南京信息工程大学 实验（实习）报告

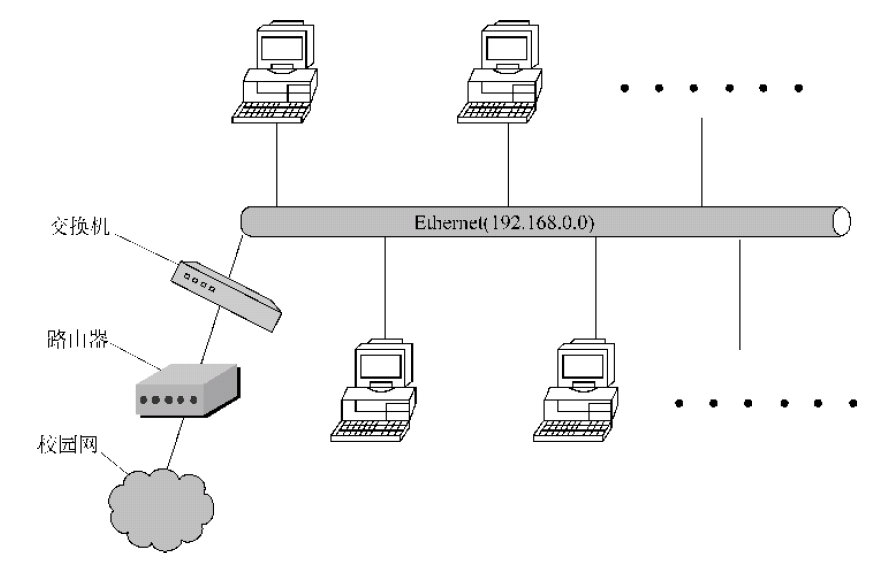
实验名称 密码学实验 实验日期 2021.12.01 得分 指导教师 王玉祥

学院 物联网学院 年级 19 专业班次 计嵌1班 姓名 曹恒翔 学号 20192375001

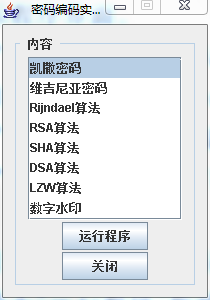
1. **实验目的**
2. 编程实现代换密码和置换密码算法，加深对古典密码体制的理解
3. 掌握加密算法设计的基本原则
4. 掌握对古典密码体制进行攻击的方法
5. 理解和掌握对称密码体制的原理与技术
6. 掌握AES算法原理，编程实现AES算法
7. **实验准备**

若干安装Windows XP的PC，其上安装密码编码实验软件包

网络拓扑如下图：



1. **实验内容和步骤**
2. 运行密码编码实验软件包，出现如下图所示的密码编码实验程序主界面



1. 选择“凯撒密码”，单击“运行程序”按钮，弹出“凯撒密码”演示程序界面
2. 在“输入字符”域的文本框中输入明文，例如If you do not work hard you will be sorry when you grow old.



1. 在“加密操作”域中单击“加密”按钮，得到密文



1. 在“解密操作”域中单击“解密”按钮，得到解密后的明文



1. 单击“关闭”按钮，回到密码编码实验程序主界面，选择“维吉尼亚密码”并单击“运行程序”按钮，弹出 “维吉尼亚密码”演示程序界面
2. 在“输入字符”域文本框中输入明文，例如To enjoy a grander sight,climb to a greater height.



