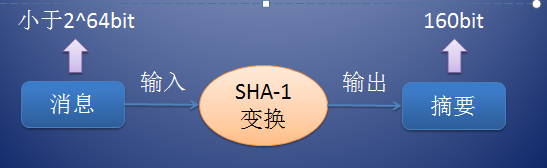
**实验原理**

* 可以对长度不超过2^64比特的消息进行计算，输入以512位数据块为单位处理，产生160比特的消息摘要作为输出。



* 准备工作：把原始消息（如字符串、文件等）转换成bit序列。

“abc”

01100001 01100010 01100011

原始消息

bit序列

转换

‘a’=0x61 ‘b’=0x62 ‘c’=0x63

* 步骤1：补位。最高位补1，其余补0，使得数据位总长度对512取余的结果为448。

01100001 01100010 01100011

原始序列

补位后序列

01100001 01100010 01100011

10000000000 … … 00000000000

24位

补1位1，补423位0

448位

* 补位。最高位补1，其余补0，使得数据位总长度对512取余的结果为448。

**61626380 00000000 00000000 00000000**

**00000000 00000000 00000000 00000000**

**00000000 00000000 00000000 00000000**

**00000000 00000000**

补位后的序列

转换成16进制

* 步骤2：补长度。将原始数据的长度补到补位操作后的消息后面。

**61626380 00000000 00000000 00000000**

**00000000 00000000 00000000 00000000**

**00000000 00000000** **00000000 00000000**

00000000 00000000 00000000 00000018

补位后的序列

转换成16进制

* 步骤3：将步骤2得到的消息M以512bit分组。

M1

**M = M1 || M2 || … || Mi || … || Mn**

**512bit**

**512bit**

**512bit**

**512bit**

**M = 61626380 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000**

**00000000 00000000 00000000 00000018**

* 步骤4：对于Mi进行以下处理
* （1）将Mi分成16个字W0，W1，…,W15

M1 = 61626380 00000000 00000000 00000000

W0 W1 W2 W3

00000000 00000000 00000000 00000000

W4 W5 W6 W7

00000000 00000000 00000000 00000000

W8 W9 W10 W11

00000000 00000000 00000000 00000018

W12 W13 W14 W15

* （2）将16个字扩展至80个字,W16，W17，…,W79

Wt = S1(Wt-3 ⊕Wt-8 ⊕Wt-14 ⊕Wt-16) (0 ≤ t ≤ 19)

St(W) 将W循环左移t位

* 步骤5：进行散列函数的计算, SHA-1算法的核心共4轮，每轮20步，共80步。
* （1）初始化MD缓冲区{Hi}，160bit(5个32位的寄存器)。

H0= 0x67452301

H1 = 0xEFCDAB89

H2= 0x98BADCFE

H3= 0x10325476

H4= 0xC3D2E1F0

* (2) 更新缓存ABCDE的内容，缓存ABCDE的初始值为：

A = H0

B = H1

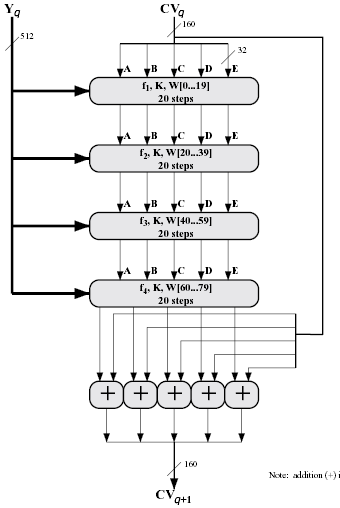
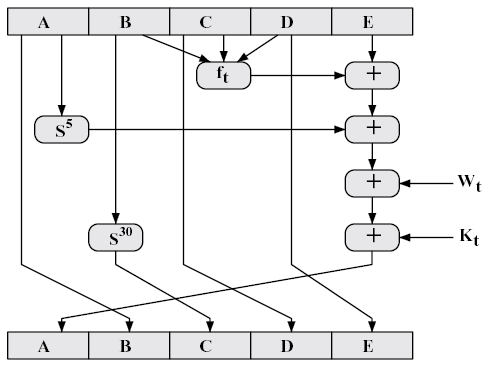
C = H2

D = H3

E = H4

* 共4轮，每轮的常数K为：

Kt = 5A827999 ( 0 ≤ t ≤ 19)   
 Kt = 6ED9EBA1 (20 ≤ t ≤ 39)   
 Kt = 8F1BBCDC (40 ≤ t ≤ 59)   
 Kt = CA62C1D6 (60 ≤ t ≤ 79)

* 
* 
* （3）对于0 ≤ t ≤ 79，执行以下循环：

**TEMP = S5(A) + ft(B,C,D) + E + Wt + Kt**

**ft(B,C,D) = (B ∧C) ∨((¬ B) ∧ D) ( 0 ≤ t ≤ 19)   
ft(B,C,D) = B ⊕ C ⊕ D (20 ≤ t ≤ 39)   
ft(B,C,D) = (B ∧ C) ∨ (B ∧ D) ∨ (C ∧ D) (40 ≤ t ≤ 59)   
ft(B,C,D) = B ⊕ C ⊕ D (60 ≤ t ≤ 79)**

**B = A，C = (B<<30)，D = C，E = D**

E = D ; D = C ; C = S30(B) ; B = A ; A = TMP

* （4）上一步循环执行完成后，令

H0 = H0 + A

H1 = H1 + B

H2 = H2 + C

H3 = H3 + D

H4 = H4 + E

* 步骤6：重复步骤5，对消息块M1…Mn进行处理。

TEMP = S5(A) + ft(B,C,D) + E + Wt + Kt

E = D ; D = C ; C = S30(B) ; B = A ; A = TMP

* 处理完所有的Mn后，得到160bit消息摘要

H0 H1 H2 H3 H4