**信息科学与工程学院**

**2021－2022学年第一学期**

实 验 报 告

课程名称： 信息安全

实验名称： 实验三

专 业 班 级 通信工程 二班

学 生 学 号 201800121050

学 生 姓 名 孟麟芝

实 验 时 间 2021年10月21日

实验报告

### 【实验目的】

1. 掌握转轮机的加密流程。
2. 通过转轮机感受古典加密蕴含的的智慧。

### 【实验要求】

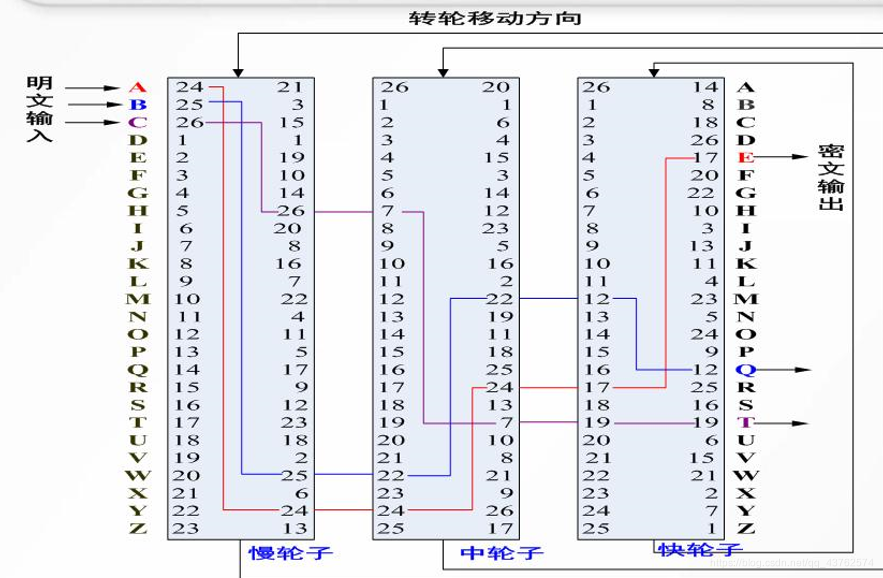
编写一个二轮转轮机。

### 【源代码】

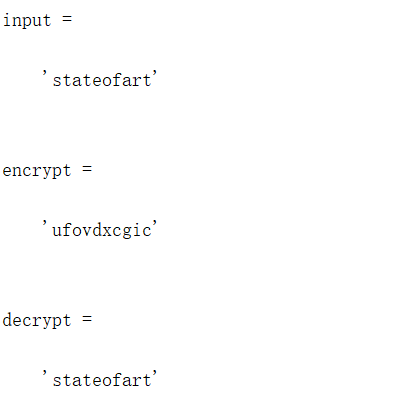
|  |  |
| --- | --- |
|  | %% |
|  | %---------------二轮转轮机编写--------------- |
|  | clear all |
|  | close all |
|  | %输入输出初始化 |
|  | input='helloworldhelloworldhelloworldhelloworldhelloworld'; |
|  | encrypt=''; |
|  | decrypt=''; |
|  | %初始化两个轮子 |
|  | rotate1=0; |
|  | rotate2=0; |
|  | wheel1L=[24,25,26,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23]; |
|  | wheel1R=[21,3,15,1,19,10,14,26,20,8,16,7,22,4,11,5,17,9,12,23,18,2,25,6,24,13]; |
|  | wheel2L=[26,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25]; |
|  | wheel2R=[20,1,6,4,15,3,14,12,23,5,16,2,22,19,11,18,25,24,13,7,10,8,21,9,26,17]; |
|  | %循环处理明文的每一位 |
|  | for i=1:length(input) |
|  | index1=abs(input(i)-96); |
|  | index2=find(wheel1R==wheel1L(index1)); |
|  | indexOut=find(wheel2R==wheel2L(index2))+96; |
|  | encrypt=strcat(encrypt,char(indexOut)); |
|  | %下面开始转动转轮 |
|  | rotate2=rotate2+1; |
|  | wheel2R=circshift(wheel2R,[0,1]); |
|  | wheel2L=circshift(wheel2L,[0,1]); |
|  | %转轮二转动26次后，转轮一转动1次 |
|  | if rem(rotate2,26)==0 |
|  | rotate1=rotate1+1; |
|  | wheel1R=circshift(wheel1R,[0,1]); |
|  | wheel1L=circshift(wheel1L,[0,1]); |
|  | end |
|  | end |
|  | %循环解密密文的每一位 |
|  | for j=length(encrypt):-1:1 |
|  | %先转动转轮 |
|  | if rem(rotate2,26)==0 |
|  | rotate1=rotate1-1; |
|  | wheel1R=circshift(wheel1R,[0,-1]); |
|  | wheel1L=circshift(wheel1L,[0,-1]); |
|  | end |
|  | rotate2=rotate2-1; |
|  | wheel2R=circshift(wheel2R,[0,-1]); |
|  | wheel2L=circshift(wheel2L,[0,-1]); |
|  | %进行解密 |
|  | index1=abs(encrypt(j)-96); |
|  | index2=find(wheel2L==wheel2R(index1)); |
|  | indexOut=find(wheel1L==wheel1R(index2))+96; |
|  | decrypt=strcat(decrypt,char(indexOut)); |
|  | end |
|  | decrypt=reverse(decrypt); |

### 【实验过程】

取下图中左边两个轮子作为本实验中的两个轮子：



根据二轮转轮机的原理编写加密、解密程序，运行可得到如下输出：



实验中需要注意的是每处理一个字母，转轮机都需要转动。