**题目名称：量子信息试题**

1. **环境准备**
2. 选择一个编程语言（不限），参赛团队自行准备并安装相应的开发环境（IDE、依赖包等）。
3. 实现一个简单的HTTPS客户端，具体要求如下：
4. 客户端能够向指定的服务器发起HTTPS请求。
5. 客户端能够解析服务器返回的响应头和响应体。
6. 支持常见的HTTPS方法（GET、POST等）。
7. 量子密码服务能力接口公网IP及端口（通过云主机访问）：117.71.57.240:902

**题目一（公共题目）：对称密钥加密和解密**

1、要求学员调用提供的登录接口，实现平台登录功能。

2、要求学员调用提供的接口，实现一个简单的密钥申请功能。

3、要求学员通过页面调用提供的接口，实现对字符串“黑客马拉松”数据的加密，将加密后的数据以文本展现在页面；解密后将文本展现在页面上。

1. **任务要求**
2. 选择一个编程语言（不限），并安装相应的开发环境。
3. 调用密码服务平台提供的登录接口，实现以下功能：
4. 输入APPID和APPKEY进行登录。
5. 系统验证APPID和APPKE的正确性。
6. 如果验证通过，显示登录成功信息，并返回token；否则，显示错误提示信息。
7. 打印并保存token信息。
8. 调用密码服务平台提供的申请会话密钥接口，实现以下功能：
9. 将步骤2中返回的token参数置于请求header中。
10. 系统生成一个随机的密钥，并将其与用户关联，并将密钥标识返回给客户端。
11. 打印并保存密钥标识信息。
12. 调用密码服务平台提供的数据加密接口，实现以下功能：
13. 将步骤2中返回的token参数置于请求header中。
14. 使用步骤3生成的密钥，对给定的源数据进行加密，并展示在页面。
15. 调用密码服务平台提供的数据解密接口，实现以下功能：
16. 将步骤2中返回的token参数置于请求header中。
17. 使用步骤3生成的密钥，对步骤4返回的密文数据进行解密。
18. 在页面进行直观比对：加密前数据和解密后数据。
19. **评分标准**
20. 成功完成步骤2，能够正确打印token信息，实现平台登录功能。（15分）
21. 成功完成步骤3，能够正确打印密钥标识信息，实现密钥申请功能。（15分）
22. 能够正确对数据进行加密，实现数据加密功能。（30分）
23. 通过页面能够正确展示解密后的明文数据，并比对成功，实现数据解密功能。（30分）
24. **预计完成时间**

8小时

1. **平台登录接口说明**
2. 参数定义

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 数据接口定义 | | | | | | | |
| 数据接口名称 | | 应用key登录 | | | | | |
| 请求地址 | | https://IP:PORT/csp-server/v2/sys/login | | | | | |
| 提供类型： | | HTTPS | 请求方式： | | POST | | |
| 是否压缩（GZIP） | | 否 | Content-Type： | | application/json | | |
| 响应时间要求 | | 1S | | | | | |
| 备注 | |  | | | | | |
| 输入字段定义 | | | | | | | |
| 序号 | 字段名称 | 字段定义 | | 数据类型 | | 非空 | 备注 |
|  | 登录类型 | type | | Integer | | 是 | 固定值1 |
|  | 应用ID | appId | | String | | 是 | 见附录应用信息 |
|  | 应用Key | appKey | | String | | 是 | 见附录应用信息 |
| 输出字段定义 | | | | | | | |
| 序号 | 字段名称 | 字段定义 | | 数据类型 | | 非空 | 备注 |
|  | 接入token | token | | String | | 是 |  |
|  | 有效期单位 | standard | | Integer | | 是 | 本次考核不涉及，忽略 |
|  | 认证有效期 | validity | | Integer | | 是 | 本次考核不涉及，忽略 |

1. 请求样例

{

"appId": "e16cr3f4",

"appKey": "8uy1056i",

"type": 1

}

1. 返回样例

{

"code": 200,

"msg": "成功",

"data": {

"token": "eyJ0eXAiOiJKV1QiLCJ0b2tlbl9wYXJhbSI6InRva2VuX3BhcmFtIiwiYWxnIjoiSFMyNTYifQ.eyJ0b2tlbl9wYXJhbSI6ImUxNmNyM2Y0IiwiZXhwIjoxNjk3MDkyMzMzfQ.sW-pCBPPOoLgV61\_kTS1zAtDYd4yD5YEN7NN3m-NOds",

