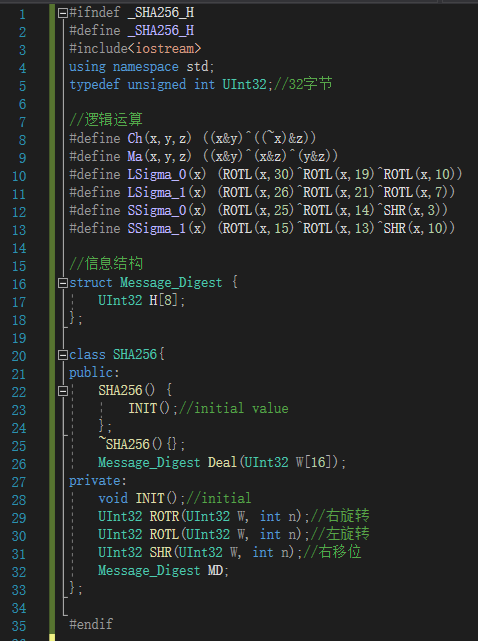
**姓名：姚熙源 学号：3190300677**

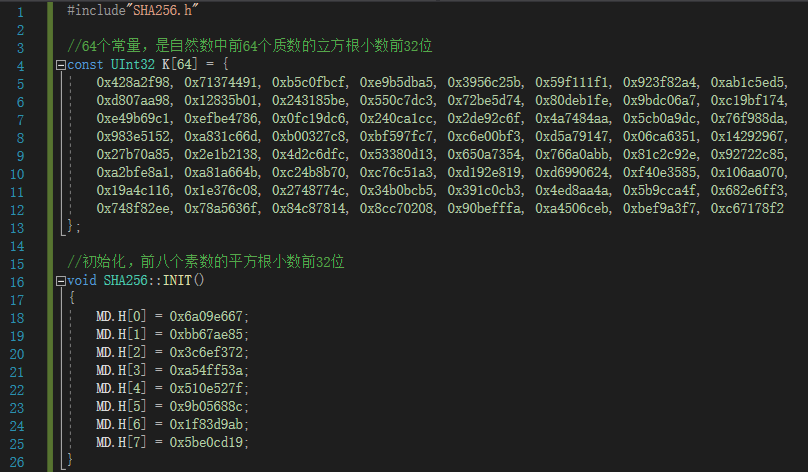
**作业1：SHA-256算法**

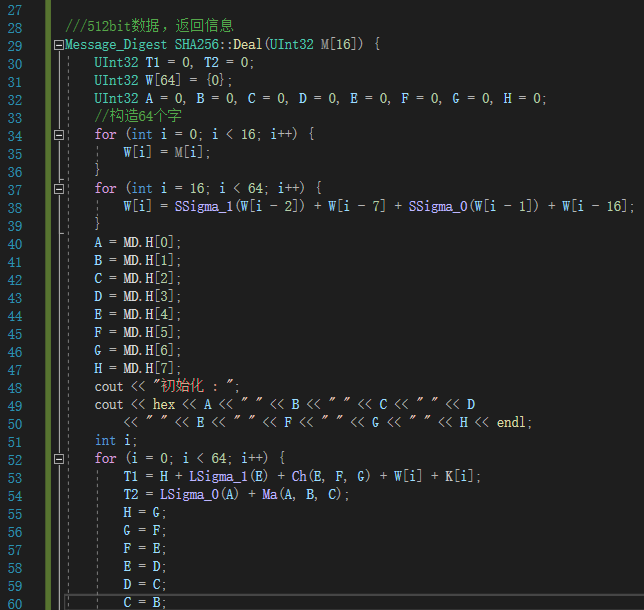
使用C++语言完成代码.

