（1）MD5原理

MD5以512位分组来处理输入的信息，且每一分组又被划分为16个32位子分组，经过了一系列的处理后，算法的输出由四个32位分组组成，将这四个32位分组级联后将生成一个128位散列值。

第一步、填充

如果输入信息的长度(bit)对512求余的结果不等于448，就需要填充使得对512求余的结果等于448。填充的方法是填充一个1和n个0。填充完后，信息的长度就为N\*512+448(bit)；

第二步、记录信息长度

用64位来存储填充前信息长度。这64位加在第一步结果的后面，这样信息长度就变为N\*512+448+64=(N+1)\*512位。

第三步、装入标准的幻数（四个整数）

标准的幻数（物理顺序）是（A=(01234567)16，B=(89ABCDEF)16，C=(FEDCBA98)16，D=(76543210)16）。如果在程序中定义应该是（A=0X67452301L，B=0XEFCDAB89L，C=0X98BADCFEL，D=0X10325476L）。有点晕哈，其实想一想就明白了。

首先清楚整型的位表示方法，其次标准文档上要求的是：四个幻数在内存地址上从低到高为：

A: 01 23 45 67

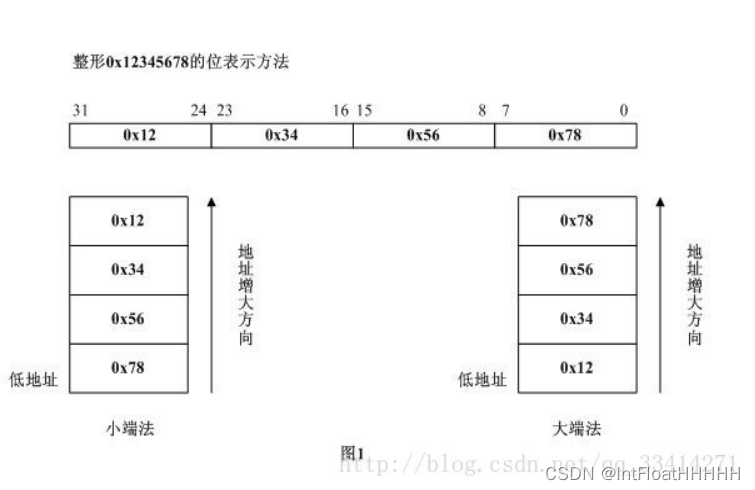
B: 89 ab cd ef

C: fe dc ba 98

D: 76 54 32 10

采用小端表示法表示为A=0X67452301L，则在地址中就是A=01 23 45 67

小端法和大端法区别如下图：

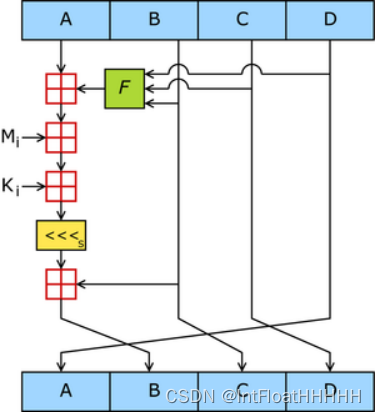


第四步、四轮循环运算

1.把消息分以12位一分组进行处理。

2.每一个分组进行4轮变换，以上面所说4个标准的幻数为起始变量进行计算，重新输出4个变量。

3.以这4个变量再进行下一分组的运算，如果已经是最后一个分组，则这4个变量为最后的结果，即MD5值。



循环的次数是分组的个数（N+1）

（1）将每一512字节细分成16个小组，每个小组64位（8个字节）

（2）先认识四个线性函数(&是与,|是或,~是非,^是异或)

F(X,Y,Z)=(X&Y)|((~X)&Z)

G(X,Y,Z)=(X&Z)|(Y&(~Z))

H(X,Y,Z)=X^Y^Z

I(X,Y,Z)=Y^(X|(~Z))

（3）设Mj表示消息的第j个子分组（从0到15），<<< s表示循环左移s位，则四种操作为：

FF(a,b,c,d,Mj,s,ti)表示a=b+((a+F(b,c,d)+Mj+ti)<<<s)

GG(a,b,c,d,Mj,s,ti)表示a=b+((a+G(b,c,d)+Mj+ti)<<<s)

HH(a,b,c,d,Mj,s,ti)表示a=b+((a+H(b,c,d)+Mj+ti)<<<s)

II(a,b,c,d,Mj,s,ti)表示a=b+((a+I(b,c,d)+Mj+ti)<<<s)

