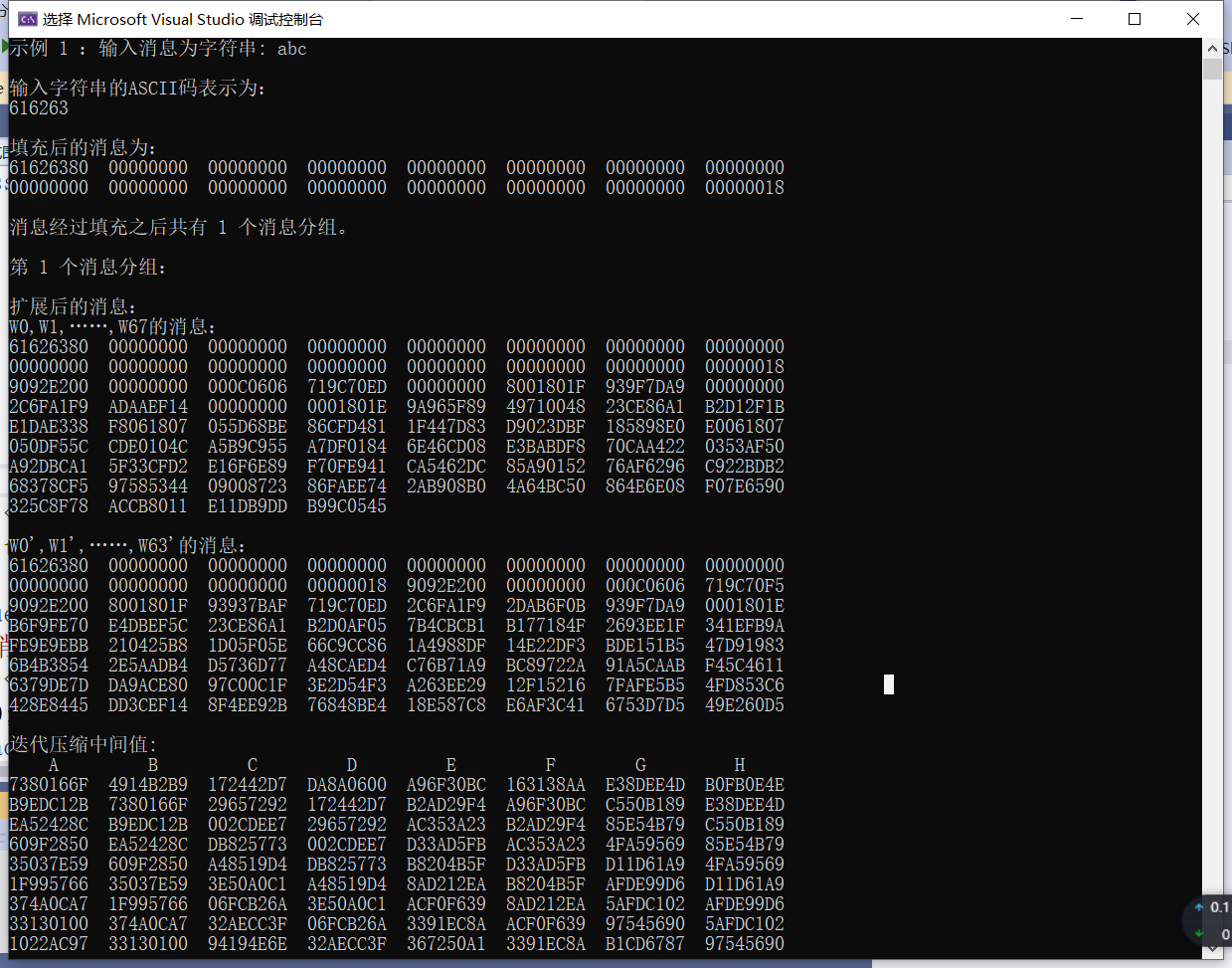
**项目名称：**SM3算法实现

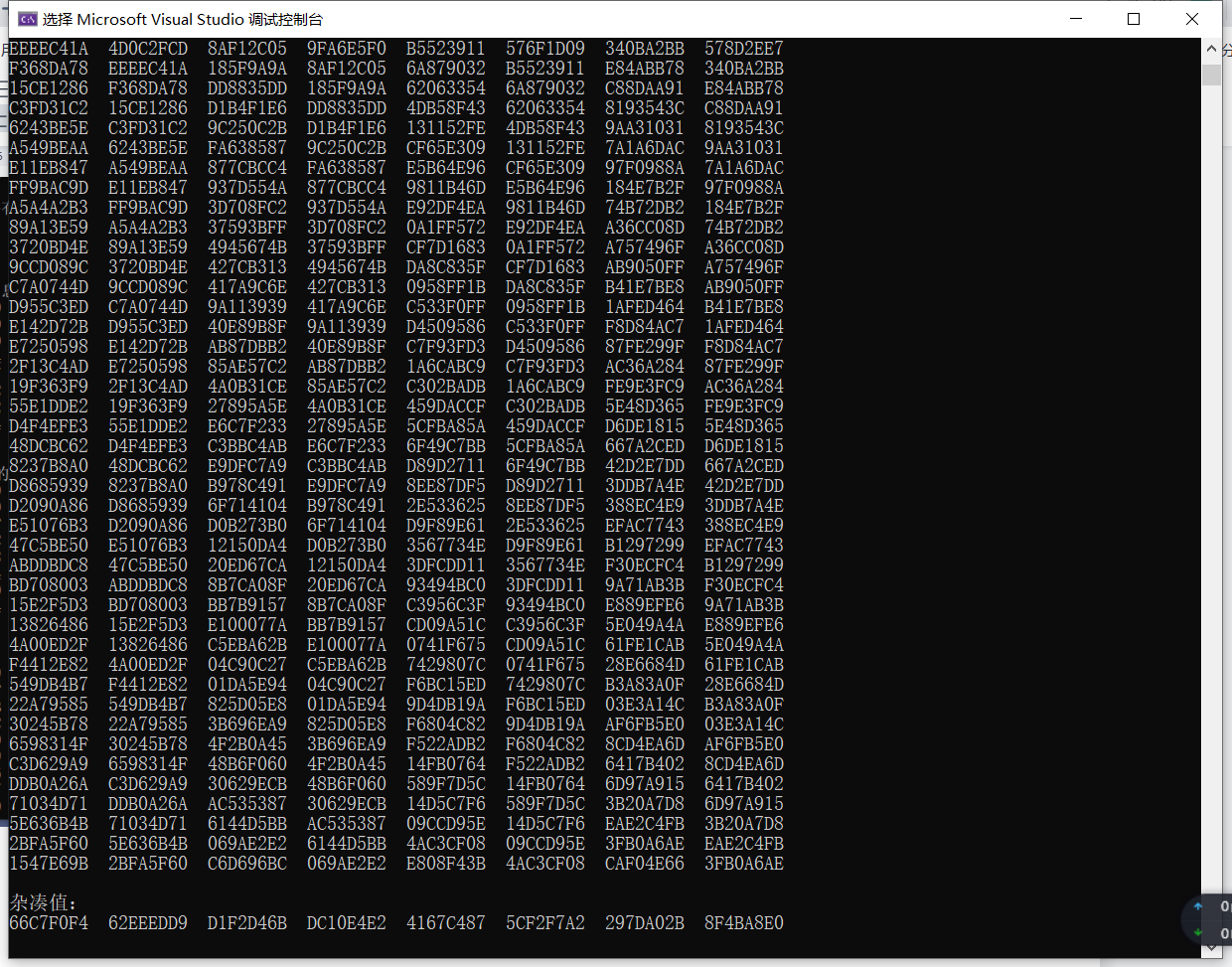
