1-5 通关测试情况

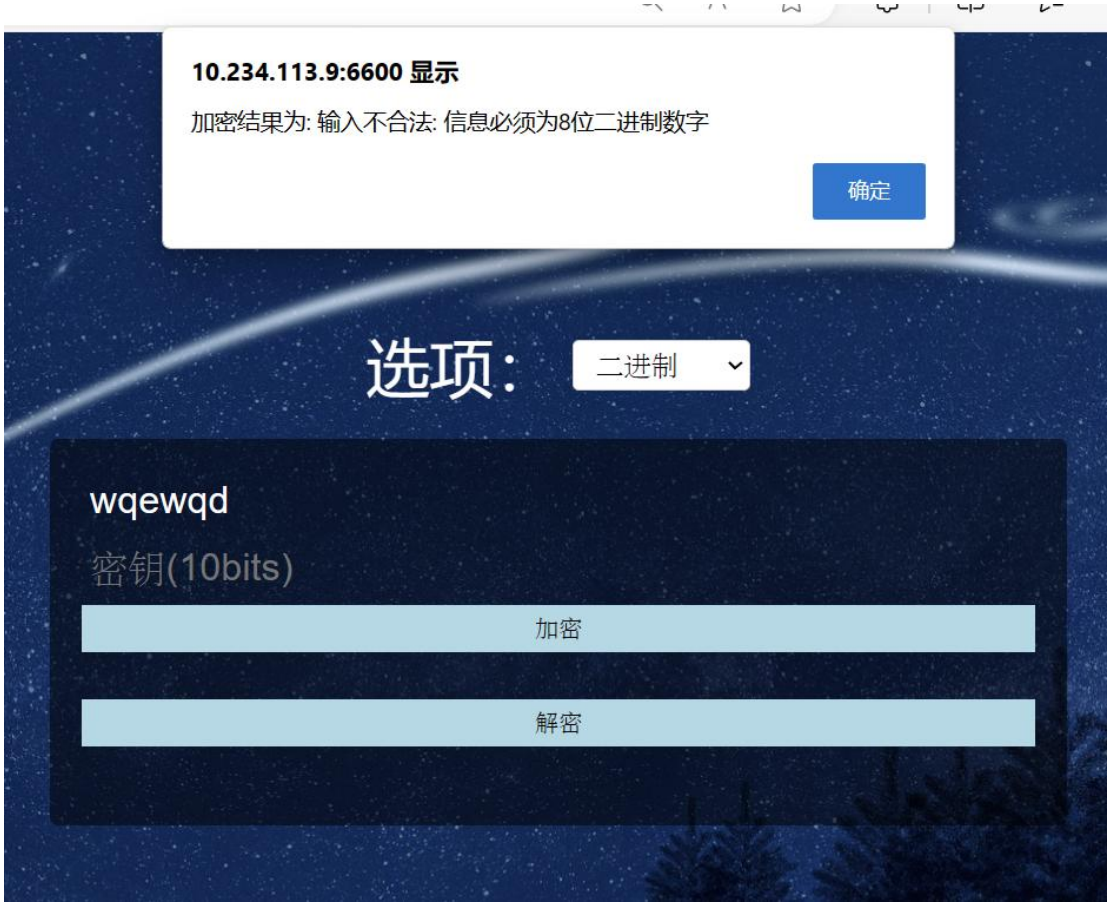
小组:RNG

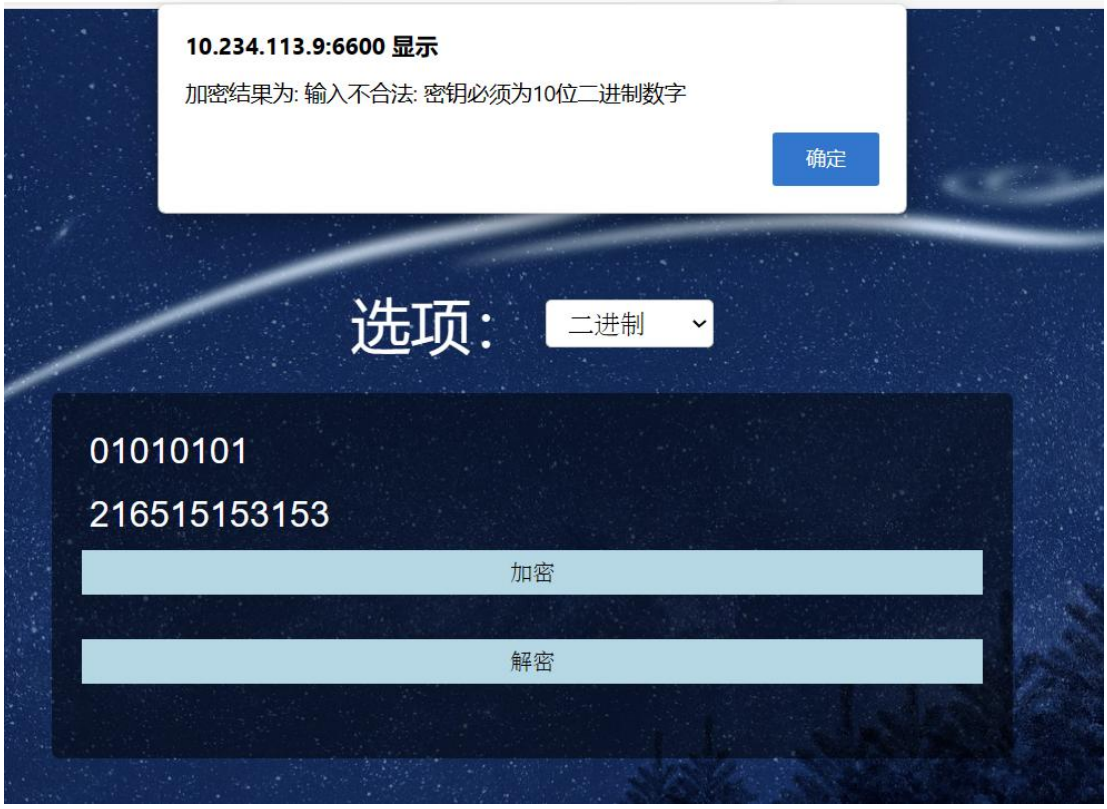
成员：李泽坤、吴科明

第一关：基本测试

用户界面总览

当输入的信息和密钥内容或者位数不合法时，会重新输入：

