

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

16进制 H0 10 H1 11 H2 12 H3 13 H4 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

16进制 A 23 B 24 C 25 D 26 E 27

4轮共80步计算 28

16进制 A 29 B 30 C 31 D 32 E 33

求和运算 34

16进制 H0 35 H1 36 H2 37 H3 38 H4 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； $M_i=0, 1\cdots 15$ 

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=H3=0x10325476 E=H4=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； $W_i=0, 1\cdots 79$ 扩充公式为： $W_t = M_t$ ，当 $0 \leq t \leq 15$

扩充第16--79组 明文

扩充公式为： $W_t = (W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16}) \lll 1$ ，当 $16 \leq t \leq 79$

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) + f_t(B, D, C) + E + W_t + K_t], A, (B << 30), C, D

其中 $f_t(B, D, C)$ 为逻辑函数， W_t 为子明文分组 $W[t]$ ， K_t 为固定常数。 $K_t = 0x5A827999$ ($0 \leq t \leq 19$) $K_t = 0x6ED9EBA1$ ($20 \leq t \leq 39$) $K_t = 0x8F1BBCDC$ ($40 \leq t \leq 59$) $K_t = 0xCA62C1D6$ ($60 \leq t \leq 79$) $f_t(B, C, D) = (B \text{ AND } C) \text{ or } ((\text{NOT } B) \text{ AND } D)$ ($0 \leq t \leq 19$) $f_t(B, C, D) = B \text{ XOR } C \text{ XOR } D$ ($20 \leq t \leq 39$) $f_t(B, C, D) = (B \text{ AND } C) \text{ or } (B \text{ AND } D) \text{ or } (C \text{ AND } D)$ ($40 \leq t \leq 59$) $f_t(B, C, D) = B \text{ XOR } C \text{ XOR } D$ ($60 \leq t \leq 79$)

