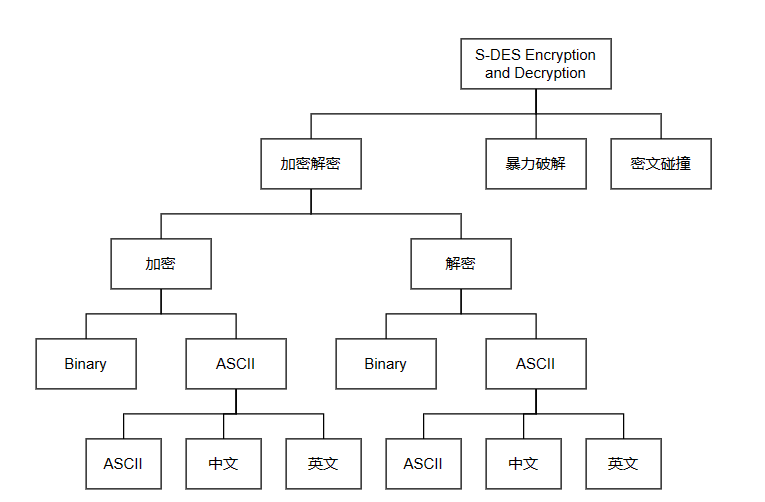
**开发手册**

1. **系统概述**

该程序是一个实现了S-DES算法的加密和解密功能的应用程序。它提供了一个用户界面，用户可以输入要加密或解密的数据，并选择加密或解密模式、输入类型等选项。程序还提供了暴力破解和密钥碰撞功能，用于分析密文以找到可能的密钥。该程序由ui.py、sdes.py、key\_collisions.py和brute\_force.py四个文件组成。

1. **系统设计**

系统包括加密解密、暴力破解、密文碰撞三个模块，其中加密解密又包含二进制加解密、ASCII加解密两个模块。



1. **系统生成**

Ui.py

sdes.py

brute\_force.py

ciphertext\_collisions.py

brute\_force.cpython-310.pyc

ciphertext\_collisions.cpython-310.pyc

sdes.cpython-310.pyc

1. **文件结构和组织方式**

• ui.py：负责创建和管理用户界面。

• sdes.py：实现了S-DES算法的加密和解密功能。

• key\_collisions.py：提供了密钥碰撞算法的实现。

• brute\_force.py：提供了暴力破解算法的实现。

1. **接口文档**

**a. sdes.py**

* + - encrypt(input\_data: str, key: str) -> str
* 功能：使用S-DES算法对输入数据进行加密。
* 参数：

input\_data：要加密的数据，可以是二进制或ASCII。

key：加密密钥，必须是10位二进制字符串。

* 返回值：加密后的数据，以二进制字符串形式返回。
  + - decrypt(input\_data: str, key: str) -> str
    - 功能：使用S-DES算法对输入数据进行解密。
    - 参数：

input\_data：要解密的数据，可以是二进制或ASCII。

key：解密密钥，必须是10位二进制字符串。

* + - 返回值：解密后的数据，以二进制字符串形式返回。

**b. brute\_force.py**

* + - brute\_force\_crack(known\_plaintexts: List[str], known\_ciphertexts: List[str], num\_threads: int) -> List[str]
      * 功能：使用暴力破解算法对S-DES算法的密钥进行破解。
      * 参数：

known\_plaintexts：已知的明文列表，每个明文必须是8位二进制字符串。

known\_ciphertexts：已知的密文列表，每个密文必须是8位二进制字符串。

num\_threads：要使用的线程数，用于加快破解速度。

* + - * 返回值：找到的密钥列表，以二进制字符串形式返回。

**c. key\_collisions.py**

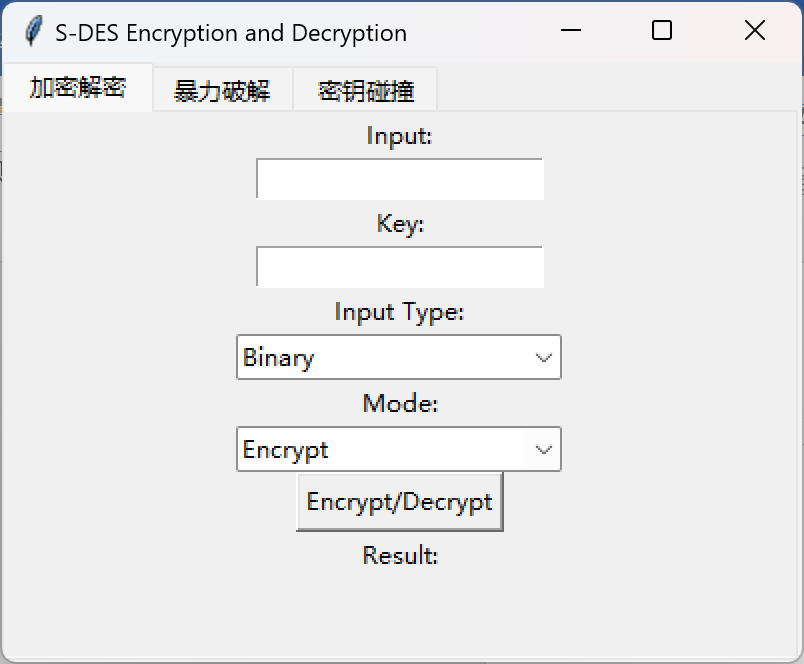
* + - find\_collision(plaintext: str) -> Tuple[List[str], str]
      * 功能：使用密钥碰撞算法查找与给定明文产生相同密文的密钥。
      * 参数：

plaintext：要查找密钥碰撞的明文，必须是8位二进制字符串。

* + - * 返回值：包含相同密文密钥的列表以及对应的密文，均以二进制字符串形式返回。

1. **系统验收**

加密解密模块：

****

暴力破解模块：

****

密钥碰撞模块：

****