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

In every iteration new a b c d is generated. The a b c d → 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).

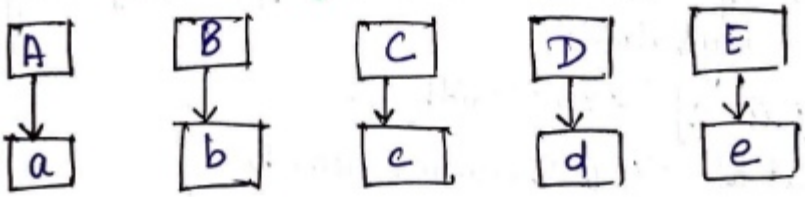
Step 4: Initialize Chaining Variables

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.



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

Step 5.2: Divide 512 bit blocks into 16 sub-blocks of each blocking having 32 bits

Same as MD5 → Refer MD5.

Step 5.3:

* It undergoes 4 Rounds.
* Each round has 20 iterations → 20 × 4 = 80 iterations.

INPUT FOR EACH ROUND

Round	Constant K[t]	Message Block W[t]	Chaining variables	Iterations
Round 1.	K[0]..... K[19] =5A827999	W[0].... W[19]	abcde	20
Round 2	K[20] ....K[39] =6ED9EBA1	W[20]....W[39]	abcde.	20
Round 3.	K[40].....K[59] =9F1BBCDC.	W[40].....W[59]	abcde	20
Round 4	K[60]....K[79] =CA62C1D6	W[60]....W[79]	abcde	20

* In SHA the constants are repeated for every 20 iterations, but the message blocks are unique for all 80 iteration.
* First 16 message blocks are from W[0] to W[15]. The remaing blocks are generated using them.

for i from 16 to 79.

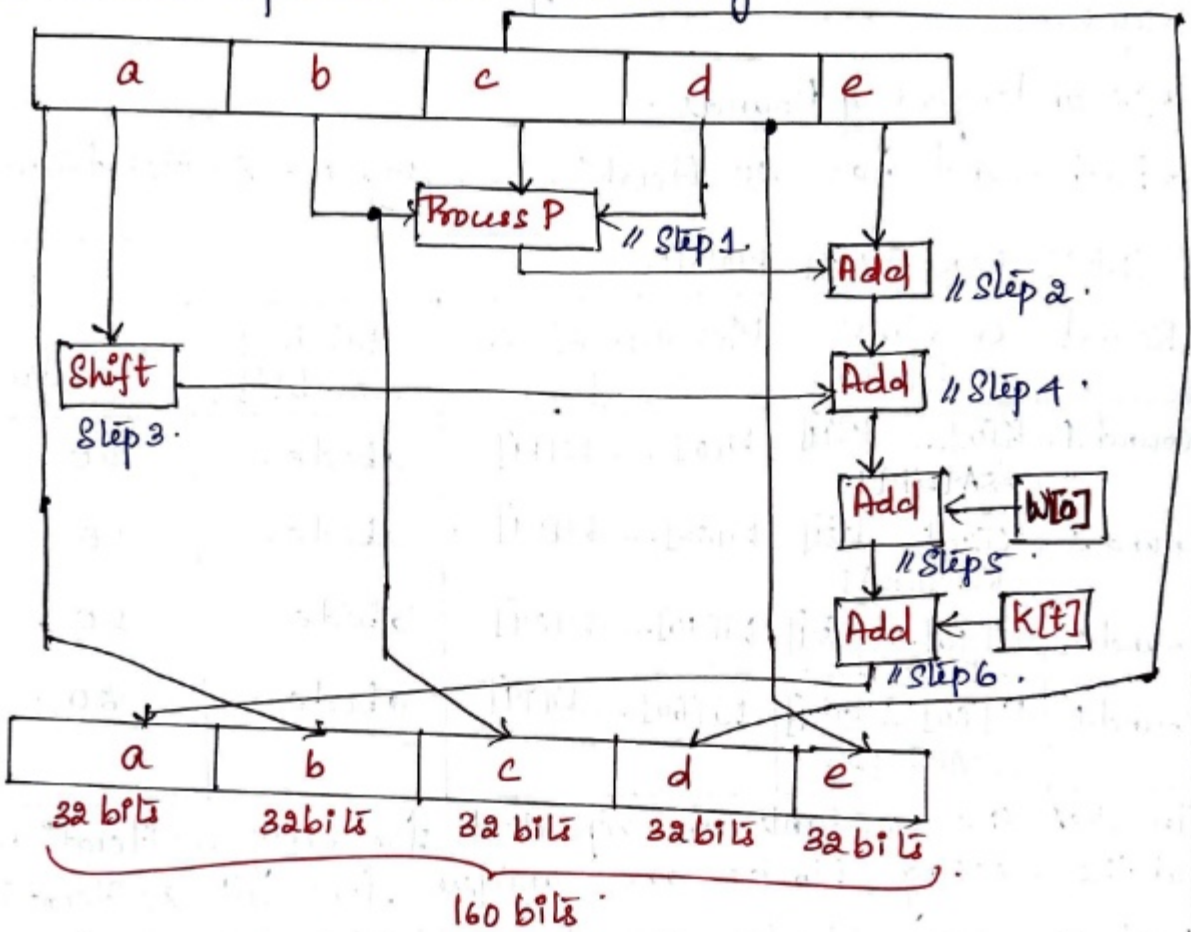
W[i] = (W[i-3] XOR W[i-8] XOR W[i-14] XOR W[i-16]) left rotate 1.

(eg) To find W[16].

W[16] = (W[16-3] XOR W[16-8] XOR W[16-14] XOR W[16-16]) left rotate 1

W[16] = (W[13] XOR W[8] XOR W[2] XOR W[0]) left rotate 1.

Substitute W[13], W[8], W[2], W[0] in the above equation and W[16] is generated.
The same is repeated till W[79] is generated.



ROUND 1 – ITERATION 1.

Step 1: Process P(b, c, d).
Step 2: Add output of step 1 with e.
Step 3: Left shift a by s bits. s can be any value.
Step 4: Add the output of step 3 and step 2.
Step 5: Add the output of step 4 with W[0].

Semester: VI Subject: CSS Academic Year: 2023 2024

Step 6: Add the output of step 5 with K[0].
Step 7: Output of step 6 is new a.
Step 8: Previous a is new b.
Step 9: Previous b is new c.
Step 10: Previous c is new d.
Step 11: Previous d is new e.

A new abcde is generated. The ~~sb~~ same steps are repeated 80 times. The final abcde that is generated after 80th iteration is the final hash value.