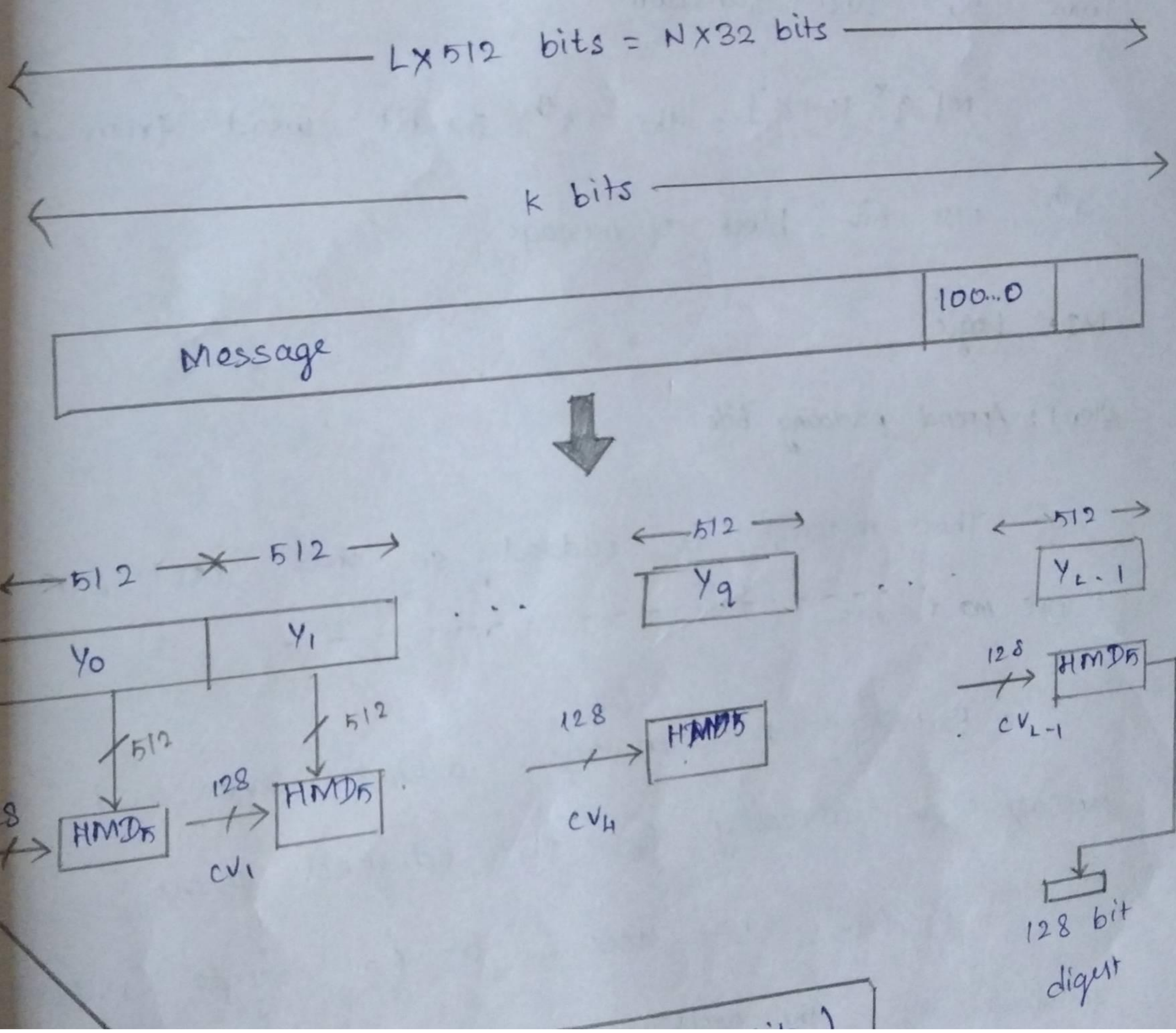
19CS6602 CNS - Assignment.

Write a neat diagram, explain the steps involved in MD5 algorithm.

MD5 is a cryptographic hash function algorithm that takes the message as input of any length and changes it into a fixed length message of 16-bytes. MD5 algorithm stands for the message-digest algorithm. MD5 was developed as an improvement of MD4, with advanced security purposes. the output of MD5 is always 128 bits. MD5 was developed in 1991 by Ronald Rivet



MD5 Logic

Step 1: Append padding bits

The message is padded so that its bit len

$= 448 \mod 512$

Padding is always added, even if the message is already of the desired length

Padding bits : 1000 . . . 0 (a single 1-bit followed by the necessary no. of 0-bits)

Step 2: Append Length

A 64 bit length : contains the length of original message modulo 2^{64}

The expanded message is $Y_0, Y_1, \ldots Y_{L-1}$ total length is $L \times 512$ bits

The expanded message can be through as a multiple of 16 32 bits word.

