Simple-Des简易加密系统API帮助文档

## 1.轮密钥生成算法

|  |  |
| --- | --- |
| 方法名称 | *Key\_permutation* |
| 功能描述 | *P10置换盒* |
| 输入参数 | **形式参数1：Numpy.array对象arr**  **描述：由Int类型的0或1组成的长度为10的数组** |
| 输出参数 | ***Numpy.array对象***  ***描述：经置换后的长度为10的数组*** |
| 补充说明 |  |

|  |  |
| --- | --- |
| 方法名称 | *split* |
| 功能描述 | *拆分长度为10的数组* |
| 输入参数 | **形式参数1：Numpy.array对象arr**  **描述：由Int类型的0或1组成的长度为10的数组** |
| 输出参数 | ***输出1：Numpy.array对象***  ***描述：将arr的前五位作为新数组返回***  ***输出2：Numpy.array对象***  ***描述：将arr的后五位作为新数组返回*** |
| 补充说明 |  |

|  |  |
| --- | --- |
| 方法名称 | *left\_shift* |
| 功能描述 | *循环左移1位* |
| 输入参数 | **形式参数1：Numpy.array对象arr**  **描述：由Int类型的0或1组成的数组** |
| 输出参数 | ***Numpy.array对象***  ***描述：经循环左移1位后的数组*** |
| 补充说明 |  |

|  |  |
| --- | --- |
| 方法名称 | *compression\_permutation\_box* |
| 功能描述 | *P8压缩置换盒* |
| 输入参数 | **形式参数1：Numpy.array对象arr**  **描述：由Int类型的0或1组成长度为5的数组** |
| 输出参数 | ***Numpy.array对象***  ***描述：经压缩置换后长度为4的数组*** |
| 补充说明 |  |

|  |  |
| --- | --- |
| 方法名称 | *generate\_ke* |
| 功能描述 | *轮密钥生成算法，生成两个轮密钥* |
| 输入参数 | **形式参数1：Numpy.array对象arr**  **描述：由Int类型的0或1组成的10位数组** |
| 输出参数 | ***输出1：Numpy.array对象***  ***描述：第一轮生成的轮密钥***  ***输出2：Numpy.array对象***  ***描述：第二轮生成的轮密钥*** |
| 补充说明 |  |

## 2.Simple-Des加密算法

|  |  |
| --- | --- |
| 方法名称 | *initial\_permutation* |
| 功能描述 | *初始置换盒* |
| 输入参数 | **形式参数1：Numpy.array对象arr**  **描述：由Int类型的0或1组成长度为8的数组** |
| 输出参数 | ***Numpy.array对象***  ***描述：经置换后长度为8的数组*** |
| 补充说明 |  |

|  |  |
| --- | --- |
| 方法名称 | *f\_function* |
| 功能描述 | *轮函数* |
| 输入参数 | **形式参数1：Numpy.array对象arr**  **描述：由Int类型的0或1组成长度为4的数组**  **形式参数2：Numpy.array对象k**  **描述：轮密钥** |
| 输出参数 | ***Numpy.array对象***  ***描述：经轮函数处理后长度为4的数组*** |
| 补充说明 |  |

|  |  |
| --- | --- |
| 方法名称 | *expansion\_permutation\_box* |
| 功能描述 | *拓展置换盒* |
| 输入参数 | **形式参数1：Numpy.array对象arr**  **描述：由Int类型的0或1组成长度为4的数组** |
| 输出参数 | ***Numpy.array对象***  ***描述：经拓展置换处理后长度为8的数组*** |
| 补充说明 |  |

|  |  |
| --- | --- |
| 方法名称 | *sub* |
| 功能描述 | *替换盒函数* |
| 输入参数 | **形式参数1：Numpy.array对象arr**  **描述：由Int类型的0或1组成长度为8的数组** |
| 输出参数 | ***Numpy.array对象***  ***描述：经替换处理后长度为4的数组*** |
| 补充说明 |  |