**项目完成人：**202000460080杜浩菘

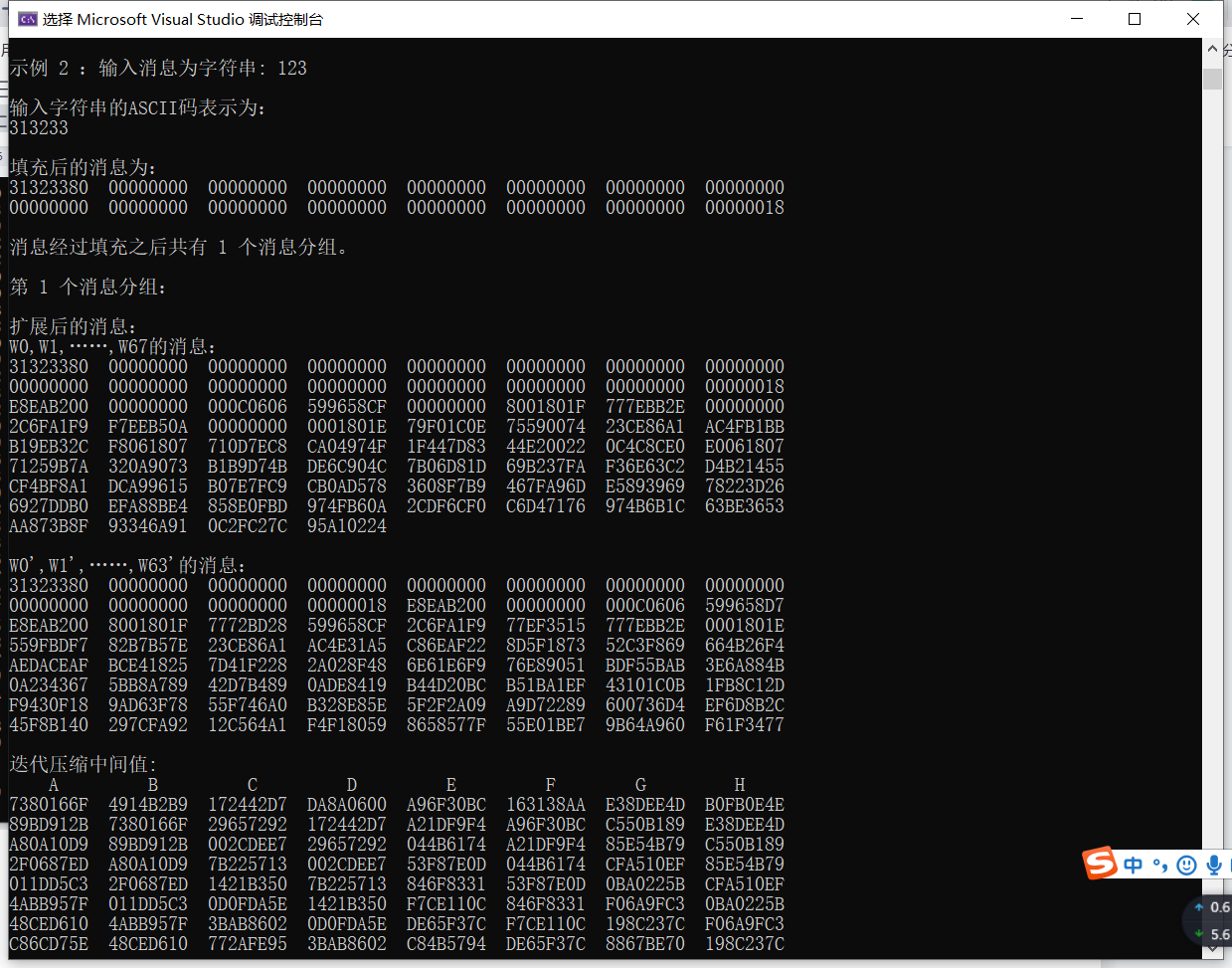
**项目简介：**笔者先学习了SM3算法的基本内容与过程，随后搜集了有关材料，学习了他人的实现方法，最后经过对比，并结合自身经验，选择一种较为易懂的方法实现了该算法。

