S-DES测试结果

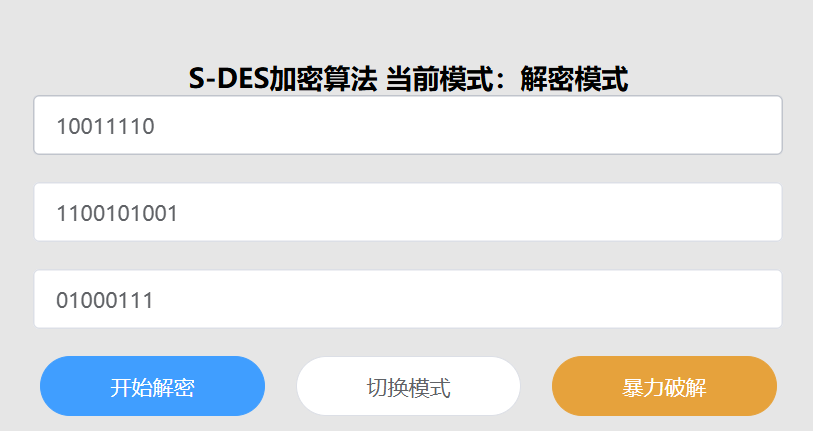
第1关：基本测试

**测试内容**：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。

**测试结果**：



图表 1输入明文：01000111，输入密钥：1100101001，经加密获得密文：10011110



图表 2输入密文：10011110，输入相同密钥，解密得到明文：01000111

