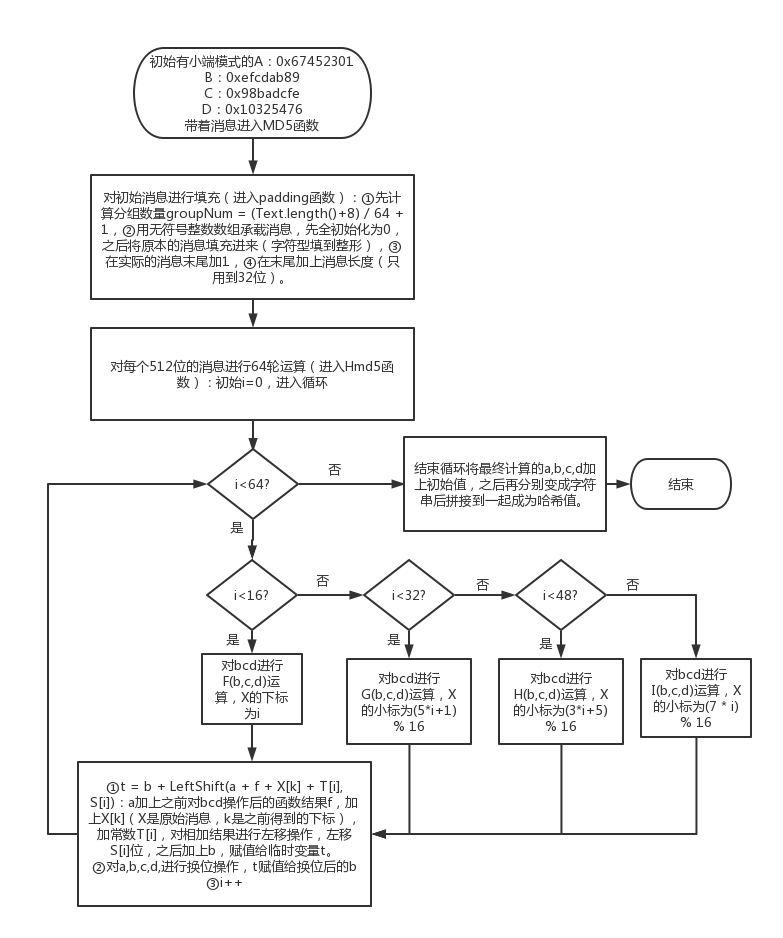
**Hash函数MD5报告**

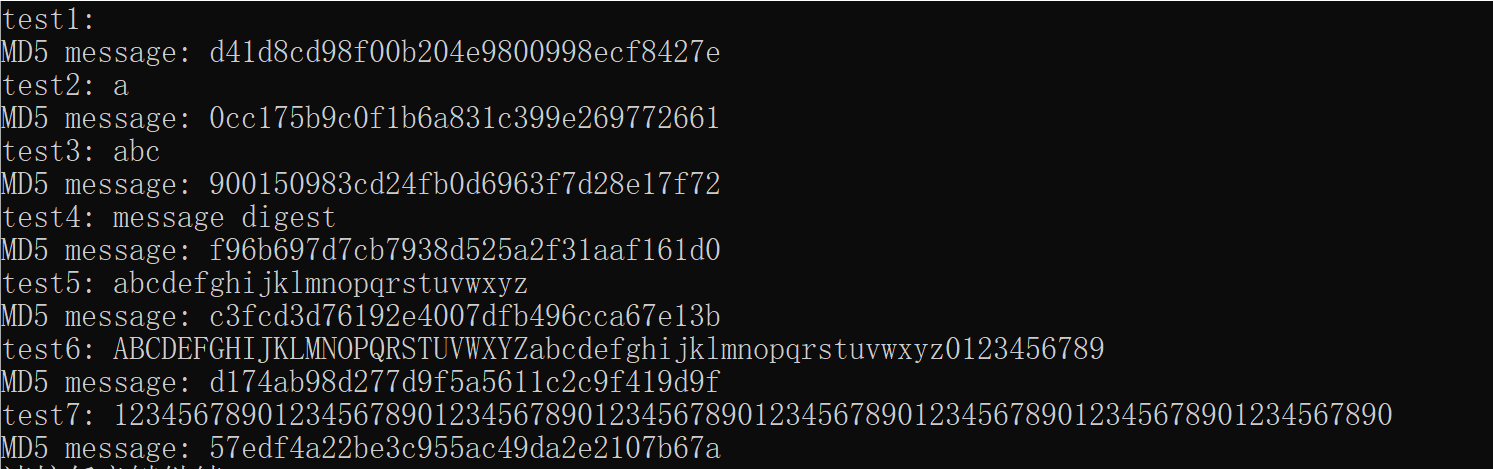
1. **程序流图**

程序主要分为几个大步骤：对消息填充补0、对每个512位的消息进行64轮的运算、最终将计算得到的A,B,C,D加上原始初值后连接在一起得到结果。

程序流图如下：

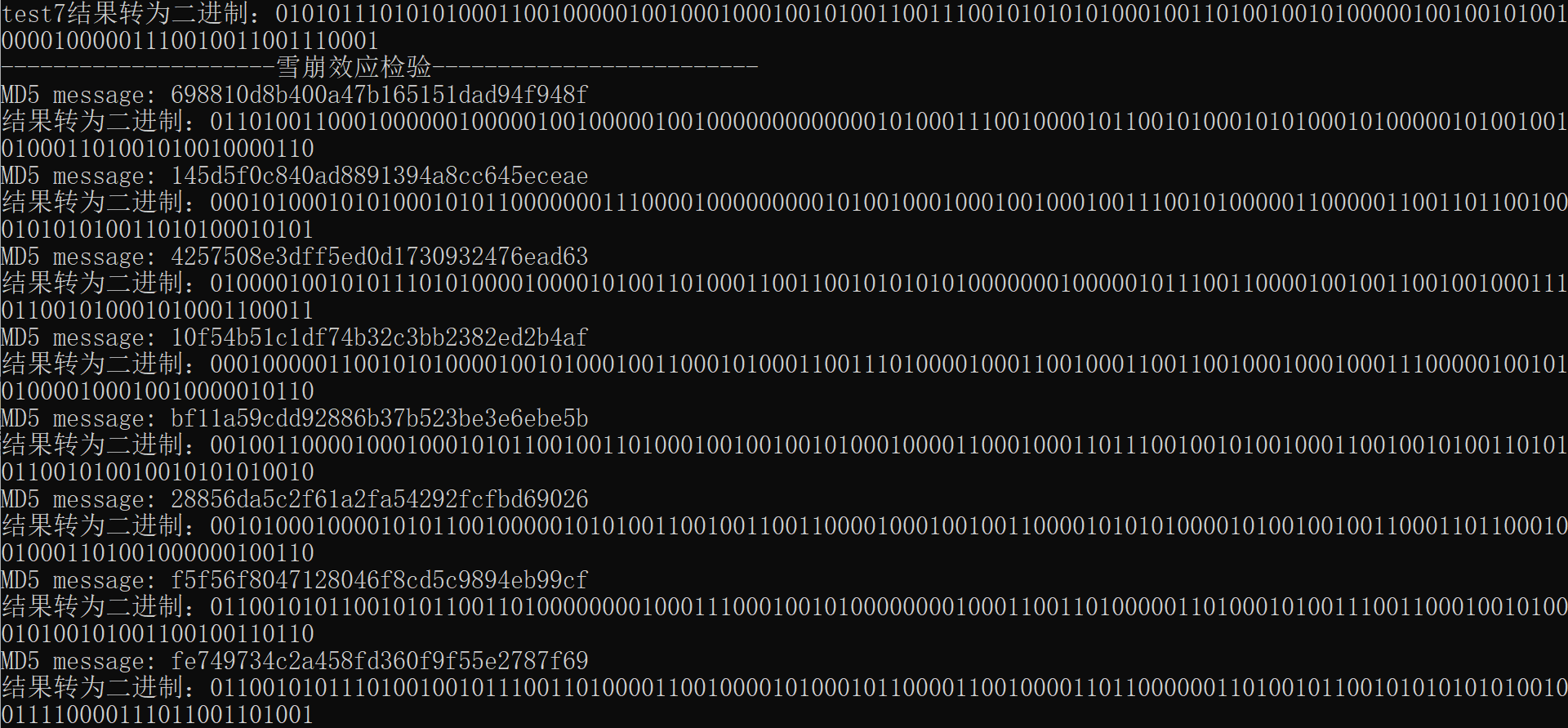


1. **实验结果**



1. **雪崩效应检测**

编写程序，对第七次测试的结果转化为128为二进制数进行显示，之后进行8次轻微的改动，结果如下：



编写程序，将上面得到的二进制数用字符串表示后，和初始未改动的二进制字符串进行对比，对MD5结果变化的位数进行统计：

string t1 = "01101001100010000001000001001000001001000000000000010100011100100001011001010001010100010100000101001001010001101001010010000110";

string t2 = "00010100010101000101011000000011100001000000000101001000100010010001001110010100000110000011001101100100010101010011010100010101";

string t3 = "01000010010101110101000010000101001101000110011001010101010000000100000101110011000010010011001001000111011001010001010001100011";

