Computer Network Security

TE - IT

Lecture -12
08/08/2022

Session: 12:00 - 1:00 PM

Prof. Stella J
Department of Information Technology
Xavier Institute of Engineering

Module-2

Authentication Algorithms

Hash Functions

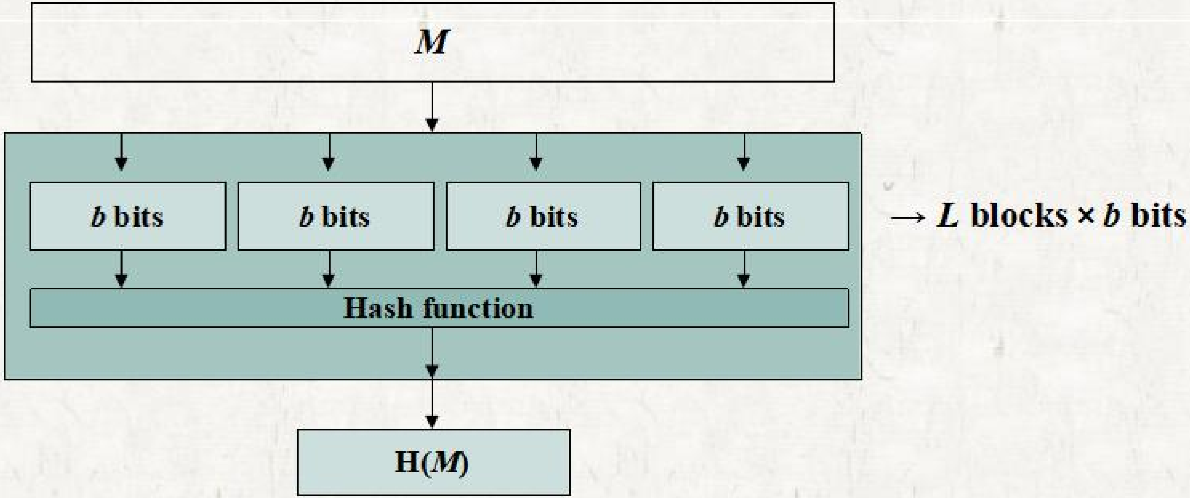
✓ SHA - 512

✓ SHA - 256

Module-2

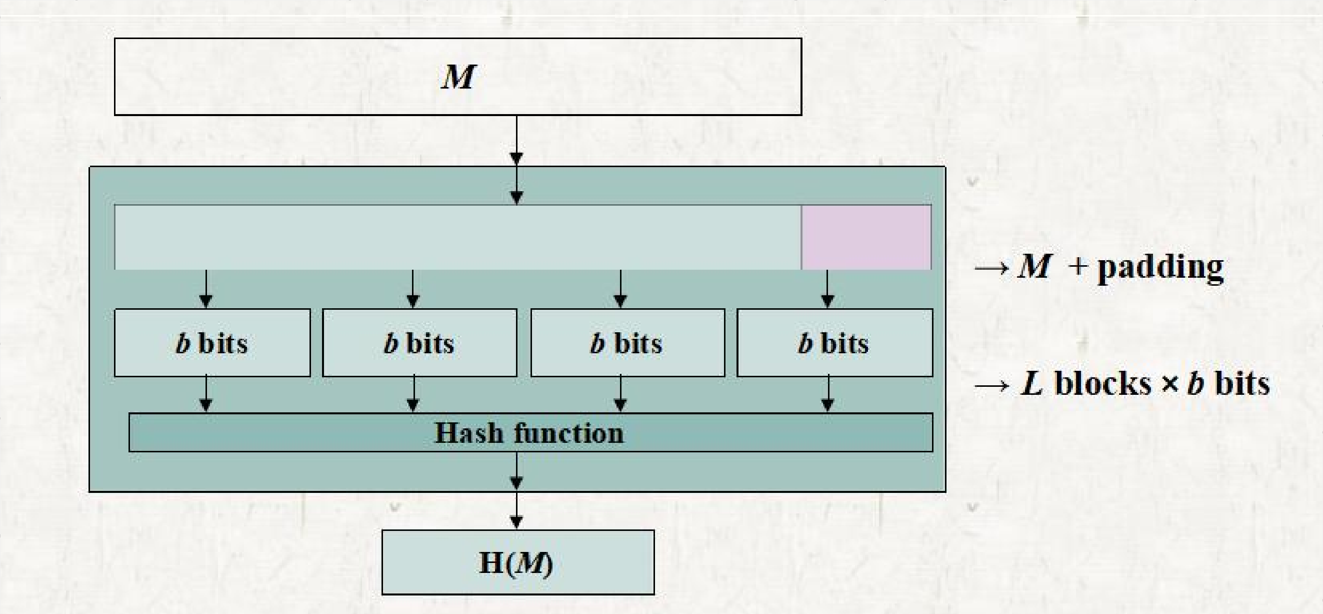
Hash Algorithm: It has no Key and No encryption and decryption