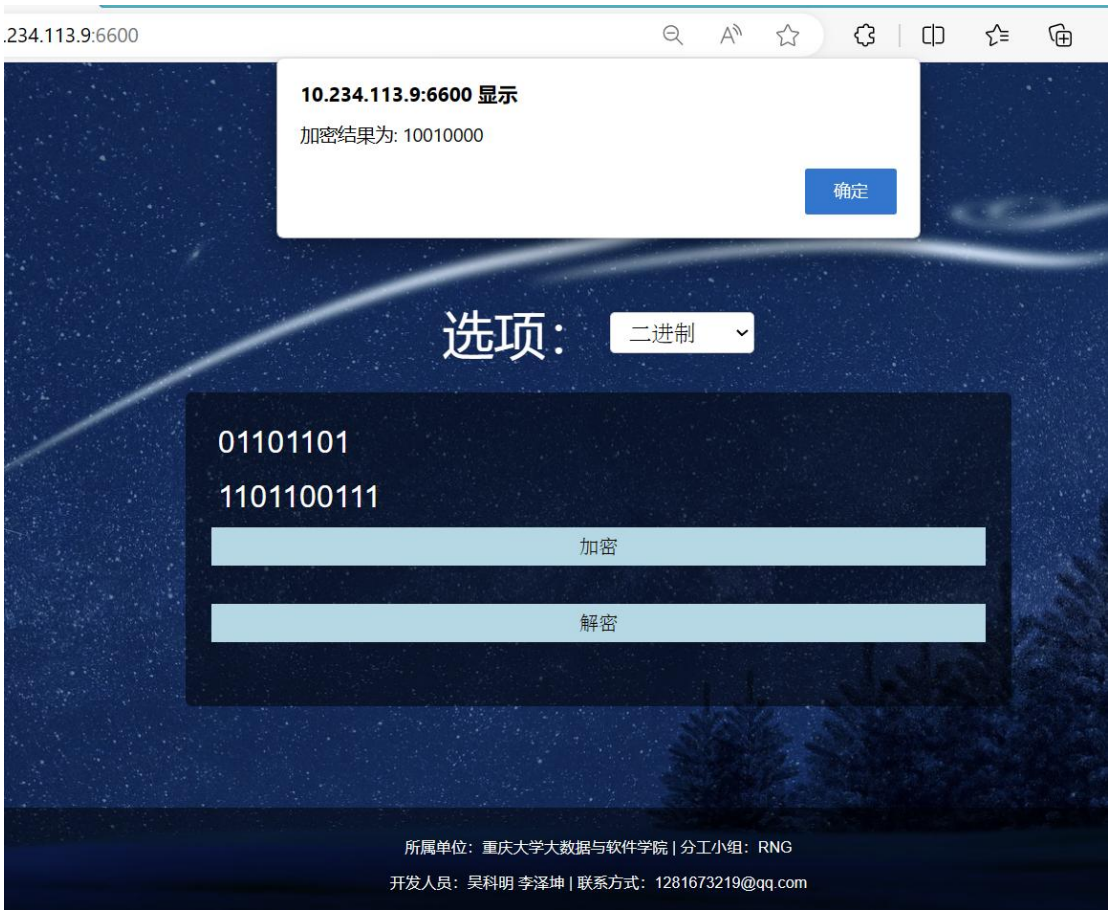




接下来，我们展示级别的加加解密操作：

输入明文：01101101

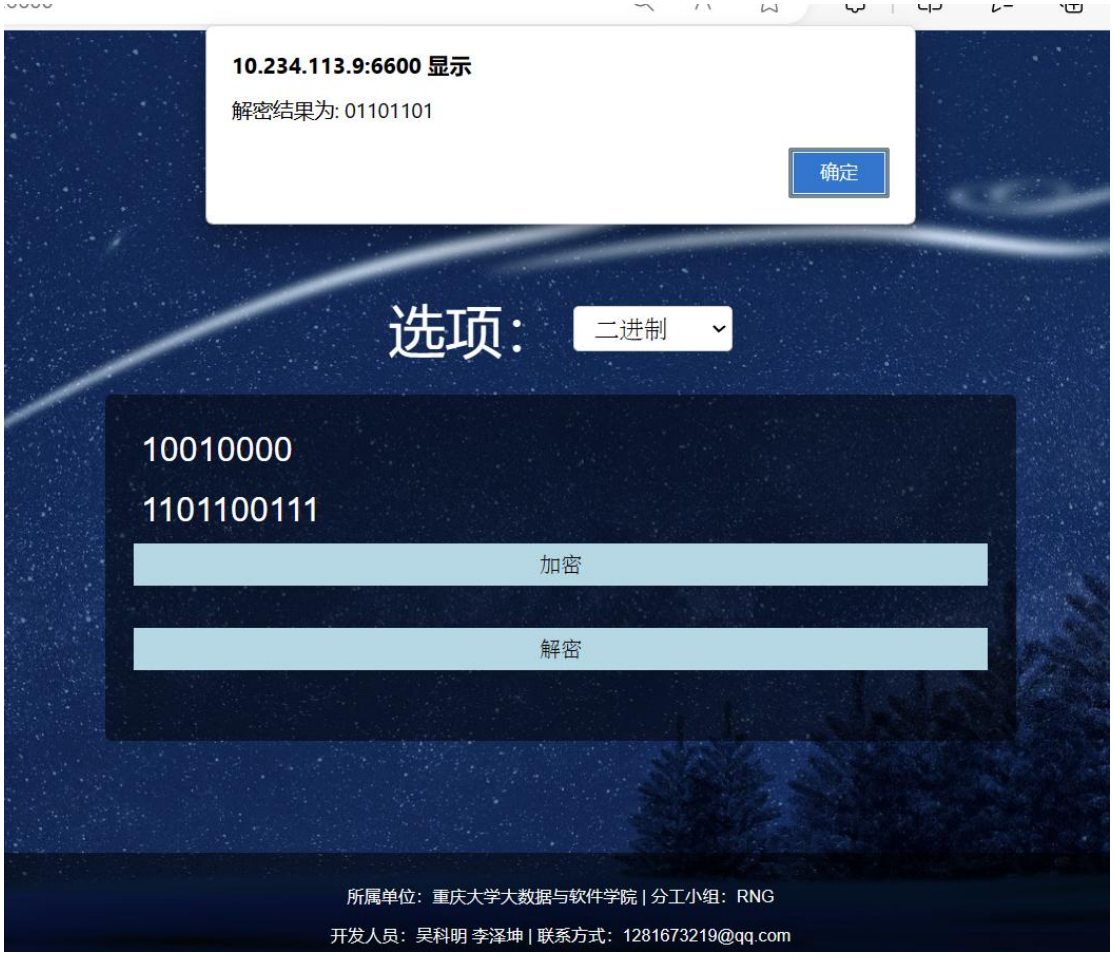
我们得到了下面的加密结果：



接下来，我们用刚才得到的密文和密钥进行解密：

