03/03/2022

⇒ SHA [Secure Hash Algo] :-

→ Hashing algo.
→ Published by NIST [National Institute of Stds & Technolgy]
→ O/p is fixed of 160 bits.

Step I] Step II] Same as MD5

Step III] Same as MD5

Step IV] Initialize Chaining var i.e. Buffers. There are 5 buffers each of 32 bits.

Total buffer length = 5 x 32 = 160 bits.

A = a
B = b
C = c
D = d
E = e

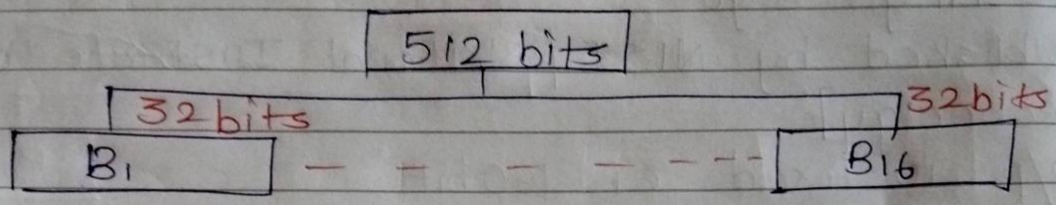
} Variables or Buffers.

Step V] Each Block of 512 bits will go for 4 rounds & every round has total 20 operations.

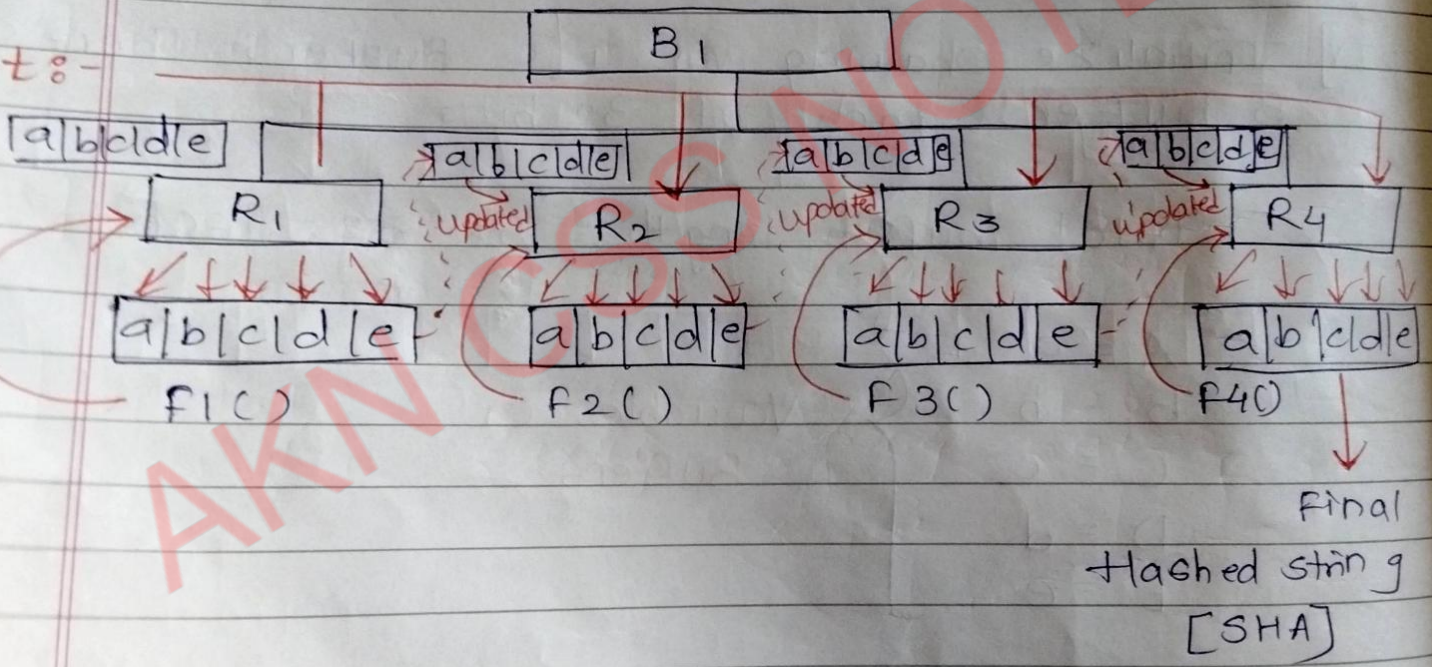
∴ Total Operation performed in Single Block = 20 x 4 = 80 bits