Let $M[0, \ldots, N-1]$ denote the word of the resulting message, where $N = L \times 16$

Sample processing:

Type	bits	data processed
MD5	128	469.7 MB/s
SHA-1	160	339.4 MB/s
SHA-512	512	177.7 MB/s.

⇒ MAC intel 2.66 Ghz core iM

⇒ 1024 bytes block of data

Step 3: Initialize MD Buffer

128 bit buffer is used to hold intermediate and final result of the hash function

A, B, C, D are initialized to the following values

A = 67452301

B = EFCDAB89

C = 98BADCFE

D = 1032 5476

Stored in little in diar format

Eg: word A : 01 23 45 67

word B : 89 AB CD EF

word C : FE DC BA 98

word D : 76 54 32 10

Step 4: Process Message in 512 bit

Heart of the algorithm called compression function consists of 4 rounds.

The 4 rounds have a similar structure, but each uses a different primitive logical fun reffered to as F, G, H and I

$$T[i] = 232 \times abs(\sin(i))$$

The output of 4th rounded is added to the CV_q to produce CV_{q+1}

Step 5: Output

After all L 512 bits blocks have bee processed, the output from the L^{th} stage is the 128-bit message digest

$$CV_q = IV$$

$$CV_{q+1} = SUM\ 32(CV_q; PFI[Y_q, RFH[Yq$$

$$RFG[Y_q, RFF[Y_q, CV_q$$

