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

团队名称： yema

团队人员： 叶力天 PB23151830

2025 年 6 月 7 日

基本信息表

作品题目：单表代换辅助工具

作品内容摘要：

本作品为单表代换辅助工具，主要分为密钥管理模块、加密解密模块、辅助破译模块。密钥管理模块具有自定义密钥、逆置换密钥、使用预设和随机密钥的功能。加密解密模块可以根据用户输入的明密文和指定的密钥进行加密解密操作。辅助破译模块包含明密文对照，智能破译，单字母、双字母、三字母词频分析图表和破译，字典匹配破译的功能，能够半自动化解密密钥的过程。整体采用 TypeScript 编写完成，并用 Vue3 完成界面编写，具有美观、高效、易操作的特点。

关键词（五个）：

单表代换，加密解密，频率分析，字典匹配，辅助破译

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	叶力天	PB23151830	设计、代码、测试

1.作品功能与性能说明

功能说明：

密钥管理模块：

自定义密钥功能：允许用户单独指定每个字母的映射，管理密钥。

随机填充密钥：用随机填充密钥，用于临时加密。

逆置换密钥：方便用户快速切换加密密钥和解密密钥。

预设密钥：预设 ROT13 等常见置换密钥，方便在此场景下进行加解密测试。

加密解密模块：

加密功能：用户可以用指定的密钥对明文文本进行加密。

解密功能：用户可以用指定的密钥对密文文本进行解密。

辅助破译模块：

字频分析图：提供多级分类可视化字频分析图和参照频率对比图，方便用户进行根据字频破译。

字频自动分析：根据字频和参照频率自动破译可能的映射。

字典匹配：根据英文单词字典，自动对未完成的单词进行匹配，并根据频率和单词常用性等计算可能的概率。

性能说明：

采用 O(nm) 复杂度算法，以及字典预加载等方式，处理效率高。采用 TypeScript 语言开发，跨平台执行。具有异常处理功能，稳定性高。无内存泄漏，可以长期稳定运行。

2.设计与实现方案

2.1 实现原理

软件流程：

1. 启动阶段

用户通过浏览器访问网页版应用或打开客户端应用程序，进入美观、直观的主界面。

2. **功能选择**

主界面左侧导航菜单提供加密、解密和辅助解密功能模块，用户可选择所需功能，系统加载对应页面。

3. **操作执行**

- **加密/解密：**在加密/解密界面，用户输入明文（加密）或密文（解密）及密钥，点击操作按钮后，系统调用后台加密/解密函数，处理输入文本与密钥，生成相应结果。
- **辅助解密：**在辅助解密界面，用户输入密文并可选择字频分析、字典匹配等辅助工具。系统实时监测输入，调用分析函数，动态生成破译建议并展示于界面。

4. **界面交互**

基于 Vue 技术构建的前端界面，通过数据绑定和事件监听机制，与后台功能函数实现实时通信，确保用户操作与界面反馈的无缝交互。

5. **功能实现**

核心功能位于 Utils 模块：

- **funcs.ts** 提供加密/解密算法，处理文本与密钥的运算。
- **analyse.ts** 实现字频统计、字典匹配等分析功能，生成智能破译建议。

6. **结果反馈**

后台处理完成后，加密/解密结果或破译建议以可视化形式实时推送至前端界面，完成操作流程。

相关描述：

1. **字频分析：**统计密文中每个单字符、双字符组合、三字符组合出现的次数和频率，对比标准字频分布，找出字符出现规律，辅助推测加密时的字符映射关系。
2. **字典匹配：**将密文与预设词典中的单词进行比对，尝试识别可能的明文单词或短语，结合上下文和字频分析，生成高概率的破译候选结果。
3. **明密文对照：**将明密文上下双排放置，方便进行对照破译。

2.2 参考文献

1. 张肖，and 王薇. "替换式密码算法及其破译能力的分析." 科学与财富 7.27 (2015): 242-242.
2. 吴干华. "基于频率分析的代替密码破译方法及其程序实现." *福建电脑* 9 (2006): 125-125.
3. 邓勇进. "古典密码学." *硅谷* 7 (2011): 14-14.
4. Vue3 文档：https://cn.vuejs.org/

