南京信息工程大学 滨江学院 实验（实习）报告

实验（实习）名称 密码学 实验（实习）日期 2021.5.31 学院： 物联网工程学院 班级： 软件工程 2 班 学号： 20182344050 姓名： 毛济洲

一、实验目的

1、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；

2、掌握加密算法设计的基本原则；

3、掌握对古典密码体制进行攻击的方法。

二、实验设备与环境

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

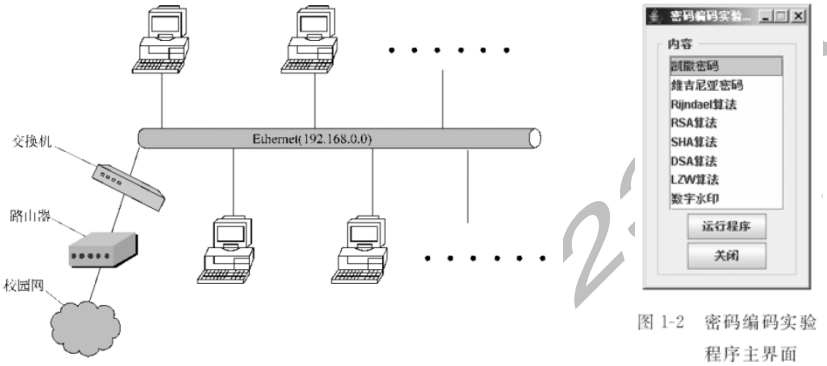


图 1-2 密码编码实验程序主界面

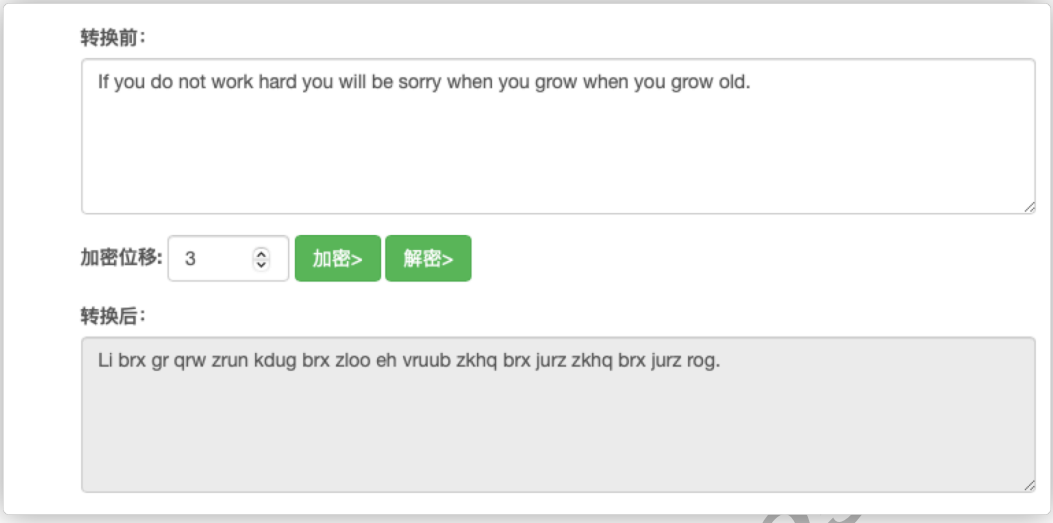
三、实验内容和步骤

(1) 运行密码编码实验软件包，出现如图 1-2 所示的密码编码实验程序主界面。

(2) 选择“恺撒密码”单击“运行程序”投,弹出如图所示的“恺撒密码”演示程序界面。

(3) 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 when you grow old.

(4) 在“加密操作”域中单击“加密”按钮,得到密文。



(5) 在“解密操作”域中单击“解密”按钮,得到解密后的明文。

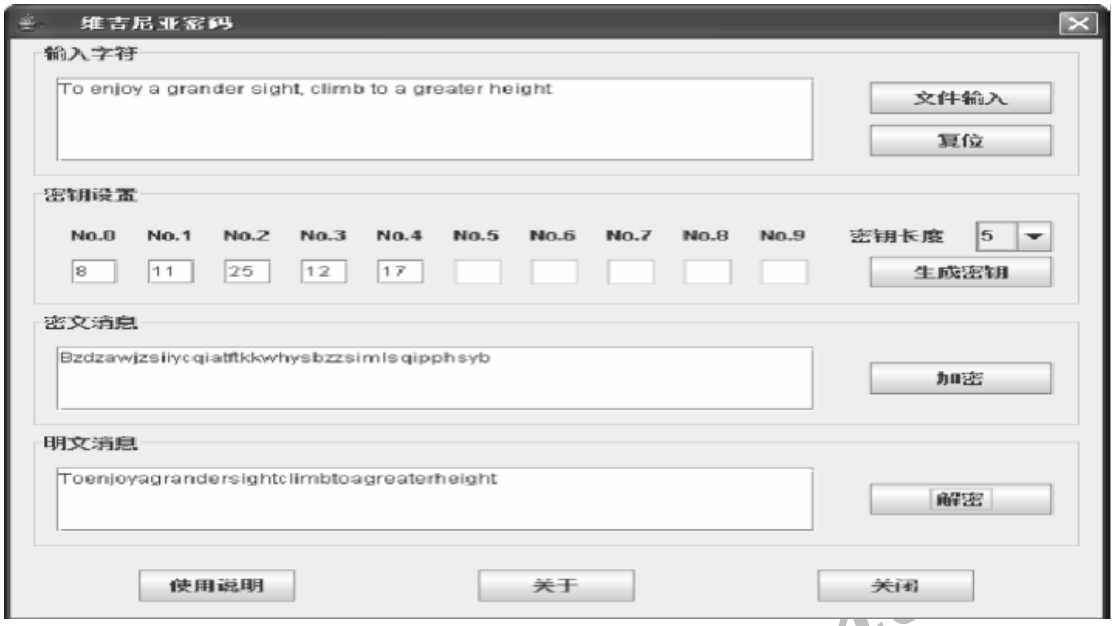
(6) 单击“关闭”按钮,回到密码编码实验程序主界面,选择“维吉尼亚密码”并单击“运行程序”按钮,弹出如图 1-4 所示的“维吉尼亚密码”演示程序界面。

(7) 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.

(8) 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）.

(9) 在“加密操作”域中单击“加密”按钮，得到密文。

(10) 在“解密操作”域中单击“解密”按钮，得到解密后的明文。


维吉尼亚密码
输入字符
To enjoy a grander sight, climb to a greater height
文件输入
复位
密钥设置
No.0
No.1
No.2
No.3
No.4
No.5
No.6
No.7
No.8
No.9
密钥长度
5
8
11
25
12
17
生成密钥
密文消息
Bzdzawjzsiiycqiatttkkwhysbzzsimlsqipphsyb
加密
明文消息
Toenjoyagrandersightclimbtoagreaterheight
解密
使用说明
关于
关闭