80步运算

A, B, C, D, E ←

[(A << 5) + f_t(B, D, C) + E + W_t + K_t], A, (B << 30), C, D

第1轮： $F_t, W[0\sim 19], K_t$ 20第2轮： $F_t, W[20\sim 39], K_t$ 20第3轮： $F_t, W[40\sim 59], K_t$ 20第4轮： $F_t, W[60\sim 79], K_t$ 20第5轮： $F_t, W[80\sim 89], K_t$ 20第6轮： $F_t, W[90\sim 99], K_t$ 20第7轮： $F_t, W[100\sim 109], K_t$ 20第8轮： $F_t, W[110\sim 119], K_t$ 20第9轮： $F_t, W[120\sim 129], K_t$ 20第10轮： $F_t, W[130\sim 139], K_t$ 20第11轮： $F_t, W[140\sim 149], K_t$ 20第12轮： $F_t, W[150\sim 159], K_t$ 20第13轮： $F_t, W[160\sim 169], K_t$ 20第14轮： $F_t, W[170\sim 179], K_t$ 20第15轮： $F_t, W[180\sim 189], K_t$ 20第16轮： $F_t, W[190\sim 199], K_t$ 20第17轮： $F_t, W[200\sim 209], K_t$ 20第18轮： $F_t, W[210\sim 219], K_t$ 20第19轮： $F_t, W[220\sim 229], K_t$ 20第20轮： $F_t, W[230\sim 239], K_t$ 20第21轮： $F_t, W[240\sim 249], K_t$ 20第22轮： $F_t, W[250\sim 259], K_t$ 20第23轮： $F_t, W[260\sim 269], K_t$ 20第24轮： $F_t, W[270\sim 279], K_t$ 20第25轮： $F_t, W[280\sim 289], K_t$ 20第26轮： $F_t, W[290\sim 299], K_t$ 20第27轮： $F_t, W[300\sim 309], K_t$ 20第28轮： $F_t, W[310\sim 319], K_t$ 20第29轮： $F_t, W[320\sim 329], K_t$ 20第30轮： $F_t, W[330\sim 339], K_t$ 20第31轮： $F_t, W[340\sim 349], K_t$ 20第32轮： $F_t, W[350\sim 359], K_t$ 20第33轮： $F_t, W[360\sim 369], K_t$ 20第34轮： $F_t, W[370\sim 379], K_t$ 20第35轮： $F_t, W[380\sim 389], K_t$ 20第36轮： $F_t, W[390\sim 399], K_t$ 20第37轮： $F_t, W[400\sim 409], K_t$ 20第38轮： $F_t, W[410\sim 419], K_t$ 20第39轮： $F_t, W[420\sim 429], K_t$ 20第40轮： $F_t, W[430\sim 439], K_t$ 20第41轮： $F_t, W[440\sim 449], K_t$ 20第42轮： $F_t, W[450\sim 459], K_t$ 20第43轮： $F_t, W[460\sim 469], K_t$ 20第44轮： $F_t, W[470\sim 479], K_t$ 20第45轮： $F_t, W[480\sim 489], K_t$ 20第46轮： $F_t, W[490\sim 499], K_t$ 20第47轮： $F_t, W[500\sim 509], K_t$ 20第48轮： $F_t, W[510\sim 519], K_t$ 20第49轮： $F_t, W[520\sim 529], K_t$ 20第50轮： $F_t, W[530\sim 539], K_t$ 20第51轮： $F_t, W[540\sim 549], K_t$ 20第52轮： $F_t, W[550\sim 559], K_t$ 20第53轮： $F_t, W[560\sim 569], K_t$ 20第54轮： $F_t, W[570\sim 579], K_t$ 20第55轮： $F_t, W[580\sim 589], K_t$ 20第56轮： $F_t, W[590\sim 599], K_t$ 20第57轮： $F_t, W[600\sim 609], K_t$ 20第58轮： $F_t, W[610\sim 619], K_t$ 20第59轮： $F_t, W[620\sim 629], K_t$ 20第60轮： $F_t, W[630\sim 639], K_t$ 20第61轮： $F_t, W[640\sim 649], K_t$ 20第62轮： $F_t, W[650\sim 659], K_t$ 20第63轮： $F_t, W[660\sim 669], K_t$ 20第64轮： $F_t, W[670\sim 679], K_t$ 20第65轮： $F_t, W[680\sim 689], K_t$ 20第66轮： $F_t, W[690\sim 699], K_t$ 20第67轮： $F_t, W[700\sim 709], K_t$ 20第68轮： $F_t, W[710\sim 719], K_t$ 20第69轮： $F_t, W[720\sim 729], K_t$ 20第70轮： $F_t, W[730\sim 739], K_t$ 20第71轮： $F_t, W[740\sim 749], K_t$ 20第72轮： $F_t, W[750\sim 759], K_t$ 20第73轮： $F_t, W[760\sim 769], K_t$ 20第74轮： $F_t, W[770\sim 779], K_t$ 20第75轮： $F_t, W[780\sim 789], K_t$ 20第76轮： $F_t, W[790\sim 799], K_t$ 20第77轮： $F_t, W[800\sim 809], K_t$ 20第78轮： $F_t, W[810\sim 819], K_t$ 20第79轮： $F_t, W[820\sim 