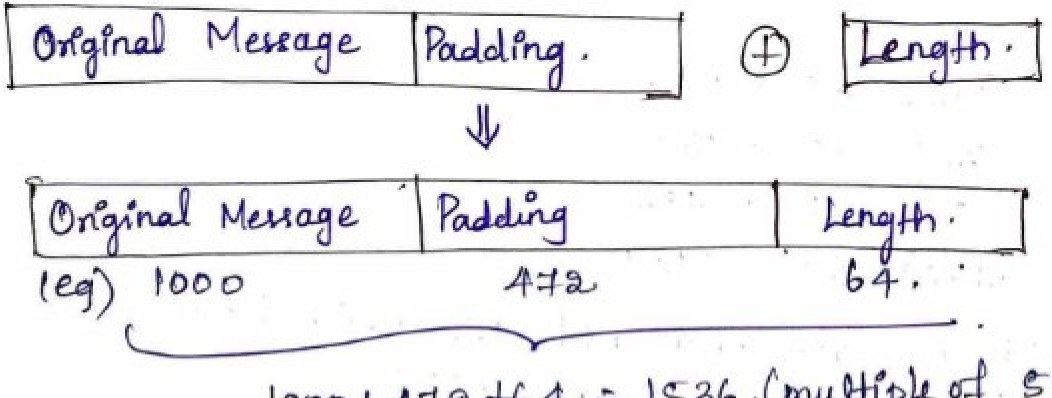
* The padding bits length can be from 1 to 512.





Step 2: Append Length:

* Calculate the original length of the message and add it to the end of the message after padding.
* Only 64 bits should be added for the length.

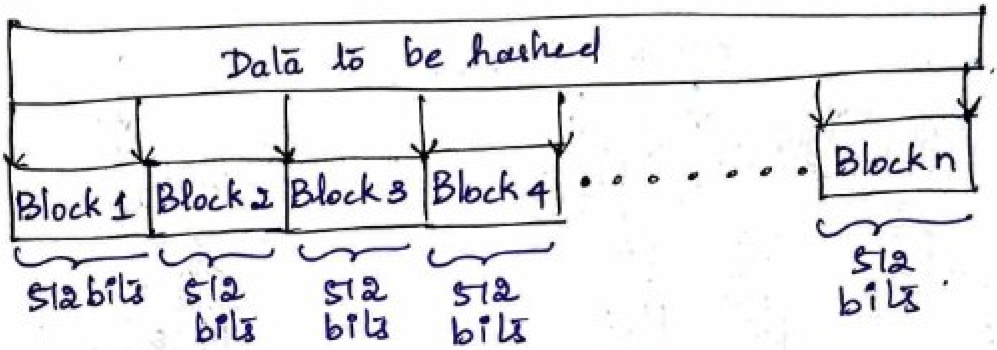


1000+472+64 = 1536. (multiple of 512 bits).

Step 3: Divide the input into 512-bits block

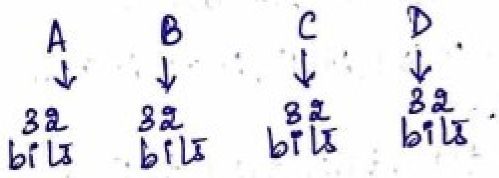
* The input bits message block generated in the previous step is divided into ~~16~~ sub-blocks. Each block consists of 512 bits.

Semester : VI Subject : CSS Academic Year: 2023 - 2024



Step 4 : Initializing Chaining variables.

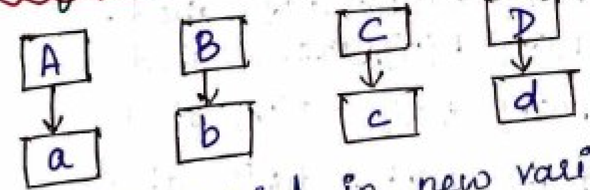
- ✱ It is the next input for the Algorithm.
- ✱ It used 4 variables of 32 bits each.



