MD5 & SHA Algorithm

DR. VASUDHA ARORA

VASUDHA.ARORA@GDGU.ORG, VASUDHARORA6@GMAIL.COM

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

GD GOENKA UNIVERSITY, GURUGRAM

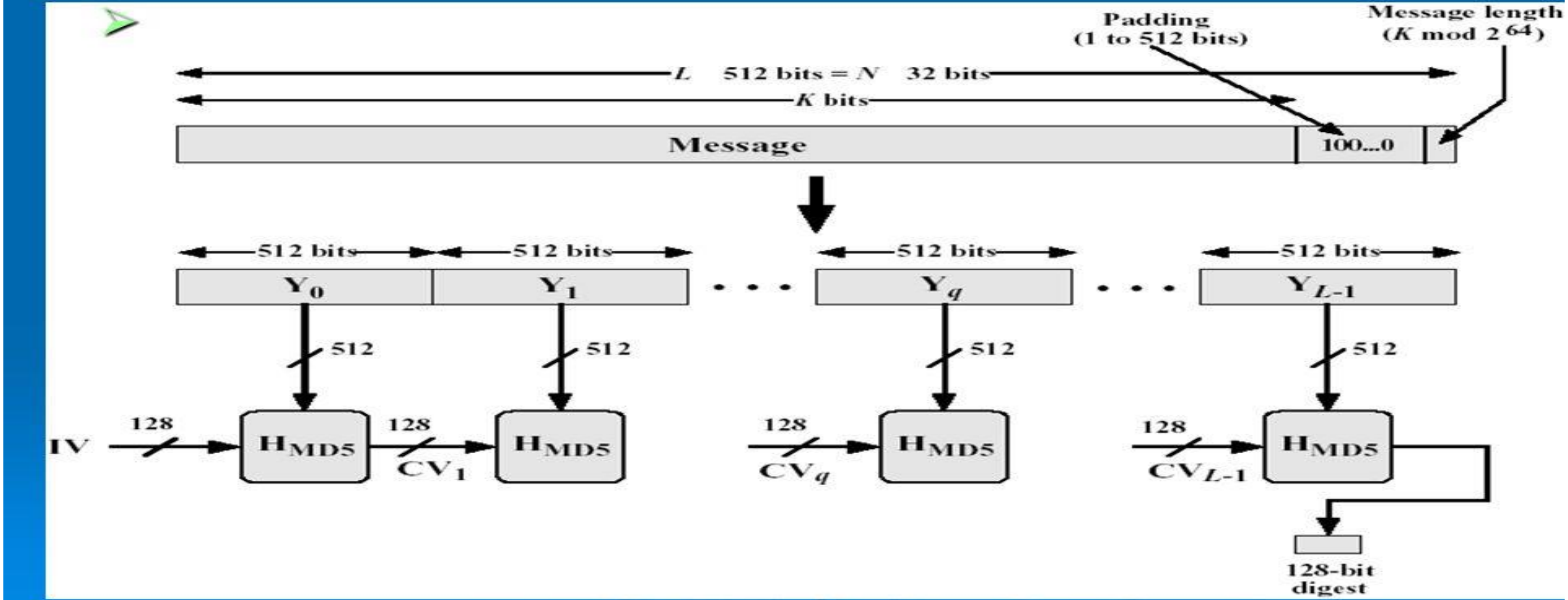
MD5-Introduction

- MD5 message digest algorithm is the 5th version of the Message Digest Algorithm developed by Ron Rivest to produce 128 bit message digest.
- MD5 is quite fast than other versions of message digest which takes the plain text of 512 bit blocks which is further divided into 16 blocks, each of 32 bit and produces the 128 bit message digest which is a set of four blocks, each of 32 bits.
- MD5 produces the message digest through five steps i.e. padding, append length, divide input into 512 bit blocks, initialize chaining variables a process blocks and 4 rounds, uses different constant it in each iteration.

