**2021年北京邮电大学**

**《信息安全编程技术与实例开发》**

**课程设计题目及要求**

**[信息安全专业]**

**任课老师: 马兆丰 联系方式：**[**mzf@bupt.edu.cn**](mailto:mzf@bupt.edu.cn)

**第一部分 课程设计题目及要求**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **课程设计题目** | **所属类别** | **课程设计主要要求** |
| 1 | 通用密码算法库实现及应用 | 算法实现 | 研究OpenSSL1.1.1（已支持SM2/SM3/SM4）/Crypto/MIRACL/ BouncyCastle系列密码算法库，包括哈希算法 SHA1/SHA3/SHA256/ RIPEMD160，对称加密算法3DES/AES/RC，RSA/ECC/DSA/ECDSA公钥密码及数字签名等。  在代码层面实现SHA3/SHA256/ AES/RC6/ECDSA等国际密码算法并进行实现和验证。  研究[国家密码管理局](https://baike.baidu.com/item/%E5%9B%BD%E5%AE%B6%E5%AF%86%E7%A0%81%E7%AE%A1%E7%90%86%E5%B1%80)颁布的国产密码算法SM2，SM3，SM4相关技术原理，实现国产自主密码算法SM2，SM3，SM4。  基于标准数据集和自定义数据进行验证。  要求支持不定长明文加密与解密。  要求支持不同字符集兼容和混编输入。  可基于支持Windows平台和Linux平台。  可采用OpenSSL1.1.1（已支持SM2/SM3/SM4）/Crypto/MIRACL/ BouncyCastle系列密码算法库实现相关算法，并基于实现的密码算法，进行可视化编程调用，实现相关算法功能集成。 |
| 2 | 同态加密算法技术实现 | 算法实现 | 同态加密是一种特殊的加密方法，它允许对密文进行特定的代数运算得到仍然是加密的结果，将其解密所得到的结果与对明文进行同样的运算结果一样，它可以在加密的数据中进行诸如检索、比较等操作，得出正确的结果，而在整个处理过程中无需对数据进行解密。其意义在于，对隐私保护或受限安全访问。  研究当前已有的同态加密技术，并深入研究相关同态加密算法，等。  深入剖析并理解相关同态加密算法原理及流程，包括HEANN、NFLib、FV-NFLib、cuHE、PALISADE、HELib、SEAL等算法及相关技术。  结合一定现实应用场景，基于Java/C语言对上述2种算法进行代码实现、调试、跟踪、分析及验证，确保其正确性和安全性及效率。 |
| 3 | 自动化渗透测试工具 | 网络安全  系统安全 | 搭建Web应用系统、微信服务号或微信小程序作为测试对象，对安全策略、主机安全、网络应用安全、数据安全、业务交易安全性等进行自动化渗透测试工具开发并测试验证所开发工具的有效性和可行性，相关内部包括但不限于如下内容：  针对安全策略，对现有网络的访问控制、网络攻击防护等安全策略及防护措进行绕过、规避或逃逸测试，进而验证安全防护策略的有效性和实际实现的可靠性。  针对主机安全，对Windows、Linux、Unix、AIX、Solaris等主流操作系统进行漏洞扫描和渗透测试，检测系统存在的潜在安全风险和漏洞。  针对Web应用安全，通过漏洞扫描及安全检测，根据OWASP提出的安全测试规范，对注入攻击、跨站脚本攻击XSS、跨站请求伪造CSRF进行安全渗透测试。针对特定应用系统对登录安全认证、访问控制（特别是非授权访问）、安全审计、链接保护、Cookie安全、支付逻辑漏洞等安全隐患进行安全测试和验证。  同时，可根据情况，可对对网络安全漏洞扫描、系统安全漏洞的其他维度进行安全渗透测试开发。  可根据自身情况，选择任何开发语言及数据库进行开发，对有基础的同学，可实现基于Kubernetes、kuberSphere进行集群化管理，基于微服务方式进行技术实现，采用RocketMQ/RabbitMQ消息中间件或Redis技术进行高可用性部署与缓存管理，增强系统的性能和效率及稳健性。 |
| 4 | 移动智能终端数字图像证据系统 | 数据安全 | 基于DCT/DWT水印算法实现移动智能终端数字图像存证、取证系统。  要求支持将日期、时间、位置、移动终端IMEI设备信息等关键信息以不可见水印形式嵌入到图像之中作为证据信息，并能有效提取证据。  系统实现存证、取证，存证实现拍照时自动嵌入证据信息，取证实现从载体中提取证据信息。具备系统配置、水印信息生成、实时拍照存证、取证效果展示等功能。  水印信息可以为文本信息、图片信息，但图像载体必须为JPG格式。  具备良好的鲁棒性和安全性，具备抗几何攻击（位移攻击、旋转攻击、缩放攻击和剪切攻击）、去除攻击（如去噪、量化、有损压缩、重新调制、统计均衡、共谋攻击、Oracle攻击等攻击）、稳健性攻击（如线性滤波、非线性滤波、压缩、添加噪声）能力，暂不考虑协议攻击、解释性攻击等。  Android/iOS实现均可。 |
| 5 | 关键交易数据安全管理及实时同步技术实现 | 数据安全 | 构建基于公钥密码体制的用户账户安全模型。  针对关键交易数据（数据库记录或关键字段）进行基于数字签名的数据完整性和安全性实现，即：写入时每条记录进行签名，并在查询时数据记录进行签名验证。  并对数据进行多节点实时同步，使得任意节点的数据访问得到同样的访问结果。  数据组织可以采用单一交易数据或多交易数据归集式管理。采用JAVA/Python/C语言实现，可以采用NoSQL数据库（Level DB, Berkeley DB, Redis， MongoDB, CouchDB）或传统的关系数据库技术实现。 |
| 6 | 驱动层终端全键盘记录系统 | 系统安全 | 基于内核驱动技术(ring0级)实现终端键盘监控与记录。  \*密码查看器功能。  全键盘内容记录。  支持中英文。  使用内核技术对用户进程进行保护，拒绝软件或者非授权用户通过任务管理器强行结束进程。  可选择Windows或Linux平台下实现。 |
| 7 | 去中心化高可信存证平台开发 | 数据安全 | 基于区块链实现分布式去中心化的高可信存证平台开发  实现数据的存证，查询，链上链下协同认证等核心功能  完成标准的智能合约的编写与开发  完成相应区块链网络构建和部署  完成完整的代码实现  实现基础可基于Hyperledger Fabric或其他开源技术  系统应有完成系统界面和相关数据表现形式 |
| 8 | 数字图像篡改检测系统开发 | 数据安全 | 多媒体处理技术的快速发展使得编辑多媒体数据更加容易,处理效果更加逼真,难以辨别。无论是新闻,司法鉴定等特殊领域中的伪造多媒体数据,还是在互联网上快速传播的非真实多媒体数据,都会给社会安定带来负面影响，多媒体取证技术的研究及发展,对保证多媒体数据真实性及完整性有重要意义。完成包括但不限于如下内容的技术开发及实现：  设计数字图像篡改检测的依据、方法与模型。  实现数字图像篡改检测算法（如基于CNN算法、深度学习算法等的检测算法）。  实现数字图像的篡改检测定位。  可通过数字图像检测算法或方法，有效检测给出数字图像复制粘贴检测、拼接检测。  部分参考资料：  <https://blog.csdn.net/u010183397/article/details/54799471>  <http://fotoforensics.com> （可展示ELA方法的测试结果）  <https://29a.ch/photo-forensics/#forensic-magnifier> （clone detect、ELA等多种方法都有展示）. |
| 9 | 智能合约安全漏洞监测技术 | 系统安全 | 深入理解区块链智能合约技术，并熟练掌握以太坊智能合约开发工作。  对以太坊如下合约漏洞或缺陷安全监测：智能合约调用安全漏洞、重入攻击漏洞、权限控制漏洞、数值溢出安全漏洞、账户冻结及绕过安全漏洞、逻辑设计缺陷安全问题、随机数安全误用等安全漏洞或安全缺陷。  针对以太坊区块链智能合约进行缺陷代码/正常代码编写。  通过智能合约安全缺陷代码和正常代码对比，增强智能合约安全编写能力。  要求基于以太坊平台进行智能合约监测和代码实现，并对能对智能合约进行3类以上安全漏洞监测。 |
| 10 | 支持隐私保护的Web3.0社交平台 | 应用安全 | Web3.0时代的人们将拥有对自己“信息和数据”的绝对掌控权，人们可以实时的将自己的信息上传到互联网上，而不会受制于某些中心化的机构的控制。  实现基于Web3.0社交软件App,的账户管理、身份认证、安全社交、安全共享、隐私保护、安全监管等。  实现有偿模式的有价值内容分享、转发、打偿等。 |