Step 5 : Process Blocks

The Algorithm begins here.

Step 5.1 : Copy A, B, C, D in 4 corresponding variables a,b,c,d.



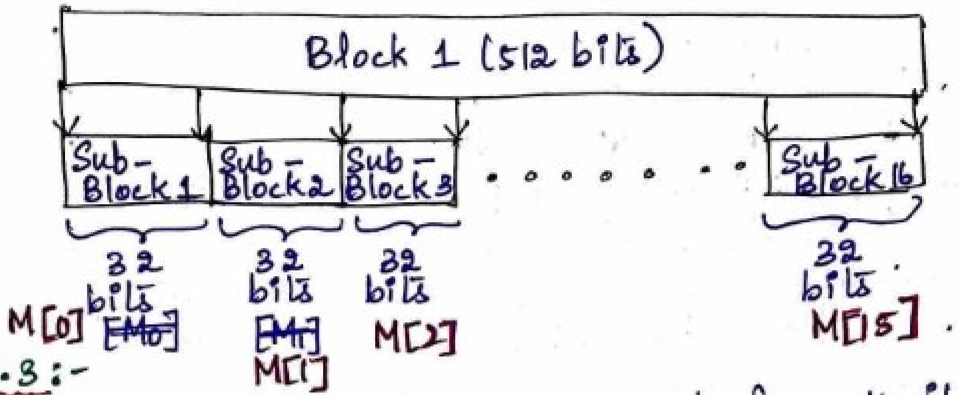
The values are copied in new variables to retain the original values.

Step 5.2 : Divide 512-bits block into 16 sub-blocks.

The 512 bit blocks are divided into 16 sub-blocks.

- ✱ The 512 bit blocks are divided
- ✱ Each sub-block consists of 32 bits

Semester : VI Subject : CSS Academic Year: 2023 - 2024 .



Step 5.3 :-

MD5 undergoes 4 rounds . Each round has 16 iterations . So 16 X 4 = 64 iterations .

The inputs for each iterations are as follows .

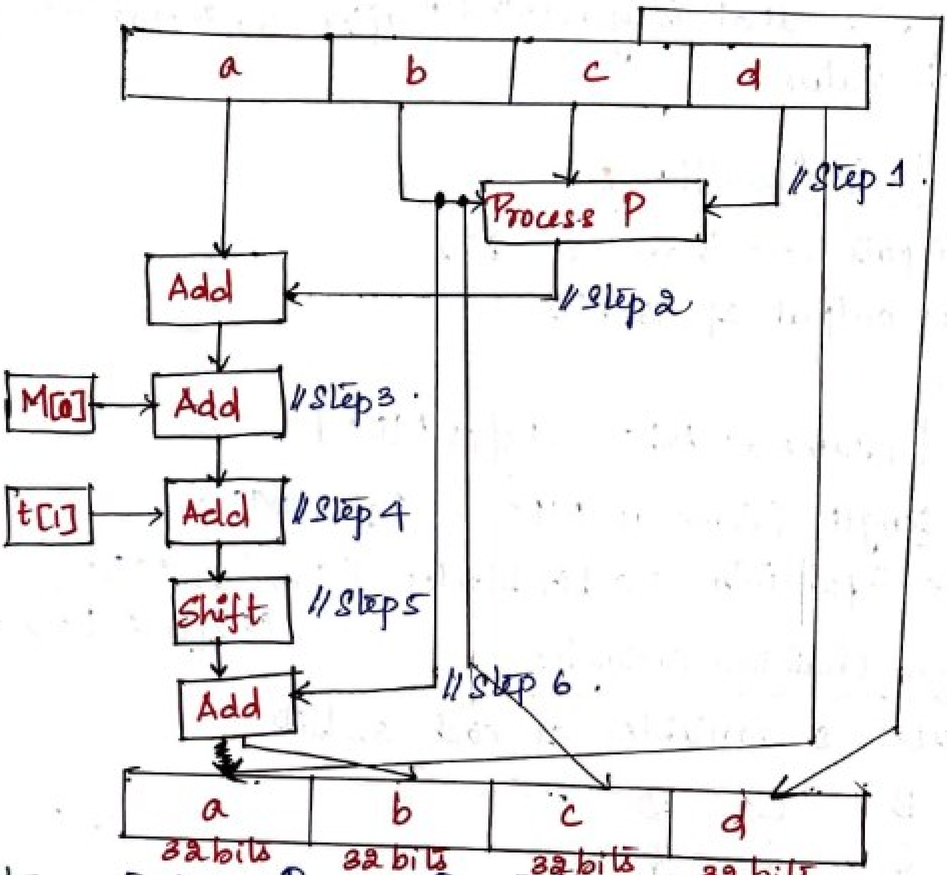
(1) All the subblocks → M[0], M[1], M[2], M[3], ..., M[15]
(2) Variables → a, b, c, d .
(3) Constant t → t[i] = t[1], t[2], t[3], t[4], ... t[64] .
i → 1 to 64 → Each iteration uses each constant .

