**采购需求**

**一、项目概况**

依照我校办学定位，加强新时代高技能人才队伍建设，健全完善技能人才评价体系，根据省人社厅《关于全面实施职业技能等级认定的通知》（陕人社发〔2020〕30号）和市人社局《关于印发<西安市全面实施职业技能等级认定细则>（试行）的通知》等精神，结合学校教育教学工作实际，落实“1+X证书制度”工作部署，确保2025年职业技能等级认定项目工作的顺利开展，健全完善职业技能人才培养，建设知识型、技能型、创新型人才职业队伍。因此需设立职业技能设备购置项目，为从事密码技术应用的学员提供符合真实应用场景的密码技术综合实验训练环境，模拟教学、学习、训练、测试与考试，满足开展“密码技术应用员”职业工种的考评工作。

**二、采购内容**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **类别** | **名称** | **形态** | **单位** | **数量** | **备注** |
| 1 | 密码技术应用员培训平台 | 国密安全门禁系统 | 硬件 | 套 | 1 | / |
| 2 | 国密安全音视频系统 | 硬件 | 套 | 1 | / |
| 3 | 服务器密码机 | 硬件 | 台 | 1 | 核心产品 |
| 4 | SSL VPN/IPSEC VPN 综合安全网关 | 硬件 | 台 | 2 | / |
| 5 | 数字证书认证系统（CA） | 硬件 | 台 | 1 | / |
| 6 | 证书认证密钥管理系统（KM） | 软件 | 套 | 1 | / |
| 7 | 签名验签服务器 | 硬件 | 台 | 1 | / |
| 8 | 安全认证网关 | 硬件 | 台 | 1 | / |
| 9 | 智能密码钥匙 | 硬件 | 个 | 100 | / |
| 10 | 时间戳服务器 | 硬件 | 台 | 1 | / |
| 11 | 协同签名服务器 | 硬件 | 台 | 1 | / |
| 12 | 题库管理系统 | 软硬件 | 台 | 1 | / |
| 13 | 理论考试系统 | 软硬件 | 台 | 1 | / |
| 14 | 实操考试系统 | 软硬件 | 台 | 1 | / |
| 15 | 密码技术应用员培训平台 | 软硬件 | 台 | 2 | / |

**备注：本项目的核心产品为：服务器密码机**

**三、技术要求**

|  |  |  |
| --- | --- | --- |
| 序号 | 设备 | 技术参数 |
| 1 | 国密安全门禁系统 | ▲1.配合密码技术应用员培训系统使用，基于产品提供实操课程≥5个，课程能与密码技术应用员培训平台、实操考试系统无缝对接。教室和学生课直接通过实训平台对产品进行课程实训。课程必须包含门禁日志完整性(SM2和HMAC-SM3)和身份鉴别实验，支持调用平台内的服务器密码机和签名验签服务器实现门禁日志完整性保护。（提供能证明上述参数的产品认证证书、产品彩页、产品说明书、测试报告、检测/检验报告、官网截图、系统截图等相关证明材料中的任意一项或者多项）。2.网关内置国密二级及以上加密卡；并具有国密二级及以上密码模块的相关证明材料。3.即插即用，无需与密码机或签名验签服务器联调。4.系统功能至少具备基础信息管理、消费业务管理、门禁业务管理、考勤业务管理、巡更业务管理、访客管理、报表与查询等功能。5.支持数据导入、导入查询功能，在有大量的部门数据、人员数据时，可以通过数据导入添加部门及人员。6.支持对门禁进出记录完整性保护，可通过页面直接查看完整性记录情况。