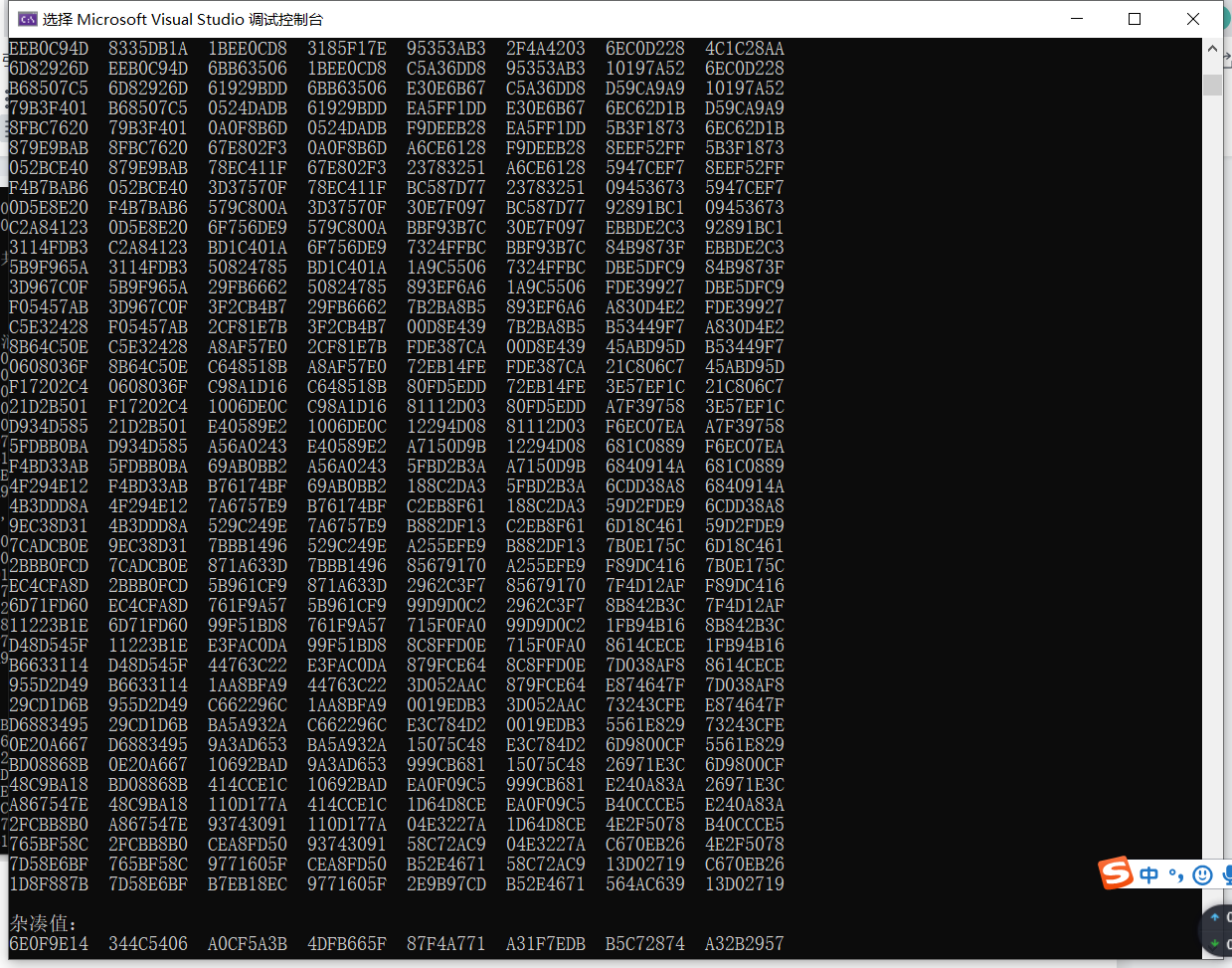
**项目代码具体说明：**由于笔者使用C++实现该算法，所以先写了二进制、十进制和十六进制间相互转换的6个函数，接下来，在明文填充函数中，使用了size()函数来得到字符串的长度，进而判断填充的值，在循环左移函数中，使用了substr()函数，将字符串的前后两部分拼接起来，实现循环移位的效果，之后又实现了参数为字符串的与、或、非和异或功能，参数为字符型的单比特与、单比特异或功能，以及mod 2^32的加法运算，有了这些函数，就可以轻松实现SM3算法中的P1、P0、T、FF、GG等函数，最后按照SM3算法的步骤与规定实现了消息扩展、消息压缩和迭代压缩函数。在主函数中笔者选择了abc和123两组消息进行测试，都正确输出了结果。

**代码运行结果：**









参考文献：

<http://t.csdn.cn/yiv5p>

<http://t.csdn.cn/AyXGf>

<http://t.csdn.cn/cNYGK>

<http://t.csdn.cn/W1YcC>