SM3 设计及实现

SM3 算法步骤

1.填充过程

设消息 M 的长度为 Lbit，首先将 bit"1"添加到消息末尾，再加 k 个“0”，k 是满足 l+1+k =448 mod 512 的最小非负整数。然后再添加一个 64bit 串，该串是 L 的二进制表示，填充后的消息 M'长度为 512 的整数倍。

例如：对消息 01100001 01100010 01100011，其长度 l=24，经填充得到比特串：01100001 01100010 01100011 1 00...00(423 比特) 00...011000(64 比特 l 的二进制表示)

2.迭代压缩过程

(1)迭代过程:

M'按照 512bit 进行分组：M'=B(0)B(1)...B(n-1)

n=(l+k+65)/512.

迭代过程如下：

```
FOR i=0 to n-1
V(i+1) = CF(V(i),B(i)
ENDFOR
```

CF 为压缩函数，V(0)为初始值 IV，迭代压缩的结果为 V(n)

(2)消息扩展：

消息分组 B(i)扩展生成 132 个字 W0，W1，...W67,W0',W1'...W63'。

a)消息分组 B(i)划分为 16 个字 W0，W1，...W15.

```
b)FOR j=16 to 67
Wj=P1(Wj-16 ^ Wj-9 ^ (Wj-3 <<<15)^(Wj-13<<<7)^Wj-6
ENDFOR
c)FOR j=0 to 63
Wj'=Wj^Wj+4
ENDFOR
```

(3)压缩函数：

A/B/C/D/E/F/G/H 为字寄存器，SS1/SS2/TT1/TT2 为中间变量，压缩函数 V(i+1) = CF(V(i),B(i))计算过程如下：

```
ABCDEFGH = V(i)
FOR j=0 to 63
SS1 = ((A<<<12)+E+(Tj<<
SS2 = SS1^(A<<<12)
TT1 = FFj(A,B,C)+D+SS2+Wj'
TT2 = GGj(E,F,G)+H+SS1+Wj
D = C
C = B<<<9
B = A
A = TT1
H = G
G = F<<<19
F = E
```

E = P0(TT2)

ENDFOR

V(i+1) = ABCDEFGH^V(i)

运算过程中，字按照大端格式存储。

3.杂凑结果

杂凑结果为 256bit 值 y=ABCDEFGH=V(n)

实验结果：

输入数据，带入计算函数，得出结果