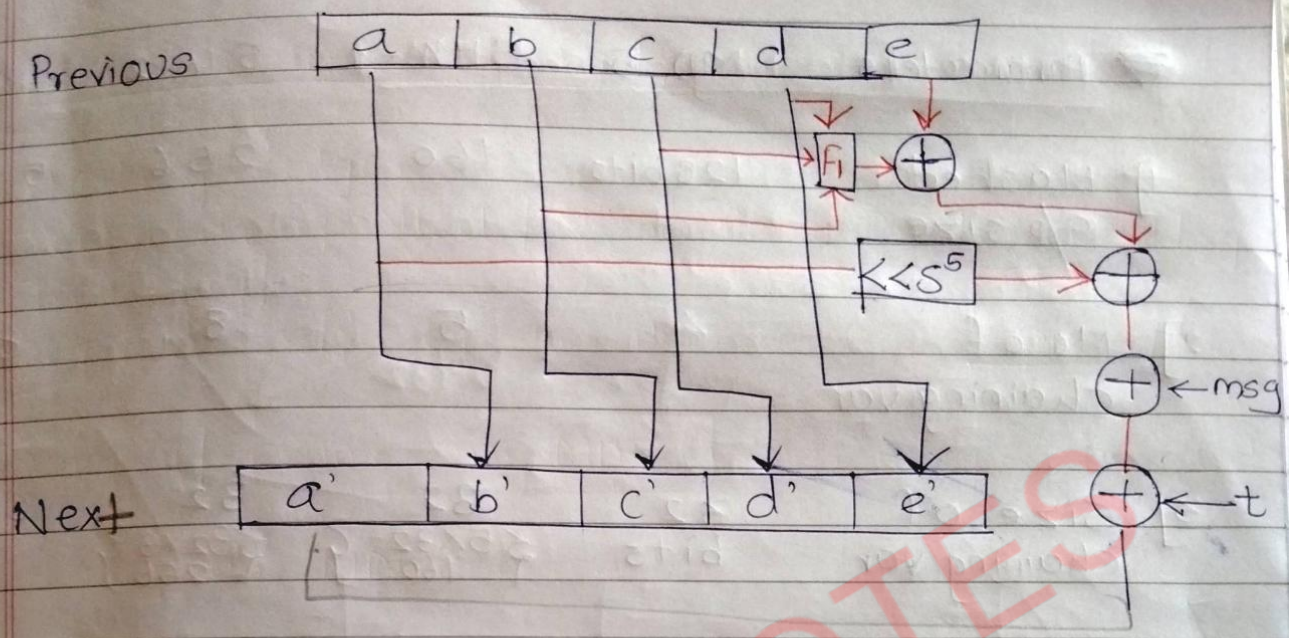
NOTE: All rounds have different operations

Step VI] Block Diag: Now 512 bits Block is divided into 16 blocks each of 32 bits.



Now on each block 4 rounds of oper^n will be performed where chaining var will be updated by some Func(x)





Operation performed on every Round :-

$b' = a$
$c' = b$
$d' = c$
$e' = d$

$$a' = \left[e \oplus f_1(b,c,d) \oplus [<<S^5(a)] \oplus msg \oplus t \right]$$

Where $\oplus$ → XOR

⇒ Parameters	MD-5	SHA-1	SHA-2	SHA
1] Hashed o/p size	128 bits	160	256	512
2] No. of chaining var	4 (128/32)	5 (160/32)	8	8
3] Size of chaining var	32 bits	32 {5×32 = 160}	32 {32×8 = 256}	64
4] Total Rounds in each block	4	4	4	4
5] Total oper^n per round	16 {4×4}	20 {5×4}	32 {8×4}	32 {8×4}
6] Total operation	64 {4×16}	80 {4×20} Rounds × oper^n	128 {4×32}	128 {4×32}