"standard": 2,

"validity": 1440

}

}

1. **申请会话密钥接口说明**
2. 参数定义

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 数据接口定义 | | | | | | | |
| 数据接口名称 | | 创建会话密钥 | | | | | |
| 请求地址 | | https://IP:PORT/csp-server/v2/sessionKey/add | | | | | |
| 提供类型： | | HTTPS | 请求方式： | | POST | | |
| 是否压缩（GZIP） | | 否 | Content-Type： | | application/json | | |
| 响应时间要求 | | 1S | | | | | |
| 备注 | |  | | | | | |
| 输入字段定义 | | | | | | | |
| 序号 | 字段名称 | 字段定义 | | 数据类型 | | 非空 | 备注 |
|  | 安全密码介质标识 | spmId | | String | | 否 | 本次考核不涉及，忽略 |
|  | 加密公钥 | publicKey | | String | | 否 | 本次考核不涉及，忽略 |
|  | 凭证 | voucher | | String | | 否 | 本次考核不涉及，忽略 |
|  | 会话id | sessionId | | String | | 否 | 默认uuid用生成  数字和英文字母，长度不大于64 |
|  | 密钥长度 | keyLength | | Integer | | 否 | 默认16字节，最大256字节，须为16的整数倍 |
|  | 密钥算法 | algorithm | | Integer | | 否 | 固定值3，见附录算法类型 |
|  | 运算模式 | calcMode | | Integer | | 否 | 取值范围1和2，见附录运算模式 |
|  | 初始化向量 | iv | | Integer | | 否 | 运算模式为2时有效，见附录初始化向量 |
|  | 有效期 | validity | | Integer | | 否 | 默认有效期1天 |
|  | 有效期单位 | standard | | Integer | | 否 | 见附录有效期单位 |
|  | 鉴权模式 | authType | | Integer | | 否 | 默认不鉴权，见附录鉴权模式 |
|  | 接收方 | receiveId | | String | | 否 | 接收方（群组密钥则传群组id） |
| 输出字段定义 | | | | | | | |
| 序号 | 字段名称 | 字段定义 | | 数据类型 | | 非空 | 备注 |
|  | 密钥id | keyId | | String | | 是 |  |
|  | 密钥长度 | keyLength | | Integer | | 是 |  |
|  | 密钥哈希值 | keyHash | | String | | 否 | Hex形式 |
|  | 密钥密文 | keyCipher | | String | | 否 | Hex形式 |
|  | 密钥解密算法 | decKeyAlg | | String | | 是 | 固定sm4-ecb |
|  | 解密密钥块标识 | decKeyTag | | Integer | | 否 |  |
|  | 解密密钥序号 | decKeySn | | Integer | | 否 |  |
|  | ka密文 | kaCipher | | String | | 否 | 见附录加密数据 |
|  | ka解密算法 | kaAlg | | String | | 否 | 固定sm2 |

1. 请求样例

{

"sessionId": "c40dfb203c074035ab589b387ec95527"

}

1. 返回样例

{

"code": 200,

"msg": "成功",

"data": {

"keyId": "c40dfb203c074035ab589b387ec95527",

"keyLength": 16

}

}

1. **数据加密接口说明**
2. 参数定义

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 数据接口定义 | | | | | | | |
| 数据接口名称 | | 对称密钥-加密 | | | | | |
| 请求地址 | | https://IP:PORT/csp-server/v2/operation/sym/encrypt | | | | | |
| 提供类型： | | HTTPS | 请求方式： | | POST | | |
| 是否压缩（GZIP） | | 否 | Content-Type： | | application/json | | |
| 响应时间要求 | | 1S | | | | | |
| 备注 | |  | | | | | |
| 输入字段定义 | | | | | | | |
| 序号 | 字段名称 | 字段定义 | | 数据类型 | | 非空 | 备注 |
|  | 密钥类型 | keyType | | Integer | | 否 | 此处固定值2 |
|  | 对称密钥id | keyId | | String | | 是 |  |
|  | 源数据 | data | | String | | 是 | 按编码方式编码后的数据 |
|  | 算法 | algorithm | | String | | 否 | 取值范围31或32；见附录算法类型 |
|  | 初始化向量 | iv | | String | | 否 | 32位hex |
|  | 补位模式 | padding | | Integer | | 否 | 默认2；见附录补位模式 |
|  | 编码方式 | encoding | | Integer | | 否 | 默认1，见附录编码方式，按此解码源数据 |
| 输出字段定义 | | | | | | | |
| 序号 | 字段名称 | 字段定义 | | 数据类型 | | 非空 | 备注 |
| 1 | 加密结果 |  | | String | | 是 | 请求入参编码方式为2时，按hex形式编码返回，其他值时按base64形式编码返回 |

