**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： 实验二

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20日

实验报告

### 【实验目的】

1. 掌握Playfair密码的原理。
2. 了解代换密码的特点、优缺点。

### 【实验要求】

实现Playfair加密下面的明文（语言不限）：

明文：量子通信保密技术的诞生和快速发展主要取决于以下两个因素：a、经典保密通信面临着三个难以彻底解决的关键问题，即密钥协商、身份识别和窃听检测，这些问题的有效解决需要新技术。b、在对新技术的探索中，人们发现了量子内在的安全特性及其可能的应用。

### 【源代码】

|  |  |
| --- | --- |
|  | %% |
|  | %---------------Playfair编写--------------- |
|  | clear all |
|  | close all |
|  | %加密矩阵如下： |
|  | %   [H,A,R,P,S; |
|  | %    I,C,O,D,B; |
|  | %    E,F,G,K,L; |
|  | %    M,N,Q,T,U; |
|  | %    V,W,X,Y,Z] |
|  | KEY=[8,1,18,16,19; |
|  | 9,3,15,4,2; |
|  | 5,6,7,11,12; |
|  | 13,14,17,20,21; |
|  | 22,23,24,25,26]; |
|  | input='speciallity'; |
|  | encrypt=''; |
|  | %预处理 |
|  | input=strrep(input,'j','i'); |
|  | i=1; |
|  | while(1) |
|  | if i==length(input) |
|  | break; |
|  | end |
|  | if input(i)==input(i+1) |
|  | input=[input(1:i) 'q' input(i+1:end)]; |
|  | end |
|  | i=i+1; |
|  | end |
|  | if rem(length(input),2)~=0 |
|  | input=strcat(input,'q'); |
|  | end |
|  | %加密处理 |
|  | for i=1:2:length(input)-1 |
|  | char1=abs(input(i))-96; |
|  | char2=abs(input(i+1))-96; |
|  | [row1,col1]=find(KEY==char1); |
|  | [row2,col2]=find(KEY==char2); |
|  | if row1==row2 |
|  | out1=KEY(row1,rem(col1,5)+1); |
|  | out2=KEY(row2,rem(col2,5)+1); |
|  | end |
|  | if col1==col2 |
|  | out1=KEY(rem(row1,5)+1,col1); |
|  | out2=KEY(rem(row2,5)+1,col2); |
|  | end |
|  | if row1~=row2 && col1~=col2 |
|  | out1=KEY(row1,col2); |
|  | out2=KEY(row2,col1); |
|  | end |
|  | encrypt=[encrypt char(out1+96) char(out2+96)]; |
|  | end |

### 【实验过程】

对于密码学的实现而言，Matlab显得高效而方便，故接下来的实现都将采用Matlab进行。

先将明文转换为仅含26个字母的拼音，如下：

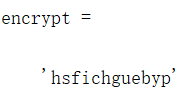
Liangzitongxinbaomijishudedanshenghekuaisufazhanzhuyaoqujueyuyixialianggeyinsuajingdianbaomitongxinmianlinzhesangenanyichedijiejuedeguanjianwentijimiyaoxieshangshenfenshibiehejiantingjiancezhexiewentideyouxiaojiejuexuyaoxinjishubzaiduixinjishudetansuozhongrenmenfaxianleliangzineizaideanquantexingjiqikenengdeyingyong

密钥设置为harpsichord，则加密矩阵如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| H | A | R | P | S |
| I | C | O | D | B |
| E | F | G | K | L |
| M | N | Q | T | U |
| V | W | X | Y | Z |

假设输入speciallity，预处理后的明文应为”SP EC IA LQ LI TY”，两两对应的关系为：SP🡪HS，EC🡪FI，IA🡪CH，LQ🡪GU，LI🡪EB，TY🡪YP。

根据playfair原理编写好代码后（见源代码部分），运行输出如下，可见该输出是正确的：



再输入前面所要求的明文，可得到如下输出：

ebcwlxdmcqqrcmcsiqomombhsmikcpuaimqfimlthcbzncvscwvstzrctmbmkvtzovchebcwqxkfvduansomcmkochucrcveqdqfvoqnchufcmvslhcwkfwctwcoimbcmomomemliklqcwomchwafmmdmomovewpgremhacwlrimwnfmhaciemimomchqucmeomocwifvsgvemvfqucbkvbqvorcomembmgvtzrcvomcmohazlwscbmbvomcmohatbkmcwbzbxriqfhgqnfmncvocwefebcwlxcmmewscbfhqtnsqugvcmeomomolfmfqfikvdqfxdqf