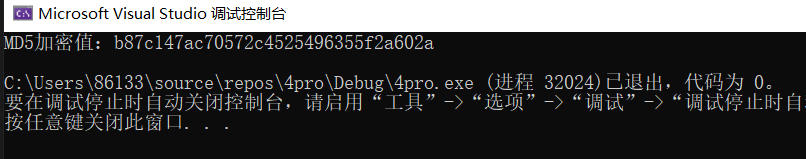
1.

该题计算量较大，故采用编程实现，在输入为0000...0000（512位）的情况下，可得结果如下：

b87c147ac70572c4525496355f2a602a



2.理论上，所有的散列函数都存在碰撞问题，因而存在安全问题，可以类比生日悖论，可以增大表示消息摘要的位数，在位数较长的情况下，在一段时间内不容易被穷举攻击攻破。