It generated fixed length of codes



Module-2

Hash Algorithm: If necessary the last bit is added with the padding bits



SHA - 512

1. Plain Text Block Size = 1024 bits
2. Number of rounds = 80
3. Each round processed with QWORD and CONSTANTS

QWORD = It is generated from PlainText

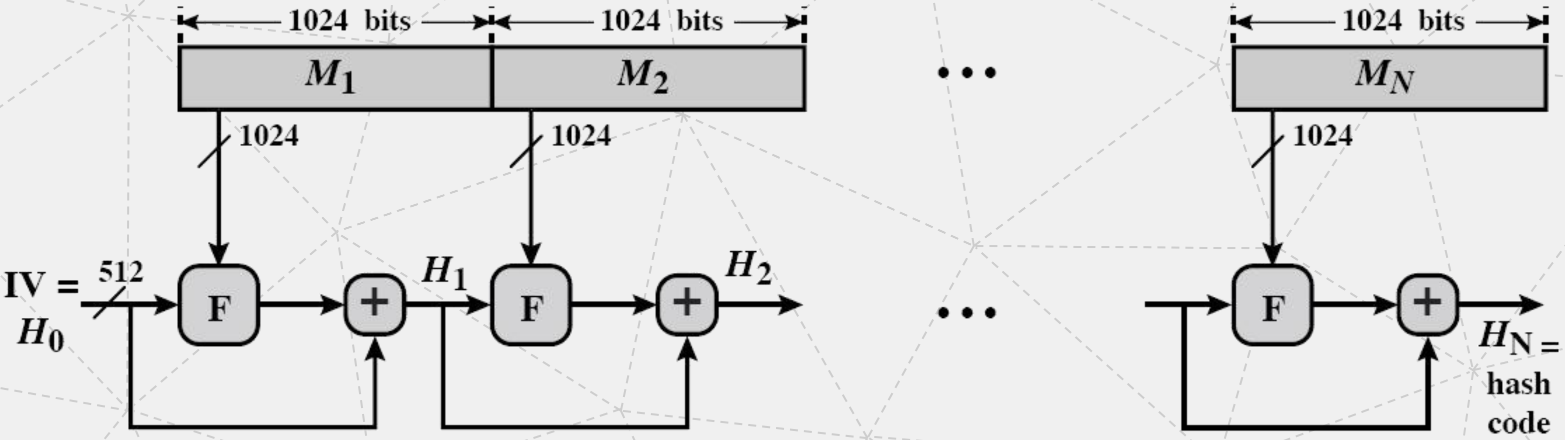
4. Each Round has buffers (a,b,c,d,e,f,g,h)
5. In SHA - 512 - 8 Buffers which is used to store intermediate results and output of each block.
6. Each buffer size = 64 bit

SHA - 512

1. Pad the bits 10000... so that the length of PT is 128 < multiple of 1024 bits
2. Append 128 bit representation of original PT such that length = multiple of 1024 bits
3. Initialize the buffers (a,b,c,d,e,f,g,h) 64 bits of hexadecimal values
4. Process each block of PT in 80 rounds
5. Output in Buffers is a Hash code (512 bits)

