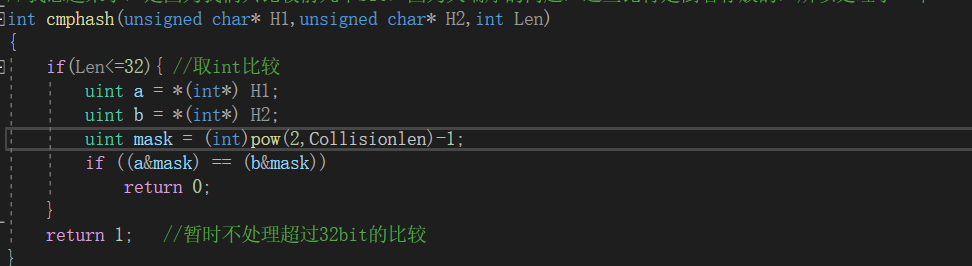
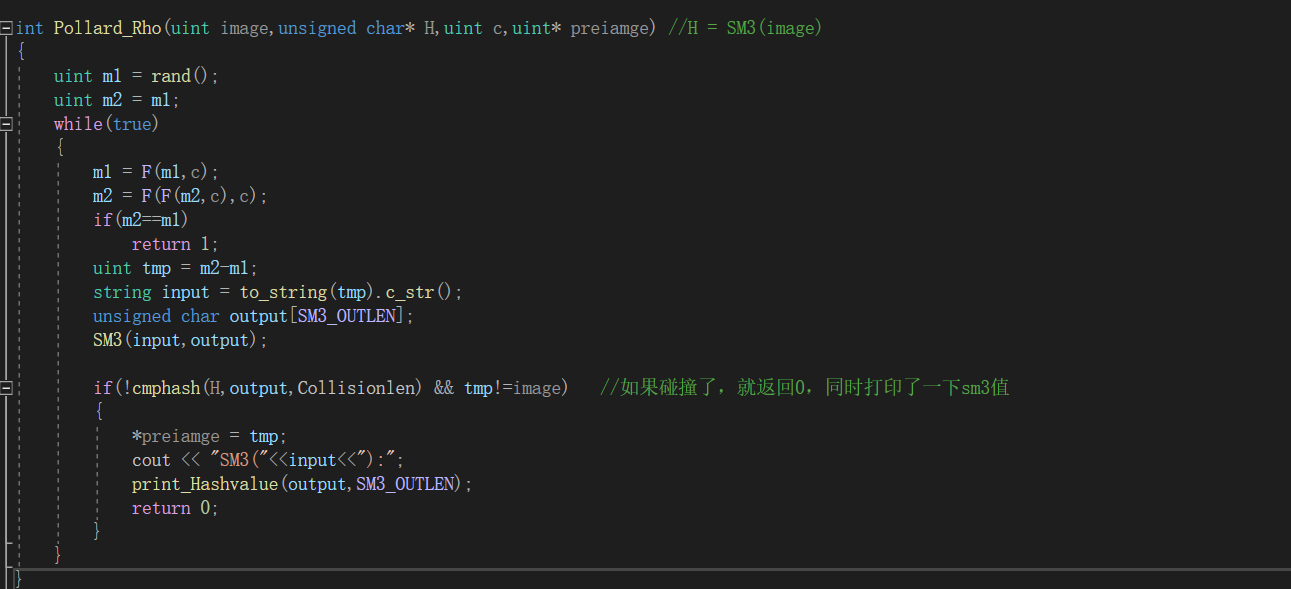
利用生日攻击找n比特碰撞的原像​ 对于任意消息（这里只考虑数字字符串，其他字符串也可以转化到数字字符串）M，我们计算H=SM3(M)，如果我们只考虑前n比特（下文中的相等都是指前n比特），那么在前0-2^n范围内，至少存在一组碰撞的概率几乎是100%。

​ 那么对于特定的消息M，如何利用生日攻击去找到这个碰撞像呢？

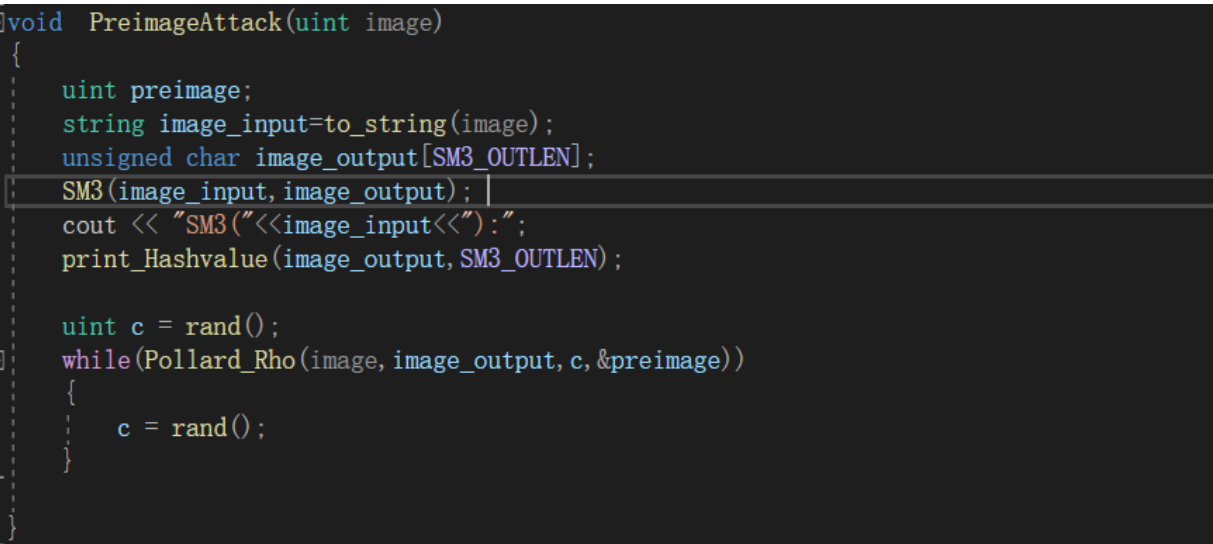
​ 我们可以任取两个消息m1，m2，计算h=SM3(abs(M1-M2)，直到得到H= h



因为只比较前几个bit，因为大端序的问题，这些比特是倒着存放的，进行处理



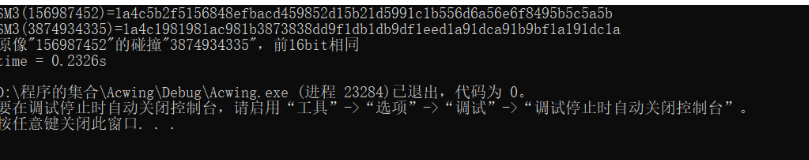
经典的pollard rho算法，使用平方加c的方式进行套圈

进行碰撞攻击

使用SM3(string input\_str)直接打印出Hash值，也可以用SM3(string input\_str,unsigned char\* ouput)来获取hash值。使用SM3(string input\_str)直接打印出Hash值，也可以用SM3(string input\_str,unsigned char\* ouput)来获取hash值。

结果分析：

16bit原像碰撞很快



24bit变慢，符合预期

