SHA1分步骤演示

消息填充

明文 1

16进制 2

填充“1” 3

2进制 4

填充“0” 5

16进制 6

填充长度与分组 7

16进制 8

第一部分 计算首个数据块的摘要

初始化 9

	H0	H1	H2	H3	H4
16进制	10	11	12	13	14

扩充第0--15组 明文 15

W(0-3) 16 W(4-7) 17

W(8-11) 18 W(12-15) 19

扩充第16--79组 明文 20

16进制 21

读取变量初始值 22

	A	B	C	D	E
16进制	23	24	25	26	27

4轮共80步计算 28

	A	B	C	D	E
16进制	29	30	31	32	33

求和运算 34

	H0	H1	H2	H3	H4
16进制	35	36	37	38	39

算法原理

填充 “1”

明文的十六进制显示（注：填充后明文长度是512位的整数倍）

明文填充一位 “1”

填充 “0”

明文填充“0”，把明文补至448位

填充长度与分组

明文填充64位（原始明文长度的64位表示），明文补至512位

512位明文分为16份子明文分组；Mi=0,1…15

初始化

初始化2组变量，每组5个32位的变量分别为A,B,C,D,E；H0,H1,H2,H3,H4

A=H0=0x67452301 B=H1=0xEFCDAB89 C=H2=0x98BADCFE

D=H1=0x10325476 E=H1=0xC3D2E1F0

扩充第0--15组 明文

利用公式将16份子明文分组扩充到80份子明文分组；Wi=0,1…79

扩充公式为：W t = M t ， 当0≤t≤15

扩充第16--79组 明文

扩充公式为：W t = (W t-3 ⊕ W t-8 ⊕ W t-14 ⊕ W t-16) <<< 1， 当16≤t≤79

读取变量初始值

读取变量A,B,C,D,E的初始值

4轮共80步计算

结果计入 A,B,C,D,E 5个变量中

SHA1的4轮每轮20步运算，共80个步骤；使用如下公式操作

A,B,C,D,E←[(A<<<5)+ft(B,D,C)+E+Wt+Kt],A,(B<<<30),C,D

其中ft(B,D,C)为逻辑函数，Wt为子明文分组W[t]，Kt为固定常数。

```
Kt = 0x5A827999      (0 <= t <= 19)
Kt = 0x6ED9EBA1     (20 <= t <= 39)
Kt = 0x8F1BBCDC     (40 <= t <= 59)
Kt = 0xCA62C1D6     (60 <= t <= 79)
ft(B,C,D) =(B AND C) or (NOT B) AND D)          ( 0 <= t <= 19)
ft(B,C,D) = B XOR C XOR D                       (20 <= t <= 39)
ft(B,C,D) =(B AND C) or (B AND D) or (C AND D)  (40 <= t <= 59)
ft(B,C,D) = B XOR C XOR D                       (60 <= t <= 79)
```