|  |  |  |
| --- | --- | --- |
| 天津大学本科生实验报告专用纸 |  | 天津大学本科生实验报告专用纸 |
| 学院 智能与计算学部 年级2017专业 软件工程 班级2班 姓名 侯雨茜 学号3017218092  课程名称 信息安全技术 实验日期 2019-10-25 成绩  同组实验者 | **教师签字：**  **年 月 日**      0123456789345678  0123456789456789  0123456789567890  1234567890123456  1234567891234567  1234567892345678  1234567893456789  测试结果如下：  RSA加密时间总和为：0.0006894260000258612 s  RSA解密时间总和为：0.03216246800001521 s  DES加密时间总和为：0.10484764400002611 s  RSA测试结果：    DES测试结果： |
| **实验2：RSA加密算法实现**  **一、实验目的**  实现RSA加密算法。  **二、实验环境**  1. 操作系统：Mac OS  2. 实现语言：Python  **三、实验内容**  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。  2. 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。  3. 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。  4. 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.）  5. RSA算法正确性检验。  **四、实验步骤**  **4.1 算法代码如下。**  Prime.py文件：        RSA.py文件：    **4.2 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。**  测试结果如下：    随机生成的素数p = 95774910269881591502996635900512935208573012503071012106153507813367363892691  随机生成的素数q = 95351721313296420393677056213518656825529237863167943342184121657382959809863  素数生成的时间为： 0.22799048700000002 s  **4.3 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.**  测试结果如下：    n = pq =  9132302552859720767109227066276439064478143638447566443440017705675090241991356119801721394562441636135110291587167413779920820227463887675101476895411333  利用Euclidean算法生成的私钥a = 65537  利用扩展Euclidean算法生成的公钥b =  8285080380325318791675134865489696468509040485697803653319699295456365724980830630009260538954266320276686888788480420275763717269484849154875354529107053  **4.4 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。**  测试结果如下：    请输入明文：  7345874874086706  RSA加密后的密文为:  3899893164165662650305062235305811581694247742952136769146324534199029087754317272019098344422525827117140346252602799872341380795588940691844422411975878  RSA解密后的密文为: 7345874874086706  解密成功  4.5. **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.）**  选取的10组明文为：  0123456789012345  0123456789123456  0123456789234567      **4.6. RSA算法正确性检验。**  检验通过。  **五、结论**  通过本次实验的实践和学习，我掌握了使用python语言编写RSA加密算法的方法。同时，我还在对算法的测试过程中发现，RSA算法生成素数和加密的速度都是非常快的，加密一组数据仅需要不到秒的时间。在与DES加密算法的对比过程中发现，虽然DES加密算法的速度也很快，加密一组数据仅需要0.01s，但是这还远远比RSA算法慢了许多。 |