密文：10010000

密钥：1101100111



解密结果为:01101101

这和我们最开始使用的明文是一致的，至此我们结束了第一关的测试

第二关 交叉测试

本次测试使用内容如下：

明文 1：11001100

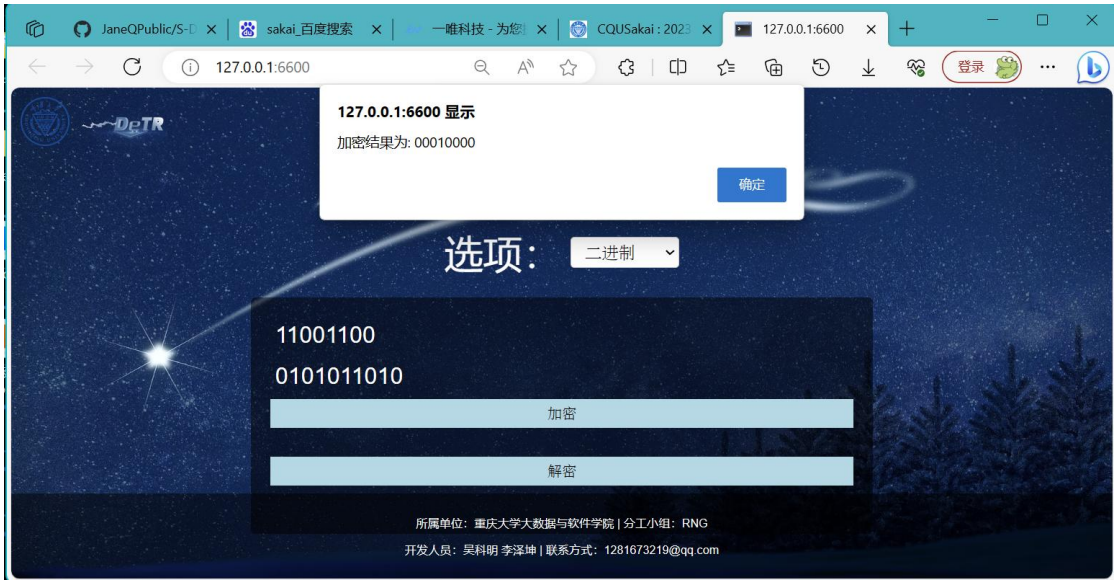