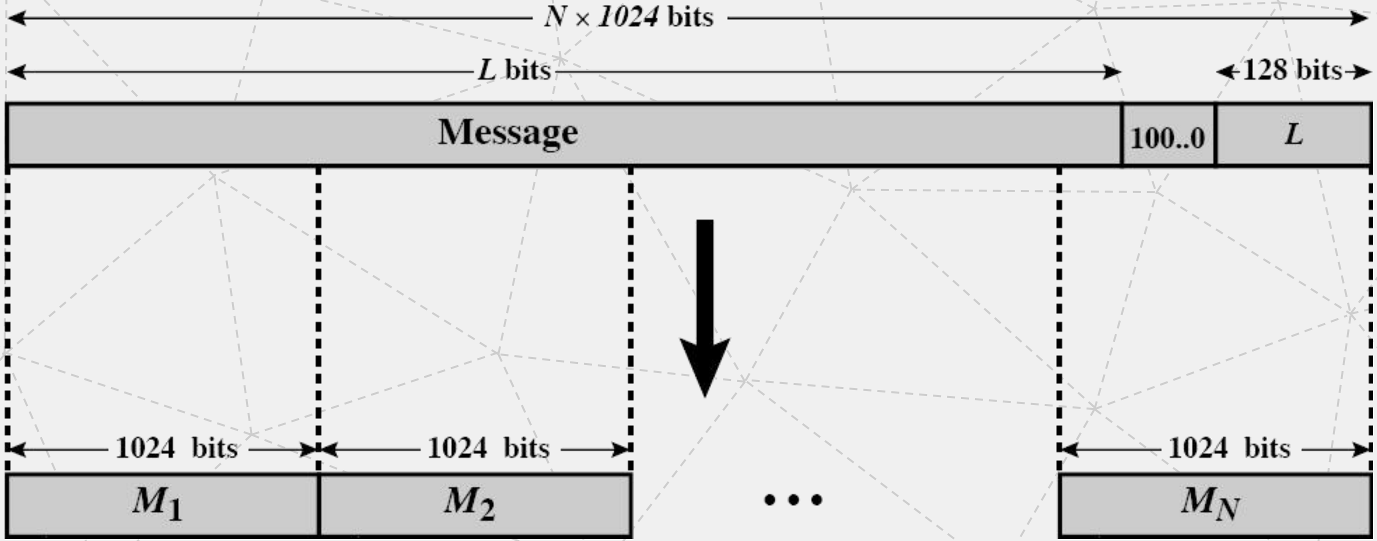
SHA - 512

SHA - 512 Architecture Diagram:



SHA - 512

1. Pad the bits 10000... so that the length of PT is 128 < multiple of 1024 bits
2. Append 128 bit representation of original PT such that length = multiple of 1024 bits