Use of MD5 Algorithm

- It was developed with the main motive of security as it takes an input of any size and produces an output if a 128-bit hash value.
- To be considered cryptographically secure MD5 should meet two requirements:
  - It is impossible to generate two inputs that cannot produce the same hash function.
  - It is impossible to generate a message having the same hash value.
- Initially, MD5 was developed to store one way hash of a password and some file servers also provide pre-computed MD5 checksum of a file so that the user can compare the checksum of the downloaded file to it.
- Most Unix based Operating Systems include MD5 checksum utilities in their distribution packages.

MD5 Algorithm Architecture



How do the MD5 Algorithm works?

Step1: Padding Bits

- Padding means adding extra bits to the original message. So in MD5 original message is padded such that its length in bits is congruent to 448 modulo 512. Padding is done such that the total bits are 64 less being a multiple of 512 bits length.
- Padding is done even if the length of the original message is already congruent to 448 modulo 512. In padding bits, the only first bit is 1 and the rest of the bits are 0.

How do the MD5 Algorithm works?

Step2: Append Length

- Calculate the length of the original message and add it to the end of the message after padding.
- express length in 64 bits
- The total length of the message becomes a multiple of 512 bits

How do the MD5 Algorithm works?

Step3: Divide the input into 512 bit blocks

- Input message into blocks, each of length 512 bits

How do the MD5 Algorithm works?

Step4: Initialize MD Buffer

A four-word buffer (A, B, C, D) is used to compute the message digest. Each of A, B, C, D is a 32-bit register. These registers are initialized to the following values in hexadecimal, low-order bytes first):

word A: 01 23 45 67

word B: 89 ab cd ef

word C: fe dc ba 98

word D: 76 54 32 10

Actually algorithm considers the combination of ABCD as a 28-bit single register. This register is useful in actual algorithm operation for holding intermediate as well as final results.

How do the MD5 Algorithm works?

Step5: Process message in 16-word blocks

- Divide the current 512 bit block into 16 sub blocks. Thus, each sub block contains 32-bits

How do the MD5 Algorithm works?

Step5 (A) : Rounds in MD5

Now we have 4 rounds. In each round, we process all 16 subblocks belonging to a block.

The inputs of each round are:

a) All the 16 subblocks named M[i], from m[1] to M[16]

b) the memory words ABCD

c) some constants designated as t, where t is an array of 64 elements with each element consisting of 32 bits, denoted as t[k], from t[1] to t[64]. Since there are 4 rounds 16 out of 64 values are used in each round.

How do the MD5 Algorithm works?