第2关：交叉测试

**测试内容**：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；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。

**测试结果**： 

Figure 1其他组加密



Figure 2我们组解密



Figure 3我们组加密

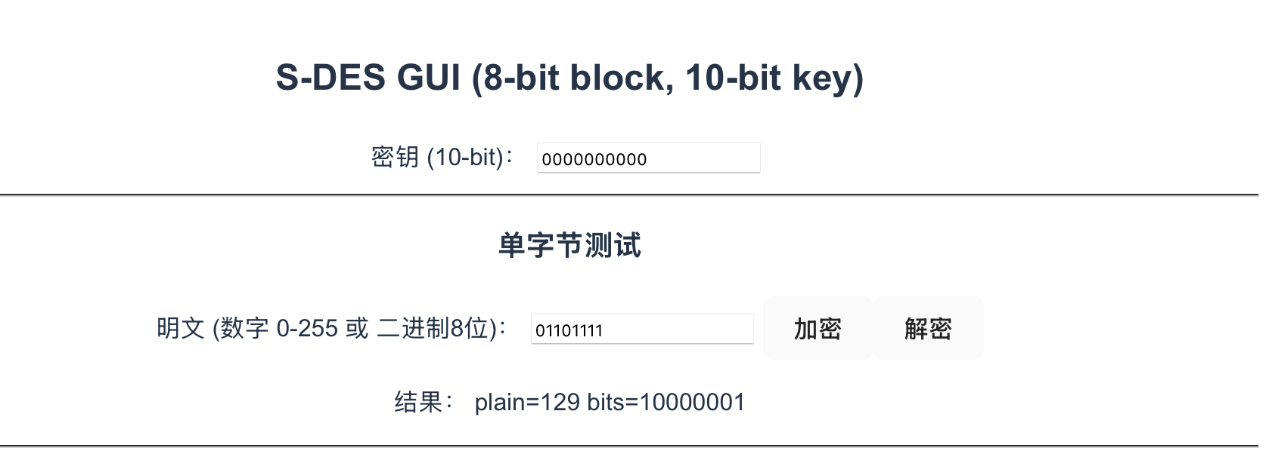


Figure 4其他组解密