门禁完整性的设计采用的SM2算法，提供产品的进出记录完整性保护实现的代码片段。7.报表功能：按自定义时间加按可以按员工姓名，门，部门、工号等查询通行，拒绝明细表，未关门员工表。可以查询员工详细报表。8.支持巡更任务的管理能力，巡更任务管理用来管理在线巡更的巡更人员、巡更事件、巡更任务等。9.授权管理，支持可进行分时段、分级别、分区域管理，权限组管理用来管理访问组、门组、时间段和假日设置，支持授权仅卡方式开门、卡+密码方式开门等。10.事件记录应包括如下内容：允许通行、拒绝通行、报警、强行开门、常开、故障、网络连接、网络断开、远程控制及读卡器型号变更等。11.门禁控制器（2门和4门）通信端口：支持≥4个RS-485口/4个维根口/1个TCP IP协议。 12.具备≥3个LED灯分别显示设备状态，总线状态和电锁状态。需提供门禁控制箱。支持CPU读卡协议，满足国密CPU要求，可自定义密钥。13.读卡器和卡之间的通讯采用高安全的相互认证机制，数据加密传输，64位读/写多样化密钥。支持PSAM卡。门禁卡可存储数据，实现一卡通系统，基于13.56 MHz 的读/写非接触智能卡技术。 |
| 2 | 国密安全音视频系统 | ▲1.配合密码技术应用员培训系统使用，基于产品提供实操课程≥5个，课程能与密码技术应用员培训平台、实操考试系统无缝对接。教室和学生课直接通过实训平台对产品进行课程实训。课程必须包视频数据完整性实验(需包含SM2算法和HMAC-SM3算法)，支持调用平台内的服务器密码机和签名验签服务器实现频数据完整性完整性保护。（提供能证明上述参数的产品认证证书、产品彩页、产品说明书、测试报告、检测/检验报告、官网截图、系统截图等相关证明材料中的任意一项或者多项）。2.具备≥32路10M/100M/1000M自适应以太网电口；内置国密安全芯片，支持国密SM1/SM2/SM3/SM4算法；支持海康、宇视、大华等主流IPC、NVR产品的接入，可适配各种视频监控场景。3.支持≥32路1080P视频的签名及验签；支持≥32路1080P视频接入，支持 PoE供电，符合IEEE802.3af/at标准。4.产品内置视频数据安全与防护系统密码模块，串联于 IPC (网络摄像头)和 NVR(网络视频录像机)之间，具有密钥管理、视频数据加解密、视频数据签名验签功能；符合 GM/T0028《密码模块安全技术要求》安全等级第二级相关要求，通过密码检测。5.支持TCP/UDP协议、SIP，兼容H.264和H.265编码协议；支持对符合GB/T28181的视频流进行传输的机密性保护。6.视频数据完整性采用关键帧方式进行签名，能通过设备自身进行完整性抓包分析，查看签名值，验签公钥等信息。7.产品配置可选、即插即用、使用便捷、安全可控；设备部署不需改变原有网络架构，无需更换摄像头和NVR就可以实现视频数据的传输、存储进行机密性、完整性保护。8.采用B/S架构设计，支持web界面管理方式查看或修改设备的配置信息；支持流量负载、安全业务统计、设备性能监控等功能，用户可实时查看设备性能。9.支持对NVR存储的视频数据进行机密性、完整性保护；支持对符合GB/T28181的视频流进行传输的完整性保护。10.板载国密二级安全芯片，基于音视频设备标识产生、存储密钥信息，保证密钥不出硬件密码模块，保证密钥的安全性，设备对待传输的指令明文进行非对称加密,得到指令密文,采用私钥对所述指令密文进行签名,将签名后的指令密文发送视音频监控设备,视音频监控设备根据签名后的指令密文进行安全认证,确保在开放互联网场景下系统运行的安全性。11.产品经过密码应用适配验证，符合GB/T39786-2021《信息安全技术 信息系统密码应用基本要求》中8.3.e指标要求；基本符合8.1.c、8.3.a指标要求。 |