**第二部分 作业答疑及课程验收**

**1.答疑辅导：**课程设计相关问题需要答疑辅导，请同学们邮件、电话或微信咨询，老师给予及时响应和回复。

**2.作业提交：**课程验收前每个组长以组为单位向任课老师提交：（1）选题项目代码及执行程序；（2）项目技术内容PPT；（3）填写好的课程评分表。（4）项目材料以压缩文件提交，要求格式：XXXX项目名称-组长姓名-联系电话，验收前拷贝到老师电脑，随后由任课老师交教学主管老师留存备查。

**3.验收时间地点：**2021年09月09日（星期四）8：00-12：00， 14：00-18：00.地点：教2-339。

**4.课程验收：**课程验收按选题顺序进行，先[2018211801-2018211803]和2018211806班验收，后[2018211804-2018211805]班验收，验收时保持1-2组人员候场，验收完成的同学离场。

**5.注意事项：**作业里面需要准备并提交项目技术PPT（以备核验），**但鉴于时间紧张，课程验收时不讲PPT，只演示编程实现的代码结构及执行程序。**

**祝大家身体健康，学习进步！**

**任课老师：马兆丰 博导/硕导**

**所在学院：网络空间安全学院**

**电子邮件： mzf@bupt.edu.cn**

**电话/微信：13718841885**

**2021-08-08**