密钥 1：0101011010

明文 2：rng

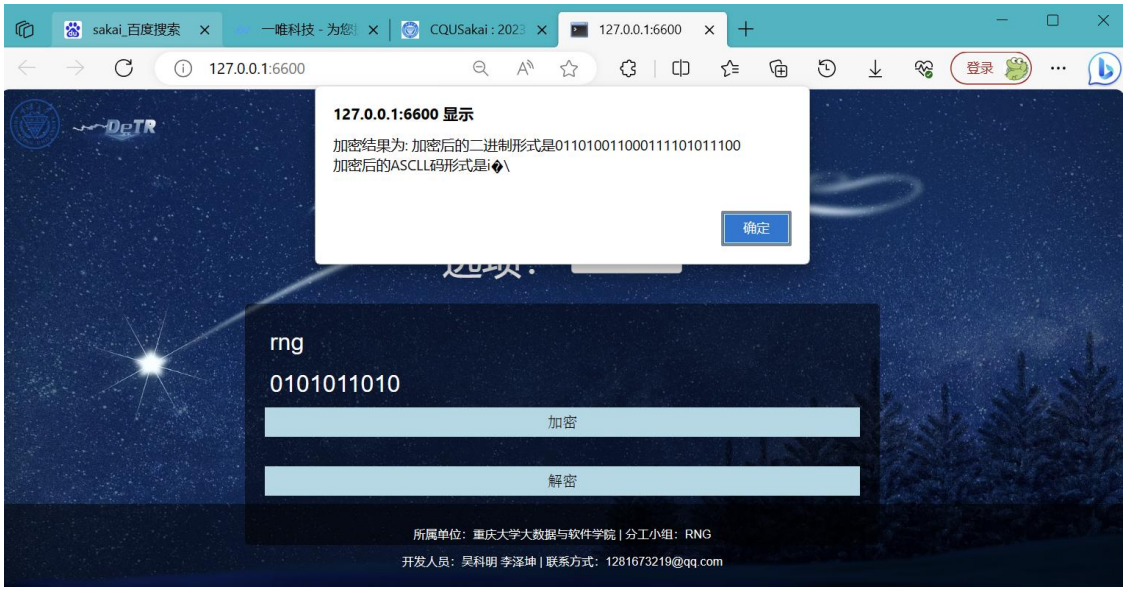
密钥 2：0101011010

我们程序的二进制明文加密测

试：



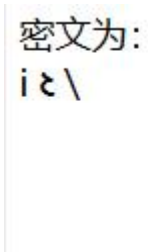
我们程序的 ASCII 码明文加密测试：



交叉测试组的两个加密结果：

密文为： ['00010000']

密文为： i\



可以看出，我们和其他小组的交叉测试结果是一样的， 交叉测试通过！

第三关 拓展功能

我们的作品进行了拓展，加密算法的数据输入可以是 ASII 编码字符串(分组为 1 Byte)