| 3 | 服务器密码机（**核心产品**） | ▲1.配合密码技术应用员培训系统使用，基于产品提供实操课程≥10个，课程能与密码技术应用员培训平台、实操考试系统无缝对接。教室和学生课直接通过实训平台对产品进行课程实训。（提供能证明上述参数的产品认证证书、产品彩页、产品说明书、测试报告、检测/检验报告、官网截图、系统截图等相关证明材料中的任意一项或者多项）。2.标准2U机架式设备，国产CPU：主频不低于3.3GHz,核心数不少于8个；国产操作系统，千兆网口≥4。3.具备开盖密钥销毁功能，具备密钥一键销毁功能。4.管理后台为B/S模式，管理登录支持国密浏览器并使用TLCP协议进行双向身份鉴别。5.实现对应用层数据的加密/解密、数字签名/验证、数据摘要、密钥管理等提供高速运算。6.内置国密二级密码卡。7.支持设备初始化配置，包括密钥产生安装、生成管理员、按照安全机制对密钥安全存储和备份、系统配置、一键检测等功能，保证设备处于正常工作状态。8.至少支持三层密钥结构，包括：管理密钥、用户密钥/设备密钥/密钥加密密钥、会话密钥。9.支持SM2、SM3、SM4；SM4算法的ECB和CBC、MAC模式的数据加密和解密运算。10.支持审计日志的记录，查询和导出功能，支持审计审计日志签名。11.支持设备运行状态监控，支持监控CPU使用率、内存使用率、磁盘使用率等。12.支持多种调用方式，提供多种调用接口，提供标准API，支持SDF、JCE、P11等接口。 |
| 4 | SSL VPN/IPSEC VPN 综合安全网关 | ▲1.配合密码技术应用员培训系统使用，基于产品提供实操课程≥10个，课程能与密码技术应用员培训平台、实操考试系统无缝对接。教师和学生课直接通过实训平台对产品进行课程实训。（提供能证明上述参数的产品认证证书、产品彩页、产品说明书、测试报告、检测/检验报告、官网截图、系统截图等相关证明材料中的任意一项或者多项）。2.标准2U机架式设备，国产CPU：主频不低于3.3GHz,核心数不少于8个；国产操作系统，千兆网口≥4。3.具备开盖密钥销毁功能，具备密钥一键销毁功能。4.管理后台为B/S模式，管理登录支持国密浏览器并使用TLCP协议进行双向身份鉴别。5.支持SSL认证、SSL卸载、数据压缩、数据缓存功能。6.支持“多对一”地址转换，使得内部网络主机访问外部网络时，其源IP地址被转换；支持“一对多”地址转换，将内网服务器的IP地址/端口映射外网接口的IP地址/端口，使外部网络的主机通过访问映射地址和端口实现对内部服务器的访问。7.支持TLS1.1、TLS1.2、TLS1.3、GMSSL等协议；支持我国自行扩展定义X509数字证书标准（SM2+SM3）。8.内置轻量级CA证书认证与管理中心，可为自身和其他节点签发数字证书。9.支持SNAT模式，代理内网原地址转换模式，或普通路由模式。10.支持基于用户名、群组、角色；基于用户数字证书信息；基于目标应用系统；基于CRL证书吊销列表的访问控制。 |
