# S-Aes用户指南

## 首页

程序开始运行后，首先进入项目的首页（见图1）。首页介绍了项目的简要信息。包括项目基本功能，项目开发人员，开发环境，项目两点等。

在项目首页上方有“首页”“加密”“解密”“中间相遇破解”的目录栏，用户可根据自身需求点击相应的目录栏目，则可进入需要的功能界面。

功能页面将在后面进行详细介绍。



图 1

## 加密

用户选择加密功能后则会进入加密页面（见图2）。

在加密页面，用户可在加密方式（红色序号1）处点击，进入复选框选择需要的加密模式。可选择的加密模式有16位明文加密、16位明文双重加密、16位明文三重加密、长文本明文加密和长文本明文CBC模式加密。

用户在密钥输入框（红色序号2）处输入自己的密钥。

用户在加密明文输入框（红色序号3）处输入需要加密的明文，然后点击下方的加密按钮进行加密。

加密结果在页面底部输出框（红色序号4）处显示。

如需使用CBC模式进行加密，则可在CBC模式拨动按钮（绿色序号1）处点击，拨动按钮显示如图3所示即表示进入CBC模式加密。

点击复制图标（绿色序号2）即可复制所需的密文。

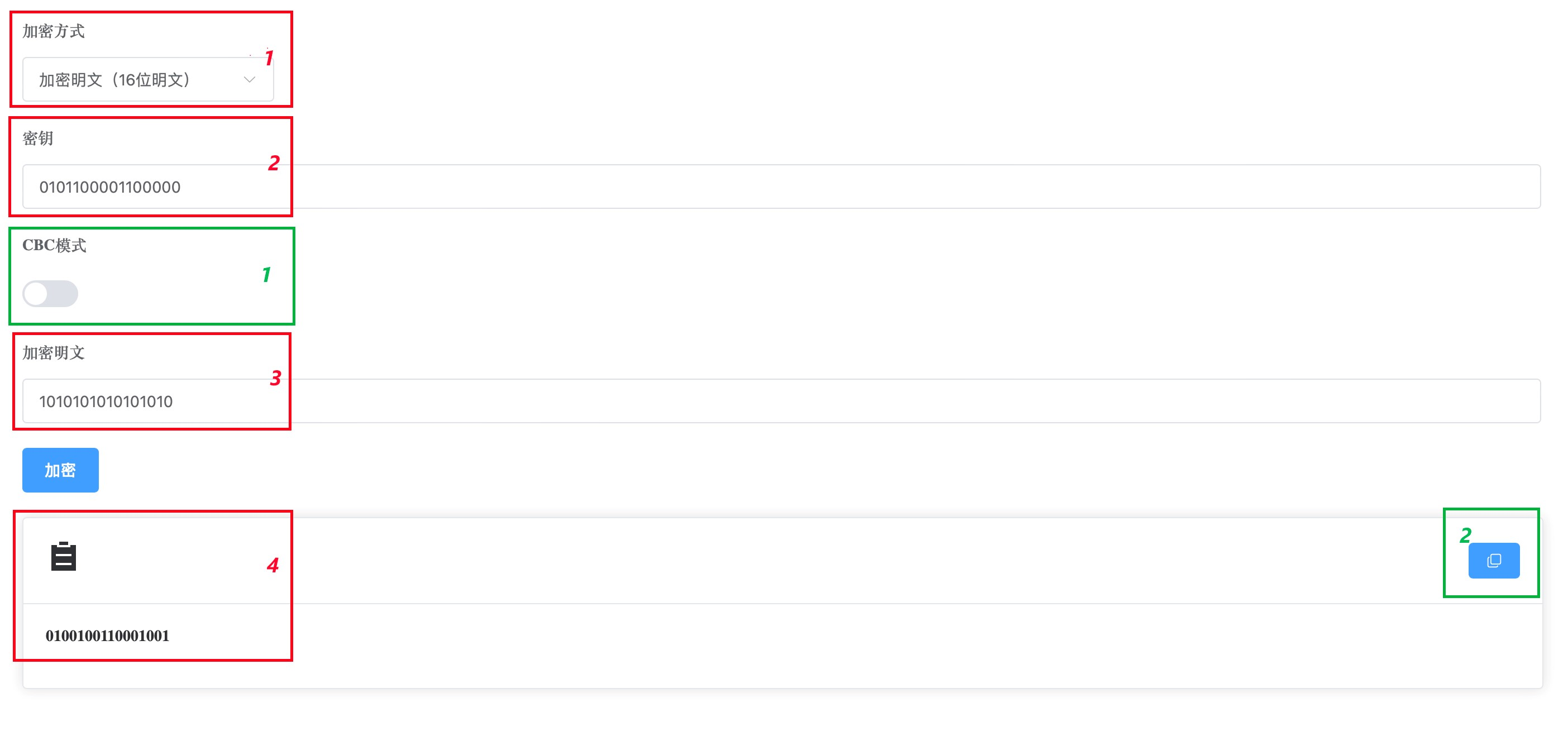


图2



图3



## 解密

用户选择解密功能后则会进入解密页面（如图4）。

在解密页面，用户可在解密方式（红色序号1）处选择所需的解密模式。可选择的解密模式包括：16位密文解密，16位密文双重解密，16位密文三重解密，长文本密文解密和长文本密文CBC模式解密。

