网络空间安全学院课程答辩记录及评分表

<table>
<tr><th colspan="3">课程答辩记录</th></tr>
<tr><td>教师主要提问记录</td><td colspan="2">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？</td></tr>
<tr><td>学生回答问题情况</td><td colspan="2">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</td></tr>
<tr><th colspan="3">课程答辩成绩评定</th></tr>
<tr><td colspan="2">答辩成绩</td><td></td></tr>
<tr><td>是否同意通过</td><td colspan="2">□同意 □不同意</td></tr>
<tr><td colspan="3">答辩教师签名： 年 月 日</td></tr>
</table>

注：课程设计类课程答辩不通过则课程考核不通过。