实验1-2　古典密码体制的统计分析——Playfair密码

- 密码学基础　COMP130188.01
  - 任课教师：李景涛
  - 实验课助教：马琦珉 19210240035@fudan.edu.cn

实验目的

1. 了解古典密码中的加密和解密运算；
2. 了解古典密码体制；
3. 掌握古典密码的统计分析方法。

实验原理

playfair加密算法

提高单字母表密码安全性的思路之一。

加密

以FUDAN为密钥，举例说明playfair密码的加密过程：

$$\begin{bmatrix} F & U & D & A & N \\ B & C & E & G & H \\ I/J & K & L & M & O \\ P & Q & R & S & T \\ V & W & X & Y & Z \end{bmatrix}$$

1. **构建加密矩阵**
   playfair加密算法基于一个 5*5 的字母矩阵，该矩阵使用一个关键词（密钥）构造，方法是按约定的顺序（例如从左到右、从上到下），填入关键词的字母（去除重复字母）后，将字母表其余字母填入。
2. **整理明文**
   - 若明文出现相同字母在一组，则在重复的明文字母中插入一个填充字母(eg:x)进行分隔后重新分组(eg: balloon 被重新分组为 ba lx lo on)。
   - 若分组到最后一组时只有一个字母，则补充字母x。
3. **编写密文**
   - 若明文字母在矩阵中同行，则循环取其右边下一个字母为密文(矩阵最右边的下一个是最左边的第一个)(eg: an 被加密为 NF)。
   - 若明文字母在矩阵中同列，则循环取其下边下一个字母为密文(矩阵最下边的下一个是最上边的第一个)(eg: cq 被加密为 KW)。
   - 若明文字母在矩阵中不同行不同列，则取其同行且与同组另一字母同列的字母为密文(eg: hs 被加密为 GT，fm 被加密为 AI 或 AJ)。

解密过程与加密过程相反。

实验环境

- 运行 Windows 操作系统的计算机，具有 C/C++、python语言编译环境 （ 原则上操作系统和编程语言环境不限 ）

实验要求

1. 给定密钥，打印出加密矩阵，实现Playfair密码的解密算法；（ 提供测试用例帮助同学们检测代码的准确性；原则上使用的编程语言不限，要求工作量相近 ）
    - 解密测试用例（ 密文为EQ VS ZT ES FS GZ，密钥为FUDAN ）
      Input:EQ VS ZT ES FS GZ
      Output:CR YP TO GR AP HY
2. 解密文档Playfair-Cipher.txt（ 密钥为SECURITY ）
3. 独立完成实验报告（ 包含实验思路，实验结果截图等 ），提供源代码和可执行程序，不得抄袭。

   注：本次实验为同学们提供了代码模板，可在模板的基础上修改，也可完全自己编写，无强制要求。

提示

- 首先先根据密钥创建加密矩阵，我们约定矩阵、密钥、密文、原文中的J在算法处理中都用I替代；矩阵的数据结构可以是列表、二维数组等。
- 原文和密文的对应关系可以通过矩阵的下标来实现；

实验提交

- 截止日期：2020年11月2日（ 待定 ）
- 提交清单：
    - 实验报告pdf格式，文件名格式：学号_姓名_lab1-2；
    - 项目源代码，文件名格式：学号_lab1-2；
    - Playfair-Cipher.txt的解密文档：学号_lab1-2_Plaintext.txt
- 提交方式：
    - elearning提交。