用户在密钥输入框（红色序号2）中输入解密的密钥。

用户在解密文字输入框（红色序号3）中输入需要解密的密文，随后点击下方的解密按钮则可进行解密。若密文较长则可对密文输入框右下角（绿色序号2）进行拖动，改变密文输入框的大小

解密结果将在页面底部显示，与加密页面相同的是，点击解密结果输出框右上角的复制按钮也可对解密结果进行复制。

如需进入CBC解密模式，则可点击CBC模式（绿色序号2）处的拨动按钮，拨动按钮变为图2状态即表示进入了CBC模式解密。



图4

## 中间相遇攻击

若用户发现了使用相同密钥的明密文对，则可选择目录栏中的“中间相遇破解”功能，进入寻找正确的密钥。

进入中间相遇破解功能页面（如图5）后，用户在左侧明文栏（红色序号1）中输入明文，在右侧密文栏（红色序号2）中输入密文。点击“增加明密文对”按钮（红色序号3）并在上方明密文栏中输入具有相同密钥的明密文对，则可得到可能的正确密钥，结果显示在页面底部的文本框（红色序号4）中。

如需对密钥进行全文本复制，则可点击复制图标（绿色序号1）。

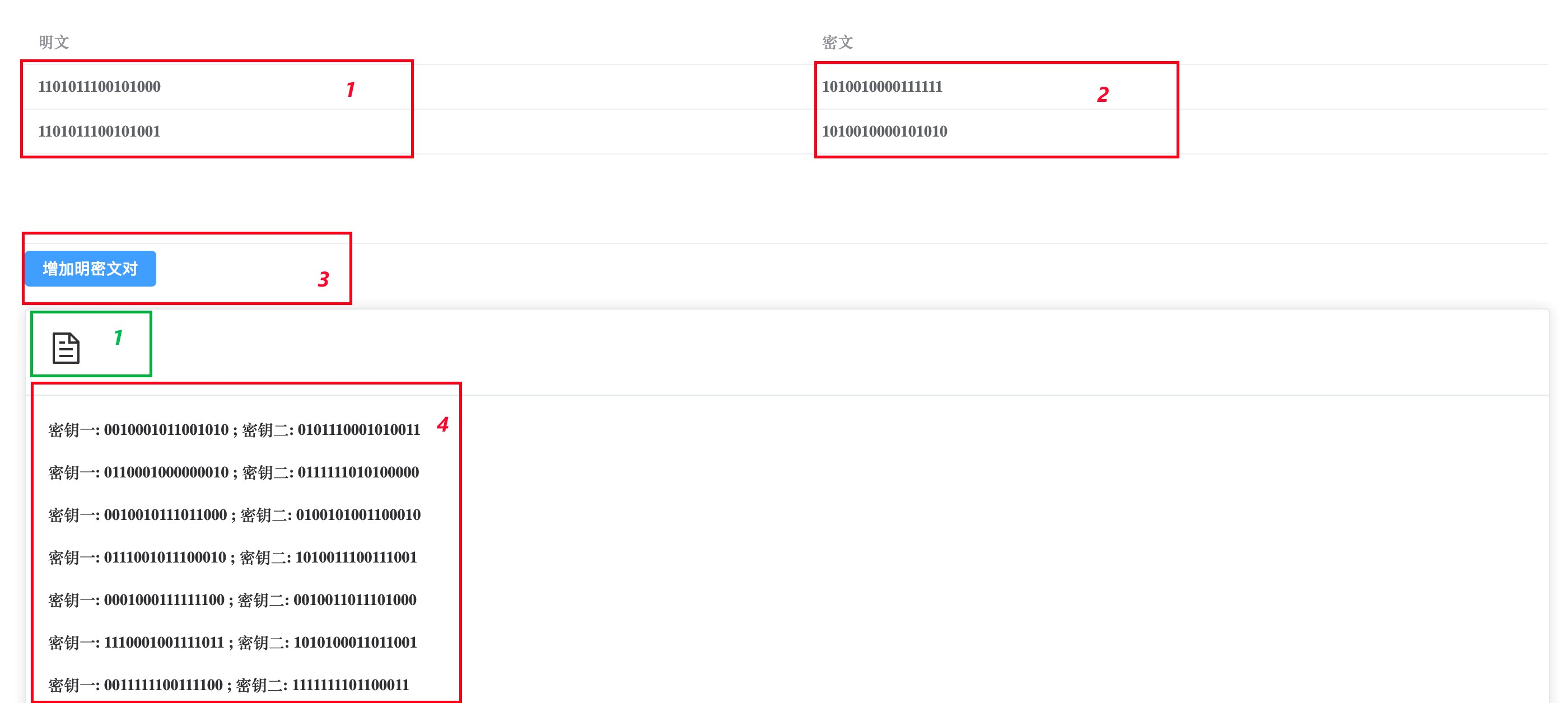


图5