第3关：扩展功能

**测试内容**：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)。

**测试结果**：



图表 3输入字符串：hello有加密输出，但结果为乱码

第4关：暴力破解

**测试内容**：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。

**测试结果**：

（1）

图表 4设定密钥1100100111进行加密获取密文

（2）现在对同一个密钥进行多个明密文对的暴力破解（4个）

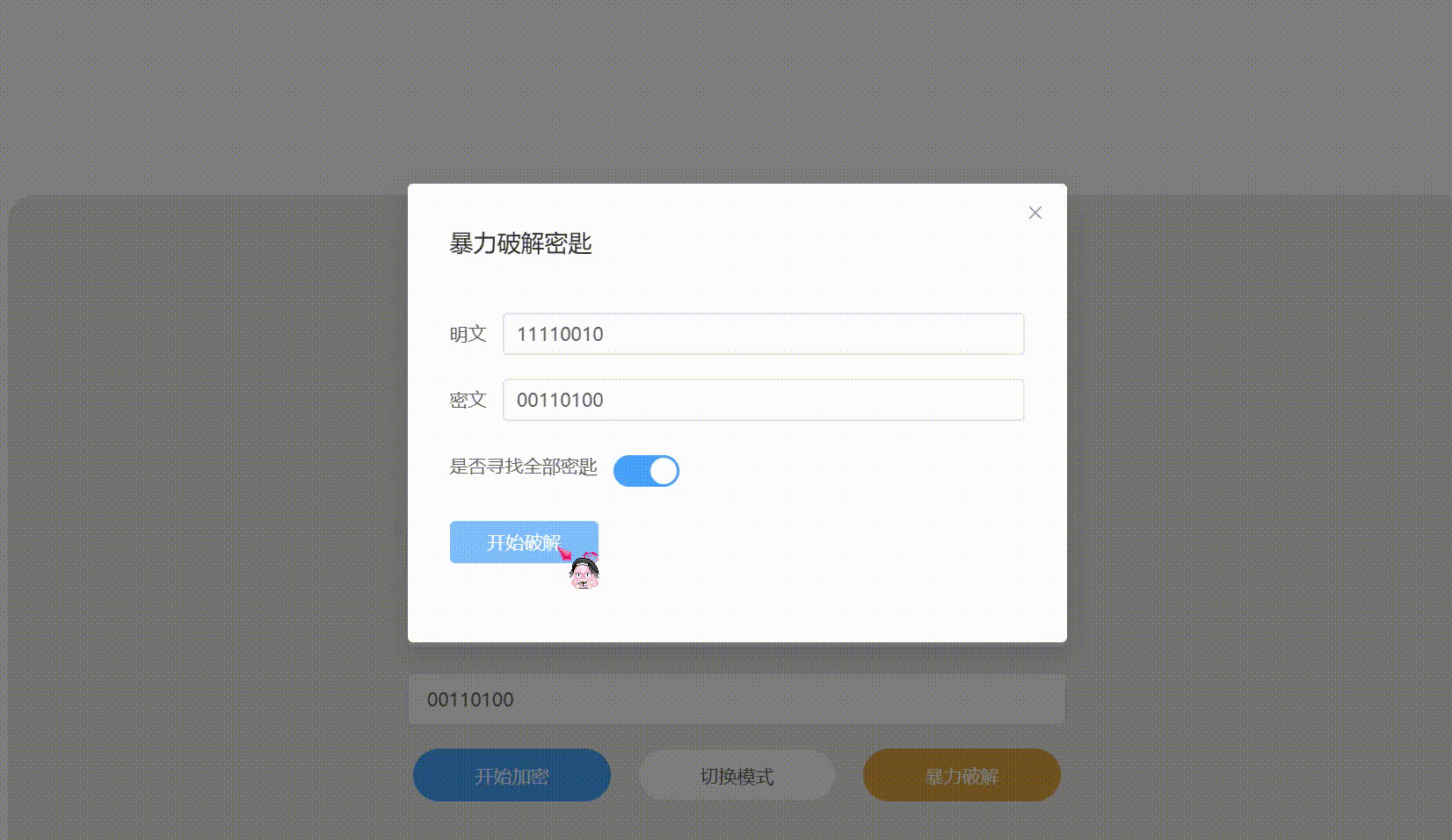


Figure 5暴力破解1

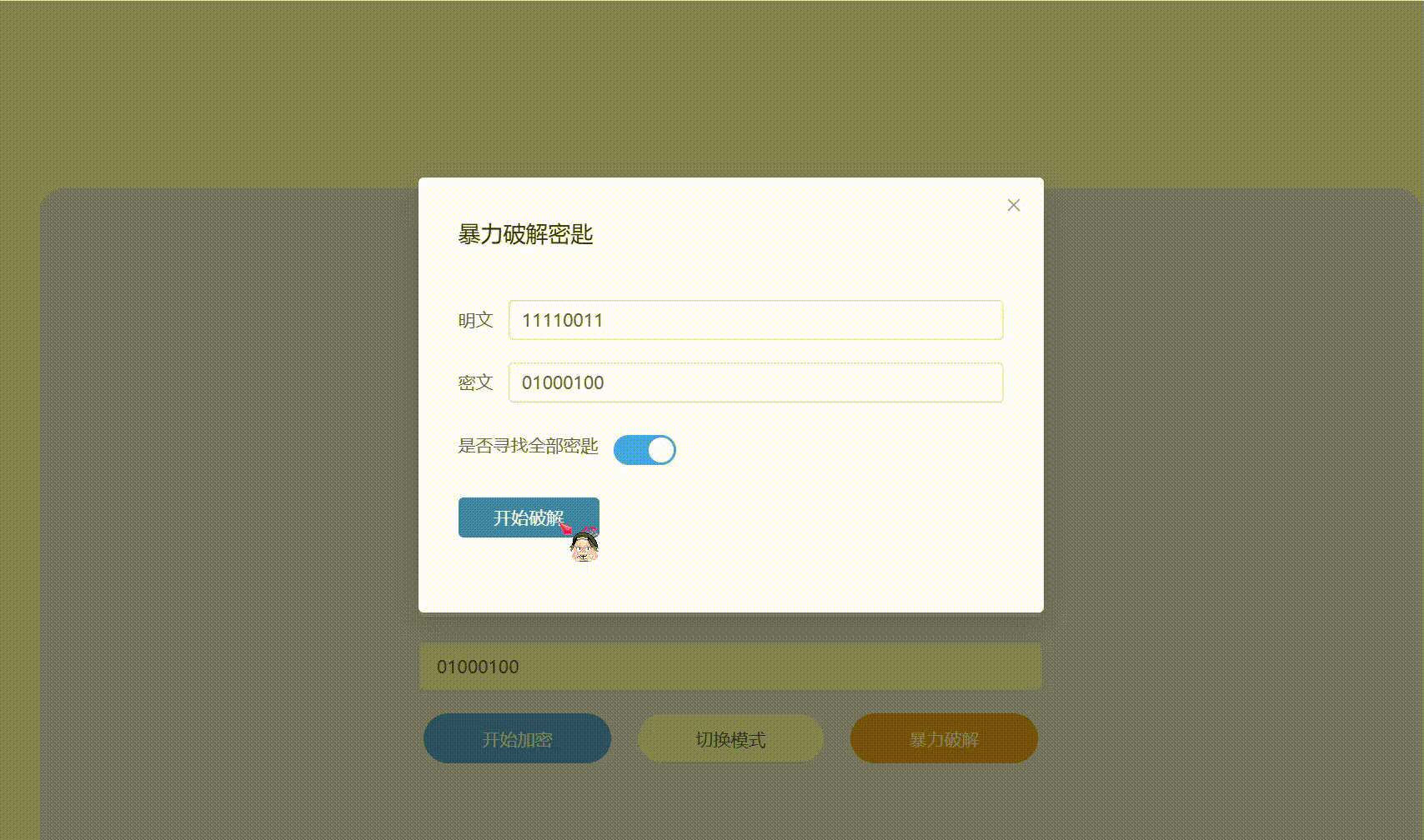


Figure 6暴力破解2

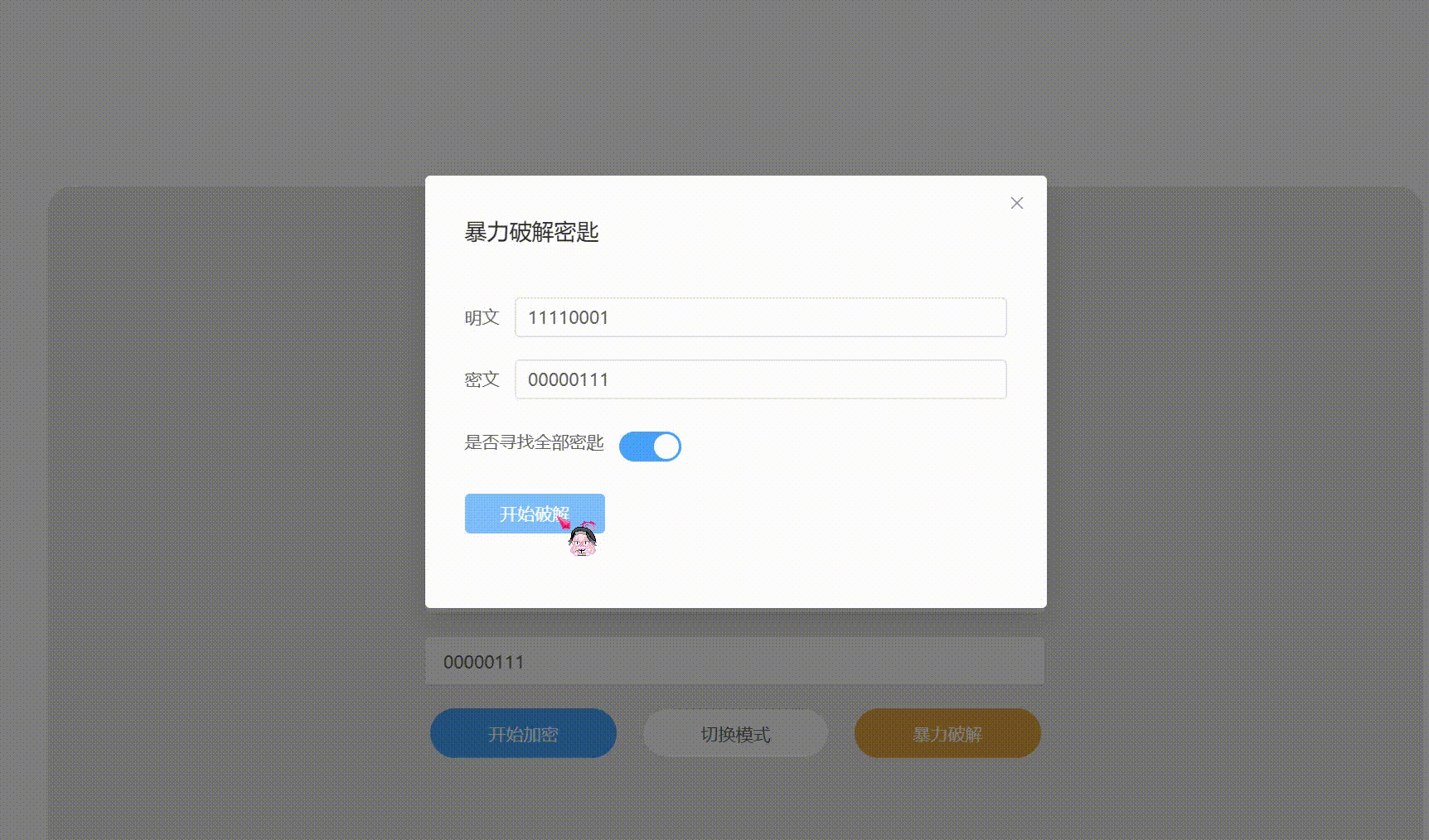


Figure 7暴力破解3

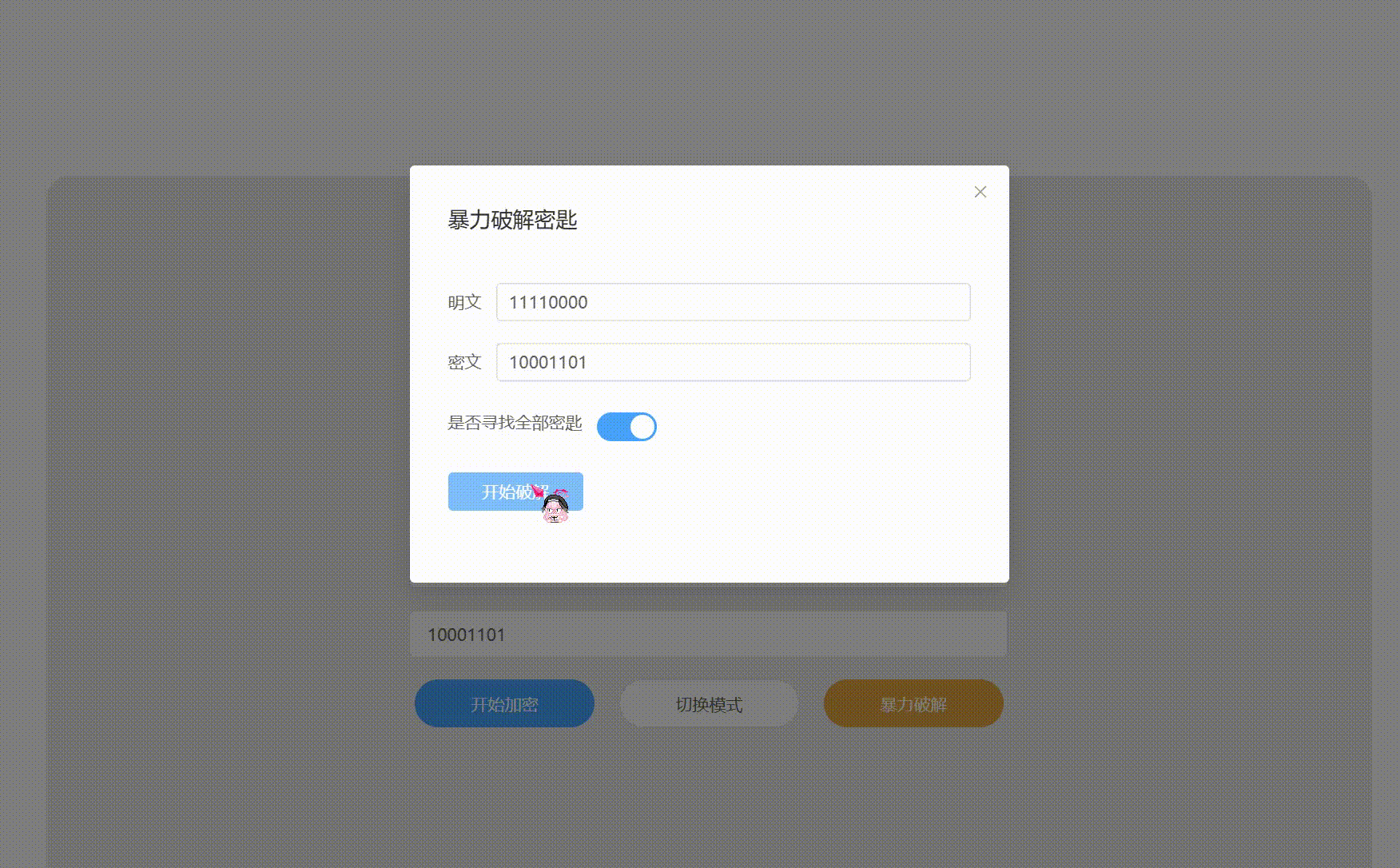


Figure 8暴力破解4

第5关：封闭测试

**测试内容**：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，是不是有不止一个密钥Key？进一步扩展，对应明文空间任意给定的明文分组Pn，是否会出现选择不同的密钥KiKj加密得到相同密文Cn的情况？

**测试结果**：

（1）由测试4可知不只一个密钥。

（2）如上面四个明文分组，选择密钥1000100111和1100100111均会得到相同的密文。