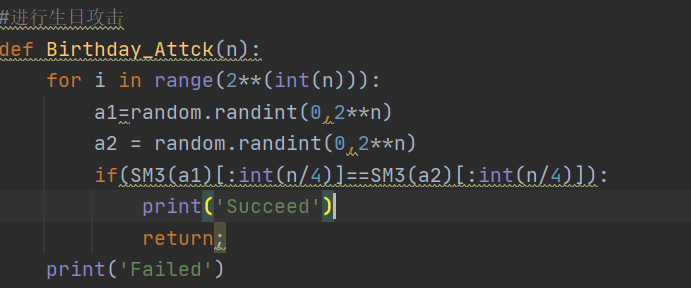
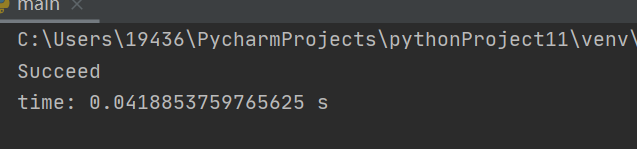
利用生日攻击找n比特碰撞的原像​ 对于任意消息（这里只考虑数字字符串，其他字符串也可以转化到数字字符串）M，我们计算H=SM3(M)，如果我们只考虑前n比特（下文中的相等都是指前n比特），那么在前0-2^n范围内，至少存在一组碰撞的概率几乎是100%。

​ 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



结果分析：

8bit原像碰撞很快



16bit变慢，符合预期