ROUNDS	Message Blocks .	Constants	Variables	Iterations .
Round 1.	M[0], M[1] .... M[15]	t[1], t[2] ... t[16]	abcd .	16 .
Round 2	M[0], M[1] ... M[15]	t [17], t[18] . t[32]	abcd	16 .
Round 3	M[0], M[1] ... M[15]	t[33], ... t[48]	abcd	16 .
Round 4	M[0], M[1] .... M[15]	t [49], ... t[64]	abcd	16 ,

In Round 1, Iteration 1 will use input M[0], t[1] , abcd and generate new abcd . Iteration 2 will use input M[1], t[2], previous round abcd and generate new abcd . The same process are repeated 64 times . The 64 iteration will use input as M[15], t [64] and abcd generated in 63rd iteration .

Semester : VI Subject : CSS Academic Year: 2023 - 2024

Process of Round 1 → Iteration 1 :-



Step 1: Perform Process P = P(b,c,d).

Step 2: Add a to the output of step 1.

Step 3: Add M[0] to the output of step 2.

Step 4: Add t[1] to the output of Step 3.

Step 5: The output of step 4 is circular left shift by s bits s can be any value.

Step 6: Add output of Step 5 with b.

Step 7: The output of step 6 becomes new b.

Step 8: The previous b becomes new c.

Step 9: The previous c is new d. Previous d is new a.

Semester : VI Subject : CSS Academic Year: 2023-2024

In every iteration new abcd is generated. The abcd → 128 bits that is generated after 64 iterations is the hash value.

SHA - Secure Hash Algorithm :-

- * It takes inputs less than 2^{64} bits.
- * It produces output of 160 bits.

How SHA Works?

Step 1 : Padding. [Same as MD5 → Refer MD5].

Step 2 : Append length [Same as MD5 → Refer MD5]

Step 3 : Divide the input into 512 bit blocks. [Same as MD5] (Refer MD5).

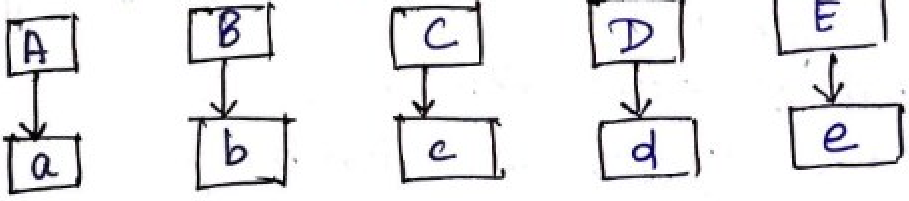
Step 4 : Initialize Chaining Variables

In SHA, it uses 5 variables of each 32 bits.

A	B	C	D	E
↓	↓	↓	↓	↓
32 bits	32 bits	32 bits	32 bits	32 bits.

Step 5 : Process Blocks.

Step 5.1 : Copying chaining variables.


A
B
C
D
E
a
b
c
d
e