（4）四轮运算

第一轮

a=FF(a,b,c,d,M0,7,0xd76aa478)

b=FF(d,a,b,c,M1,12,0xe8c7b756)

c=FF(c,d,a,b,M2,17,0x242070db)

d=FF(b,c,d,a,M3,22,0xc1bdceee)

a=FF(a,b,c,d,M4,7,0xf57c0faf)

b=FF(d,a,b,c,M5,12,0x4787c62a)

c=FF(c,d,a,b,M6,17,0xa8304613)

d=FF(b,c,d,a,M7,22,0xfd469501)

a=FF(a,b,c,d,M8,7,0x698098d8)

b=FF(d,a,b,c,M9,12,0x8b44f7af)

c=FF(c,d,a,b,M10,17,0xffff5bb1)

d=FF(b,c,d,a,M11,22,0x895cd7be)

a=FF(a,b,c,d,M12,7,0x6b901122)

b=FF(d,a,b,c,M13,12,0xfd987193)

c=FF(c,d,a,b,M14,17,0xa679438e)

d=FF(b,c,d,a,M15,22,0x49b40821)

第二轮

a=GG(a,b,c,d,M1,5,0xf61e2562)

b=GG(d,a,b,c,M6,9,0xc040b340)

c=GG(c,d,a,b,M11,14,0x265e5a51)

d=GG(b,c,d,a,M0,20,0xe9b6c7aa)

a=GG(a,b,c,d,M5,5,0xd62f105d)

b=GG(d,a,b,c,M10,9,0x02441453)

c=GG(c,d,a,b,M15,14,0xd8a1e681)

d=GG(b,c,d,a,M4,20,0xe7d3fbc8)

a=GG(a,b,c,d,M9,5,0x21e1cde6)

b=GG(d,a,b,c,M14,9,0xc33707d6)

c=GG(c,d,a,b,M3,14,0xf4d50d87)

d=GG(b,c,d,a,M8,20,0x455a14ed)

a=GG(a,b,c,d,M13,5,0xa9e3e905)

b=GG(d,a,b,c,M2,9,0xfcefa3f8)

c=GG(c,d,a,b,M7,14,0x676f02d9)

d=GG(b,c,d,a,M12,20,0x8d2a4c8a)

第三轮

a=HH(a,b,c,d,M5,4,0xfffa3942)

b=HH(d,a,b,c,M8,11,0x8771f681)

c=HH(c,d,a,b,M11,16,0x6d9d6122)

d=HH(b,c,d,a,M14,23,0xfde5380c)

a=HH(a,b,c,d,M1,4,0xa4beea44)

b=HH(d,a,b,c,M4,11,0x4bdecfa9)

c=HH(c,d,a,b,M7,16,0xf6bb4b60)

d=HH(b,c,d,a,M10,23,0xbebfbc70)

a=HH(a,b,c,d,M13,4,0x289b7ec6)

b=HH(d,a,b,c,M0,11,0xeaa127fa)

c=HH(c,d,a,b,M3,16,0xd4ef3085)

d=HH(b,c,d,a,M6,23,0x04881d05)

a=HH(a,b,c,d,M9,4,0xd9d4d039)

b=HH(d,a,b,c,M12,11,0xe6db99e5)

c=HH(c,d,a,b,M15,16,0x1fa27cf8)

d=HH(b,c,d,a,M2,23,0xc4ac5665)

第四轮

a=II(a,b,c,d,M0,6,0xf4292244)

b=II(d,a,b,c,M7,10,0x432aff97)

c=II(c,d,a,b,M14,15,0xab9423a7)

d=II(b,c,d,a,M5,21,0xfc93a039)

a=II(a,b,c,d,M12,6,0x655b59c3)

b=II(d,a,b,c,M3,10,0x8f0ccc92)

c=II(c,d,a,b,M10,15,0xffeff47d)

d=II(b,c,d,a,M1,21,0x85845dd1)

a=II(a,b,c,d,M8,6,0x6fa87e4f)

b=II(d,a,b,c,M15,10,0xfe2ce6e0)

c=II(c,d,a,b,M6,15,0xa3014314)

d=II(b,c,d,a,M13,21,0x4e0811a1)

a=II(a,b,c,d,M4,6,0xf7537e82)

b=II(d,a,b,c,M11,10,0xbd3af235)

c=II(c,d,a,b,M2,15,0x2ad7d2bb)

d=II(b,c,d,a,M9,21,0xeb86d391)

5）每轮循环后，将A，B，C，D分别加上a，b，c，d，然后进入下一循环。