

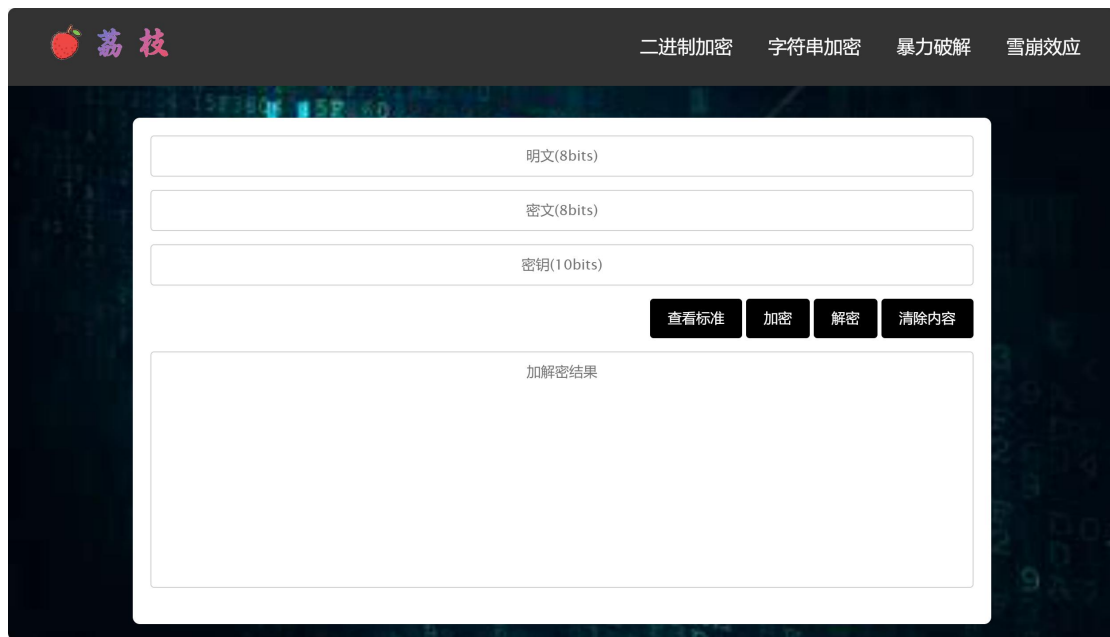
测试结果

—— written by 荔枝

小组成员：张芷芮、刘俐莹
联系方式：1635487611@qq.com

第 1 关：基本测试

【测试要求】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。



The screenshot shows a web-based GUI for S-DES. At the top, there is a navigation bar with the logo '荔枝' and four tabs: '二进制加密', '字符串加密', '暴力破解', and '雪崩效应'. The main interface has three input fields: '明文(8bits)', '密文(8bits)', and '密钥(10bits)'. Below these fields are four buttons: '查看标准', '加密', '解密', and '清除内容'. At the bottom, there is a large text area labeled '加解密结果'.

【测试用例】

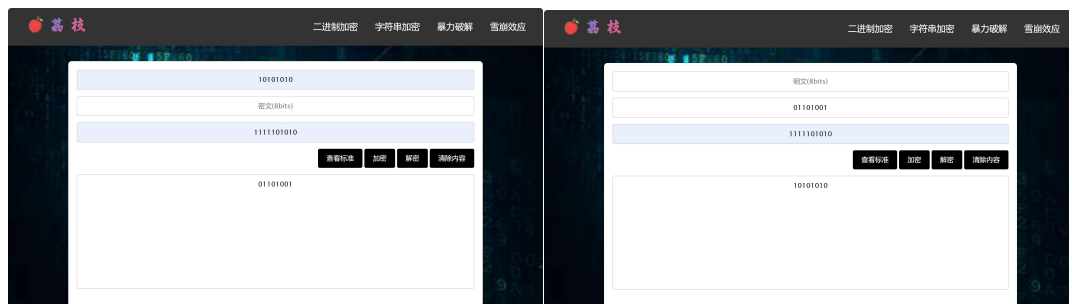
加密：明文：10101010 密钥：1111101010

解密：密文：01101001 密钥：1111101010

【测试结果】

加密结果：01101001

解密结果：10101010



The two screenshots show the GUI after performing encryption and decryption. The left screenshot shows the '加密' (Encrypt) button clicked, with the plaintext '10101010' in the '明文(8bits)' field, the ciphertext '01101001' in the '密文(8bits)' field, and the key '1111101010' in the '密钥(10bits)' field. The right screenshot shows the '解密' (Decrypt) button clicked, with the ciphertext '01101001' in the '密文(8bits)' field, the plaintext '10101010' in the '明文(8bits)' field, and the key '1111101010' in the '密钥(10bits)' field.

