# 面向字的杂凑密码设计接口文档

1. **自动化生成MDS矩阵接口**

**接口地址：**http://127.0.0.1:5000/api/hash\_function/byte/byte-mds

**请求方式：**GET

**请求头（Header）参数：**

|  |  |  |
| --- | --- | --- |
| **字段名** | **类型** | **描述** |
| Content-Type | string | 指定请求信息的格式 |

**请求体（Body）参数：**

**返回参数：**

|  |  |  |
| --- | --- | --- |
| **字段名** | **类型** | **描述** |
| status | string | 是否能成功地响应数据 |
| result | int | 异或和的个数 |

**返回示例：**

{

"status": “success”,

"result": [[1,2,3,4],[5,6,7,8],[9,10,11,12],[13,14,15,16]],[[1,2,3,4], [5,6,7,8],[9,10,11,12],[13,14,15,16]]

}

**2**

1. **生成杂凑密码具体实例接口**

**接口地址：**http://127.0.0.1:5000/api/hash\_function/byte/generate

**请求方式：**POST

**请求头（Header）参数：**

|  |  |  |
| --- | --- | --- |
| **字段名** | **类型** | **描述** |
| Content-Type | string | 指定请求信息的格式 |

**请求体（Body）参数：**

|  |  |  |
| --- | --- | --- |
| **字段名** | **类型** | **描述** |
| round | int | 轮数 |
| constant | int | 轮常数 |
| column\_shift | array | 列位移参数 |
| mds | array | MDS矩阵 |

**返回参数：**

|  |  |  |
| --- | --- | --- |
| **字段名** | **类型** | **描述** |
| status | string | 是否能成功地响应数据 |

**返回示例：**

{

"status": “success”,

}

1. **杂凑密码输出测试接口**

**接口地址：**http://127.0.0.1:5000/api/hash\_function/byte/call-byte-algorithm

**请求方式：**POST

**请求头（Header）参数：**

|  |  |  |
| --- | --- | --- |
| **字段名** | **类型** | **描述** |
| Content-Type | string | 指定请求信息的格式 |

**请求体（Body）参数：**

|  |  |  |
| --- | --- | --- |
| **字段名** | **类型** | **描述** |
| messege | string | 待加密的明文消息 |

**返回参数：**

|  |  |  |
| --- | --- | --- |
| **字段名** | **类型** | **描述** |
| status | string | 是否能成功地响应数据 |
| hash | string | 加密后消息的杂凑值 |

**返回示例：**

{

"status": “success”,

“hash”: “a81956a77e27dab03fd87283afb14ba57efc5c9cad8a64bea8e189ddc9427459f0d9f759b07f8f32630674d8ad88cec40fd009deeb5f99d69ec2f3f3701adb71”

}

1. **杂凑密码搜索最小活跃S盒接口**

**接口地址：**http://127.0.0.1:5000/api/hash\_function/byte/calculate-active-sbox\_bytes

**请求方式：**POST

**请求头（Header）参数：**

|  |  |  |
| --- | --- | --- |
| **字段名** | **类型** | **描述** |
| Content-Type | string | 指定请求信息的格式 |

**请求体（Body）参数：**

|  |  |  |
| --- | --- | --- |
| **字段名** | **类型** | **描述** |
| rounds | int | 搜索最小活跃S盒的轮数 |

**返回参数：**

|  |  |  |
| --- | --- | --- |
| **字段名** | **类型** | **描述** |
| status | string | 是否能成功地响应数据 |
| count | int | 活跃S盒的个数 |

**返回示例：**

{

"status": “success”,

“count”: 22

}