**《密码学》课程设计实验报告**

实验序号：07　　　　　　　　　　实验项目名称：附加实验

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 学　　号 |  | 姓　　名 |  |  | | 21信安 |
| 实验地点 | C202 | 指导教师 | 余荣威 | 时间 | | 2024.01.05 |
| 1. 实验目的及要求   教学目的：   1. 掌握DES算法的基本概念 2. 掌握基于穷举法的短密钥暴力破解 3. 熟悉伪素数生成算法   实验要求：   1. 实现DES算法的暴力破解 2. 实现伪素数生成算法   二、实验设备（环境）及要求  Windows操作系统，高级语言开发环境  三、实验内容与步骤  1、实现基于穷举法的短密钥DES算法暴力破解；  2、实现伪随机素数生成算法，包括概率性算法和确定性算法  3.2 伪素数生成算法    该函数首先创建一个空列表，将最高位和最低位分别设置为 '1'，然后在中间的位数范围内随机生成 '0' 或 '1'，形成一个二进制表示的伪素数。最后，将该二进制字符串转换为整数，并返回结果。  3.2.1 概率性算法  本实验采用Miller-Rabin算法来做素性判定    上述函数通过对给定的数执行多次随机探测，检测其是否为合数。首先，通过检查 (a^(p-1)) mod p 是否等于 1 进行素性的初步验证。如果满足这个条件，算法通过循环对 u 进行迭代，其中 u 是 (p-1) >> 1，即 u 是 p-1 的一半。在迭代的过程中，算法计算 a^u mod p 的值，并检查是否等于 1 或 p-1。如果满足其中一个条件，认为通过了素性测试，返回 True，表示 p 可能为素数。如果在迭代过程中出现了 t != 1 且 t != p-1 的情况，或者 (a^(p-1)) mod p 不等于 1，说明 p 为合数，返回 False。这样，函数通过多次迭代提高了检测合数的准确性。  其中用到的X\_n\_mod\_P函数如下：    上述代码实现反复模平方运算法来进行模幂运算的优化。首先，将指数 exponent 转换为二进制形式，然后逆序处理二进制位数组。在迭代过程中，通过累积保存的底数 base\_array，依次计算底数的平方，实现快速幂的计算。最后，通过调用 \_\_multi 函数，对累积得到的底数数组与反序的指数二进制数组进行逐位相乘并取模操作，得到最终的 (base^exponent) mod n 的结果。  因此我们的概率性产生素数的算法如下    通过调用 proBin(w) 函数生成一个伪素数 d，然后利用 Miller-Rabin 素性测试验证该伪素数附近的一系列奇数是否为真素数。具体而言，循环50次，每次将伪素数 d 与偏移值 2\*i 相加，然后调用 testMillerRabin 函数进行素性测试。如果测试通过，则将当前奇数 b = d + 2\*i 作为结果返回，否则继续尝试下一个偏移值。这样，该算法利用伪素数辅助生成素数。  3.2.2 确定性算法  与上述算法的不同之处在于，我们的概率检测算法采用了确定性的概率检测，而不是概率性的Miller-Rabin算法，概率性检测算法如下：    通过计算 number 的平方根，并在范围从2到平方根的整数中迭代，检查是否存在能整除 number 的因子。如果存在，则返回 False 表示不是素数，否则返回 True 表示是素数。  更换概率性检测算法后的实现如下所示：    四、实验结果与数据处理  4.2 实现伪随机素数生成算法，包括概率性算法和确定性算法    结果如下：    这里由于准确性判定的速率比较低，所以我产生的位数就设的小一些  我们再用准确的素性判定来判断我们生成的伪素数：    测试结果如下：    测试了几次，证明在位数比较小的情况下，我们的概率性生成素数算法还是很精确的。  五、分析与讨论  5.1 如何提升准确的素性判定的运算速率  本实验使用的准确地素性判定方法速率比较低，判断60bit长的素数就要运行很长时间，因此可以尝试一些方法改进运算速率：  1.减小搜索范围：  对于一个大于1的整数n，最小的可能因子肯定小于或等于sqrt(n)。因此，只需要在2到sqrt(n)的范围内搜索可能的因子。  2.排除偶数：  除了2之外，其他偶数都不可能是素数。因此，在试除法中，可以通过跳过偶数来减少一半的试除次数。  3. 跳过特定的倍数：  在试除法中，可以跳过一些已知的非素数，例如3的倍数。这样可以进一步减少试除的次数。  4. 使用预先计算的素数表：  如果需要多次进行素数判定，可以通过预先计算一些小范围内的素数表，然后在判定时直接使用这个表，减少重复的试除操作。  如果追求更高的效率，建议使用Mill-Rabin等不确定性的素性检验，但是会降低一定的准确性。  5.2 | | | | | | |
| 六、教师评语  签名：  日期： | | | | | 成绩 | |