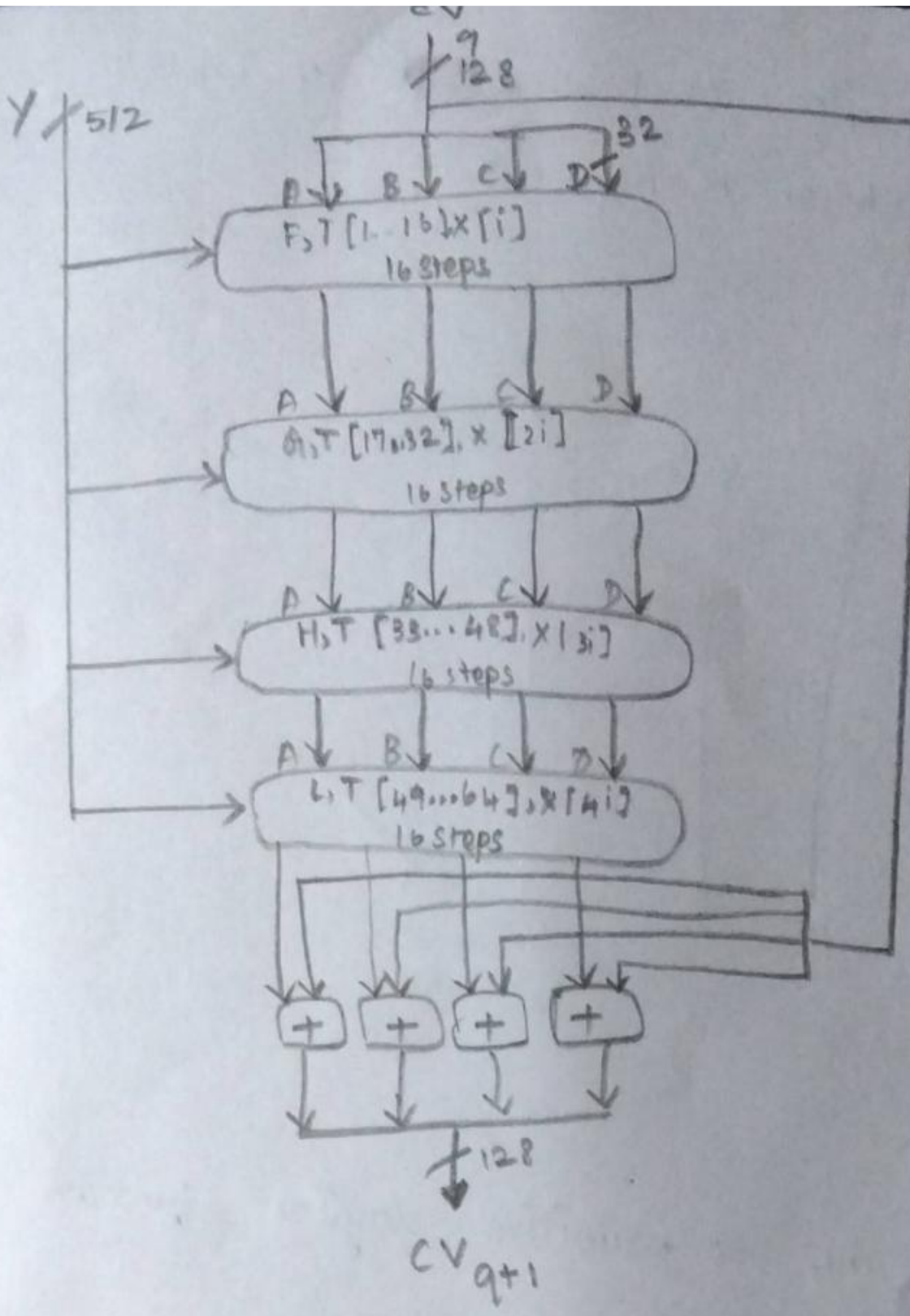
$$MD = CV_L$$

Y_q = the q^{th} 512 bit block of the message

L = the no. of block in the message

RFx = round function using primitive logic fu

MD = final message digest value.



MD5 processing of a single 512-bit block (MD5 compression function)

MD5 compression function:

Each round consists of a sequence of 16 steps operating on the buffer ABCD

Each step is of the form

$$a \leftarrow b + ((a + g(b,c,d) + X[k] + T[i]) <<< s)$$

where

a, b, c, d = the 4 words of the buffer, in a specified order that varies across steps

g = one of the primitive functions F, G, H, I

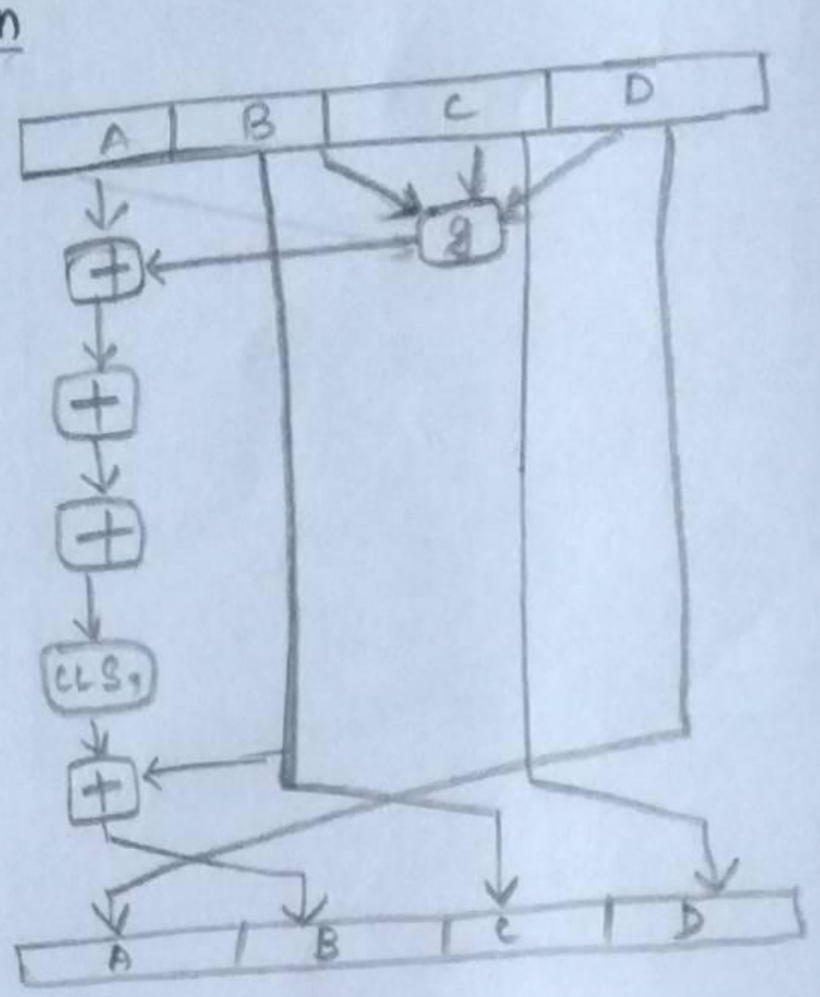
<<< s = circular left shift (rotation) of the 32-bit arguments by s bits.

X[k] = M[q × 16 + k] = the kth 32-bit word in the q^{th} 512-bit block of the message.

T[i] = the ith 32-bit world in Table T

+ = addition modulo 232

MD5 Operation



One of the 4 primitive logical function is used each 4 rounds of the algorithm.

Each primitive function takes three 32-bits word as input and produces a 32-bit word output.

Each function perform a set of bitwise logical operations