**《网络空间安全概论》实验报告**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **姓名** | | **张梓健** | | **年级** | | **2021** |
| **学号** | | **20214578** | | **专业、班级** | | **计算机科学与技术05班** |
| **实验名称** | **实验三　编程实现RSA公钥密码算法** | | | | | |
| **实验时间** | **2024.4.27** | | **实验地点** | | **DS3402** | |
| **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   1. 编程实现RSA公钥密码的加解密方法。 | | | | | | |
| 二、实验内容  (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、实验过程或算法（源程序）  （1）RSA算法流程：  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    （2）RSA算法实现  1. 计算加密密钥和解密密钥   1. 加密信息      1. 解密信息      1. 信息展示      1. 用户交互系统 | | | | | | |
| 四、实验结果及分析和（或）源程序调试过程  1. 设置密钥    2. 加密信息    3. 解密信息    4. 未设置密钥    5. 未支持功能 | | | | | | |