**开发手册：S-AES 加密系统**

**概览**

本开发手册旨在详细介绍 S-AES 加密系统的各个组成部分，包括函数功能和开发逻辑。S-AES 是一个基于 Python 的加密和解密工具，它提供了多种加密模式和功能，包括基本的字符和二进制数据的加密解密，以及扩展的双重加密、三重加密和 CBC 加密模式。

**核心模块**

**1. main\_function.py**

该模块包含了加密和解密的核心算法和函数。

**功能函数**

* **S盒和逆S盒定义**
  + S：定义了正向的S盒。
  + IS：定义了逆向的S盒。
* **轮常数**
  + RCON1 和 RCON2：定义了轮常数。
* **异或运算**
  + XOR(bits1, bits2)：执行两个二进制字符串的异或运算。
* **密钥加**
  + AddRoundKey(bits1, bits2)：将两个二进制字符串进行异或运算，模拟密钥加操作。
* **半字节代替**
  + SubNib(bits)：执行正向的半字节代替操作。
  + InvSubNib(bits)：执行逆向的半字节代替操作。
* **行移位**
  + ShiftRows(bits)：执行行移位操作。
* **列混淆**
  + MixColumns(bits)：执行列混淆操作。
  + InvMixColumns(bits)：执行逆向列混淆操作。
* **密钥扩展**
  + KeyExpansion(key)：将16位密钥扩展为多个16位的轮密钥。
* **加密和解密**
  + Encrypt(plain\_text, key)：执行加密操作。
  + Decrypt(cipher\_text, key)：执行解密操作。

**2. ascii\_function.py**

该模块提供了ASCII字符串和二进制字符串之间的转换，以及基于ASCII的加密和解密功能。

**功能函数**

* **ASCII与二进制转换**
  + ascii\_to\_binary(ascii\_text)：将ASCII字符串转换为二进制字符串。
  + binary\_to\_ascii(binary\_text)：将二进制字符串转换为ASCII字符串。
* **扩展加密和解密**
  + ascii\_encrypt(plain\_text, key)：执行基于ASCII的加密操作。
  + ascii\_decrypt(cipher\_text, key)：执行基于ASCII的解密操作。

**3. main\_gui.py**

该模块提供了图形用户界面（GUI），允许用户输入明文、密钥，并执行加密和解密操作。

**GUI组件**

* **二进制加解密部分**
  + 提供了明文（密文）输入、密钥输入和输出显示。
* **字符加解密部分**
  + 提供了明文（密文）输入、密钥输入和输出显示。

**4. multi\_gui.py**

该模块提供了双重加密和三重加密的GUI界面。

**功能函数**

* **双重加密和解密**
  + double\_encrypt(plain\_text, key1, key2)：执行双重加密。
  + double\_decrypt(cipher\_text, key1, key2)：执行双重解密。
* **三重加密和解密**
  + triple\_encrypt(plain\_text, key1, key2)：执行三重加密。
  + triple\_decrypt(cipher\_text, key1, key2)：执行三重解密。

**5. operating\_gui.py**

该模块提供了基于CBC模式的加密和解密的GUI界面。

**功能函数**

* **CBC加密和解密**
  + CBC\_encrypt(plain\_text, key, IV)：执行CBC模式的加密。
  + CBC\_decrypt(cipher\_text, key, IV)：执行CBC模式的解密。

**开发逻辑**

**加密流程**

1. **密钥扩展**：将16位密钥扩展为多个16位的轮密钥。
2. **初始密钥加**：将明文与第一个轮密钥进行异或运算。
3. **轮函数**：包括半字节代替、行移位和列混淆。
4. **密钥加**：将轮函数的输出与下一个轮密钥进行异或运算。
5. **重复**：重复轮函数和密钥加步骤，直到所有轮次完成。

**解密流程**

1. **密钥扩展**：与加密流程相同，扩展密钥。
2. **初始密钥加**：将密文与最后一个轮密钥进行异或运算。
3. **逆轮函数**：包括逆半字节代替、逆行移位和逆列混淆。
4. **密钥加**：将逆轮函数的输出与上一个轮密钥进行异或运算。
5. **重复**：重复逆轮函数和密钥加步骤，直到所有轮次完成。

**GUI操作**

* 用户通过GUI输入明文、密钥和初始向量（如果需要）。
* 用户点击加密或解密按钮，触发相应的加密或解密函数。
* 显示加密或解密的结果，并在需要时验证解密结果的正确性。