对应地输出也可以是 ACII 字符串(很可能是乱码)。而且我们使用的是 web 开发，在网页显示中，还纯在部分乱码是不可见的，不可以复制的状态

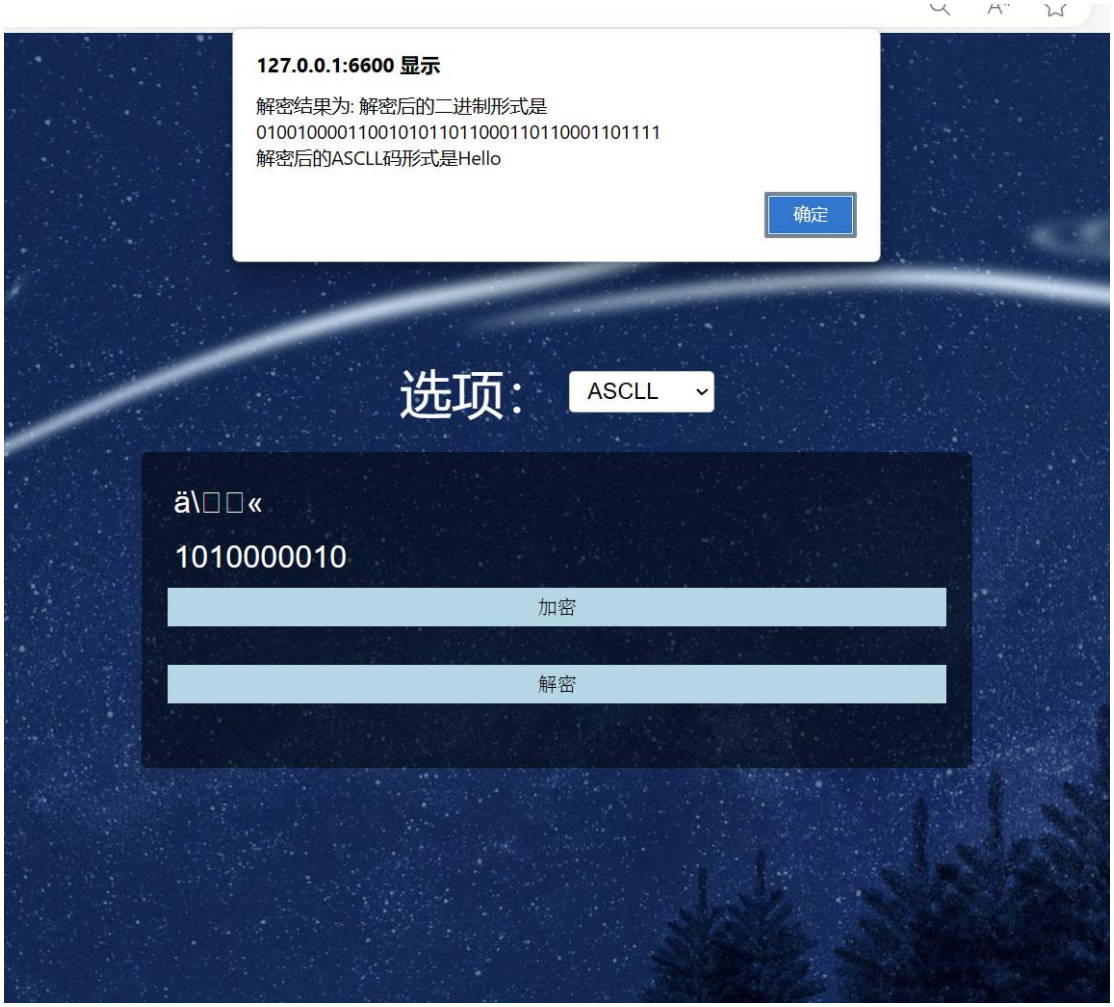
下图是加密演示：

明文：Hello

密钥：1010000010

密文：ä\��«

面是对应的解密演示：



解密成功，得到对应的明文，演示结束，第三关通过。

第四关 暴力破解

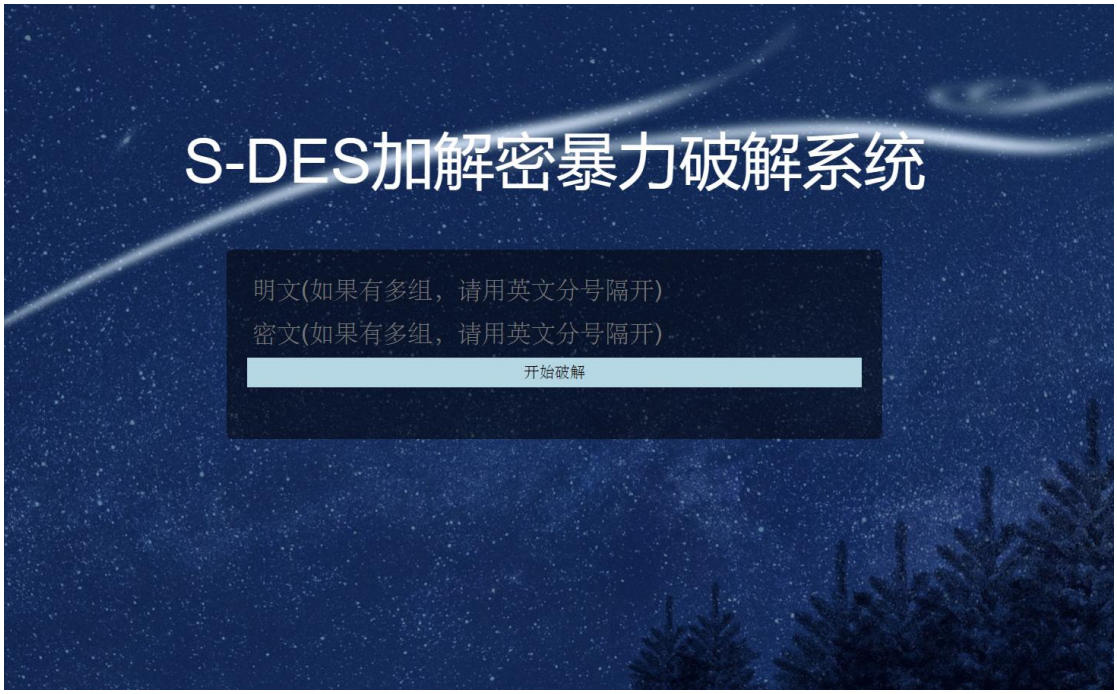
在第 4 关中，我们尝试使用暴力破解的方法来找到正确的密钥。

对于一份已知的明文密文文对，我们得到了多份密钥的解，并使用单线程与多线程的方式对比破解效率。