2.3 运行结果

应用已经部署在 Github Pages，访问：

https://yemaster.github.io/crypto-final/ 即可。

加密功能：

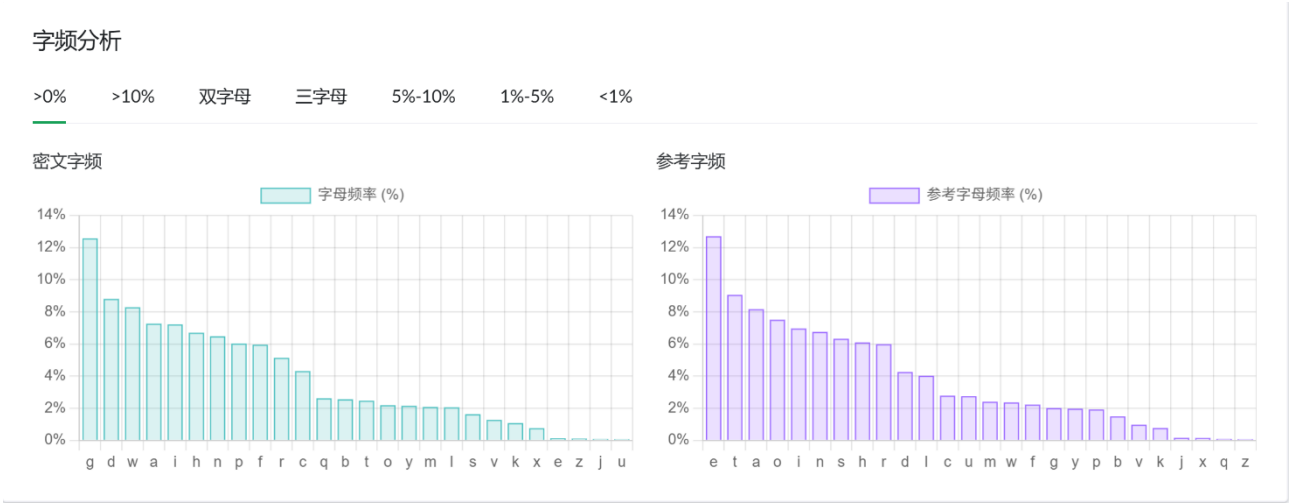
利用密钥 dbgyuwpxjhkrvatsonfqlizcme 对文本 The sun rises gently over the misty mountain peaks. 进行加密：

解密功能：

利用密钥 dbgyuwpxjhkrvatsonfqlizcme 对文本 Qxu fla njfuf puaqrm tiun qxu vjfqm vtlaqdja sudkf. 进行解密：

辅助解密功能：

尝试对密文：hzsrnqc klyy wqc flo mflwf ol zqdn nsoznj wskn lj xzsrbjnf, wzsxz gqv zqhhnf ol ozn glco zlfnco hnlnhrn; nsoznj jnrqosdnc lj fnqj kjsnfbc, wzsxz sc xnjoqsfrv gljn efeceqr. zn rsdnb qrlfn sf zsc zlecn sf cqdsrrn jlw, wzsoznj flfn hnfnojqonb. q csfyrn blgncosx cekksxnb ol crnjdn zsg. zn pjnqmkqconb qfb bsfnb qo ozn xrep, qo zlejc gqozngqosxqrrv ksanb, sf ozn cqgn jllg, qo ozn cqgn oqprn, fndnj oqmsfy zsc gnqrc wsoz loznj gngpnjc, gexz rncc pjsfysfy q yenco wsoz zsg; qfb wnfo zlgn qo naqxorv gsbfsyzo, lfrv ol jnosjn qo lfxn ol pnb. zn fdnlj ecnb ozn xlcv xzgqpnjc wszsz ozn jnkljg hjldsbnc klj soc kqdlejnb gngpnjc. zn hqccnb onf zlejc leo lk ozn ownfov-klej sf cdssrrn jlw, nsoznj sf crnnhsfv lj aamsfv zsc olsrno.进行破译。在网页仅需用智能建议就可以完成破译：



