## AES加密算法用户指南

1. **介绍(introduction)**

S-AES(simplified Data Encryption Standard)是一种简化的数据加密标准，通常用于教育和学术目的，本用户指南意在向用户介绍如何使用S-AES算法来加解密文本数据。

* 1. **主要功能(Main Function)**

**·**加密：将明文转换为密文，使用密钥进行加密

**·**解密：将密文转换为明文，使用密钥进行解密

**·**蛮力破解：已知明密文，暴力拆解出密钥

1. **安装和使用**

**2.1)代码下载及导入**

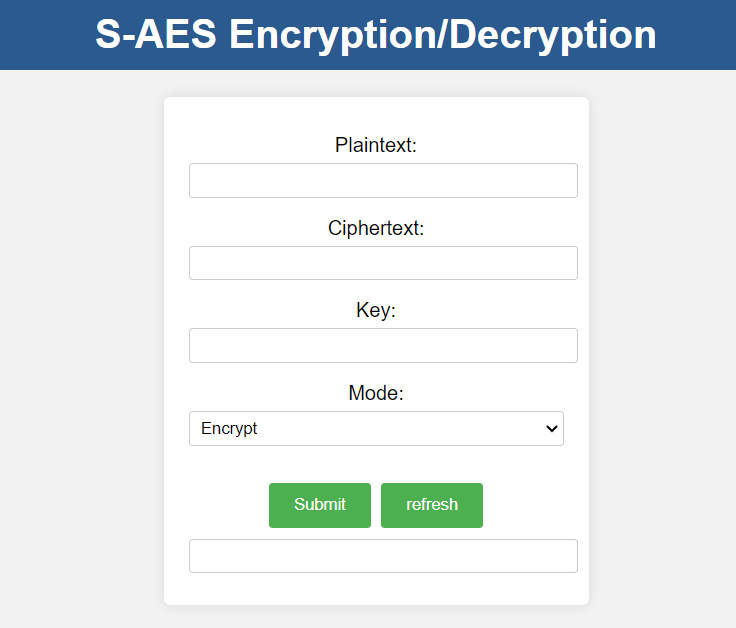
1.下载地址:

2.运行环境:python环境下

3.操作步骤:您可以从提供下载地址中下载响应html文件，然后直接点击打开应用网页**进行使用**

**2.2)应用网页样式以及可视化**

下图为可视化操作界面



**2.3)加解密操作以及密钥生成**

注意！在普通输入中信息规格为16位二进制字符串或者ASCII字符码密钥规格为16位二进制字符串，在双重加密中，输入为16位的二进制字符串或者等二进制位数的ASCII字符码，密钥规格为32位bit的二进制字符串。在三重加密中，输入为16位的二进制字符串或者等二进制的ASCII字符码，密钥规格为48位的二进制字符串。在CBC模式下，输入的明文格式以及长度不限，密钥仍然为16位二进制字符串。

2.3.1)加密操作

·选择将要输入的信息格式

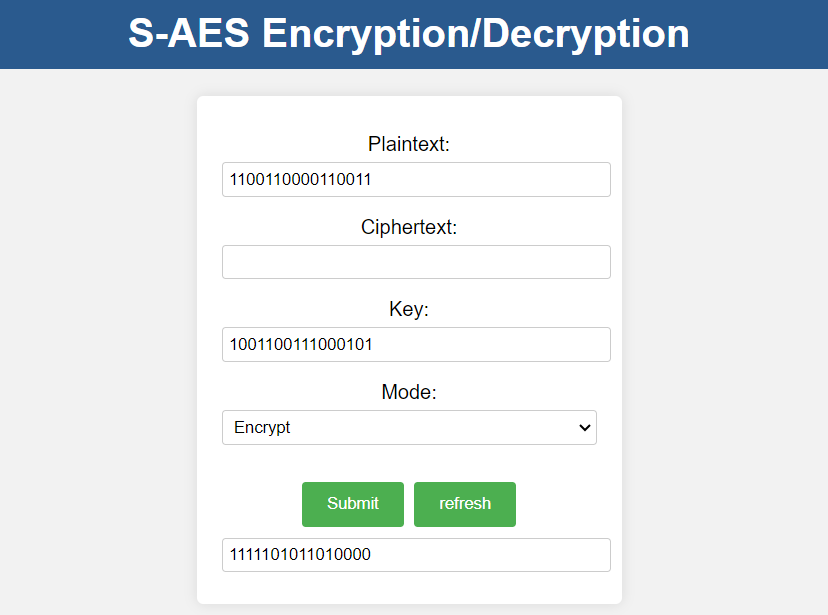
·在加密信息栏输入明文信息(如上述输入规格要求)

·在密钥输入框输入符合要求的密钥

·点击加密按钮

·输出栏获取到加密信息

2.3.2)加密示例



2.3.3)解密操作

·选择输入信息的格式

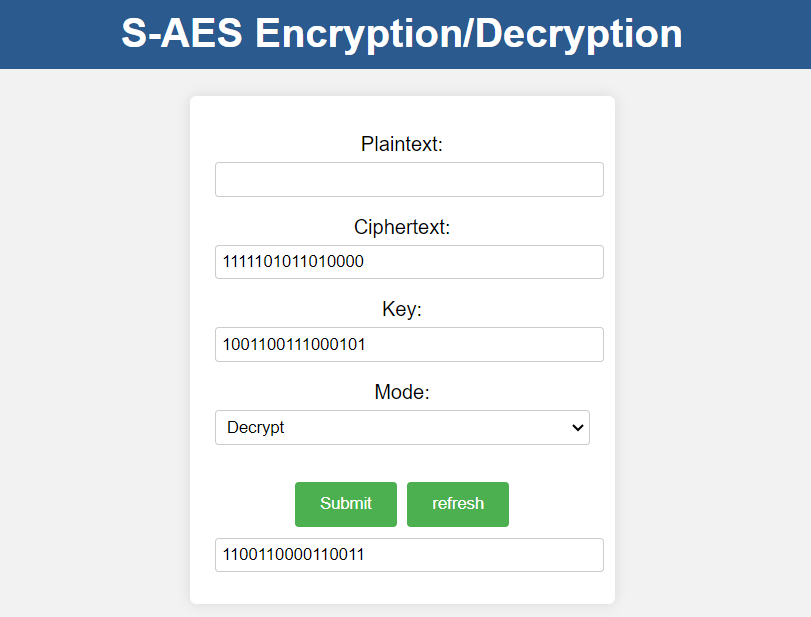
·在输入信息栏中输入密文的内容

·在密钥栏目中输入密钥

·选择解密按钮

·输出栏目获得明文

2.3.4)解密示例



2.3.5)注意事项

请选择与选择框相同的输入信息格式进行加解密操作，否则会弹出信息框提示

**2.4)蛮力破解操作**

·在明文输入栏中输入需要破解密钥的明文

·在密文输入栏中输入需要破解密钥的密文

·点击暴力破解按钮

·得到有效密钥

1. **注意事项**

请选择与选择框相同的输入信息格式进行加解密操作，否则会弹出信息框提示

1. **常见问题以及基础知识解答**

**S-AES并不是一个安全的算法，不适合于真正的安全性要求**