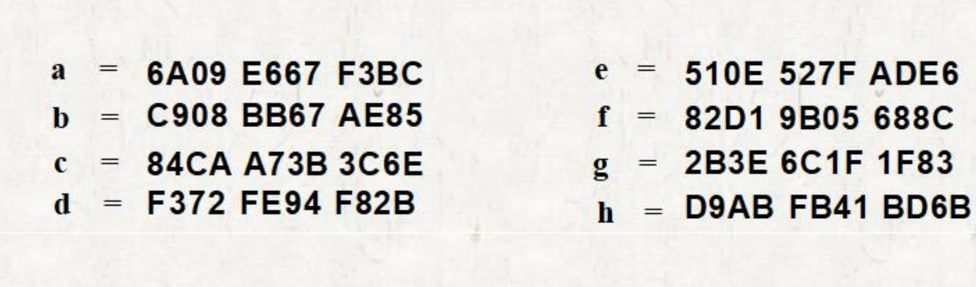
SHA - 512

3. Initialize the buffers (a,b,c,d,e,f,g,h) 64 bits of hexadecimal values for the round function

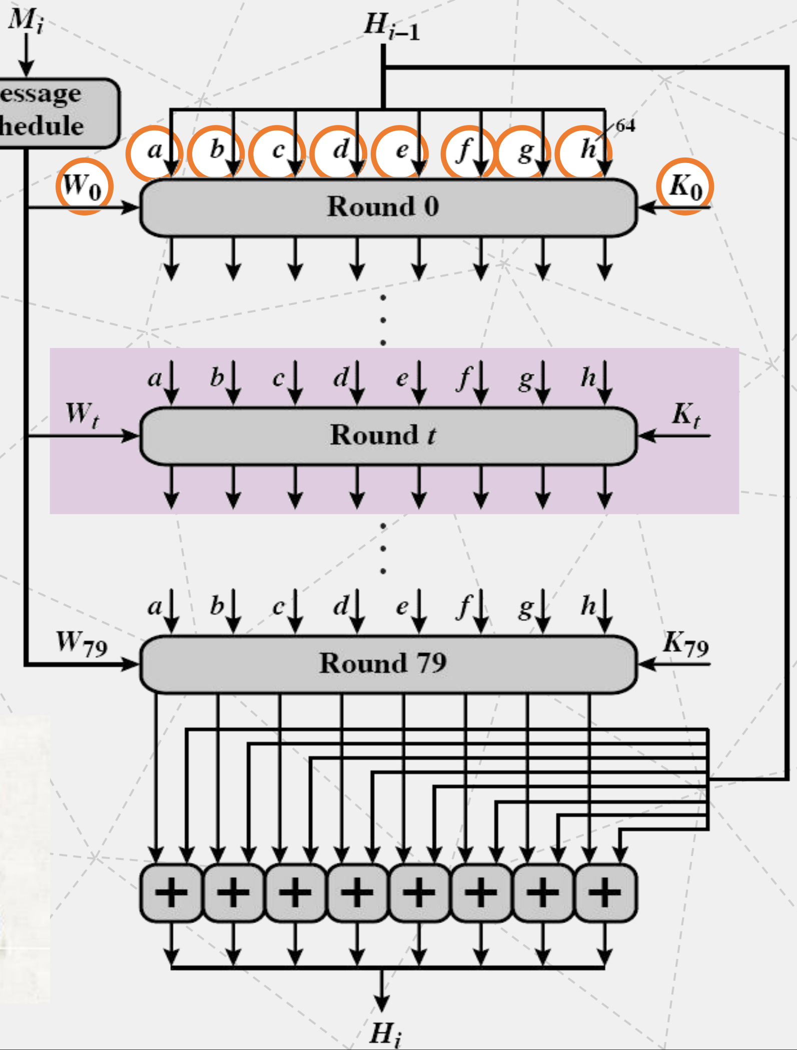
4. Process each block of PT in 80 rounds

