密码学综合设计实验

实验5：MD5算法实现

学号：\_\_\_\_\_\_\_031803134\_\_

姓名：\_\_\_\_\_\_\_郑晟\_\_\_\_\_\_\_\_\_

19年 10月 14日

1. 实验要求

1.实现MD5压缩函数

2.实现MD5的分组处理

3.实现消息分组和消息填充

4.消息的MD5值计算的实现

1. 实验原理

简单概括起来，MD5算法的过程分为四步：处理原文，设置初始值，循环加工，拼接结果。

第一步:处理原文

首先，我们计算出原文长度(bit)对512求余的结果，如果不等于448，就需要填充原文使得原文对512求余的结果等于448。填充的方法是第一位填充1，其余位填充0。填充完后，信息的长度就是512\*N+448。

之后，用剩余的位置（512-448=64位）记录原文的真正长度，把长度的二进制值补在最后。这样处理后的信息长度就是512\*(N+1)。

第二步:设置初始值

MD5的哈希结果长度为128位，按每32位分成一组共4组。这4组结果是由4个初始值A、B、C、D经过不断演变得到。MD5的官方实现中，A、B、C、D的初始值如下（16进制）：

A=0x01234567

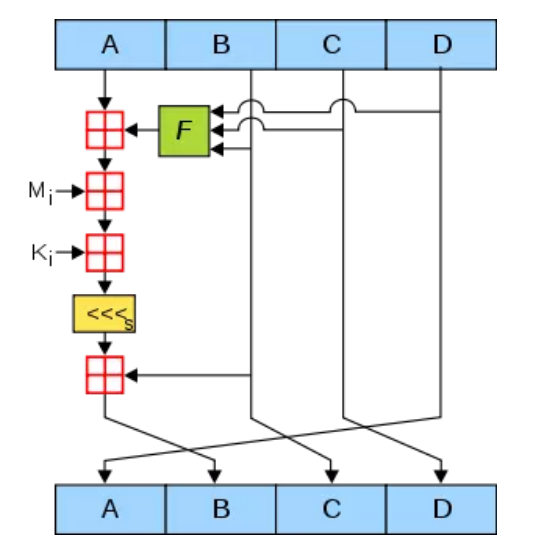
B=0x89ABCDEF

C=0xFEDCBA98

D=0x76543210

第三步:循环加工

这一步是最复杂的一步，我们看看下面这张图，此图代表了单次A,B,C,D值演变的流程。



图中，A，B，C，D就是哈希值的四个分组。每一次循环都会让旧的ABCD产生新的ABCD。一共进行多少次循环由处理后的原文长度决定。

假设处理后的原文长度是M

主循环次数 = M / 512

每个主循环中包含 512 / 32 \* 4 = 64 次 子循环。

上面这张图所表达的就是单次子循环的流程。

下面对图中其他元素一一解释：

1.绿色F

图中的绿色F，代表非线性函数。官方MD5所用到的函数有四种：

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

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

H(X, Y, Z) =XYZ

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

在主循环下面64次子循环中，F、G、H、I 交替使用，第一个16次使用F，第二个16次使用G，第三个16次使用H，第四个16次使用I。

2.红色“田”字

红色的田字代表相加的意思。

3.Mi

Mi是第一步处理后的原文。在第一步中，处理后原文的长度是512的整数倍。把原文的每512位再分成16等份，命名为M0M15，每一等份长度32。在64次子循环中，每16次循环，都会交替用到M1M16之一。

4.Ki

一个常量，在64次子循环中，每一次用到的常量都是不同的。

5.黄色的<<<S

左移S位，S的值也是常量。

“流水线”的最后，让计算的结果和B相加，取代原先的B。新ABCD的产生可以归纳为：

新A = 原d

新B = b+((a+F(b,c,d)+Mj+Ki)<<<s)

