

说明文档

1. 算法

a. 加密过程

1. 首先对密钥的字母字符进行排序（为列置换算法做准备）
2. 明文字符长度应为密钥字母字符的整数倍，不足时用字符 a 补充
3. 然后使用维吉尼亚加密算法对明文进行加密，得到中间密文
4. 最后使用列置换算法对中间密文进行加密，得到最终密文

b. 解密过程

1. 与加密过程相反

2. 注意点

1. 加密时自动忽略密钥中包含的非字母符号
2. 只对明文中的字符进行加密，但保留明文中非字母符号和相对位置
3. 列置换时，最后一行不足时，填充字符 a
4. 密钥、明文、密文长度最多255字符

3. 运行环境

1. 要求有gcc编译器
2. 编译命令

```
gcc -o main main.c -w -g
```

3. 运行命令

linux: `./main`

windows: 直接双击 `main.exe` 文件

 注：windows环境运行起来可能会有乱码问题

4. 运行示例

密钥: `I am, I exist, that is cert`

明文: `Machines cannot think`

密文: `akna aiataaaMnhaeaoacahasata acanaiana`

```
realguo@realguo-virtual-machine: ~/work/信息安全/encrypti...
realguo@realguo-virtual-machine:~/work/信息安全/encryption$ gcc -o main main.c -w -g
/usr/bin/ld: /tmp/ccuaMzmo.o: in function `main':
/home/realguo/work/信息安全/encryption/main.c:240: 警告: the `gets' function is dangerous and should not be used.
realguo@realguo-virtual-machine:~/work/信息安全/encryption$ ./main
=====
自定义加密算法
作者: 刘陈陈(RealGUO)
描述:
a. 使用维吉尼亚算法+列置换算法加密
b. 加密时自动忽略密钥中包含的非字母符号
c. 只对明文中的字符进行加密, 但保留明文中非字母符号和相对位置
d. 列置换时, 最后一行不足时, 填充字符'a'
e. 密钥、明文、密文长度最多255字符
=====
-----
1. 加密
2. 解密
3. 退出
请选择操作编号: █
```

```
realguo@realguo-virtual-machine: ~/work/信息安全/encrypti...
d. 列置换时, 最后一行不足时, 填充字符'a'
e. 密钥、明文、密文长度最多255字符
=====
-----
1. 加密
2. 解密
3. 退出
请选择操作编号: 1
请输入密钥: I am, I exist, that is cert
请输入明文: Machines cannot think
加密结果 (密文): adut immlsttUepamehaoijckxbt ivsnhmeki
加密

1. 加密
2. 解密
3. 退出
请选择操作编号: 2
请输入密钥: I am, I exist, that is cert
请输入密文: adut immlsttUepamehaoijckxbt ivsnhmeki
解密结果 (明文): Machines cannot thinkaaaaaaaaaaaaaaaaa
解密

1. 加密
2. 解密
3. 退出
请选择操作编号:
```