| 5 | 数字证书认证系统（CA） | ▲1.配合密码技术应用员培训系统使用，基于产品提供实操课程≥10个，课程能与密码技术应用员培训平台、实操考试系统无缝对接。教师和学生课直接通过实训平台对产品进行课程实训。（提供能证明上述参数的产品认证证书、产品彩页、产品说明书、测试报告、检测/检验报告、官网截图、系统截图等相关证明材料中的任意一项或者多项）。2.能与所采购的服务器密码机进行无缝对接。3.标准2U机架式设备，国产CPU：主频不低于3.3GHz,核心数不少于8个；国产操作系统，千兆网口≥4。4.具备开盖密钥销毁功能，具备密钥一键销毁功能。5.管理后台为B/S模式，管理登录支持国密浏览器并使用TLCP协议进行双向身份鉴别。6.包括CA签发系统、RA注册系统。7.实现证书在线申请、审核、签发和制作。8.实现证书在线撤销的申请、审核。9.实现证书黑名单（CRL）在线签发和OCSP。10.实现证书的冻结、解冻。11.支持证书模板功能，系统内置多种标准证书模板，并且支持自定义证书模板。12.支持双证书签发和管理。13.证书支持智能卡登录、安全SSL连接、安全电子邮件、VPN等。14.证书介质支持文件、USB KEY等。15.支持主流加密机、加密卡和USB KEY等密码设备。16.支持LDAP进行证书和CRL发布。17.备份恢复功能。 |
| 6 | 证书认证密钥管理系统（KM） | 1.配合密码技术应用员培训系统使用，课程能与密码技术应用员培训平台、实操考试系统无缝对接。教师和学生课直接通过实训平台对产品进行课程实训。2.与采购的服务器密码机和证书认证系统（CA）进行无缝对接。3.提供颁发者证书、通讯证书、密钥保护证书等证书体系配置功能。4.提供系统人员管理、角色管理、权限管理等功能。5.提供日志查询、审计的功能。6.提供配置密码机信息、密钥的功能。7.提供密钥对定时任务配置、备用密钥对查询、在用密钥对查询、历史密钥对查询的功能。8.提供配置外部CA服务的功能。 |
| 7 | 签名验签服务器 | ▲1.配合密码技术应用员培训系统使用，基于产品提供实操课程≥10个，课程能与密码技术应用员培训平台、实操考试系统无缝对接。教室和学生课直接通过实训平台对产品进行课程实训。（提供能证明上述参数的产品认证证书、产品彩页、产品说明书、测试报告、检测/检验报告、官网截图、系统截图等相关证明材料中的任意一项或者多项）。2.标准2U机架式设备，国产CPU：主频不低于3.3GHz,核心数不少于8个；国产操作系统，千兆网口≥4。3.具备开盖密钥销毁功能，具备密钥一键销毁功能。4.管理后台为B/S模式，管理登录支持国密浏览器并使用TLCP协议进行双向身份鉴别。5.支持 SM2、SM3、SM4算法。6.支持 PKCS#1 和 PKCS#7 签名/验签；符合 GM/T0019-2012《通用密码服务接口规范》数字信封和带 签名的数字信封封装解封。7.支持基于 SM2等算法的 PKCS#1 签名/验证、 PKCS#7 Attached 签名/验证、P7 Detached 签名/验证功能；签名格式符合 PKCS#7、GM/T0010 等标准中 定义的数据类型。8.支持配置不同的证书信任域，证书验证策略支持配 置不验证、根证书、CRL、OCSP 等多种验证策略。9.权限控制：所投产品支持管理员、审计员、操作员多级权限，对设备的不同管理操作需不同管理人员登 录，从而具备相应的管理权限。10.支持 IP 白名单、连接口令等访问控制功能。11.密钥结构采用“系统保护密钥-用户密钥-会话密钥”的三层密钥保护结构，保证关键密钥在任何时候 不以明文形式出现在设备外，密钥备份文件受备份密钥加密保护。 |
| 8 | 安全认证网关 | ▲1.配合密码技术应用员培训系统使用，基于产品提供实操课程≥10个，课程能与密码技术应用员培训平台、实操考试系统无缝对接。教师和学生课直接通过实训平台对产品进行课程实训。（提供能证明上述参数的产品认证证书、产品彩页、产品说明书、测试报告、检测/检验报告、官网截图、系统截图等相关证明材料中的任意一项或者多项）。2.标准2U机架式设备，国产CPU：主频不低于3.3GHz,核心数不少于8个；国产操作系统，千兆网口≥4。2.具备开盖密钥销毁功能，具备密钥一键销毁功能。4.管理后台为B/S模式，管理登录支持国密浏览器并使用TLCP协议进行双向身份鉴别。5.支持业务系统单点登录。6.支持证书透传功能。7.支持国密TLCP协议。8.支持SSL认证、SSL卸载、数据压缩、数据缓存功能。 |