在软件界面上选择对应的破解功能：

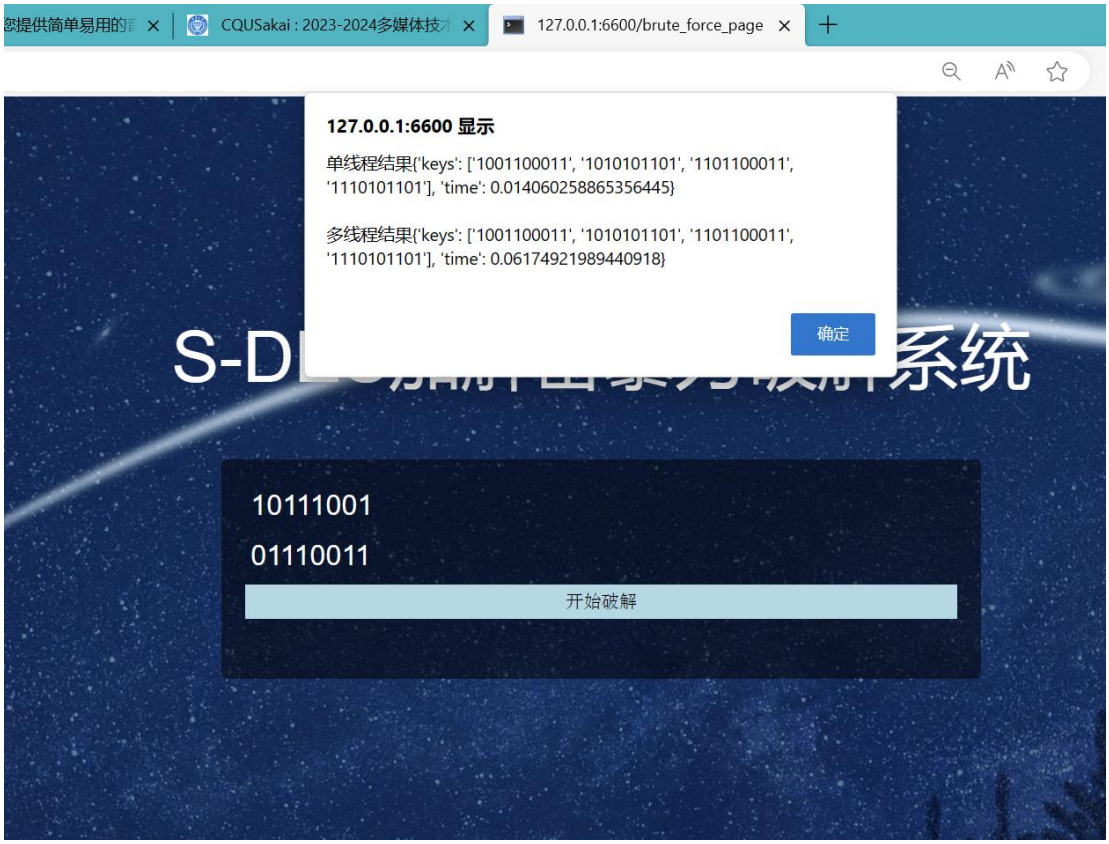
首先，我们展示单密文对破解功能：

进入破解界面：



输入明文、密文对。

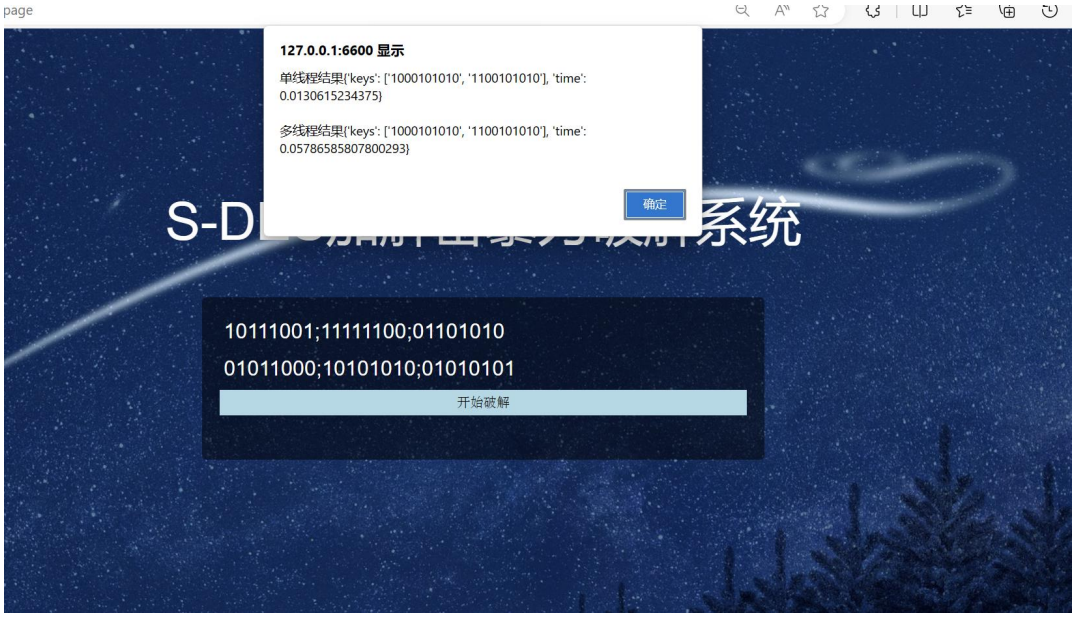
轻松得到破解结果。



然后，我们展示多密文对破解功能：

输入多组明密文对，注意以英文分号隔开。

轻松得到破解结



果

第四关测试通过。

第五关：封闭测试

在第四关中，我们使用了

明文：10111001

密文：01110011

得到了 4 个正确密钥： ['1001100011', '1010101101', '1101100011', '1110101101']

所以，一个明文"10111001"与密文"01110011"存在 4 个可能的密钥：'1001100011', '1010101101', '1101100011', 和 '1110101101'。这说明对于这个特定的明密文对，确实存在不止一个密钥 Key。

下面解释问题二：


127.0.0.1:6600 显示
加密结果为: 01110011
确定
S-DES加解密系统
选项:
二进制
10111001
1001100011
加密
解密

同时，如上图，我们使用明文：10111001，密钥 1001100011 和 1010101101，都得到了密文 01110011。

对于明文空间内任意给定的明文分组，确实存在可能性，即选择不同的密钥，加密可以得到相同的密文。