密码学基础实验报告实验三

姓名：王天行 学号：2011428

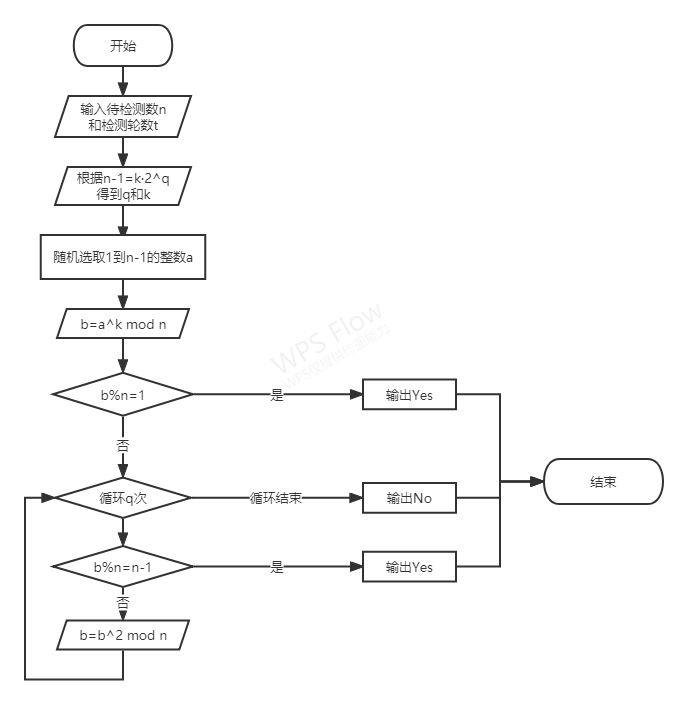
1. 题目要求

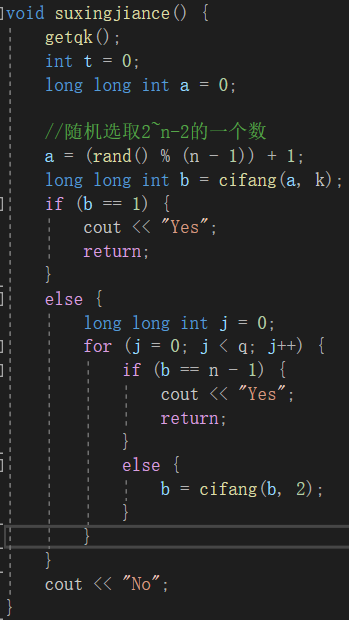
根据书上伪代码实现Miller-Rabin算法，并通过OJ平台检测

1. 主要代码

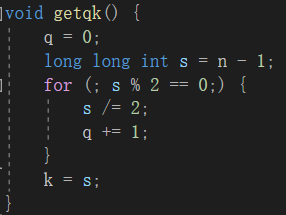
由于大于2的偶数显然不会是素数且方便判断，这部分数单独判断，减少时间

对于奇数进行素性检测

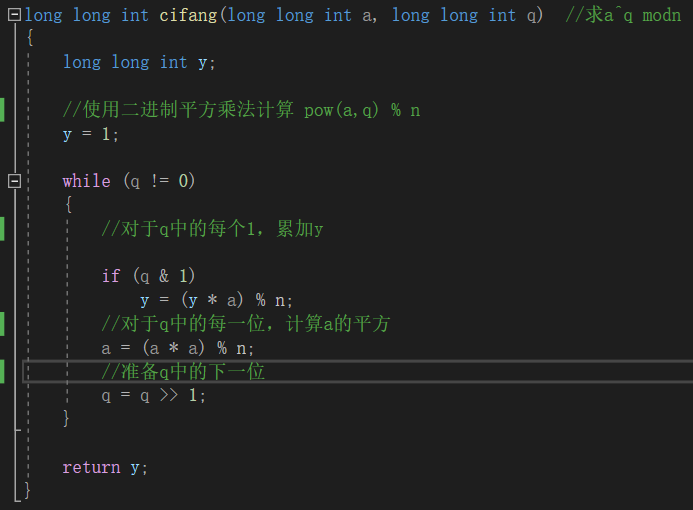
1. 主体代码



1. 得到qk



1. 次方运算



1. 实验结果



1. 心得感想
2. 此处有两个加速点：
   1. 使用二进制平方乘进行次方运算；
   2. 根据费马小定理和二次探测定理，判断一个数的是否为合数，而不是求出一个数的因数，从而降低时间复杂度。
3. Miller-Rabin算法的特点：素数一定能通过测试，不通过测试的必为合数，通过测试的很可能是素数。
4. 这个算法是从可能性的角度上判断一个数是否为素数，且其错误概率至多为1/4，比较低。