密文

```
gqoznggosxqrrv ksanb,sf ozn cqgn jllg,qo ozn cqgn
oqprn,fndnj oqmsfy zsc gnqrc wsoz loznj
gngpnjc,gexz rncc pjsfysfy q yenco wsoz zsg;qfb
wnfo zlgn qo naqxorv gsbfsyzo,lfrv ol jnosjn qo
lfxn ol pnb.zn fndnj ecnb ozn xlcv xzqgpnjc wzsxz
ozn jnkljg hjldsbnc klj soc kqdlejnb gngpnjc.zn
hqccnb onf zlejc leo lk ozn ownfov-klejsf cqdsrrn
jlw,nsoznj sf crnnhsfy lj gqmsfy zsc olsrno.
```

明文对照

```
hzsrnqc klyy wqc flo mflwf ol zqdn nsoznj wskn lj
_h__e__ ____ ___ __t _____ t_ h__e e_the_ ___e __
xzsrbjnf,wzsxz gqv zqhhnf ol ozn glco zlfnco hnlhr
_h____e_,_h__h ___ h___e_ t_ the ___t h__e_t _e___
n;nsoznj jnrqosdnc lj fnqj kjsnfbc,wzsxz sc xnjoqs
e;e_the_ _e__t__e_ __ _e__ ___e___,_h__h __ _e_t__
frv gljn efeceqr.zn rsdnb qrlfn sf zsc zlecn sf cq
___ ___e _______.he ___e_ ____e __ h__ h___e __ __
dsrrn jlw,wzsoznj flfn hnfnojqonb.q csfyrn blgncos
```

字母映射

a	b	c	d	e	f	g	h	j	k	l

密钥(需要逆置换才可以用作解密)

```
__________et_________h
```

撤销操作 | 智能建议 | 字符频率分析 | 字典分析

破译建议(点击即可自动应用)

参考建议1

可能性: 99%

根据字典分析，ol 仅匹配 to，建议应用该替换

参考建议2

可能性: 85%

根据字典分析，gqoznggosxqrrv 仅匹配 mathematically，建议应用该替换

参考建议3

可能性: 85%

密文

```
hzsrnqc klyy wqc flo mflwf ol zqdn nsoznj wskn lj
xzsrbjnf, wzsxz gqv zqhhnf ol ozn glco zlfnco
hnlnhrn; nsoznj jnrqosdnc lj fnqj kjsnfbc, wzsxz
sc xnjoqsfrv gljn efeceqr. zn rsdnb qrlfn sf zsc
zlecn sf cqdsrrn jlw, wzsoznj flfn hnfnojqonb.
q csfyrn blgncosx cekksxnb ol crnjdn zsg. zn
pjnqmkqconb qfb bsfnb qo ozn xrep, qo zlejc
gqoznggosxqrrv ksanb, sf ozn cqgn jllg, qo ozn
cqgn oqprn, fndnj oqmsfy zsc gnqrc wsoz loznj
gngpnjc, gexz rncc pjsfysfy q yenco wsoz zsg; qfb
wnfo zlgn qo naqxorv gsbfsyzo, lfrv ol jnosjn qo
lfxn ol pnb. zn fdnlj ecnb ozn xlcv xzgqpnjc
wszsz ozn jnkljg hjldsbnc klj soc kqdlejnb
gngpnjc. zn hqccnb onf zlejc leo lk ozn ownfov-
klej sf cdssrrn jlw, nsoznj sf crnnhsfv lj aamsfv
zsc olsrno.
```

明文对照

```
hzsrnqc klyy wqc flo mflwf ol zqdn nsoznj wskn lj
phileas fogg was not known to have either wife or
xzsrbjnf, wzsxz gqv zqhhnf ol ozn glco zlfnco hnln
children, which may happen to the most honest peoe
hrn; nsoznj jnrqosdnc lj fnqj kjsnfbc, wzsxz sc xn
ple; either relatives or near friends, which is ce
joqsfrv gljn efeceqr. zn rsdnb qrlfn sf zsc zlecn
rtainly more unusual. he lived alone in his house
sf cqdsrrn jlw, wzsoznj flfn hnfnojqonb.
in saville row, whither none penetrated.
q csfyrn blgncosx cekksxnb ol crnjdn zsg. zn pjnqm
a single domestic sufficed to slerve him. he break
kqconb qfb bsfnb qo ozn xrep, qo zlejc gqoznggosxq
fasted and dined at the club, at hours mathematica
rrv ksanb, sf ozn cqgn jllg, qo ozn cqgn oqprn, fn
lly fixed, in the same room, at the same table, ne
dnj oqmsfy zsc gnqrc wsoz loznj
```