1. 在“密钥设置”域中选择“密钥长度”为5，并设置密钥为(8,11,25,12,17)



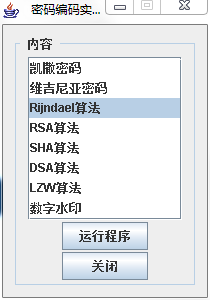
1. 在“加密操作”域中单击“加密”按钮，得到密文



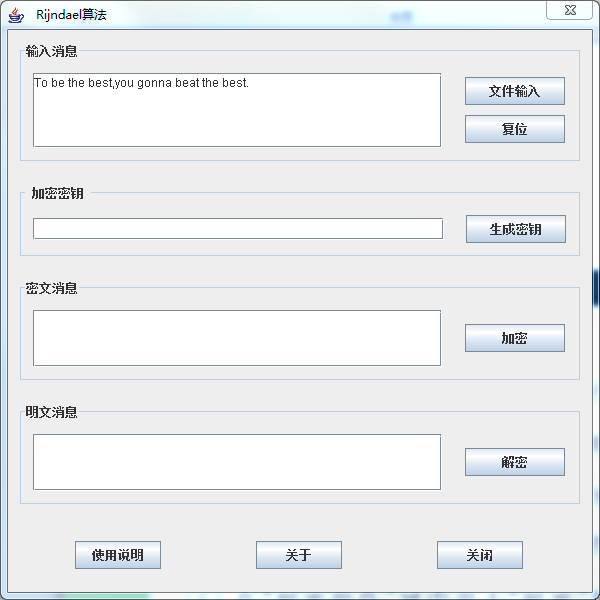
1. 在“解密操作”域中单击“解密”按钮，得到解密后的明文



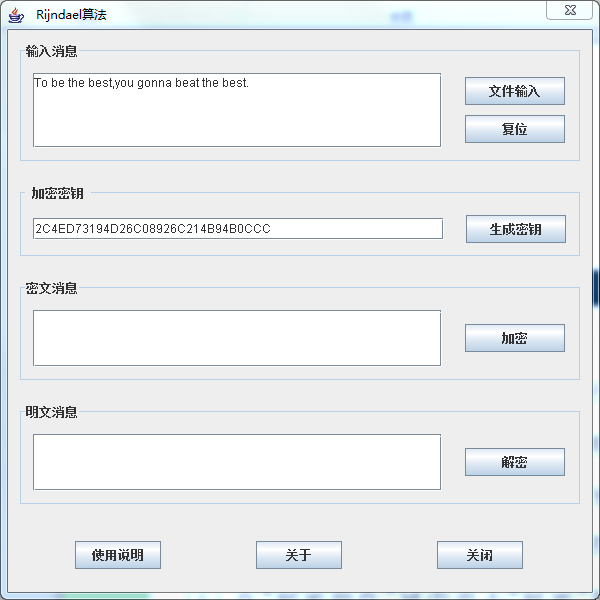
1. 选择“Rijndael算法”，单击“运行程序”按钮



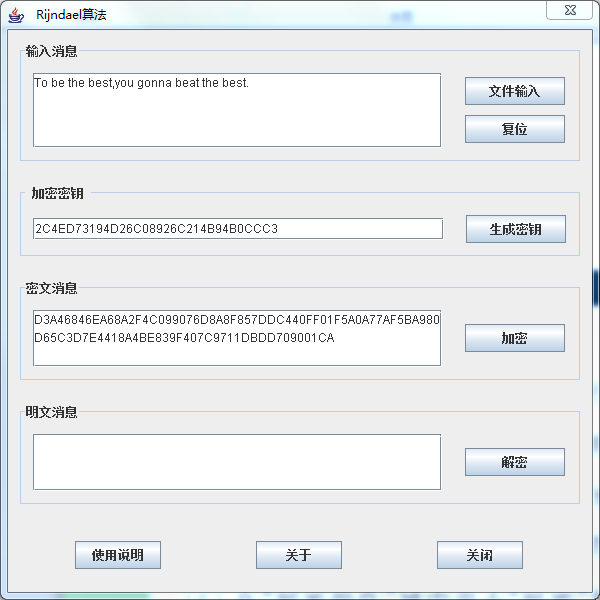
1. 在“输入字符”的文本框中输入明文



1. 在“密钥设置”域中单击“生成”密钥按钮



1. 在“加密操作”域中单击“加密”按钮，得到密文



1. 在“解密操作”域中单击“解密”按钮，得到解密后的明文

