

**实 验 报 告**

**（ 2020/ 2021 学年 第 一 学期）**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 课程名称 | 网络信息安全 | | | | | |
| 实验名称 | 使用OpenSSL进行加密操作 | | | | | |
| 实验时间 | 2020 | 年 | 10 | 月 | 21 | 日 |
| 指导单位 | 计算机学院信息安全系 | | | | | |
| 指导教师 | 吴礼发 | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 学生姓名 | 殷祥 | 班级学号 | B180308 |
| 学院(系) | 计算机学院 | 专 业 | 信息安全 |

**实 验 报 告**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **实验名称** | | 使用OpenSSL进行加密操作 | | | | | **指导教师** | | 吴礼发 |
| **实验类型** | | 实验 | | **实验学时** | | 2 | **实验时间** | |  |
| 1. **实验目的和要求**   1.在VMWare中开启Linux虚拟机，运行Openssl  2.对照ssl\_commands.doc文档，执行所有加密操作 | | | | | | | | | |
| 二、**实验环境(实验设备)**  1. Linux  2. Openssl | | | | | | | | | |
| **三、实验内容**  1. 使用AES加密算法对文本加密，对不同参数加密后的密文进行截图、比较  （1）使用base64编码和不使用base64编码  Screen Shot 2020-10-21 at 8.19.51 AM   1. 使用CBC模式和使用ECB模式      1. 对于较长的文本使用AES-CBC base64编码加密，生成密文文件（使用 –out cihper.txt参数），打开密文cipher.txt，分别修改（不要删除或增加，只是修改）密文最开始的1个字符、中间任意1个字符、最后1个字符，再进行解密。分别看看三次解密会有什么问题，截图比较。   CBC模式  修改最开始的1个字符U为A：    修改中间任意1个字符J为A：    修改最后1个字符=为A：    ECB模式：  修改最开始1个字符U为A  修改中间1个字符m为A  修改最后1个字符=为A：     1. 生成1024位的RSA私钥和公钥，粘贴到下方。为什么私钥会比公钥长？     原因：  如下图所示，公钥中只有n、e的信息，但是私钥中不光有n、e，还有p、q、d、u等信息。  4．以自己的学号建立文本文件，内容任意，如“B16040740.txt”,使用上一步（3）生成的私钥对“B16040740.txt”进行签名，将签名信息直接粘贴到下方。再使用对应的公钥进行验证操作，对验证结果截图保存到下方。（截图需要能看清学号信息，不得使用他人学号文件进行操作，否则按抄袭处理）     1. 完成openssl\_commands.doc其他剩余所有操作 | | | | | | | | | |
| **四、实验小结（包括问题和解决方法、心得体会、意见与建议等）**  心得体会：学会了openssl的命令行使用，加深了对AES的ECB模式和CBC模式的理解。 | | | | | | | | | | |
| **五、指导教师评语** | | | | | | | | | | |
| **成 绩** |  | | **批阅人** | |  | | **日 期** |  | | |