可以看出，基础加解密功能无误，可以正常进行运算。

第2关：交叉测试

【测试要求】设有 A 和 B 两组同学(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；或者 B 组同学接收到 A 组程序加密的密文 C，使用 B 组程序进行解密可得到与 A 相同的 P。

我们与卞咯吩组进行了交叉测试，分别使用了如下三种测试方式，测试用例和测试结果如下（A 组为荔枝，B 组为卞咯吩）：

【测试用例】

密钥 K: 1111000010

1、同时对明文加密

明文: 10101100

2、A 组加密，B 组解密

明文: 11110000 密文: 11111101

3、B 组加密，A 组解密

明文: 10010101 密文: 01100011

【测试结果】

1、A、B 两组选择相同的密钥，同时对明文 P 进行加密：

可以发现，两组的加密结果均为 11001001。说明测试成功，两组加密算法无误

8bit 加解密

加密 解密

请输入8位二进制明文


10101100

请输入10位二进制密钥

1111000010

确认 重置

加密后的密文是:
1,1,0,0,1,0,0,1



二进制加密 字符串加密 暴力破解 雪崩效应

10101100

密文(8bits)

1111000010

查看标准

加密


解密

清除内容

11001001

2、A 组对明文进行加密，B 组用 A 组的加密结果进行解密：

可以发现，B 组的解密结果与明文一致，说明测试成功，B 组解密算法无误
加密过程（荔枝组）：



二进制加密 字符串加密 暴力破解 雪崩效应

11110000

密文(8bits)

1111000010

查看标准

加密

解密

清除内容

11111101

解密过程（卜咯吩组）：

8bit 加解密

加密解密

请输入8位二进制密文

11111101

请输入10位二进制密钥

1111000010

确认重置

解密后的明文是:
1,1,1,1,0,0,0,0

3、B 组对明文进行加密，A 组用 B 组的加密结果进行解密：

可以发现，A 组的解密结果与明文一致，说明测试成功，两组加解密算法均无误

加密过程（卜咯吩组）：

8bit 加解密

加密解密

请输入8位二进制明文

10010101


请输入10位二进制密钥

1111000010

确认重置

加密后的密文是:
0,1,1,0,0,0,1,1

解密过程（荔枝组）：



二进制加密 字符串加密 暴力破解 雪崩效应

明文(8bits)

01100011

1111000010

查看标准

加密


解密

清除内容

10010101

第3关：扩展功能

【测试要求】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(分组为 1 Byte)，对应地输出也可以是 ASCII 字符串(很可能是乱码)。



二进制加密 字符串加密 暴力破解 雪崩效应

明文(字符串 1 byte)

密文(二进制 16 bits)

密钥(10bits)

加密

解密

清除内容

加解密结果

【测试用例】

加密：明文：abcd

密钥：1111101010

解密：密文：10011001111101011010000010010011

密钥：1111101010

【测试结果】

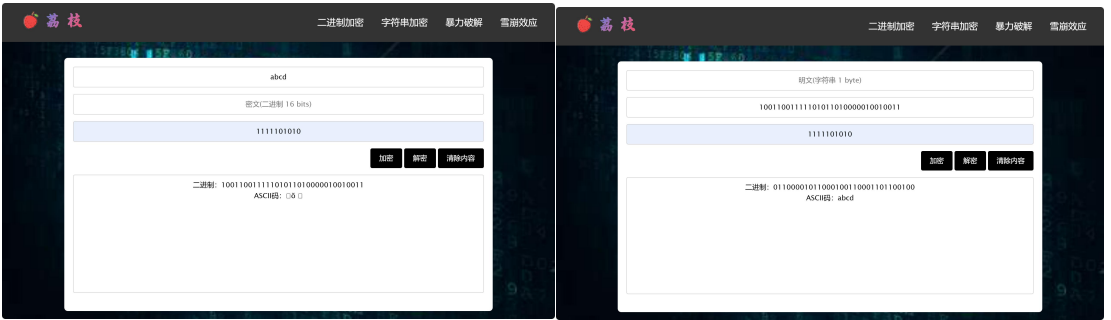
加密结果：二进制：10011001111101011010000010010011

