Lec 8

17 March 2022 18:04

Message Digest - 5

- Hashing algorithm
- Ron Rivest is the developer
- o/p is fixed of 128 bits

I Accept the message & do padding

message	padding

For padding:

Total Length of bits = should be multiple of 512 less 64

eg Message = 1000 bits

(1) $512 \times 1 = 512$ ×

(2) $512 \times 2 = 1024$ ×

(3) $512 \times 3 = 1536$ ✓

Padding bits = (Selected − 64) − message

$= (1536 - 64) - 1000$

$= 1472 - 1000$

$= 472$

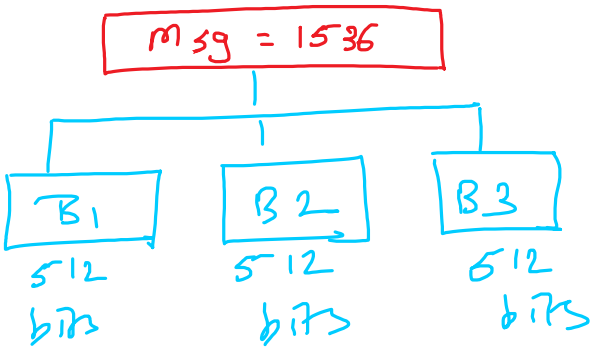
II Append a random string in the message appended with padding, random string = 64 bits

Note. kyu?

- To get randomness

Message	Padding	String
1000	472	64

III Divide the above message block into sub blocks each of 512 bits



IV Initialize the chaining variables i.e Buffers There are 4 buffers each of 32 bits

Total buffer length = $4 \times 32 = 128$ bits

Variables or Buffers:

- A = a
- B = b
- C = c
- D = d

V Round Explanation

Each Block of 512 bits will go for 4 Rounds & every round has total 16 operations.

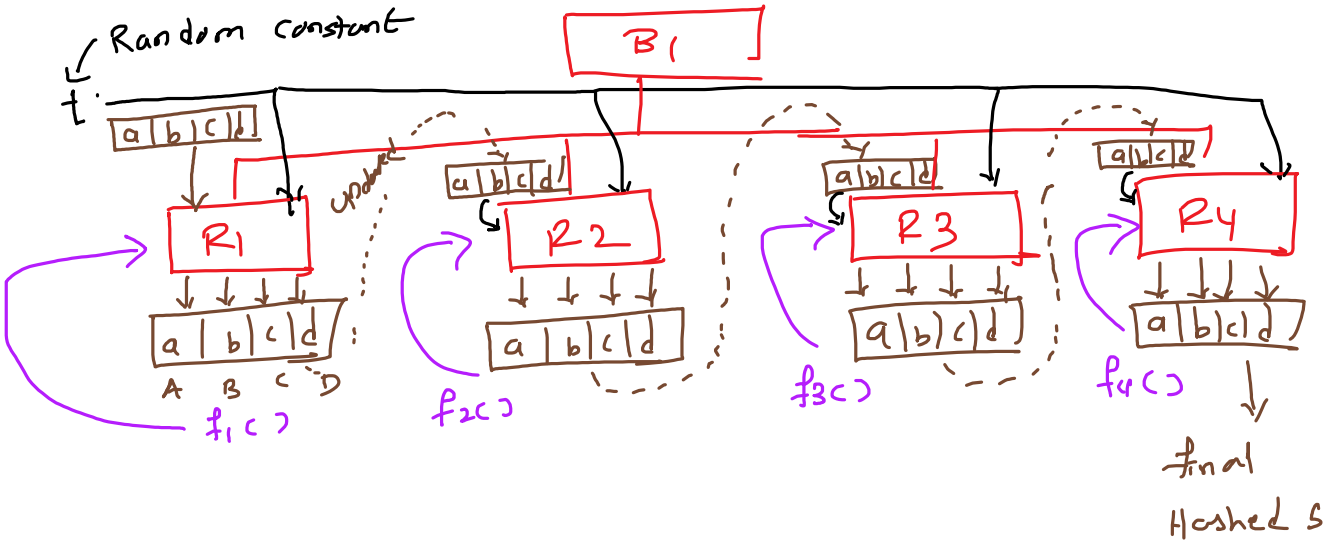
∴ Total operations performed in Single block = $16 \times 4 = 64$

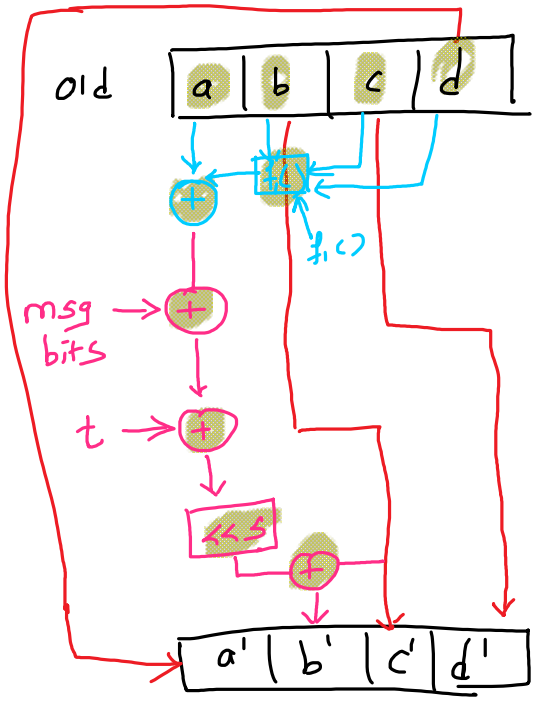
* All Rounds will have different operations

VII Block Digram Now 512bits Block is divided into 16 blocks each of 32bits

Now on every block 4 Rounds of operation will be performed where the chaining variables will be updated by some function

Random constant t





Operation performed on every Round:

$$a' = d$$
$$c' = b$$
$$d' = c$$
$$b' = b + \left[\{[a \oplus f_1(b,c,d)] \oplus msg \oplus t\} <<< s\right]$$

<<<: Left shift by random bits s