**深 圳 大 学 实 验 报 告**

**课程名称：­ 计算机安全导论**

**实验项目名称­： 对称密码实验**

**学院： 计算机与软件学院**

**专业： 计算机科学与技术**

**指导教师： 闫巧**

**报告人： 黄铭召 学号： 2016150063 班级： 06**

**实验时间： 2018年 10月 16 日**

**实验报告提交时间： 2018.10.21**

**教务部制**

|  |
| --- |
| 实验目的与要求：   1. 理解对称密码体制和分组密码算法的基本思想 2. 理解维吉尼亚密码/DES/AES加密算法的基本原理 3. 掌握维吉尼亚密码/DES/AES加密算法的输入输出格式和密钥格式 4. 掌握维吉尼亚密码/DES/AES加密算法的加解密过程和实现方法 |
| 实验环境：  SimpleISES客户端  Microsoft Visual Studio 2005等 |
| 实验原理： |
| 实验内容：   1. 通过SimpleISES客户端演示维吉尼亚密码/DES/AES的加解密计算及分步演算过程。 2. 画出维吉尼亚密码/DES/AES加密的流程图。 3. 采用自己熟悉的编程语言实现维吉尼亚密码/DES/AES加密算法（选做）。 |
| 实验步骤与结果：  （依照实验内容，逐条撰写实验过程与实验所得结果，第二项请附上代码）  1.**使用visio作出DES密码加密流程图，如下**     1. **使用java编写DES加解密程序，实现对明文的分组及加解密。**   **以下是程序代码：**  **主程序负责接收明文，并对明文分段，不足64位则填充0，判断密钥长度是否合格。**  **1**  **2**  **转字符为二进制序列**  3  **产生子密钥过程**：  4  **加解密过程：**  5  6  7 |
| 实验结论：  （撰写实验收获及思考） |
| 指导教师批阅意见：  成绩评定：  指导教师签字：  年 月 日 |
| 备注： |

注：1、报告内的项目或内容设置，可根据实际情况加以调整和补充。

2、教师批改学生实验报告时间应在学生提交实验报告时间后10日内。