新C = 原b

新D = 原c

总结一下主循环中的64次子循环，可以归纳为下面的四部分：

第一轮

FF(a,b,c,d,M0,7,0xd76aa478) s[0]=7, k[0] = 0xd76aa478

FF(a,b,c,d,M1,12,0xe8c7b756） s[1]=12, K[1] = 0xe8c7b756

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

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

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

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

FF(a,b,c,d,M6,17,0xa8304613）

FF(a,b,c,d,M7,22,0xfd469501）

FF(a,b,c,d,M8,7,0x698098d8）

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

FF(a,b,c,d,M10,17,0xffff5bb1）

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

FF(a,b,c,d,M12,7,0x6b901122）

FF(a,b,c,d,M13,12,0xfd987193）

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

FF(a,b,c,d,M15,22,0x49b40821）

第二轮：

GG(a,b,c,d,M1,5,0xf61e2562）

GG(a,b,c,d,M6,9,0xc040b340）

GG(a,b,c,d,M11,14,0x265e5a51）

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

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

GG(a,b,c,d,M10,9,0x02441453）

GG(a,b,c,d,M15,14,0xd8a1e681）

GG(a,b,c,d,M4,20,0xe7d3fbc8）

GG(a,b,c,d,M9,5,0x21e1cde6）

GG(a,b,c,d,M14,9,0xc33707d6）

GG(a,b,c,d,M3,14,0xf4d50d87）

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

GG(a,b,c,d,M13,5,0xa9e3e905）

GG(a,b,c,d,M2,9,0xfcefa3f8）

GG(a,b,c,d,M7,14,0x676f02d9）

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

第三轮：

HH(a,b,c,d,M5,4,0xfffa3942）

HH(a,b,c,d,M8,11,0x8771f681）

HH(a,b,c,d,M11,16,0x6d9d6122）

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

HH(a,b,c,d,M1,4,0xa4beea44）

HH(a,b,c,d,M4,11,0x4bdecfa9）

HH(a,b,c,d,M7,16,0xf6bb4b60）

HH(a,b,c,d,M10,23,0xbebfbc70）

HH(a,b,c,d,M13,4,0x289b7ec6）

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

HH(a,b,c,d,M3,16,0xd4ef3085）

HH(a,b,c,d,M6,23,0x04881d05）

HH(a,b,c,d,M9,4,0xd9d4d039）

HH(a,b,c,d,M12,11,0xe6db99e5）

HH(a,b,c,d,M15,16,0x1fa27cf8）

HH(a,b,c,d,M2,23,0xc4ac5665）

第四轮：

Ⅱ（a,b,c,d,M0,6,0xf4292244）

Ⅱ（a,b,c,d,M7,10,0x432aff97）

Ⅱ（a,b,c,d,M14,15,0xab9423a7）

Ⅱ（a,b,c,d,M5,21,0xfc93a039）

Ⅱ（a,b,c,d,M12,6,0x655b59c3）

Ⅱ（a,b,c,d,M3,10,0x8f0ccc92）

Ⅱ（a,b,c,d,M10,15,0xffeff47d)

Ⅱ（a,b,c,d,M1,21,0x85845dd1）

Ⅱ（a,b,c,d,M8,6,0x6fa87e4f)

Ⅱ（a,b,c,d,M15,10,0xfe2ce6e0)

Ⅱ（a,b,c,d,M6,15,0xa3014314）

Ⅱ（a,b,c,d,M13,21,0x4e0811a1）

Ⅱ（a,b,c,d,M4,6,0xf7537e82）

Ⅱ（a,b,c,d,M11,10,0xbd3af235）

Ⅱ（a,b,c,d,M2,15,0x2ad7d2bb)

