

### A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering **Data Science** 



Semester:

Subject: CSS

Academic Year: 20 23- 20 24:

## MDS ALGORITHM

\* It uses an input birt of 512 bils blocks.

\* It generalis output of 128 bils message digests

## How MDS Norths?

Step 1: Padding

Stepa: Append Length

Steps: Divide the input into stabit blocks.

Step 4: Initialize chaining variables.

Steps: Process Blocks (3 steps).

Step 1: Padding.

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

Example:-

512×1 = 512 -64 = 448

512 x 2 = 1024 - 64 = 960

512 ×3 = 1536 -64 = 1472

51ax4 = 2048 - 64 = 1984

If i/p bils are 1000 then add 472 which is the exact multiple of sla less than 64 bils

leg) 1000+472 = 1472,

(eg) 500 + 460 = 960.

(eg) 448 +812 = 960.

418 is already a multiple of stab 64 bils less than the multiple of skebili But still padding has to be done. Subject Incharge: Prof. Sarala Mary Page No. 1 Department of CSE-Data Science | APSIT



## A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering
Data Science



Semester: Subject: CSS Academic Year: 209.3- 209
* The padding bili length can be from 1 to 512.
Original Message Padding (1-512) bils
Original Message Padding.
(eg) 1000. 472
Slep &: Append Length:
to the end of the message after padding.
* Calculate the original length of the message and add it to the end of the message after padding.  * Only 64 bils should be added for the length.
Original Message Padding. (1) Length.
Original Message Padding Length.
(eg) 1000 AT2 64.
1000+472+64 = 1536. (multiple of stabilis)
Steps: Divide the input into 512-bits block
*The input bils message block generated in the previous step is divided into to sub-blocks. Each
block consists of stabilis.
Subject Incharge: Prof. Sarala Mary Page No. 2 Department of CSE-Data Science   APSIT



## A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering
Data Science



Semester :	Subject : CSS	Academic Year: 2028 - 2024
Do	ita to be hashed	4 113
200 6	Black & Black 4	Blockn
Block 1 Block	Block 3 Block 4	
डाब्रेकींड डांब क्रीड	bild bild	bils.
Step 4: Instializing	Chaining vails	bles
the same	input for the A	1 gontin
* It used 4 you	tables of 32 bill	each.
A B	C D	25.75
32 32	क्षेत्र हैं है	
क्षाय क्षाय	bru bia	A Committee of the Comm
Steps: Prouse Bloc	ks.	
The Algorithm begin	here.	cables about
CLEDEL . CODY A, B,	C, D in 4 corres	onding variables a,b,c,d
مسلمات المكانة	of ICI P	
	里里	1
Tal [	b c	giables to retain the
The values are	espied in new ra	enables to retain the
original values.	e d Jern soni	" auh blocks.
0 - 1 0-10	-hile block	16 sub-blocks.
Lat 1	1- LA ave divide	d law to see
* The sta on a	ck consists of 32	ी हैं
* Each sub-bite	Contracting	
Subject Incharge: Prof. Sarala Mary	Page No. 3. De	partment of CSE-Data Science   APSIT

PARSHWANATH CHARITARIS TRUST'S



### A.P. SHAH INSTITUTE OF TECHNOLOGY

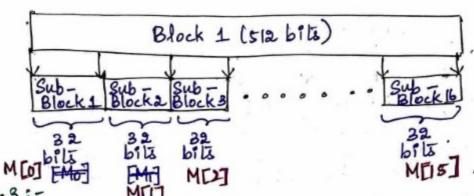
Department of Computer Science and Engineering
Data Science



Semester:

Subject: CSS

Academic Year: 2023 - 2024 .



MDs undergoes 4 rounds. Each round has 16 iterations.

So 16 X4 = 64 Herations.

The Enpuli for each iterations are as follows.

- (1) All the subblocks -> MCO], MCI], MCO], MCB]...., MCIS]
- (2) Variables a, b, c, d.
- (3) Constant t → t[1] = t[1], t[2], t[8], t[4], .... t[64].

  i → 1 to 64 → Each iteration uses.

ROUNDS	Message Blocks.	Constants	Variables	Herations
Round 1.	MITOT MITT MEIST	t[1],t[2]t[16]	abcd.	16.
Round 2	MCOJ, MCI MCIS]	f [17], f[18]. 1837	abcd	16 .
Round 3	MCOJ, MCIJ MCIS]	t[33],148	abca	16,
Round 4	MCOJ, MCI]M[IS]	t[49],t[64	abcel	10,

In Round 1, Iteration 1 will use input M[0], t[1], about and generale new about Iteration a will use input M[1], t[2], previous sound about and generale new about the same process are repeated 64 times. The 64 iteration will use input as M[15], t [64] and about generated in 63rd ileration.

Subject Incharge: Prof. Sarala Mary Page No. 4

Department of CSE-Data Science | APSIT



Semester:

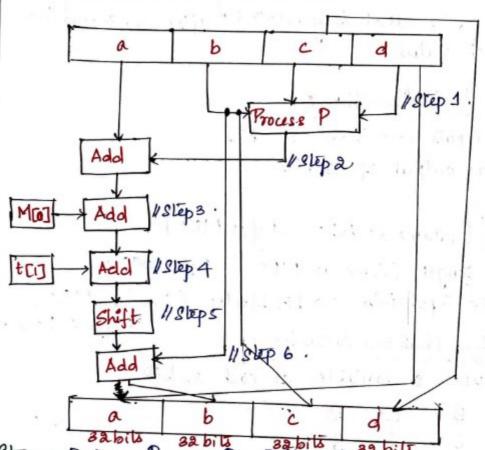
### A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering **Data Science** 



Academic Year: 2023 - 2024

Subject: CSC + Heration 1:-



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

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

Steps: Add M[o] to the output of steps.

Step4: Add t[i] to the output of step 3.

Steps: The output of slip 4 is circular left shift by shits. s can be any value.

Step 6: Add output of Step 5 with b.

Slep 7: The output of slep 6 becomes new b.

8408: The previous b becomes new c.

Stepq: The previous c is new d. Previous d'is new a.

Subject Incharge: Prof. Sarala Mary Page No. 5

Department of CSE-Data Science | APSIT



# A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering Data Science



Semester: Subject:
In every iliration new a bcd is generated. The abcd -> 1286ilis that is generated after 64 iterations
In every invalion has it agreeated after 64 iterations
abcd -> 128 bils that is garage
is the hash value.
SHA - lecure Hach Algorithm:
+ It takes inputs less than 2 64 bils.
* It produces output of 1606its.
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Pane as MDS - neget
sep 1: radating.  Refer MDS
Step 2: Padding. Lower Bame as MDS -> Refer MDS] Step 2: Append Length [Same as MDS -> Refer MDS] Step 3: Divide the input into Stabit blocks. [Same as MDS] (Refer MDS)
CIDS: Divide the man 1100 Section MDS)
Clarie Tuitalize Chaining Vallables
In SHA, it uses & variables of each 32 bits
A B C D F
1 1 1 1 1
82 82 82 82 82 bils bils.
Step 5: Process Blocks
LED S. L. Copyling chaining variables.
LEP 5.1 : Copyling enaithing
A B C D E
1 1
[a] [b] [c] [d].