- **three inputs required**

Word = W0 - W79
constant = KO - K79
Buffer = a - h

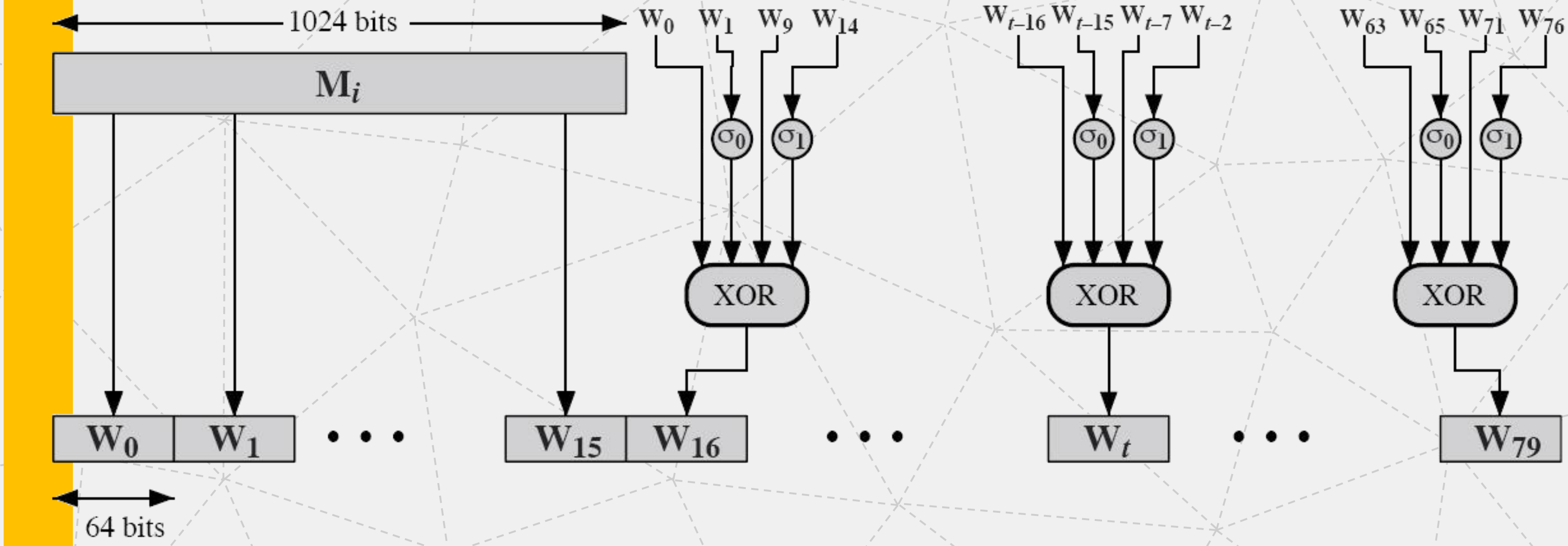


a	=	6A09 E667 F3BC	e	=	510E 527F ADE6
b	=	C908 BB67 AE85	f	=	82D1 9B05 688C
c	=	84CA A73B 3C6E	g	=	2B3E 6C1F 1F83
d	=	F372 FE94 F82B	h	=	D9AB FB41 BD6B



SHA - 512

Word Generation:

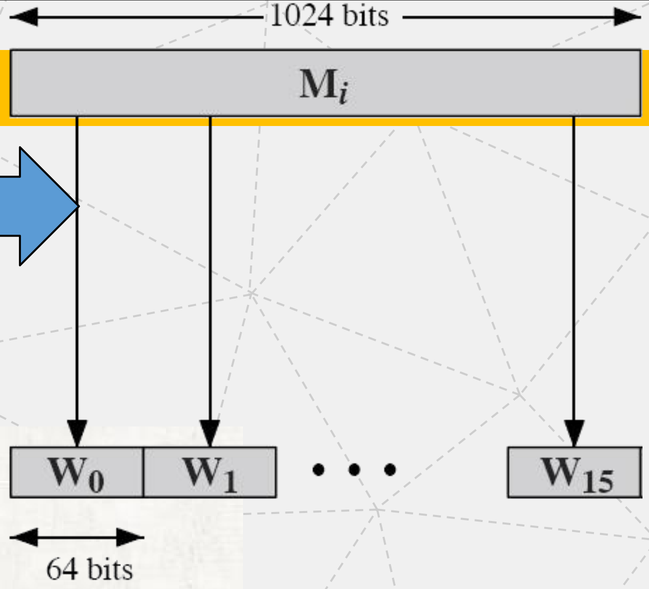


1024 bits
M_i
W_0 W_1 W_9 W_{14}
σ_0 σ_1
XOR
W_{t-16} W_{t-15} W_{t-7} W_{t-2}
σ_0 σ_1
XOR
W_{63} W_{65} W_{71} W_{76}
σ_0 σ_1
XOR
W_0 W_1 • • • W_{15} W_{16} • • • W_t • • • W_{79}
64 bits

64 bits x 16 bits = 1024 bits

SHA - 512

Word Generation: W_0 to W_{15} generated from PT



The remaining W_{16} - W_{79} values are defined as follows.

$$W_t = W_{t-16} + \sigma_0^{512}(W_{t-15}) + W_{t-7} + \sigma_1^{512}(W_{t-2})$$

where

$$\sigma_0^{512}(x) = \mathrm{ROTR}^1(x) \oplus \mathrm{ROTR}^8(x) \oplus \mathrm{SHR}^7(x)$$

$$\sigma_1^{512}(x) = \mathrm{ROTR}^{19}(x) \oplus \mathrm{ROTR}^{61}(x) \oplus \mathrm{SHR}^6(x)$$

$\mathrm{SHR}^n(x)$ = left shift of the 64 - bit argument x by n bits with padding *by zeroes on the right*