| 9 | 智能密码钥匙 | 1.配合密码技术应用员培训系统使用，课程能与密码技术应用员培训平台、实操考试系统无缝对接。教室和学生课直接通过实训平台对产品进行课程实训。2.支持国密SM2、SM3、SM4算法。3.提供第三方开发SDK接口。4.须与本项目采购的数字证书系统进行无缝对接。 |
| 10 | 时间戳服务器 | 1.配合密码技术应用员培训系统使用，课程能与密码技术应用员培训平台、实操考试系统无缝对接。教室和学生课直接通过实训平台对产品进行课程实训。2.标准2U机架式设备，国产CPU：主频不低于3.3GHz,核心数不少于8个；国产操作系统，千兆网口≥4。3.具备开盖密钥销毁功能，具备密钥一键销毁功能。4.管理后台为B/S模式，管理登录支持国密浏览器并使用TLCP协议进行双向身份鉴别。5.支持 SM2、SM3、SM4算法。6.支持NTP协议，能够与第三方授时中心、卫星授权时间源进行时间同步，确保所签发时间戳时所获取的时间的有效性。 |
| 11 | 协同签名服务器 | ▲1.配合密码技术应用员培训系统使用，基于产品提供实操课程≥10个，课程能与密码技术应用员培训平台、实操考试系统无缝对接。教室和学生课直接通过实训平台对产品进行课程实训。（提供能证明上述参数的产品认证证书、产品彩页、产品说明书、测试报告、检测/检验报告、官网截图、系统截图等相关证明材料中的任意一项或者多项）。2.标准2U机架式设备，国产CPU：主频不低于3.3GHz,核心数不少于8个；国产操作系统，千兆网口≥4。3.具备开盖密钥销毁功能，具备密钥一键销毁功能。4.管理后台为B/S模式，管理登录支持国密浏览器并使用TLCP协议进行双向身份鉴别。5.实现计算机终端和移动端，与服务端协作共同完成完整签名，客户端密码模块采用SDK形式嵌入用户客户端程序或APP，支持各种桌面及移动端操作系统。6.客户端密码模块以SDK形式嵌入用户APP，和协同签名服务端系统配合完成私钥的管理、签名、解密工作。7.具有数据加解密、数据签名验签、密钥管理、日志审计等功能，支持国密对称算法：SM4，非对称算法：SM2，摘要算法：SM3，MAC算法：HMAC。8.支持对签名结果进行验证，支持对 X.509 证书有效性进行验证，支持解析 X.509 证书内容，获取证书信息。9.支持产生随机数，该随机数可作为登录认证的挑战随机数。 |
| 12 | 题库管理系统 | 1.题库管理模块分类管理：支持按职业等级（四级至一级）、工作内容（规划/建设/评估/运维）、题型（单选/多选/案例/实操模拟题）多维度分类。支持知识点标签绑定（如“密钥管理策略”“密码应用方案合规性审查”）。题目属性：题目难度分级（初级/中级/高级），支持关联《标准》条款支持富文本编辑（公式、图表、代码块）。题目审核：支持多级审核流程（至少2名专家独立审核），记录修改痕迹。2.试卷管理模块智能组卷：支持按等级、知识点、难度比例自动组卷（如一级试卷中“密码应用策略制定”占比≥35%）。支持手动组卷模式，可自定义题目范围、权重及题型分布。3.数据分析模块按技能点生成雷达图，标记高频错误知识点（如“密码协议知识”错误率≥50%）。支持导出PDF/Excel格式的考生能力报告。题目重复率检测（相似度≥90%时预警）、无效题目自动下架▲4.题目要求理论题目不少于4600道，实操题目不少于120道，题目内容满足《密码技术应用员国家职业技能标准》要求。（提供能证明上述参数的产品认证证书、产品彩页、产品说明书、测试报告、检测/检验报告、官网截图、系统截图等相关证明材料中的任意一项或者多项）5.扩展要求须与本项目中理论考试系统和实操考试系统、密码技术应用员培训平台实现无缝对接，为上述系统提供题库服务功能。6.安全要求基于国密算法实现对题库题目存储的完整性进行保护防止非法篡改 |
