山东大学 软件 学院

**密码学原理与实践** 课程实验报告

|  |  |  |  |
| --- | --- | --- | --- |
| 学号： | 姓名： | | 班级： |
| 实验编号：实验二 | | | |
| 实验题目：**公钥加密算法实验** | | | |
| 实验学时：8 | | 实验日期： | |
| 实验目的与内容：  **目的**：理解开源密码库实现的基本架构，熟悉公钥和对称算法的加解密函数封装与调用，并能能够利用开源设计接口进行二次封装，并实现一个功能正确的采用公钥密码和对称密码算法相结合的文件加解密签名验证工具。锻炼接口分析能力和工具设计的工程能力。  **内容**：下载OPENSSL开源软件源码，编译链接形成相应操作系统下的函数库，通过阅读网站和软件说明，至少了解其中RSA算法以及DES和AES算法的函数接口，设计基于公钥和对称钥密码算法相结合的文件加解密方案。要求：能够生成用户的RSA密钥对，采用对称算法生成对称加密的密钥并用公钥加密，然后用对称密钥加密文件内容；采用公钥解密对称密钥，并用对称密钥解密文件。文件加密时要求生成签名，解密文件时要求能够验证签名。 | | | |
| 硬件环境：  *机型，CPU，内存等主要参数。*  *若用虚拟机，则宿主机与虚拟机参数分别列出。* | | | |
| 软件开发环境：  *若用虚拟机，请写明虚拟机软件及版本，以及宿主机操作系统版本。* | | | |
| 实验步骤与内容：  *根据实验的内容，以及实现的过程，可写的内容包括：*  *实验的思路*  *实验模型的描述*  *主要数据结构的分析说明*  *主要算法代码的分析说明*  *项目管理文件的说明*  *实验投入的实际学时数*  *调试排错过程的记录*  *运行结果(文本格式，必要时抓屏)*  *多种方式测试结果的记录*  *实验结果的分析综合*  *……* | | | |
| 结论分析与体会：  *实验中遇到的问题和解决的方法*  *实验结果达到设计目标的程度*  *还可以进行哪些改进*  *实验得到哪些收获和启发*  *……* | | | |