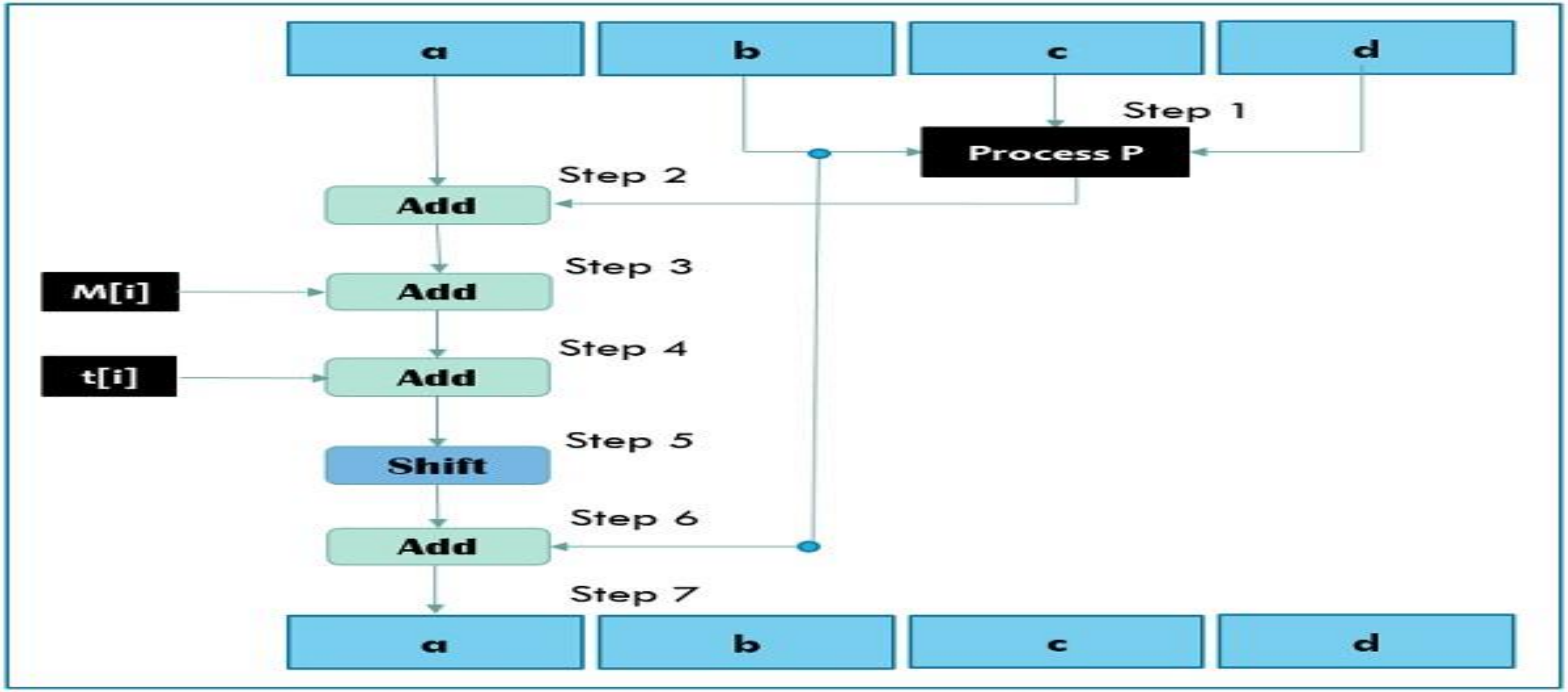
We have 16 iterations in each round.

1. A logical operation, say P, is first performed on B,C,D. This is different in all four rounds

Round No.	Logical operation P
1	(B AND C) OR ((NOT (B) AND D))
2	(B AND D) OR (C AND (NOT (D))
3	B XOR C XOR D
4	C XOR (B OR (NOT (D))

2. A is added to the output of the process P
3. The message sub-block M[i] is added to the output of the step 2
4. The constant t[k] is added to the output of step 3
5. The output of step 4 is circularly left shifted by s bits
6. B is added to the output of the step 5
7. The output of step 6 becomes new ABCD for next step.

How do the MD5 Algorithm works?



