1. **AES开发文档**
2. **项目开发环境及工具**

在该项目中，我们开发加解密以及附带实现需要以下环境以及工具。

·环境: Windows

·编码环境

·编码工具rm2022

·编码语言:python语言，前端语言，HTML标记。

1. **项目功能需求描述**

项目开发功能分为以下几个部分

·普通工作模式。实现16位明密文以及16位密钥，得到转换的结果。

·实现输入内容的泛化。使得在二进制位为16位bit的ASCII码字符也可以实现加解密得到相应的结果。

·实现二重加密，输入16位二进制bit的字符串以及32位bit密钥，以得到双重加密解密的结果。

·实现三重加密，输入16位二进制bit的字符串以及48位bit的密钥，以得到三重加密解密的结果。

·实现中间相遇攻击，在输入的密文和明文之间实现中间攻击按钮，输入明文以及密文，计算得到中间的密钥

·实现CBC模式，在此工作模式下，输入的明文没有长度限制，密钥依然为16bit二进制字符串

1. **编写目的**

·对项目应用的支持

·对加解密逻辑的探索和应用，并针对特定问题进行讨论和研究

1. **模块与关系**

·本项目采用flask框架，设计了服务器端以及客户端的内容。

·在前端，设计了可视化页面，并传递对应的输入内容，根据模式选择，返回后端处理结果，模块命名为。

·在后端，作为服务器端的实现部分，总体分为路由函数实现，负责后端调用与前端返回，为index（）函数，对应加密过程和解密过程，也分别设计了相应的响应函数，code\_decrypt,以及code\_encrypt函数，针对函数内的三轮加密，也分别设计了三轮的加密以及解密过程函数，以及单独针对密钥生成的函数进行应用。

1. **难点限制**

·如何设计加密轮和解密轮，尤其复杂在能够实现复现和调用接口

1. **软件接口注释**

**这是一个使用Python编写的Flask应用程序，用于实现S-AES（Simplified Advanced Encryption Standard）算法的加密和解密。以下是代码的主要部分的解释：**

**引入必要的库和模块：**

**Flask：用于创建Web应用。**

**sympy：用于处理数学运算。**

**定义S-AES的S盒、反向S盒、GF(16)加法表和乘法表：这些表格包含了S-AES算法中的基本替代和混淆操作所需的数据。**

**创建全局变量m0、m1、m2、m3、m4、m5：这些变量将用于存储S-AES算法中的中间状态。**

**定义各种辅助函数，如column\_reverse\_confusion、column\_confusion、generate\_m2、generate\_m4、generate\_normal\_m、key\_generate、code\_round\_1、code\_round\_2、code\_round\_3、cipher\_round\_1、cipher\_round\_2、cipher\_round\_3：这些函数用于S-AES算法中的不同阶段，如代替、混淆、轮密钥生成等。**

**创建Flask应用：**

**初始化Flask应用。**

**定义S盒、反向S盒、GF(16)加法表和乘法表作为全局变量。**

**定义路由，包括主页和处理加密/解密请求的端点。**

**使用表单来接收明文、密钥和加密/解密模式。**

**根据所选择的模式调用相应的S-AES加密或解密函数，将结果呈现在页面上。**

**实现S-AES的加密和解密功能，包括单轮加密/解密、双轮加密/解密以及三轮加密/解密。**

**启动Flask应用，使其能够在本地运行。**

**你可以使用Web浏览器访问应用程序，输入明文和密钥，选择加密或解密模式，然后点击提交按钮以执行S-AES操作。结果将显示在页面上。**

**请注意，这个应用程序实现了S-AES算法的基本版本，用于教育和演示目的。在生产环境中，需要使用更严格的安全标准和更复杂的密钥管理来确保数据的安全性。**