string t4 = "00010000011001010100001001010001001100010100011001110100001000110010001100110010001000100011100000100101010000100010010000010110";

string t5 = "00100110000100010001010110010011010001001001001010001000011000100011011100100101001000110010010100110101011001010010010101010010";

string t6 = "00101000100001010110010000010101001100100110011000010001001001100001010101000010100100100110001101100010010001101001000000100110";

string t7 = "01100101011001010110011010000000010001110001001010000000010001100110100000110100010100111001100010010100010100101001100100110110";

string t8 = "01100101011101001001011100110100001100100001010001011000011001000011011000000110100101100101010101010010011110000111011001101001";

double sum = 0;

int temp = 0;

for(int i = 0; i <128; i++){

if(t0[i]!=t1[i])

temp++;

}

cout<<"有："<<temp<<"位不同"<<endl;

sum +=temp;

temp = 0;

for(int i = 0; i <128; i++){

if(t0[i]!=t2[i])

temp++;

}

cout<<"有："<<temp<<"位不同"<<endl;

sum +=temp;

temp = 0;

for(int i = 0; i <128; i++){

if(t0[i]!=t3[i])

temp++;

}

cout<<"有："<<temp<<"位不同"<<endl;

sum +=temp;

temp = 0;

for(int i = 0; i <128; i++){

if(t0[i]!=t4[i])

temp++;

}

cout<<"有："<<temp<<"位不同"<<endl;

sum +=temp;

temp = 0;

for(int i = 0; i <128; i++){

if(t0[i]!=t5[i])

temp++;

}

cout<<"有："<<temp<<"位不同"<<endl;

sum +=temp;

temp = 0;

for(int i = 0; i <128; i++){

if(t0[i]!=t6[i])

temp++;

}

cout<<"有："<<temp<<"位不同"<<endl;

sum +=temp;

temp = 0;

for(int i = 0; i <128; i++){

if(t0[i]!=t7[i])

temp++;

}

cout<<"有："<<temp<<"位不同"<<endl;

sum +=temp;

temp = 0;

for(int i = 0; i <128; i++){

if(t0[i]!=t8[i])

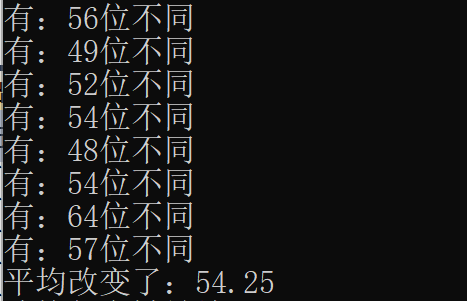
temp++;

}

cout<<"有："<<temp<<"位不同"<<endl;

sum +=temp;

cout<<"平均改变了："<<sum/8<<endl;



因此，得到平均改变的位数为54.25位。