|  |  |
| --- | --- |
| 方法名称 | *Spbox* |
| 功能描述 | *P4置换盒函数* |
| 输入参数 | **形式参数1：Numpy.array对象arr**  **描述：由Int类型的0或1组成长度为4的数组** |
| 输出参数 | ***Numpy.array对象***  ***描述：经置换处理后长度为4的数组*** |
| 补充说明 |  |

|  |  |
| --- | --- |
| 方法名称 | *final\_permutation* |
| 功能描述 | *最终置换盒，初始置换盒的逆函数* |
| 输入参数 | **形式参数1：Numpy.array对象arr**  **描述：由Int类型的0或1组成长度为8的数组** |
| 输出参数 | ***Numpy.array对象***  ***描述：经置换后长度为8的数组*** |
| 补充说明 |  |

|  |  |
| --- | --- |
| 方法名称 | *encode* |
| 功能描述 | *Simple-Des加密8-bit二进制算法* |
| 输入参数 | **形式参数1：Numpy.array对象key**  **描述：10-bit二进制密钥**  **形式参数2：Numpy.array对象content**  **描述：待加密的8-bit二进制** |
| 输出参数 | ***Numpy.array对象***  ***描述：加密后的8-bit二进制*** |
| 补充说明 |  |

|  |  |
| --- | --- |
| 方法名称 | *decode* |
| 功能描述 | *Simple-Des解密8-bit二进制算法* |
| 输入参数 | **形式参数1：Numpy.array对象key**  **描述：10-bit二进制密钥**  **形式参数2：Numpy.array对象content**  **描述：待解密的8-bit二进制** |
| 输出参数 | ***Numpy.array对象***  ***描述：解密后的8-bit二进制*** |
| 补充说明 |  |

## 3.Simple-Des拓展加密功能

|  |  |
| --- | --- |
| 方法名称 | *string\_change* |
| 功能描述 | *将字符串转换为二进制数组* |
| 输入参数 | **形式参数1：String对象string**  **描述：待加密字符串** |
| 输出参数 | ***list***  ***描述：包括每个字符的二进制编码数组*** |
| 补充说明 |  |

|  |  |
| --- | --- |
| 方法名称 | *encode\_str* |
| 功能描述 | *加密字符串算法* |
| 输入参数 | **形式参数1：Numpy.array对象key**  **描述：十位二进制密钥**  **形式参数2：String对象str**  **描述：待加密字符串** |
| 输出参数 | ***String对象***  ***描述：加密后的字符串*** |
| 补充说明 |  |

|  |  |
| --- | --- |
| 方法名称 | *decode\_str* |
| 功能描述 | *解密字符串算法* |
| 输入参数 | **形式参数1：Numpy.array对象key**  **描述：十位二进制密钥**  **形式参数2：String对象str**  **描述：待解密字符串** |
| 输出参数 | ***String对象***  ***描述：解密后的字符串*** |
| 补充说明 |  |

|  |  |
| --- | --- |
| 方法名称 | *txt\_encode* |
| 功能描述 | *加密文件算法* |
| 输入参数 | **形式参数1：String对象filename**  **描述：待加密文件名**  **形式参数2：Numpy.array对象key**  **描述：十位二进制密钥** |
| 输出参数 | *无* |
| 补充说明 |  |

|  |  |
| --- | --- |
| 方法名称 | *txt\_decode* |
| 功能描述 | *解密文件算法* |
| 输入参数 | **形式参数1：String对象filename**  **描述：待解密文件名**  **形式参数2：Numpy.array对象key**  **描述：十位二进制密钥** |
| 输出参数 | ***无*** |
| 补充说明 |  |

|  |  |
| --- | --- |
| 方法名称 | *corrected\_main* |
| 功能描述 | *寻找所有产生碰撞的名密文对以及密钥* |
| 输入参数 | **无** |
| 输出参数 | ***无*** |
| 补充说明 | *将会生成一个collisions.json文件，包括所有的* |