《密码学》课程设计实验报告

实验序号：04　　实验项目名称：分组密码工作模式

学　　号		姓　　名		专业、班	18信安3-4班
实验地点	网安基地新珈楼B308	指导教师	王张宜	时间	2020.11.24

一、　实验目的及要求

教学目的：

(1) 掌握分组密码的基本概念；

(2) 掌握DES、AES、SMS4密码算法；

(3) 了解分组密码DES、AES、SMS4的安全性；

(4) 掌握分组密码常用工作模式及其特点；

(5) 熟悉分组密码的应用。

实验要求：

(1) 掌握分组密码的ECB、CBC、OFB、CFB、CTR等常用工作模式；

(2) 掌握分组密码的短块加密技术；

(3) 熟悉分组密码各工作模式的（数据掩盖、错误传播、效率等）特点；

(4) 利用分组密码工作模式和短块处理技术实现任意长度输入的加密与解密。

二、实验设备（环境）及要求

Windows操作系统，高级语言开发环境

三、实验内容与步骤

1. 分组密码的常用工作模式

（1）电码本模式ECB（教材 p124 式3-76）

（2）密文链接模式CBC（教材 p125 图3-30、31）

（3）输出反馈模式OFB（教材 p127 图3-32）

（4）密文反馈模式CFB（教材 p128 图3-33）

（5）X CBC模式（教材 p128 式3-81-83）

（6）计数器模式（教材 p128 式3-84、85）

2. 分组密码的短块处理技术

（1）填充法

参考 X CBC 模式的填充方案

（2）序列密码加密法（教材 p130 图 3-34）

（3）密文挪用技术（教材 p130 图 3-35）

3. 各工作模式的特点比较

设明文 M=（M_1，M_2，…，M_n），相应的密文 C=(C_1，C_2，…，C_n)。试完成下列实验，总结各工作模式的特点，并完成表格 1：

（1)选择输入消息 M_i ＝M_j，判断是否满足 C_i=C_j？对于不同的工作模式分别进行上述实验，得出各工作模式是否能够掩盖明文中的数据模式的判断。

（2）选择篡改输入明文中的某个分块 M_i，并将加密后的结果与正确的密文之间进行对比。对于不同的工作模式分别进行上述实验，得出各工作模式是否具有加密错误传播无界特性的判断。

（3）选择篡改输入密文中的某个分块 C_i，并将解密后的结果与正确的明文之间进行对比。对于不同的工作模式分别进行上述实验，得出各工作模式是否具有解密错误传播无界特性的判断。

（4）比较不同的工作模式对于输入消息长度的要求。

（5）比较不同的工作模式的执行效率。

4. 短块处理技术的比较

设明文实际长度不是分组长度的整倍数，试使用填充法、序列密码加密法、密文挪用技术进行处理。总结这三种方法的特点，并完成表格 2：

（1）是否造成短块数据扩张；

（2）试分析三种方案的安全性（提示：假设攻击者进行选择明文攻击）

四、实验结果与数据处理

表 1：各工作模式的特点

工作模式	电码本模式 ECB	明密文链接模式	密文链接模式 CBC	输出反馈模式 OFB	密文反馈模式 CFB	XCBC 模式	计数器模式 CTR
能否掩盖数据模式							
加密错误传播无界							
解密错误传播无界							
是否改变消息长度							
能否处理消息短块							
执行速度							

短块处理方式	填充	序列密码加密	密文挪用
短块数据扩张			
实现难度			
安全性			

五、分析与讨论

六、教师评语

签名：

日期：

成绩