| 13 | 理论考试系统 | 1.用户管理模块角色权限控制支持考生、管理员、教师/考官三类角色，实现分级权限管理2.考试流程控制考试发布与配置设置考试时间（定时开放/限时作答）、及格线、允许重考次数等规则。3.在线考试与交互考生端功能答题卡实时保存、标记疑问题目、倒计时提醒、临时断网恢复作答。支持公式/图片/音视频等多媒体题型嵌入。断网保护（数据本地缓存后自动同步）模拟考试功能：支持模拟考试功能4.评分与数据分析自动评分与人工复核客观题自动判分，主观题支持教师手动批改。成绩统计报表（平均分、通过率、题目正确率等）。数据可视化与反馈生成考生能力分析雷达图、知识点薄弱环节热力图。导出成绩单及考试记录（PDF/Excel格式）。5.系统扩展与兼容性支持与本项目中题库管理系统无缝对接，从题库管理系统获取题目支持与本项目中密码技术应用员培训平台无缝对接，为密码技术应用员培训平台提供考试服务6.安全性要求身份鉴别：支持基于本项目中采购的智能密码钥匙采用密码技术进行系统身份鉴别，确保用户身份安全数据安全：对系统中的试卷、考试成绩、用户信息等重要数据使用国密算法进行完整性和机密性保护，防止数据非法篡改和泄露。 |
| 14 | 实操考试系统 | 1.用户管理支持多角色权限划分（考生、考官、管理员），与技能等级绑定实操场景构建2.实操场景构建按等级动态生成场景，如中级工：密码产品部署、调试工具配置；高级技师：密码策略优化、测评报告审核。3.操作任务设定支持任务模板库，任务权重可配置4.在线实操考试支持虚拟化隔离环境，考试界面分屏显示任务说明与操作终端，防作弊机制支持屏幕录制。5.实时监控与回放支持屏幕录制记录回放，全流程操作日志记录6.自动+人工评分支持自动和人工评分功能7.成绩管理按等级生成技能分析报告，数据可导出为PDF/Excel格式，符合人社部认证要求系统设计与扩展8.系统设置与扩展支持与本项目中题库管理系统无缝对接，从题库管理系统获取题目支持与本项目中密码技术应用员培训平台无缝对接，为密码技术应用员培训平台提供考试服务 |
| 15 | 密码技术应用员培训平台 | 1.用户账户管理：创建和管理用户账户，包括学生、教师和管理员。2.权限和角色管理：为不同的用户分配不同的权限和角色，3.实训课程管理：允许教师创建、编辑和管理实训课程，包括课程内容、实训项目和评估标准。4.学习进度跟踪：记录学生的学习进度，包括完成的实训项目、获得的分数和反馈。5.密码学工具集成：集成各种密码学工具和算法，供学生在实训中使用。6.实训环境：支持jupyterLab、VNC、WebSSH 独立虚拟实训环境。7.报告和分析：生成有关学生表现和课程效果的报告和分析。8.课程访问控制：控制学生对特定实训课程的访问，可能基于时间、完成度或其他条件。9.课表管理：支持对课表的管理维护选班级，起止时间，课程介绍，课程表等。10.实验教学：能够完成日常的实验教学，能够进行实验操作、录制演示视频、播放演示视频、下载演示视频。11.实验监控:支持显示实验进度实时展示，教师可查看学生本次试验每个节点的完成情况。12.