物联网安全技术实验讲义

目 录

**第一章 实验环境介绍** …………………………………………… 2

**第二章 实验项目** …………………………………………………18

2.1 实验一 古典密码的实现 ……………………………18

2.2 实验二 典型对称密码算法的实现……………………26

2.3 实验三 模拟RSA算法的实现…………………………28

**第三章 评分准则** …………………………………………………52

**第一章 实验环境介绍**

**1.1 实验的目的和要求**

**1.1.1 实验目的**

1．使学生通过实验加强对课堂上所学的攻击防御过程和加密过程的理解，增强运用所学理论解决实际问题的能力。  
 2．培养学生良好实验习惯，课中认真观察并记录实验中遇到问题，进行分析，得出结论，认真书写实验报告；正确设计实验。  
 3．使学生掌握典型的加密解密算法，并能够用语言实现。

**1.1.2 实验要求**

1．上机前要做好准备，包括程序框图、程序清单、调试步骤、测试方法等。

2．上机时，不要迟到，按照座位号坐好、签名，不要随意走动。

3．上机时要熟练掌握与实验有关的系统软件的使用方法。

4．程序调试完后，将程序写入设备上，并分析实验结果是否正确。

5．每次完成一个实验要按时给老师检查并写出实验报告（电子文档）。

实验报告要求如下：

（1） 实验目的

(2 ) 实验内容

（3） 实验设备

（4） 实验原理 程序框图 正确的程序清单

（5） 实验步骤 实验结果分析

**实验项目**

**2.1实验一 古典密码的实现**

### 2.1.1实验目的：

学会典型古典密码中的加密方法和解密方法。

使用熟悉的语言完成一个或者两个算法。

### 2.1.2实验内容及要求：

掌握古典密码中的单表代替和多表代替的加密解密过程。

在单表代替中可以实现使用密钥的加密方法（或仿射密码）；

在多表代替中可以实现playfair密码。

### 2.1.3实验设备：

1. 带有编程环境的PC机一台

### 2.1.4实验说明：

1．选择单表代替或者多表代替的古典密码实现

2．程序编写成功后，给老师检查

3．编写实验报告，将实验结果截图放到实验报告中。

### 2.1.4附加实验：

**1.使用穷举搜索法，破译如下利用移位加密的密文：BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD**

**2.2 实验二 典型对称密码算法的实现**

### 2.2.1实验目的：

掌握DES算法的加密过程和解密过程

### 2.2.2实验内容及要求：

掌握DES加密解密流程

完成DES中的每个模块：包括扩展模块、压缩模块、子密钥产生模块等，并将各个模块组合在一起完成相应的加密的功能，并进行相应的解密。

### 2.2.3实验设备：

1.具有开发环境的PC机一台

### 2.2.4实验说明：

1．程序编写成功后，给老师检查

2．编写实验报告，将实验结果截图放到实验报告中。

**2.3 实验三 模拟RSA算法的实现**

### 2.3.1实验目的：

学会写RSA的加密解密过程。

### 2.3.2实验内容及要求：

掌握RSA的加密过程和解密过程。

实现求逆的算法（扩展的欧几里德算法）。

使用随机函数产生随机数，并进行加密和解密。

加密过程：私有密钥随机产生，公开密钥利用求逆算法给出，明文键盘输入，密文利用RSA算法输出。

解密过程：密文键盘输入，私有密钥键盘输入，利用RSA解密算法输出明文。

### 2.3.3实验设备：

1.装有xmlspy的PC机一台；

### 2.3.4实验说明：

1．程序编写成功后，给老师检查

2．编写实验报告，将实验结果截图放到实验报告中。

**第三章 评分准则**

实验成绩评定：

本课程一共有3个实验,实验总成绩占期末成绩的15%.

实验成绩一共有3部分组成:实验出勤（2分）、编程能力（10分）、实验报告（3分）；

其中编程能力中，实验一满分3分，实验二满分4分，实验三满分4分。

根据学生完成的情况打分，如果全部功能都完成并且比较完善得满分，完成部分功能分数减半，拷贝0分。