**《信息安全概论》实验报告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **姓名** | **谢双骏** | | **年级** | | **2019级** |
| **学号** | **20194196** | | **专业、班级** | | **计算机科学与技术01班** |
| **实验名称** | **RSA算法的实现** | | | | |
| **实验时间** | **2022.11.12** | **实验地点** | | **线上** | |
| **实验成绩** |  | **实验性质** | | **□验证性 □设计性 □综合性** | |
| 教师评价：  □算法/实验过程正确； □源程序/实验内容提交 □程序结构/实验步骤合理；  □实验结果正确； □语法、语义正确； □报告规范；  评语：  评价教师签名（电子签名）： | | | | | |
| **一、实验目的**  编程实现RSA公钥密码的加解密方法。 | | | | | |
| **二、实验项目内容**   1. 编程实现RSA算法的加密过程； 2. 编程实现RSA算法的解密过程。 | | | | | |
| **三、实验设计**  RSA算法过程如下：  （1）选取两个保密的大素数，（二者不可相差悬殊）  （2）计算，；  （3）选取整数，满足，且；  （4）计算，满足（一般）  则为加密密钥，为解密密钥。  加密过程为    解密过程为 | | | | | |
| 1. **实验过程或算法** 2. **RSA加密解密文本** 3. **基本思想**  * 随机选择两个不相等的质数p和q，且要求p和q的乘积大于信息的数字表示 * 计算p和q的乘积n * 计算n的欧拉函数 * 随机选择一个1~n的欧拉函数值之间的数，且该数与欧拉函数值互质 * 计算e和欧拉函数值的模反函数d * 封装公钥和私钥  1. **公钥密钥的获得**   QQ截图20221112190318  该过程中使用到的函数实现如下：   1. **在给定范围内随机获得质数**   QQ截图20221112190355   1. **欧几里得方法判断两数互质**   QQ截图20221112190421   1. **大数乘法求模**   **QQ截图20221112190455**   1. **计算模反元素**   QQ截图20221112190519   1. **根据公钥加密字符串**   QQ截图20221112190545   1. **根据密钥解密**   QQ截图20221112190611   1. **加密和解密时对于大数的幂求余需要使用蒙哥马利算法**   QQ截图20221112190655QQ截图20221112190710  QQ截图20221112190719   1. **主程序**   QQ截图20221112190811 | | | | | |
| 1. **实验过程中遇到的问题及解决情况** 2. 关于大数求幂和取模的方法，参考网络博客中的蒙哥马利算法 3. 实验（二）中尝试自己写欧拉函数，发现解密后和原字符串不匹配。后来发现是实现的欧拉函数有问题，查询资料后发现了最简单的解法：euler\_n=(p-1)\*(q-1) | | | | | |
| 1. 实验结果及分析和（或）源程序调试过程 2. RSA加密解密文本   QQ截图20221112190846 | | | | | |