

1.基本测试：

根据 S-DES 算法编写和调试程序，提供 **GUI 解密**支持用户交互。输入可以是 8bit 的数据和 10bit 的密钥，输出是 8bit 的密文。GUI 界面如下所示：

加密算法系统

选择加密模式:

S-DES

bit模式

文件加解密

明密文对照

暴力破解

bit模式

密钥 (二进制):

11110000110

明文:

10101010

密文:

01101110

加密

解密

© 2024 信息安全导论 20221982潘钊威20221385江佳艺

如果密钥的格式不正确(即不是 10bit 的二进制数)，则会给出如下提醒：

选课管理 - 重庆大学

全国大学

127.0.0.1:5000 显示

加密过程中发生错误

确定

加密算法系统

选择加密模式:

S-DES

bit模式

文件加解密

明密文对照

暴力破解

bit模式

密钥 (二进制):

1010

明文:

11110000

密文:

加密/解密结果

加密

解密

© 2024 信息安全导论 20221982潘钊威20221385江佳艺

如果输入了合法的密钥，则可以输入明文二进制串，程序会自动将其转化为密文，如下所示：

加密算法系统

选择加密模式:

S-DES

bit模式

文件加解密

明密文对照

暴力破解

bit模式

密钥 (二进制):

1111100000

明文:

11110000000

密文:

11111011

加密

解密

© 2024 信息安全导论.20221982潘伽藏20221385江佳艺

明文二进制串不限制位数，明文的输入 bit 数等于密文的输出 bit 数。

由上可知，本程序提供了 **GUI 解密**，支持用户交互，要求输入的密钥是 10 位二进制数，支持输入多位的明文，并自动给出对应的密文。满足基本测试的要求。

2.交叉测试：

考虑到是**算法标准**，所有人在编写程序的时候需要使用相同算法流程和转换单元 (P-Box、S-Box 等)，以保证算法和程序在异构的系统或平台上都可以正常运行。设有 A 和 B 两组位同学(选择相同的密钥 K)；则 A、B 组同学编写的程序对明文 P 进行加密得到相同的密文 C；

采取密钥 1111100000.输入明文 10101010，两个小组都得到相同的密文  
00011011

# 加密算法系统

选择加密模式:

S-DES

bit模式

文件加解密

明密文对照

暴力破解

---

bit模式

密钥 (二进制):

1111100000

明文:

10101010

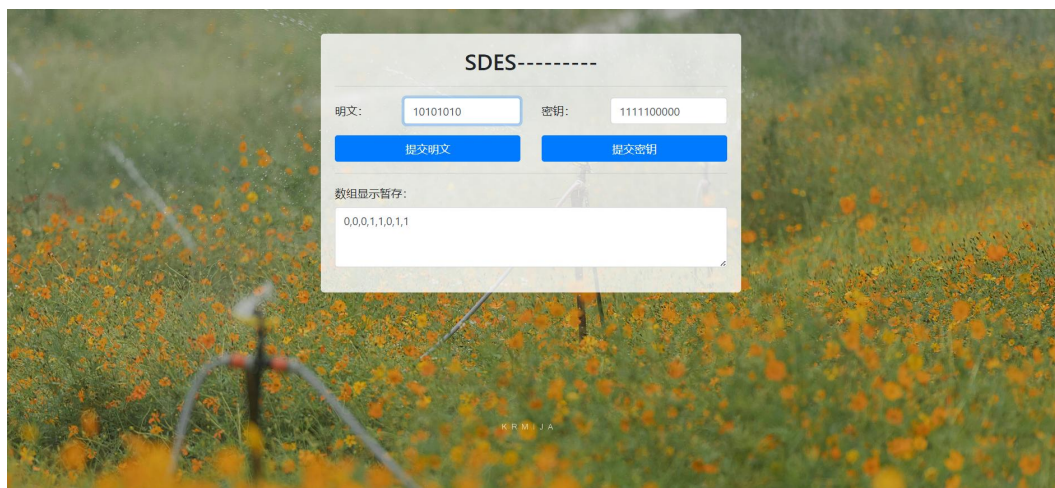
密文:

00011011

加密

解密

© 2024 信息安全导论.20221982潘钊葳20221385江佳艺



由上可知本程序可以满足交叉测试的功能。

### 3.扩展功能：

考虑到向实用性扩展，加密算法的数据输入可以是 ASCII 编码字符串(选择的文件对应内容为“hello world 123”)，对应地输出也可以是 ASCII 字符串(很可能是乱码)。

加密算法系统

选择加密模式:

S-DES

bit模式

文件加解密

明密文对照

暴力破解

文件加解密

密钥 (二进制):

1010101010

选择文件:

选择文件

test.txt

文件加密

文件解密

保存文件

U

© 2024 信息安全导论 20221982潘锐威20221385江佳艺

经过测试，本程序可以实现数据输入为 ASCII 编码字符串(字符串的长度不限)，对应的输出是乱码或者 ASCII 字符串。即本程序可以通过扩展功能的测试。

4.暴力破解

暴力破解的 GUI 如下：

加密算法系统

选择加密模式:

S-DES

bit模式

文件加解密

明密文对照

暴力破解

暴力破解

线程数量:

4

明文:

请输入明文

密文:

请输入密文

开始暴力破解

对于以下名密文对，明文：00110101，密文：11001101，密钥 1001010011。输入明文：00110101，密文：11001101，线程数量 3。得到破解结果如下：

## 加密算法系统

选择加密模式:

S-DES

bit模式文件加解密明密文对照暴力破解

### 暴力破解

线程数量:

3

明文:

00110101

密文:

11001101

开始暴力破解

破解成功，找到的密钥为: 1010101010, 1001010011

© 2024 信息安全导论.20221982潘钊威20221385江佳艺

由上图可知，对于随机选择的一对名密文对，存在多个不同的密钥，即会出现密钥碰撞的现象。暴力破解成功。

## 5.封闭测试

由第四关暴力破解的测试结果可知，对于明密文对，明文：00110101，密文：11001101，有四个不同的密钥 1001010011，1010101010 能造成这样的转化。

因此将这四个不同的密钥分别对同一个明文进行加密，观察其对应的密文是否有相同的，若相同，则说明对应明文空间任意给定的明文分组  $P_n$ ，会出现选择不同的密钥  $K_i \neq K_j$  加密得到相同密文  $C_n$  的情况。

测试结果如下：

对于不同的密钥 1001010011 和 1010101010，明文输入相同，加密得到相同的密文：

加密算法系统

选择加密模式:

S-DES

bit模式文件加解密明密文对照暴力破解

明密文对照

密钥 (二进制):1001010011

明文:00110101

密文 (二进制):10001110

© 2024 信息安全导论.20221982潘钊葳20221385江佳艺

加密算法系统

选择加密模式:

S-DES

bit模式文件加解密明密文对照暴力破解

明密文对照

密钥 (二进制):1010101010

明文:00110101|

密文 (二进制):10001110

© 2024 信息安全导论.20221982潘钊葳20221385江佳艺

由以上测试结果可知，对应明文空间任意给定的明文分组 $P_n$ ，会出现选择不同的密钥 $K_i \neq K_j$ 加密得到相同密文 $C_n$ 的情况。封闭测试完成。