SHA - 512

Constants: K_0 - K_{79}

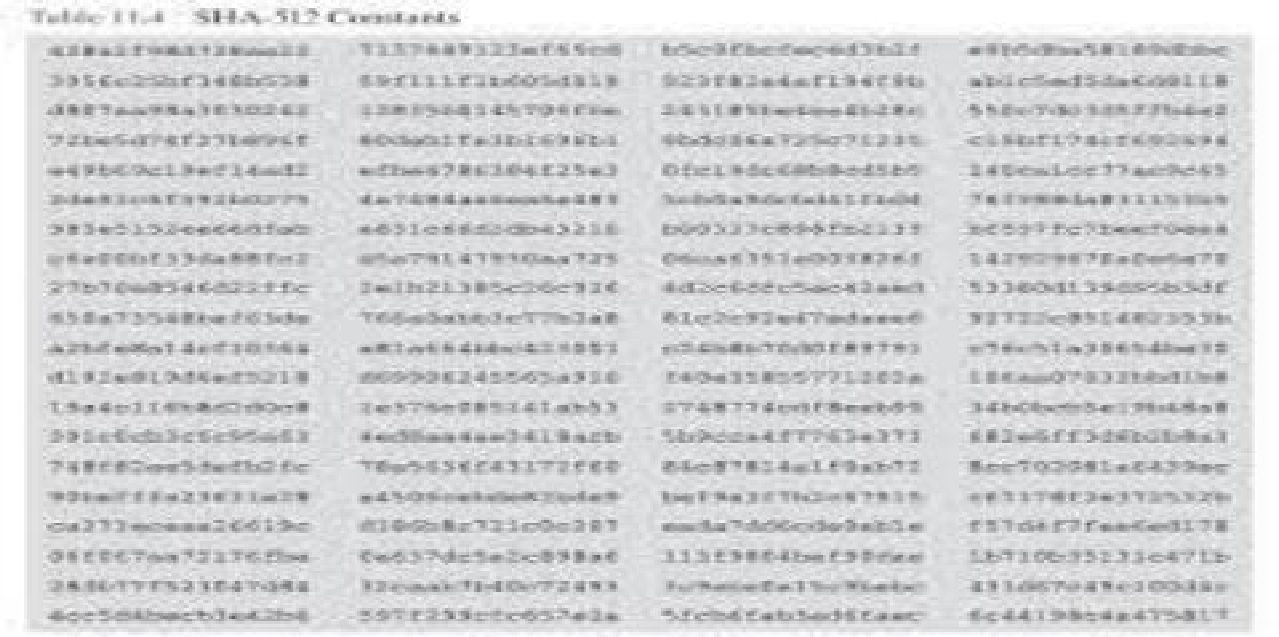
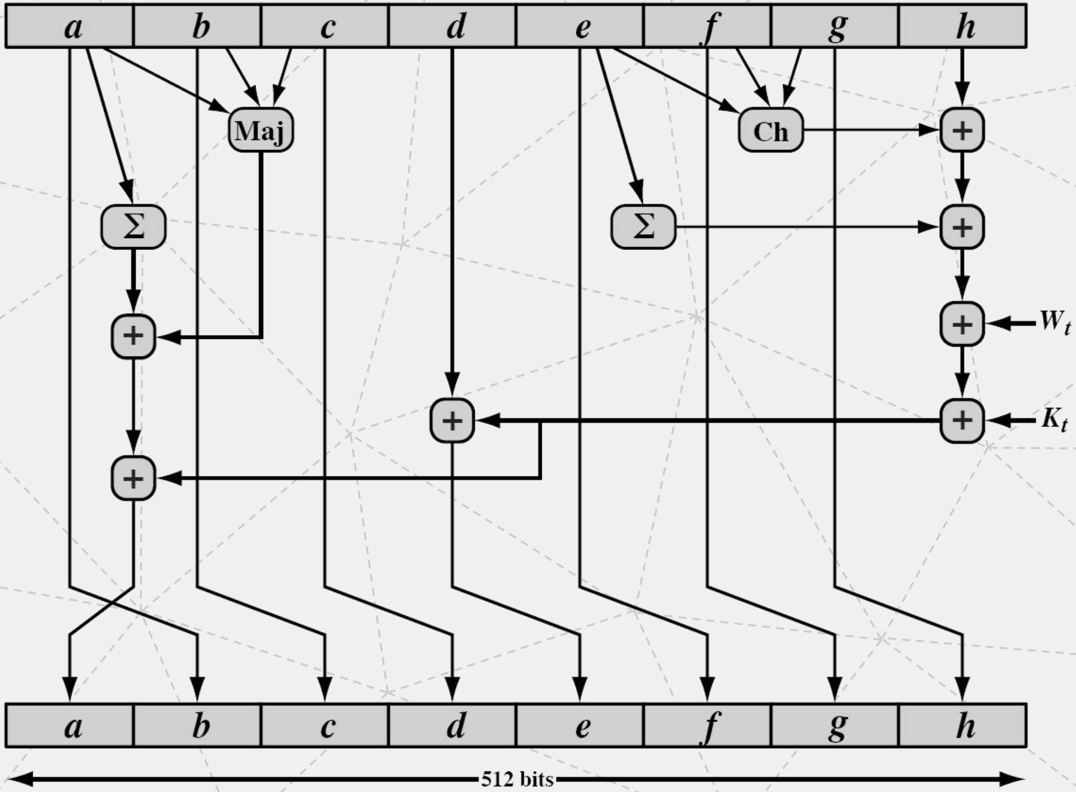