829], K_t$ 20第80轮： $F_t, W[830\sim 839], K_t$ 20第81轮： $F_t, W[840\sim 849], K_t$ 20第82轮： $F_t, W[850\sim 859], K_t$ 20第83轮： $F_t, W[860\sim 869], K_t$ 20第84轮： $F_t, W[870\sim 879], K_t$ 20第85轮： $F_t, W[880\sim 889], K_t$ 20第86轮： $F_t, W[890\sim 899], K_t$ 20第87轮： $F_t, W[900\sim 909], K_t$ 20第88轮： $F_t, W[910\sim 919], K_t$ 20第89轮： $F_t, W[920\sim 929], K_t$ 20第90轮： $F_t, W[930\sim 939], K_t$ 20第91轮： $F_t, W[940\sim 949], K_t$ 20第92轮： $F_t, W[950\sim 959], K_t$ 20第93轮： $F_t, W[960\sim 969], K_t$ 20第94轮： $F_t, W[970\sim 979], K_t$ 20第95轮： $F_t, W[980\sim 989], K_t$ 20第96轮： $F_t, W[990\sim 999], K_t$ 20第97轮： $F_t, W[1000\sim 1009], K_t$ 20第98轮： $F_t, W[1010\sim 1019], K_t$ 20第99轮： $F_t, W[1020\sim 1029], K_t$ 20第100轮： $F_t, W[1030\sim 1039], K_t$ 20第101轮： $F_t, W[1040\sim 1049], K_t$ 20第102轮： $F_t, W[1050\sim 1059], K_t$ 20第103轮： $F_t, W[1060\sim 1069], K_t$ 20第104轮： $F_t, W[1070\sim 1079], K_t$ 20第105轮： $F_t, W[1080\sim 1089], K_t$ 20第106轮： $F_t, W[1090\sim 1099], K_t$ 20第107轮： $F_t, W[1100\sim 1109], K_t$ 20第108轮： $F_t, W[1110\sim 1119], K_t$ 20第109轮： $F_t, W[1120\sim 1129], K_t$ 20第110轮： $F_t, W[1130\sim 1139], K_t$ 20第111轮： $F_t, W[1140\sim 1149], K_t$ 20第112轮： $F_t, W[1150\sim 1159], K_t$ 20第113轮： $F_t, W[1160\sim 1169], K_t$ 20第114轮： $F_t, W[1170\sim 1179], K_t$ 20第115轮： $F_t, W[1180\sim 1189], K_t$ 20第116轮： $F_t, W[1190\sim 1199], K_t$ 20第117轮： $F_t, W[1200\sim 1209], K_t$ 20第118轮： $F_t, W[1210\sim 1219], K_t$ 20第119轮： $F_t, W[1220\sim 1229], K_t$ 20第120轮： $F_t, W[1230\sim 1239], K_t$ 20第121轮： $F_t, W[1240\sim 1249], K_t$ 20第122轮： $F_t, W[1250\sim 1259], K_t$ 20第123轮： $F_t, W[1260\sim 1269], K_t$ 20第124轮： $F_t, W[1270\sim 1279], K_t$ 20第125轮： $F_t, W[1280\sim 1289], K_t$ 20第126轮： $F_t, W[1290\sim 1299], K_t$ 20第127轮： $F_t, W[1300\sim 1309], K_t$ 20第128轮： $F_t, W[1310\sim 1319], K_t$ 20第129轮： $F_t, W[1320\sim 1329], K_t$ 20第130轮： $F_t, W[1330\sim 1339], K_t$ 20第131轮： $F_t, W[1340\sim 1349], K_t$ 20第132轮： $F_t, W[1350\sim 1359], K_t$ 20第133轮： $F_t, W[1360\sim 1369], K_t$ 20第134轮： $F_t, W[1370\sim 1379], K_t$ 20第135轮： $F_t, W[1380\sim 1389], K_t$ 20第136轮： $F_t, W[1390\sim 1399], K_t$ 20第137轮： $F_t, W[1400\sim 1409], K_t$ 20第138轮： $F_t, W[1410\sim 1419], K_t$ 20第139轮： $F_t, W[1420\sim 1429], K_t$ 20第140轮： $F_t, W[1430\sim 1439], K_t$ 20第141轮： $F_t, W[1440\sim 1449], K_t$ 20第142轮： $F_t, W[1450\sim 1459], K_t$ 20第143轮： $F_t, W[1460\sim 1469], K_t$ 20第144轮： $F_t, W[1470\sim 1479], K_t$ 20第145轮： $F_t, W[1480\sim 1489], K_t$ 20第146轮： $F_t, W[1490\sim 1499], K_t$ 20第147轮： $F_t, W[1500\sim 1509], K_t$ 20第148轮： $F_t, W[1510\sim 1519], K_t$ 20第149轮： $F_t, W[1520\sim 1529], K_t$ 20第150轮： $F_t, W[1530\sim 1539], K_t$ 20第151轮： $F_t, W[1540\sim 1549], K_t$ 20第152轮： $F_t, W[1550\sim 1559], K_t$ 20第153轮： $F_t, W[1560\sim 1569], K_t$ 20第154轮： $F_t, W[1570\sim 1579], K_t$ 20