# 实验2：RSA加密算法实现

实现RSA加密算法，要求如下：

1. 利用**Miller-Rabin测试**生成两个256（或512）比特的素数, .

记录素数生成的时间.

1. 计算. 利用**Euclidean算法**生成与互素的整数作为私钥, 利用**扩展Euclidean算法**计算作为公钥.
2. 随机生成明文, 利用**平方乘积（Square and Multiply）算法**计算密文

,

并进行解密运算

,

检验解密的正确性，即是否成立.

1. 记录一组明文的RSA加密和解密时间.

使用DES对相同的明文进行加解密，记录DES加密和解密时间.

（建议选取10组以上明文，对比这些明文加密时间**总和**.）

1. RSA算法正确性检验：请依据下面的实验结果检验程序的正确性.