Table 11.4 SHA-512 Constants

428a2f98d728ae22	7137449123ef65cd	b5c0fbcfec4d3b2f	e9b5dba58189dbbc
3956c25bf348b538	59f111f1b605d019	923f82a4af194f9b	ab1c5ed5da6d8118
d807aa98a3030242	12835b0145706fbe	243185be4ee4b28c	550c7dc3d5ffb4e2
72be5d74f27b896f	80deb1fe3b1696b1	9bdc06a725c71235	c19bf174cf692694
e49b69c19ef14ad2	efbe4786384f25e3	0fc19dc68b8cd5b5	240ca1cc77ac9c65
2de92c6f592b0275	4a7484aa6ea6e483	5cb0a9dcbd41fbd4	76f988da831153b5
983e5152ee66dfab	a831c66d2db43210	b00327c898fb213f	bf597fc7beef0ee4
c6e00bf33da88fc2	d5a79147930aa725	06ca6351e003826f	142929670a0e6e70
27b70a8546d22ffc	2e1b21385c26c926	4d2c6dfc5ac42aed	53380d139d95b3df
650a73548baf63de	766a0abb3c77b2a8	81c2c92e47edaee6	92722c851482353b
a2bfe8a14cf10364	a81a664bbc423001	c24b8b70d0f89791	c76c51a30654be30
d192e819d6ef5218	d69906245565a910	f40e35855771202a	106aa07032bbd1b8
19a4c116b8d2d0c8	1e376c085141ab53	2748774cdf8eeb99	34b0bcb5e19b48a8
391c0cb3c5c95a63	4ed8aa4ae3418acb	5b9cca4f7763e373	682e6ff3d6b2b8a3
748f82ee5defb2fc	78a5636f43172f60	84c87814a1f0ab72	8cc702081a6439ec
90befffa23631e28	a4506cebde82bde9	bef9a3f7b2c67915	c67178f2e372532b
ca273eceea26619c	d186b8c721c0c207	eada7dd6cde0eb1e	f57d4f7fee6ed178
06f067aa72176fba	0a637dc5a2c898a6	113f9804bef90dae	1b710b35131c471b
28db77f523047d84	32caab7b40c72493	3c9ebe0a15c9bebc	431d67c49c100d4c
4cc5d4becb3e42b6	597f299cfc657e2a	5fcb6fab3ad6faec	6c44198c4a475817

SHA - 512

Processing the Round Function:



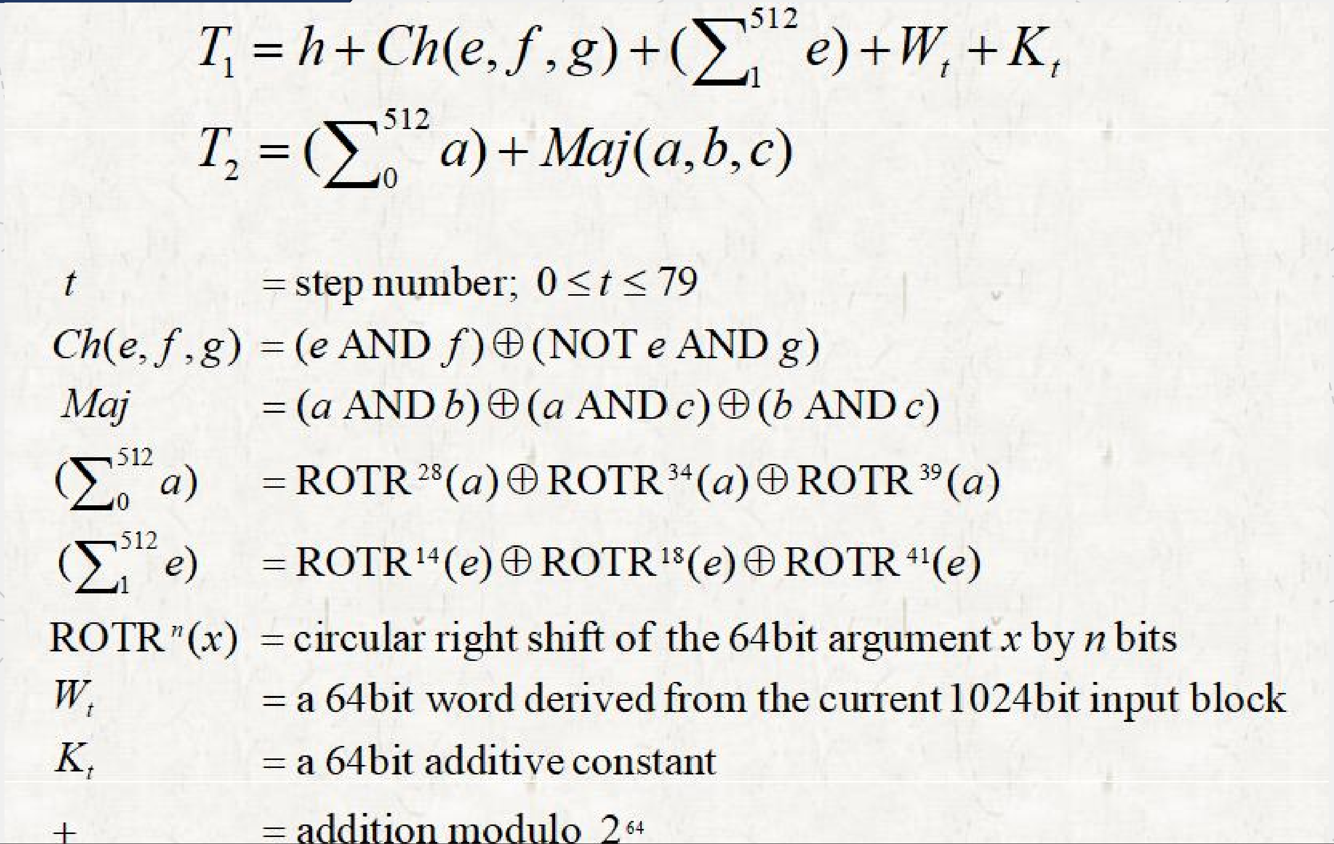
$a = T_1 + T_2$ $\quad e = d + T_1$

$b = a$ $\quad f = e$

$c = b$ $\quad g = f$

$d = c$ $\quad h = g$

SHA - 512



$$T_1 = h + Ch(e, f, g) + (\sum\nolimits_1^{512} e) + W_t + K_t$$

$$T_2 = (\sum\nolimits_0^{512} a) + Maj(a, b, c)$$

t = step number; $0 \le t \le 79$

$Ch(e, f, g)$ = $(e \text{ AND } f) \oplus (\text{NOT } e \text{ AND } g)$

Maj = $(a \text{ AND } b) \oplus (a \text{ AND } c) \oplus (b \text{ AND } c)$

$(\sum\nolimits_0^{512} a)$ = $\text{ROTR}^{28}(a) \oplus \text{ROTR}^{34}(a) \oplus \text{ROTR}^{39}(a)$

$(\sum\nolimits_1^{512} e)$ = $\text{ROTR}^{14}(e) \oplus \text{ROTR}^{18}(e) \oplus \text{ROTR}^{41}(e)$

$\text{ROTR}^{n}(x)$ = circular right shift of the 64bit argument x by n bits

W_t = a 64bit word derived from the current 1024bit input block

K_t = a 64bit additive constant

$+$ = addition modulo 2^{64}

THANK YOU