Ⅱ（a,b,c,d,M9,21,0xeb86d391）

第四步:拼接结果

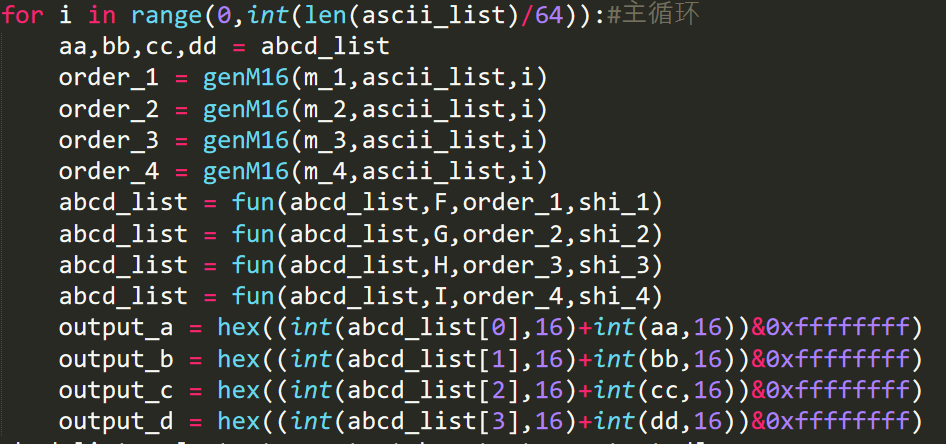
这一步就把循环加工最终产生的A，B，C，D四个值拼接在一起，转换成字符串即可。

1. 软件系统设计

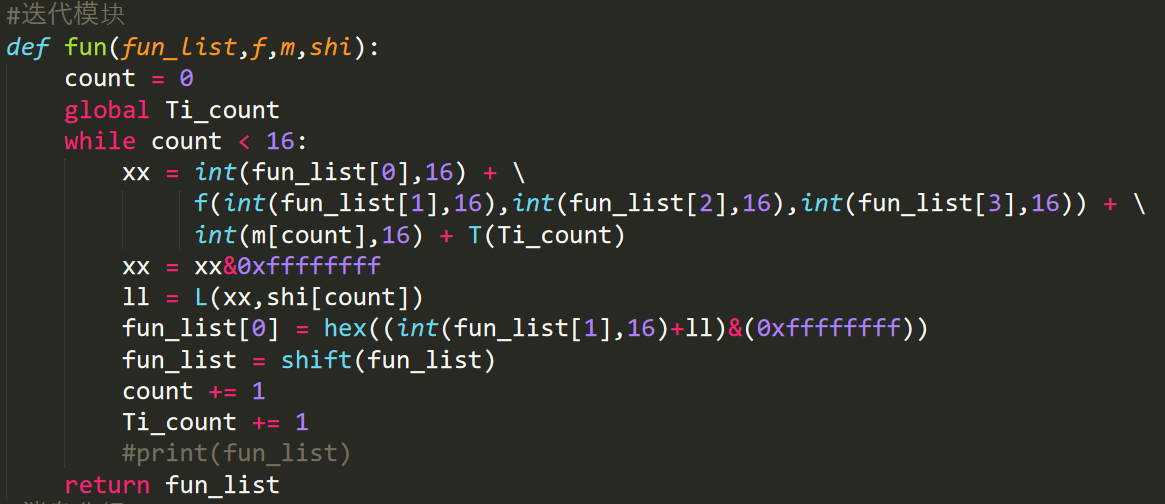
系统有md5压缩、md5分组处理、消息分组、消息填充、md5值计算功能。

实现的函数有:移位函数，迭代模块函数，消息分组函数，输出md5值函数，16进制字符串倒序函数，主函数等。

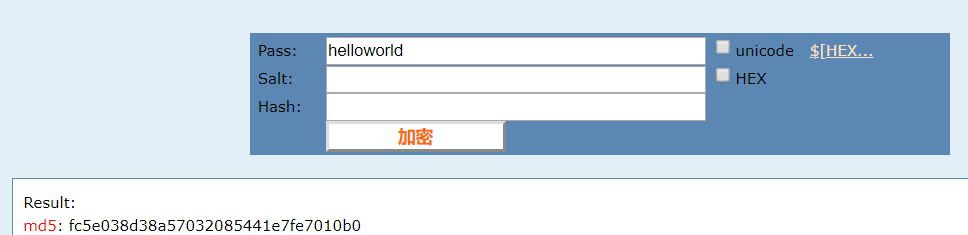
1. 重要的实现细节



其循环次数由原文处理后的长度决定。



1. 实现效果



该系统计算结果与在线md5计算结果一致。

1. 总结

该系统界面简单，操作方便，具有一定交互性，功能完整，代码逻辑清晰，就具有可读性，md5计算结果正确。