****



**《专业课程设计》任务书**

**2022-2023 第一学期**

**班级：B190307**

**指导教师：**张洁

**指导单位：**计算机学院、软件学院、网络空间安全学院

**编程语言**：可自选，例如Visual C++，C，JAVA等

**日 期：**第9-10周（2022.10.24-2022.11.06）

2022年10月

**一、专业课程设计要求**

本课程主要涉及《网络信息安全》，其他相关课程有《密码学》、《操作系统结构分析》、《网络编程》、《计算机网络与通信》等。知识点涵盖对称密码体制、非对称密码体制、IPSec安全协议、SSL安全协议、S/MIME、PGP、防火墙原理与技术、入侵检测系统、Socket编程等。

专业课程设计的目的是使学生在学习了程序设计和信息安全专业基础课程的基础上，综合运用所学的方法和理论，编写一定难度的网络安全相关的程序，从软件的分析、设计到编制调试，要求学生把信息安全、计算机网络理论知识、编程语言以及程序设计的方法等结合起来做出一个关于安全方面的应用程序（具体的内容会根据具体情况有所变动）。并通过课程设计提高学生的查阅资料、自学和独立分析问题与解决问题的能力，加深对理论知识的理解，利用仿真软件或实验系统对信息安全系统进行模拟和预测，验证并掌握信息安全学科中重要的基础理论与方法，为今后从事相关方面的工作奠定基础。

在2周的时间内，每位学生需要先完成老师布置的实验课程，在此基础上，学生以小组为单位开展拓展课题的设计。小组中的每位同学通过查阅相关资料、与同学讨论、老师辅导答疑合作完成一个课题。在完成课题的过程中，选择合适的开发平台，完成需求分析、系统软件、系统实现，最后完成课程设计报告，提交可运行的软件。教师在最后对学生进行答辩。**值得强调的是：最后每位同学都要提交一份设计报告和源文件（代码），并且另外以附件形式提交布置的实验课程结果电子文档。**

专业课程设计在OBE教学理念指导下对毕业要求指标点的支撑关系如下：

* 毕业要求2 问题分析：能够应用数学、自然科学和工程科学的基本原理，识别、表达、并通过文献研究分析信息安全领域的复杂工程问题，以获得有效结论。

2.2 M 能够根据给出的实际工程案例发现问题、提出问题及问题分析，能够针对具体的信息安全领域复杂工程问题进行需求分析和描述。

* 毕业要求3 设计/开发解决方案：能够设计针对信息安全领域复杂工程问题的解决方案，设计满足特定指标要求的软硬件系统，并能够在设计环节中体现创新意识，考虑社会、健康、安全、法律、文化以及环境等因素。

3.3 M充分理解信息安全领域软硬件系统的基础上，能够设计或开发满足特定需求和约束条件的信息安全系统、模块或算法流程，并能够进行系统级优化。

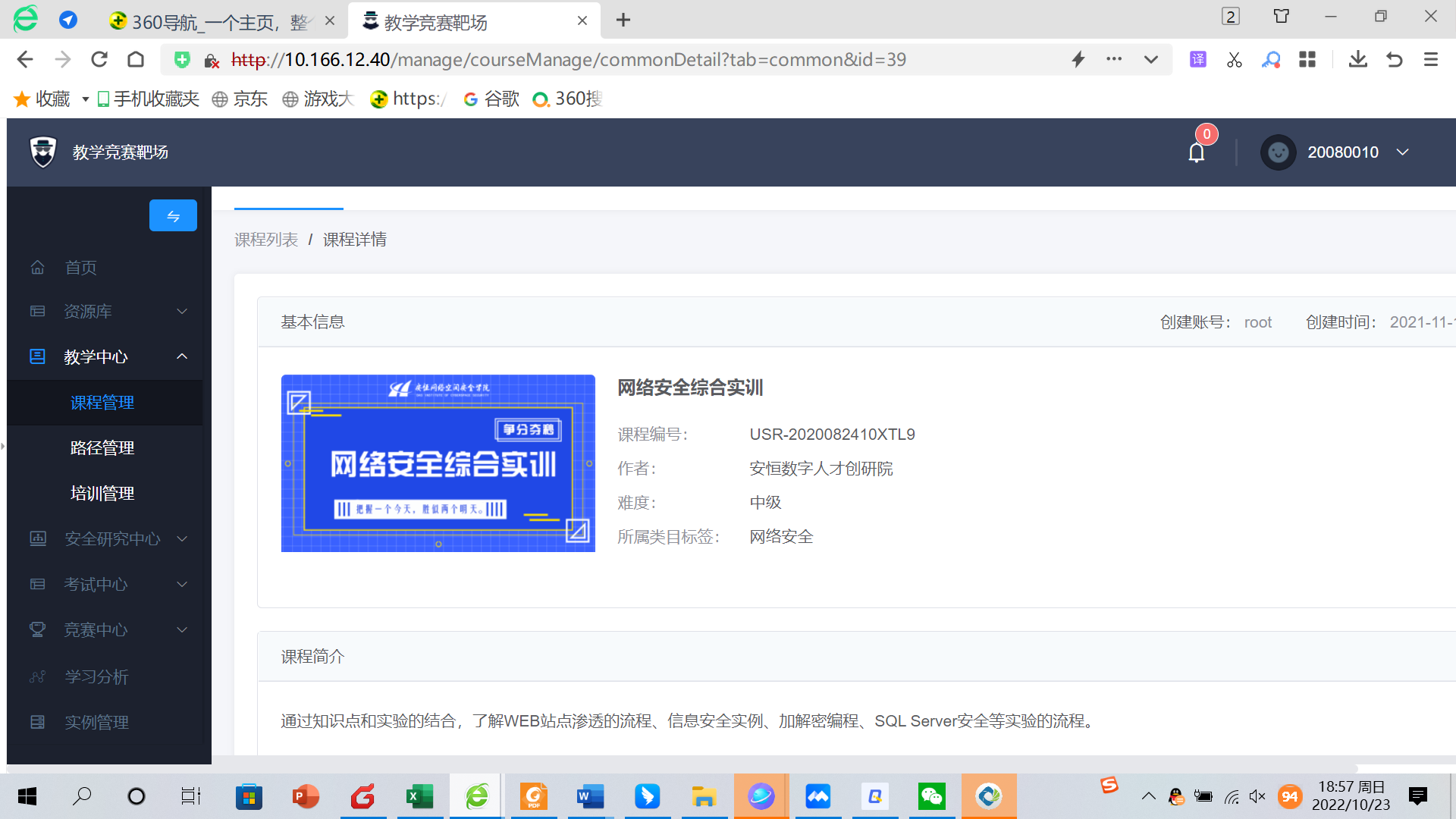
* 毕业要求5 使用现代工具：能够针对复杂工程问题，开发、选择与使用恰当的技术、资源、现代工程工具和信息技术工具，包括对信息安全领域复杂工程问题的预测与模拟，并能够理解其局限性。