自动检测评估：支持实验结果自动检测评估打分课件管理：支持对理论和实践课件管理13.数据统计:支持查看学生的在线情况，实验的完成情况，考试的成绩情况。14.实验报告管理和评价:支持对学员实验报告的查看，统计，可根据学生的学号，姓名等查询实验报告，支持对学员的实验报告进行评价。15.历史实验:支持对已做过的实验进行查看，支持对正在进行的实验。16.环境支持:支持50个用户同时在线实训操作，实训环境独立且互不影响▲17.提供实训课件不少于200个需包含如下算法课件(提供源码和教程)：分组密码:SM4密码算法、DES 密码算法、3DES 密码算法、AES密码算法、IDEA密码算法、RC5密 码算法、RC5 密码算法、Blowfish 密码算法、Camellia密码算法公钥密码:SM2密码算法、MH-Knapsack密码 算法、RSA 密码算法、ElGamal 密码算法、椭圆曲线密码算法、Pailiar 密码算法摘要算法:SM3密码算法、MD4 算法、MD5 算法、SHA-1 算法、SHA-3 算法(Keccak)、B1ake 算法、Grost1 算法、JH 算法、Skein 算法序列密码:ZUC 密码算法、RC4密码算法、SNOW3G 密码算法、A5 密码算法、SEAL密码算法实验抗量子密码算法集成：将常见的抗量子密码算法，支持aigis-enc,aigis-sig、AKCN-LWR、AKCN-MLWE、Dilithium、FrodoKEM、HEL公钥加密密钥封装算法、HEL密钥交换算法、Kyber、LAC、LAC.KEX、LAC.PKE、LADAC、LAKE、NewHope、 NTRU、qTESLA、Scloud、SKCN-MLWE、TALE、DME-Sign、MQDSS、PROV、Rainbow、SNOVA、Square-free、TUOV、VOX。（提供能证明上述参数的产品认证证书、产品彩页、产品说明书、测试报告、检测/检验报告、官网截图、系统截图等相关证明材料中的任意一项或者多项）18.系统应为开放性实训平台，满足实验室教学科研人员根据需要自行修改/增加实验。可以为密码技术竞赛提供技术支撑，并能够根据甲方要求实现定制功能。（1）密码产品开发与设计仿真支持对主流密码产品进行仿真，符合行业标准算法设计工具：提供可视化工具，允许用户设计和实现各种密码算法，如对称加密、非对称加密、哈希函数等。加密协议模拟：支持模拟各种加密协议SSL/TLS、SSH、IPsec等，以研究其安全性和性能。密码分析工具：提供密码分析工具，如频率分析、已知明文攻击、中间人攻击等，以测试算法的安全性。性能评估：评估密码算法的性能，包括加密速度、密钥生成时间、内存使用等。密钥管理：模拟密钥生成、分发、存储和销毁的过程。密码算法库：集成常用的密码算法库，Gmssl、OpenSSL、LibTomCrypt等。编程接口：提供编程接口，允许用户在自定义应用程序中使用平台的功能。（2）密码应用运维系统架构模拟：允许用户自定义和模拟不同的密码系统架构，包括硬件、软件和网络配置。密码服务管理：模拟密码服务的部署和管理，如证书颁发机构（CA）、密钥管理服务（KMS）等。配置和策略模拟：允许用户配置和测试不同的密码策略和安全设置。性能压力测试：模拟高负载情况下的密码系统性能，评估其稳定性和响应时间。故障模拟和恢复：模拟系统故障和攻击情况，测试密码系统的恢复能力和容错机制。安全事件模拟：模拟安全事件和攻击，密钥泄露、密码破解等，以评估系统的安全性合规性检查：确保密码系统的配置和管理符合相关的法律法规和安全标准。日志和监控：模拟日志记录和系统运行，以便于跟踪和分析安全事件。 |