ASCII 码： ð （乱码无法完全显示）

解密结果：二进制：01100001011000100110001101100100

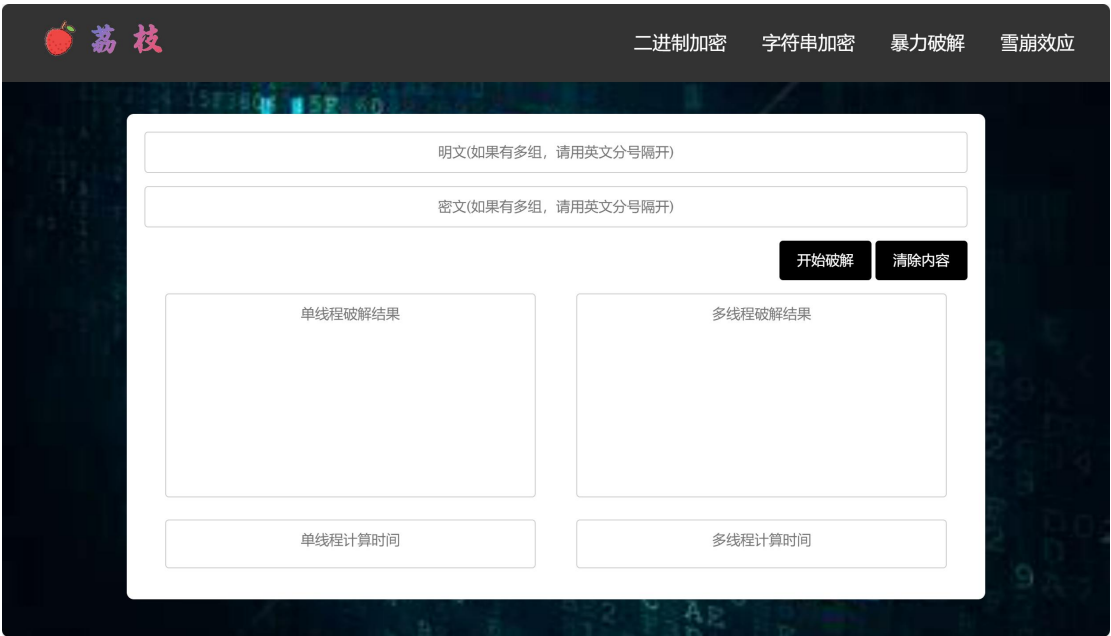
ASCII 码：abcd

可以看出，扩展 ASCII 码加解密功能无误，可以正常进行运算。



第 4 关：暴力破解

【测试要求】假设你找到了使用相同密钥的明、密文对(一个或多个)，请尝试使用暴力破解的方法找到正确的密钥 Key。在编写程序时，你也可以考虑使用多线程的方式提升破解的效率。请设定时间戳，用视频或动图展示你在多长时间内完成了暴力破解。



【测试用例】

明文：10101010 密文：10101001

【测试结果】

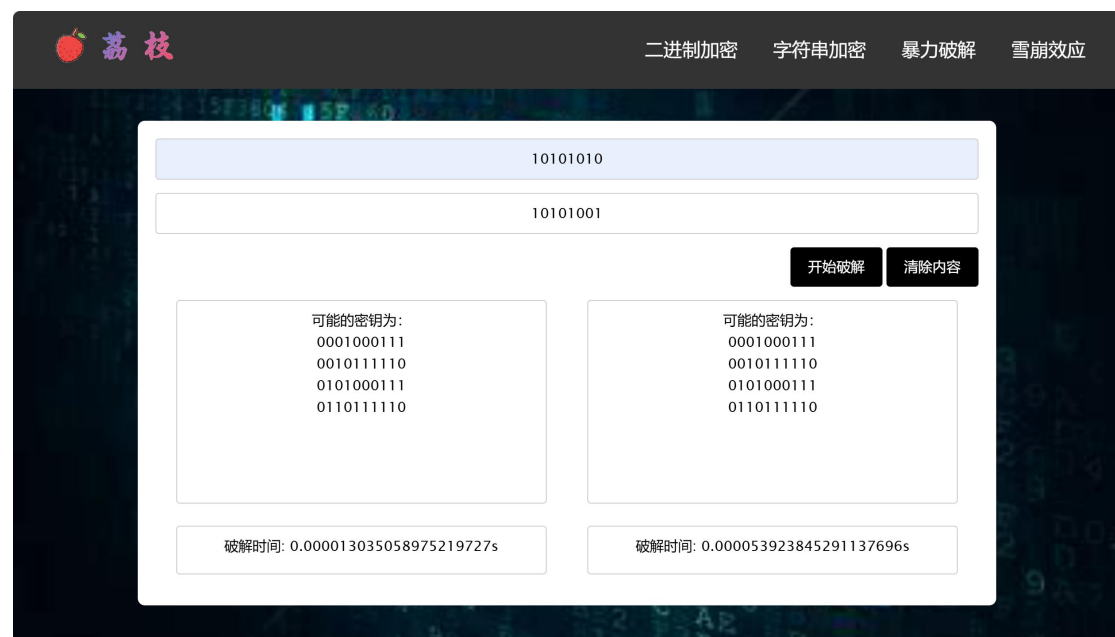
1、单线程破解结果：可能的密钥：0001000111、0010111110、0101000111、0110111110

计算时间：0.000013035058975219727s

2、多线程破解结果：可能的密钥：0001000111、0010111110、0101000111、0110111110

计算时间：0.000053923845291137696s

（本功能在计算时间的显示框中设置了计时器动画演示，但由于破解速度较快，动画演示效果一般）



第5关：封闭测试

【测试要求】根据第4关的结果，进一步分析，对于你随机选择的一个明密文对，是不是有不只一个密钥Key？进一步扩展，对应明文空间任意给定的明文分组 P_n ，是否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？

【测试用例】

明文：10101010

密钥：0001000111、0010111110、0101000111、0110111110

密文：10101001

【测试结果】

1、根据第四关暴力破解的结果我们发现，对于随机选取的一个明密文对（明文：10101010 密文：10101001），确实会存在不止有一个密钥Key的情况。

2、对于给定的明文分组：10101010，使用不同的密钥（密钥 1：0001000111；密钥 2：0010111110）都可以得到相同的加密结果，密文为 10101001。

