

实验 1-2 古典密码体制的统计分析

——Playfair 密码

课程名称：密码学基础

课程代码：COMP130188.01

任课教师：李景涛

实验课助教：郑云涛 19210240058@fudan.edu.cn

仲崇鹏 20210240037@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：

<i>F</i>	<i>U</i>	<i>D</i>	<i>A</i>	<i>N</i>
<i>B</i>	<i>C</i>	<i>E</i>	<i>G</i>	<i>H</i>
<i>I/J</i>	<i>K</i>	<i>L</i>	<i>M</i>	<i>O</i>
<i>P</i>	<i>Q</i>	<i>R</i>	<i>S</i>	<i>T</i>
<i>V</i>	<i>W</i>	<i>X</i>	<i>Y</i>	<i>Z</i>

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），依次填入关键词的字母（去除重复字母）后，将字母表其余字母按原来的先后次序填入。

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，但是**推荐使用 python**。）

实验内容

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

测试代码与结果不必提交。

2. 解密文档 lab1-2_input.txt（密钥为 SECURITY），要求**程序运行后生成一个包含明文的文本文件 lab1-2_output.txt，并将该明文写入实验报告的实验结果中**。

提示：

- 首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；
- 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。

实验提交

- 截止日期：2021 年 4 月 11 日
- 提交清单（针对实验内容 2）：
 - 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；
 - 可执行程序，文件名格式：姓名_lab1-2；
 - 资源文件，本实验中为 lab1-2_input.txt。
- 提交方式：
 - 将提交清单中所有文件打包成一个**压缩文件**（文件名：学号_姓名_lab1-2），在 elearning 上进行提交。

评分标准

源代码可编译运行	√	√	√	√	√	
源代码风格良好	√		√			
程序运行结果正确	√	√	√	√		
实验报告规范清晰	√	√			√	√
最终得分	100	90-99	80-89	60-79	40-59	20-39

- 注：1. “源代码风格良好”指的是有必要的注释、合适的缩进，变量和函数命名便于理解；
2. 若出现两位同学报告或代码完全一致的情况，则双方本次实验成绩均为 0；
3. 若源码与程序无法正常运行，则成绩不高于 60 分；
4. 其他情况酌情给分。