**MD5原理**

*13331231*

*孙圣*

MD5是一个很快速的加密算法，它能够将一长串字符转换为32位的16进制串，而且很少出现重复。主要的加密方法如下：

1. 添加补充位。在字符串后先添加一个1，之后补0，直到字符串的长度模512等于448为止。
2. 补充长度。长度为64bits，使得总长度为512的倍数。这个长度为原始字符串的长度，且是以bit衡量，即1个字符的长度为8(bits)。补充长度时，低位在前，高位在后。
3. 初始化MD的值。开始时，将A设置为0x01234567，B为0x89abcdef，C为0xfedcba98，D为76543210。
4. 加密处理。定义四个辅助函数，输入皆为32bits。

F(X,Y,Z) = XY v not(X) Z

G(X,Y,Z) = XZ v Y not(Z)

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

I(X,Y,Z) = Y xor (X v not(Z))

再定义四轮操作：

FF：a = b + ((a + F(b,c,d) + X[k] + T[i]) <<< s)

GG：a = b + ((a + G(b,c,d) + X[k] + T[i]) <<< s)

HH：a = b + ((a + H(b,c,d) + X[k] + T[i]) <<< s)

II: a = b + ((a + I(b,c,d) + X[k] + T[i]) <<< s)

在这里，a,b,c,d为预先初始化的那4个变量。X为输入的字符串，T和s皆为规定的值。”<<<”为循环左移，即左边的位会被移动到最右边。

进行操作之前，要对输入的串进行格式变更：将4个bytes组成一组成为一个word，且低位在前。而且，要保存a,b,c,d的值。

操作之后，将a,b,c,d再加上操作之前它们的值。

每64个byte组成一组，共进行length / 64次操作。

5. 输出。将a,b,c,d输出，但要注意先输出低位的byte，再输出高位的。