1. 请求样例

{

"data": "张三你好呀",

"keyId": "c40dfb203c074035ab589b387ec95527",

"keyType": 2,

"encoding": 1

}

1. 返回样例

{

"code": 200,

"msg": "成功",

"data": "CQlwyYqa637KmwC8+edPIw=="

}

1. **数据解密接口说明**
2. 参数定义

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 数据接口定义 | | | | | | | |
| 数据接口名称 | | 对称密钥-加密 | | | | | |
| 请求地址 | | https://IP:PORT/csp-server/v2/operation/sym/decrypt | | | | | |
| 提供类型： | | HTTPS | 请求方式： | | POST | | |
| 是否压缩（GZIP） | | 否 | Content-Type： | | application/json | | |
| 响应时间要求 | | 1S | | | | | |
| 备注 | |  | | | | | |
| 输入字段定义 | | | | | | | |
| 序号 | 字段名称 | 字段定义 | | 数据类型 | | 非空 | 备注 |
|  | 密钥类型 | keyType | | Integer | | 否 | 此处固定值2 |
|  | 对称密钥id | keyId | | String | | 是 |  |
|  | 密文数据 | cipher | | String | | 是 | 按编码方式编码后的数据 |
|  | 算法 | algorithm | | String | | 否 | 取值范围31或32；见附录算法类型； |
|  | 初始化向量 | iv | | String | | 否 | 32位hex |
|  | 补位模式 | padding | | Integer | | 否 | 默认2；见附录补位模式； |
|  | 编码方式 | encoding | | Integer | | 否 | 默认1，见附录编码方式，取值为2时按hex形式解码，其他值时按base64解码密文数据 |
| 输出字段定义 | | | | | | | |
| 序号 | 字段名称 | 字段定义 | | 数据类型 | | 非空 | 备注 |
| 1 | 解密结果 |  | | String | | 是 | 根据请求入参编码方式，对解密结果进行编码返回 |

1. 请求样例

{

"cipher": "CQlwyYqa637KmwC8+edPIw==",

"keyId": "c40dfb203c074035ab589b387ec95527",

"keyType": 2,

"encoding": 1

}

1. 返回样例

{

"code": 200,

"msg": "成功",

"data": "张三你好呀"

}

1. **附录**
2. 应用信息

任选一个即可

|  |  |
| --- | --- |
| 应用ID | 应用KEY |
| 6c40b2ad7c0b40c5a0533d67fcaf0521 | a20b7c8376fd4011a6b18bd310eb6e35 |
| 78ab5163ceb74a98a5a0bce382df7cf3 | 63d9b3bbc4854e2d81caacc432875d0b |
| bec6bc89208f4aa8b73424cf53bbbcc9 | ea54e5827d6f4218b41b21ab8874baec |

1. 有效期单位

|  |  |
| --- | --- |
| 字典说明 | 字典编码 |
| 秒 | 1 |
| 分 | 2 |
| 时 | 3 |
| 天 | 4 |

1. 密钥类型

|  |  |
| --- | --- |
| 字典说明 | 字典编码 |
| 对称密钥（工作密钥） | 1 |
| 会话密钥 | 2 |
| 非对称密钥 | 3 |
| 充注密钥 | 4 |
| 跨域密钥 | 5 |

1. 算法类型

|  |  |
| --- | --- |
| 字典说明 | 字典编码 |
| sm2 | 1 |
| sm3 | 2 |
| sm4 | 3 |
| sm4-ecb | 31 |
| sm4-cbc | 32 |

1. 运算模式

|  |  |
| --- | --- |
| 字典说明 | 字典编码 |
| ECB | 1 |
| CBC | 2 |

1. 补位模式

|  |  |
| --- | --- |
| 字典说明 | 字典编码 |
| 不补位 | 1 |
| Pkcs7补位 | 2 |

1. 鉴权模式

|  |  |
| --- | --- |
| 字典说明 | 字典编码 |
| 不鉴权 | 1 |
| 单对单 | 2 |
| 群组 | 3 |

1. 认证类型

|  |  |
| --- | --- |
| 字典说明 | 字典编码 |
| Ukey盾 | 1 |
| X509证书 | 2 |
| P12证书 | 3 |
| 协同密钥 | 4 |

1. 编码方式

|  |  |
| --- | --- |
| 字典说明 | 字典编码 |
| 无（即原始字符串） | 1 |
| HEX编码 | 2 |
| BASE64编码 | 3 |

1. 初始化向量

本文档中使用的初始化向量为：32字节，默认为全0，转换为hex形式的长度64字符。样例如：

0000000000000000000000000000000000000000000000000000000000000000