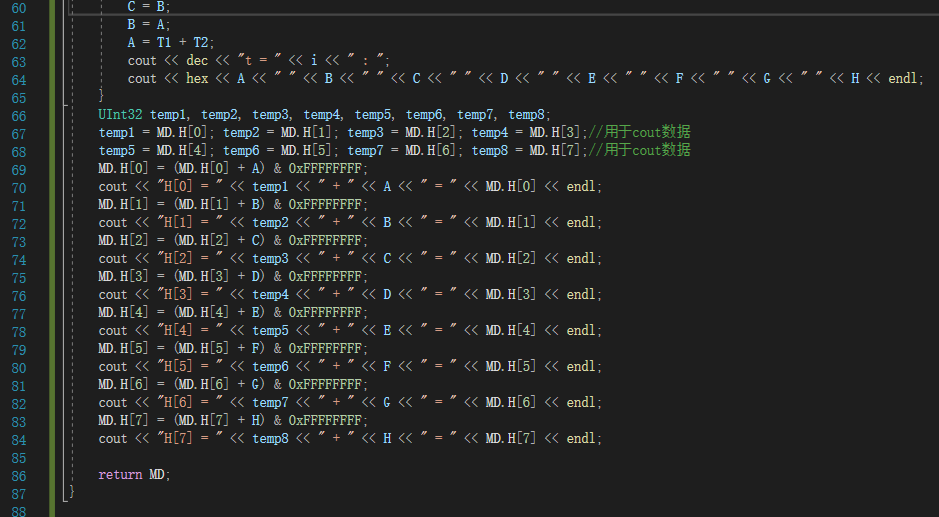
**SHA256.h (头文件)**

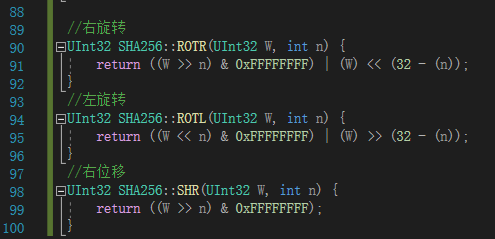


**SHA256.cpp (加密)**



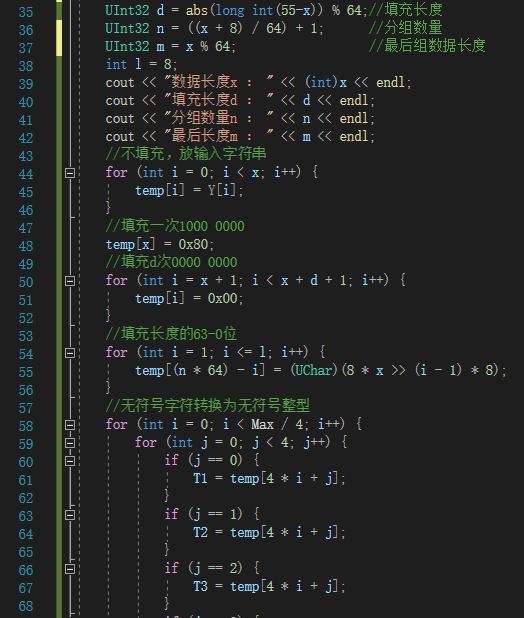


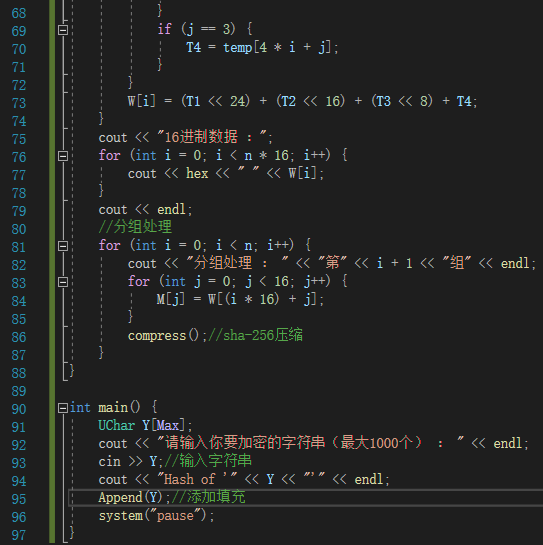




**Experiment.cpp 主代码(main)**







**实验数据：**

**输入“hello”，得哈希值：**



**再次输入“hello”，得哈希值：**



**∴相同得输入值，得出同一个输出值。**

**输入“Hello”，得哈希值：**



**∴改变一点输入值，得出不同的输出值，而且无法逆推。**

**输入“abcde”，得哈希值：**



**∴不同的输入值，不会得出同一个输出值。**

SHA256算法的输入的长度不同，但是输出的长度是固定的，输出的哈希值长度

均为256位。具有确定性的特征，就是同一个输入值，总能得到相同的输出值。

SHA256函数是一种单向散列算法，单向代表了函数很难逆推，要逆推两个大素

数的乘法公式就很难。

SHA256算法有两个**特点**：

第一点是如果你得到了同样的哈希值，或者说是数字指纹，就是因为你输入了完全相同的输入值，两个不同的输入值不会得出同一个输出值（数字指纹）。

第二点就是只要输入的值改变一点点，输出值就会变。假设你现在拍一张照片，像素：1000x1000，文件长度：2400万位，用SHA 256算法来运行一下，得出一个哈希值。现在来改变输入值中的某一个小单位，放大这个电线杆的像素，把绿色值的0改为1，重新用SHA 256算法运行一遍，就得到一个完全不同的输出值，这还只是改变了2400万单位中的一个。

SHA256算法适用于密码学、数字签名、比特币、认证等。

SHA256算法在比特币中发挥着很大的作用，这个算法每个人都可以运行，但是就没有人能够逆推它。如果一旦你可以逆推，那就可以比任何人挖矿挖得更快，然后赚钱，因为比特币挖矿的过程中就是要找出它的输入值。

文献参考：

http://www.iwar.org.uk/comsec/resources/cipher/sha256-384-512.pdf

<https://blog.csdn.net/u011583927/article/details/80905740>