字母映射

a	b	c	d	e	f	g	h	j	k	l
x	d	s	v	u	n	m	p	r	f	o

密钥(需要逆置换才可以用作解密)

```
xdsvunmpjrfoketbaliqzywcgh
```

撤销操作 | 智能建议 | 字符频率分析 | 字典分析

破译建议(点击即可自动应用)

Wow

已经破译完成。

2.4 技术指标

性能指标：处理速度、分析效率、资源占用
兼容性：平台支持
易用性：界面美观性、用户引导

3.系统测试与结果

3.1 测试方案

对于加密解密功能，采用 Vue 的单元测试工具 Vitest 进行自动化功能和性能测试。对于辅助解密功能，采用人工手动破译密文的方式进行测试，并计算解密所需时间。

3.2 功能测试

逆置换密钥功能：指定密钥，对逆置换结果和答案进行比对。

加密功能：指定明文和密钥，对加密结果和答案进行比对。

解密功能：因为解密功能使用上述两个功能，上述两个功能的正确性可以保证正确性。

辅助功能：输入密文和不完整的密钥，手工观察是否能给出合适的提示。

3.3 性能测试

加密解密功能：自动化工具给出短文本和长文本加解密的耗时

辅助功能：观察辅助解密复杂文本的耗时。

3.4 测试数据与结果

单元测试的代码放在项目的 /test 文件夹下，运行命令 yarn test 进行单元测试，全部数据均通过。在大数据（明文长度 870000）下，处理速度仅为 87ms，可见加解密算法效率高：

```
yarn run v1.22.22
$ vitest run --reporter verbose

 RUN  v3.2.2 E:/Projects/crypto-final

 ✓ test/keyTransform.test.ts (9 tests) 7ms
   ✓ reverseKey (7)
     ✓ should throw an error for keys with less than 26 letters 1ms
     ✓ should throw an error for keys with more than 26 letters 1ms
     ✓ should throw an error for keys with non-letter characters 1ms
     ✓ should throw an error for keys with repeated letters 0ms
     ✓ should return the same key for the identity transformation 0ms
     ✓ should return the correct reversed key for a valid key 0ms
     ✓ should return the correct reversed key for various valid keys 0ms
   ✓ randomKey (2)
     ✓ should generate a key with 26 unique lowercase letters 0ms
     ✓ should generate different keys on multiple calls 1ms
 ✓ test/encrypt.test.ts (4 tests) 90ms
   ✓ encrypt (4)
     ✓ should throw an error if plaintext or key is not provided 1ms
     ✓ should throw an error if key is not 26 characters long 0ms
     ✓ should encrypt plaintext using the provided key 0ms
     ✓ should handle large plaintext 87ms

 Test Files  2 passed (2)
      Tests  13 passed (13)
   Start at  16:44:47
   Duration  1.22s (transform 63ms, setup 0ms, collect 87ms, tests 97ms, environment 0ms, prepare 144ms)

Done in 2.28s.
```

对于辅助破译功能，对 examples 下的密文进行半自动化破译，均能在 30 秒内正确破译。

4.应用前景

该工具凭借多层级辅助解密能力与跨场景适配性，在密码教育、实战分析及轻量化加密领域具备显著前景。在密码学教育中，其可视化频率分析与字典匹配功能，可动态演示古典密码破解逻辑，成为高校信息安全、密码学课程的实验标配，助力学生掌握单表代换核心原理。在 CTF 竞赛与密码分析实战中，实时频率统计与自定义字典扫描能快速定位密文特征，大幅缩短人工分析时间，满足竞赛选手高效破解需求。在轻量级数据保护场景，支持多语言字符集的加密解密功能，适配日记、备忘录等非敏感数据的个性化加密，相较专业软件更易上手。

5.结论

单表代换辅助工具通过高效算法、直观界面和跨平台兼容性，为密码学教育、分析和轻量级数据保护提供了强大支持。其性能优异，兼容性强，并通过

本地化处理确保数据安全。测试结果表明，工具在功能正确性和性能稳定性方面表现优异，适合学术研究和实际应用。未来可通过增加机器学习算法和多语言支持，进一步提升破译效率和应用范围。