



中国科学技术大学  
University of Science and Technology of China

网络空间安全学院  
School of Cyber Science and Technology

作品类别: ☐ 软件设计 ☐ 硬件制作 ☐ 工程实践

## 《密码学导论》课程大作业作品设计报告

---

作品题目: 单表代换辅助工具

团队人员: 李智勤 PB23071400

2025 年 6 月 6 日

## 基本信息表

作品题目：单表代换辅助工具

作品内容摘要：： 单表代换辅助工具

- 功能 1：完成单表代换加密和解密
- 功能 2：辅助破译单表代换密文（唯密文攻击）
  - 根据一般英文的统计分布规律给出破译建议
  - 根据上下文给出破译建议（包括但不限于字母连接、字典等）
  - 使用者根据建议指定部分密钥字，软件更新破译结果并进一步给出建议，反复迭代直至完成破译
  - 界面友好、直观、易用

关键词（五个）：

团队成员（按在作品中的贡献大小排序）：

序号	姓名	学号	任务分工
1			
2			
3			

## 1.作品功能与性能说明

完成单表代换加密和解密

辅助破译单表代换密文（唯密文攻击）

## 2.设计与实现方案

### 1. 加密：

- 输入明文（仅字母）
- 输入 26 个字母的密钥（小写）
- 系统输出加密结果

### 2. 解密：

- 输入密文
- 输入正确的密钥
- 系统输出解密结果

### 3. 破译：

- 输入要破译的密文
- 系统提供分析：
  - 频率分析：显示字母频率统计和基于英文频率的映射
  - 字母连接分析：显示常见双字母组合和映射
  - 字典分析：基于单词模式匹配提供可能的单词
- 用户可以指定密钥映射（格式：密文字母=明文字母）
- 系统实时更新解密结果
- 反复迭代直至完成破译

## 2.1 实现原理

（硬件框图、软件流程、相关描述等）

见源代码

## 2.2 参考文献

## 2.3 运行结果

```
主菜单：
1. 加密文本
2. 解密文本
3. 破译密文
4. 退出
请选择：1

输入要加密的文本（仅字母）：substitution
输入26个字母的密钥（小写）：qwertyuiopasdfghjklzxcvbnm
加密结果：lxwlzozogf
```

```
主菜单：
1. 加密文本
2. 解密文本
3. 破译密文
4. 退出
请选择：2

输入要解密的文本：substitution
输入26个字母的密钥（小写）：qwertyuiopasdfghjklzxcvbnm
解密结果：lgxlehehiy
```

```
主菜单：
1. 加密文本
2. 解密文本
3. 破译密文
4. 退出
请选择：3

输入要破译的密文：substitution

当前密钥映射：
密文字母：a b c d e f g h i j k l m n o p q r s t u v w x y z
明文字母：? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?

当前解密文本：
SUBSTITUTION
```

```
破译菜单：
1. 显示字母频率分析
2. 显示字母位置分析
3. 显示字母映射
4. 显示字母频率
5. 显示字母位置
6. 返回主菜单
请选择：1

字母频率统计（降序）：
i a t b n o u a c d e f g h j k l m p q r v w x y z

建议映射：
密文字母 -> 明文字母（基于英文频率）

a -> i
b -> a
c -> t
d -> b
e -> n
f -> o
g -> u
h -> a
i -> c
j -> d
k -> e
l -> f
m -> g
n -> h
o -> i
p -> j
q -> k
r -> l
s -> m
t -> n
u -> o
v -> p
w -> q
x -> r
y -> s
z -> t

当前密钥映射：
密文字母：a b c d e f g h i j k l m n o p q r s t u v w x y z
明文字母：i a t b n o u a c d e f g h j k l m p q r v w x y z

当前解密文本：
SUBSTITUTION
```

## 2.4 技术指标

## 3.系统测试与结果

### 3.1 测试方案

### 3.2 功能测试

### 3.3 性能测试

### 3.4 测试数据与结果

## 4.应用前景

## 5.结论