**网络空间安全学院课程答辩记录及评分表**

|  |  |  |  |
| --- | --- | --- | --- |
| **课程答辩记录** | | | |
| 教师主要  提问记录 | 问：  1、RSA加解密文件的算法实现是怎样的？  2、加解密的密钥是怎么生成的？  3、怎么实现私钥长度不小于1024bit？ | | |
| 学生回答  问题情况 | 答：   1. 大致的实现流程：使用openssl命令行工具或OpenSSL库来生成RSA密钥对。使用OpenSSL函数（如PEM\_read\_RSAPublicKey或PEM\_read\_RSAPrivateKey）从文件中读取公钥或私钥。使用RSA公钥和OpenSSL的加密函数（如RSA\_public\_encrypt）来加密数据块。确保数据块的大小适合你的RSA密钥长度。使用RSA私钥和OpenSSL的解密函数（如RSA\_private\_decrypt）来解密数据块。RSA加密通常涉及填充（如PKCS#1 v1.5或OAEP）和编码（如Base64）。确保在加密和解密过程中正确处理。在完成加密或解密操作后，清理任何分配的内存，并关闭OpenSSL库。   2、初始化安装好openssl库并添加环境变量后在命令行中生成  3、命令行生成命令openssl genrsa -out C:\Users\annie\Desktop\testkey.txt 1024  **其中1024**这个参数可以指定生成的RSA密钥的长度 | | |
| **课程答辩成绩评定** | | | |
| 答辩成绩 | | |  |
| 是否同意通过 | | □同意 □不同意 | |
| 答辩教师签名： 年 月 日 | | | |

注：课程设计类课程答辩不通过则课程考核不通过。