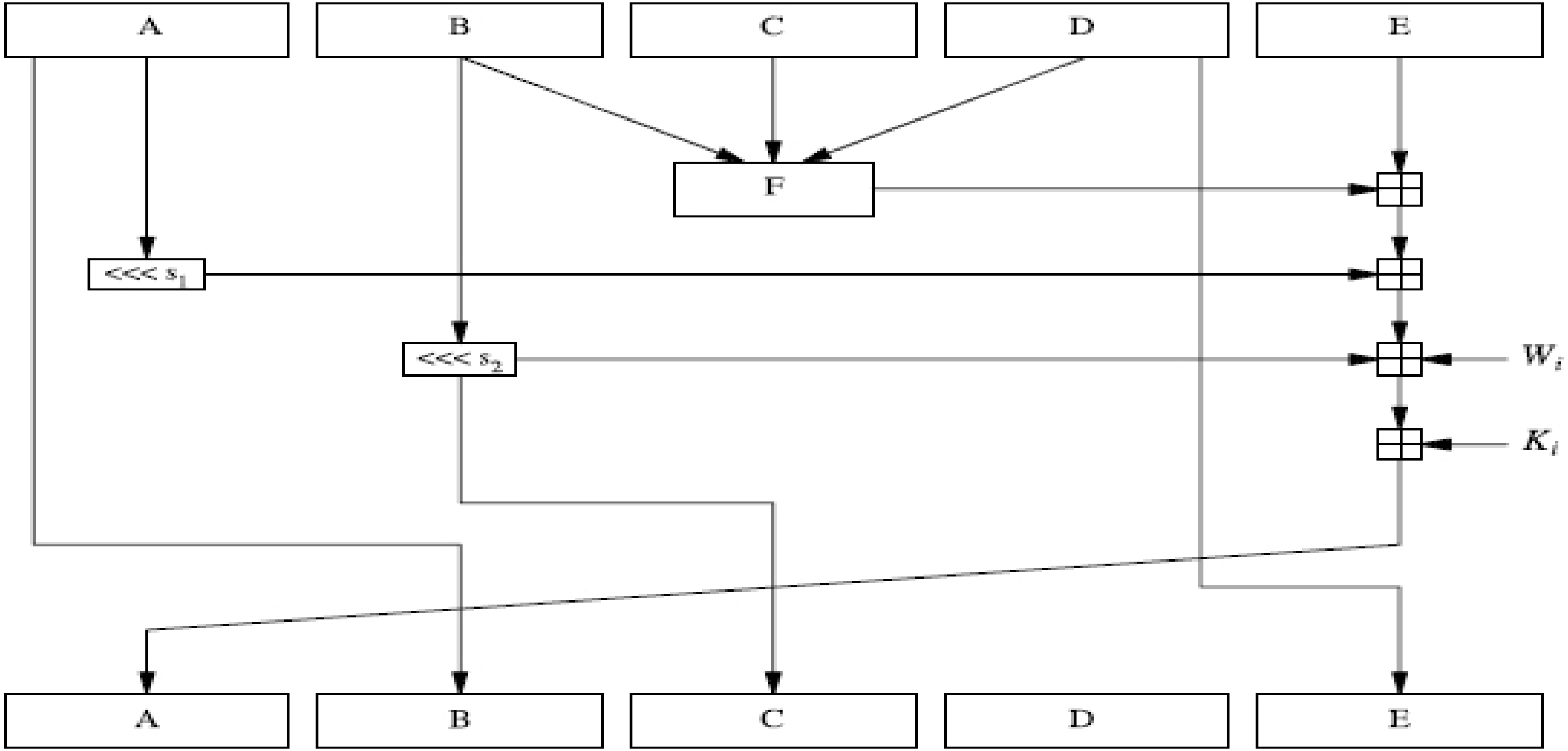
One MD5 Operation

How do the MD5 Algorithm works?

Mathematically, single MD5 operation can be expressed as follows:

$A = B + ((A + \text{Process } P\ (B,C,D) + M[i] + t[k]) <<< s)$

How SHA works



MD5 Vs SHA1

S.NO	MD5	SHA1
1.	MD5 stands for Message Digest.	While SHA1 stands for Secure Hash Algorithm.
2.	MD5 can have 128 bits length of message digest.	Whereas SHA1 can have 160 bits length of message digest.
3.	The speed of MD5 is fast in comparison of SHA1's speed.	While the speed of SHA1 is slow in comparison of MD5's speed.
4.	To make out the initial message the aggressor would want 2^128 operations whereas exploitation the MD5 algorithmic program.	On the opposite hand, in SHA1 it'll be 2^160 that makes it quite troublesome to seek out.
5.	MD5 is simple than SHA1.	While SHA1 is more complex than MD5.
6.	MD5 provides indigent or poor security.	While it provides balanced or tolerable security.
7.	In MD5, if the assailant needs to seek out the 2 messages having identical message digest then assailant would need to perform 2^64 operations.	Whereas in SHA1, assailant would need to perform 2^80 operations which is greater than MD5.
8.	MD5 was presented in the year 1992.	While SHA1 was presented in the year 1995.