5.2 H能够分析比较所使用的技术、资源和工具的优势和不足，并理解与表述问题解决方案的局限性。

* 毕业要求10 沟通：能够就信息安全领域复杂工程问题与业界同行及社会公众进行有效沟通和交流，包括撰写报告和设计文稿、陈述发言、清晰表达或回应指令。并具备一定的国际视野，能够在跨文化背景下进行沟通和交流。

10.3 H 能够就复杂工程问题具备较强的沟通能力和表达能力，能够结合复杂工程问题撰写报告、设计文稿，能够清晰陈述观点和回答问题。

**二、实验课程内容**



本次专业课程设计实验课程为安恒平台的《网络安全综合实训》，通过知识点和实验的结合，了解WEB站点渗透的流程、信息安全实例、加解密编程、SQL Server安全等实验的流程。每位同学需完成课程中的每一道实验，并在完成课程所有内容后，**以附件形式提交实验课程结果的电子文档，请参考《专业课程设计附件》。**

**三、专业课程设计课题内容及课题分配**

本次专业课程设计的题目包含6道题目，每位同学需完成其中一道题目。

**3.1 课题内容**

**题目1：密钥管理系统**

**（一）课题内容**

设计一个密钥管理系统，可以完成密钥生成和管理。

**（二）课题要求**

1.可以生成随机数，必要时可以生成大素数；

2.检测密钥和密码的安全性能；

3.密钥的加密保存和管理；

4.生成公钥对；

5.可以对密钥进行签名。

**题目2： 多功能数字签名系统**

**（一）课题内容**

该系统实现一个多功能的数字签名系统。

**（二）课题要求**

1.对文件进行签名，生成一个独立于原文的签名文件；

2.可以对文件进行签名，在文件后追加签名信息；

3.能够比对已经实施的签名，防止进行重复的签名，这里指的是进行hash以后的值，或者说是签名得到的最后的签名值，以防止重放攻击‘

4.具有密钥管理的功能，比如密钥的生成、导入、导出；

5.对私钥加密保护。

**题目3：Hash算法的设计与实现**

**（一）课题内容**

理解和掌握密码学中哈希算法的过程和综合应用，重点体现在MD5和SHA1的综合应用。

**（二）课题要求**

1.采用hash算法（包括MD5及SHA1两种）计算明文摘要；

2.实现对相同或不同明文所产生摘要的差异比较；

3.要求界面简洁、交互操作性强。

**题目4： U盘加密系统**

**（一）课题内容**

实现一个对u盘进行完全加密或者部分加密的系统。

**（二）课题要求**

1.对u盘进行部分或者全部加密；

2.采用对称加密算法进行u盘数据加密；

3.对称加密算法的密钥要用口令或者公钥加密；

4.可以将部分加密的u盘文件加载为一个新的虚拟磁盘。

**题目5：网络监控与管理软件设计**

**（一）课题内容**

设计一个网络监控和管理系统，能够对所监控的系统进行必要的控制。

**（二）课题要求**

1.可以远程对对方主机进行操作；

2.能够进行监控机和被监控机之间的通行；

3.能够上传文件到指定的地址；

4.能够下载特定的文件。

**题目6：CA系统**

**（一）课题内容**

实现一个CA系统，可以接受用户的认证请求，安全存储用户信息，记录储存对用户的一些认证信息，给用户颁发证书，可以吊销。

**（二）课题要求**

1.接受用户的提交申请，提交时候让用户自己产生公钥对；

2.接受用户的申请，包括用户信息的表单提交，公钥的提交；

3.在对用户实施认证的过程中，储存相应的电子文档，比如证书、营业执照的扫描文档；

4.通过验证的给予颁发证书；

5.用户密钥丢失时，可以吊销证书，密钥作废。

**3.2 课题分配**

表1 课题分配表

|  |  |  |  |
| --- | --- | --- | --- |
| **学号** | **姓名** | **组别** | **课题名称** |
| B15070512 | 王剑樵 | 1 | 题目1：密钥管理系统 |
| B19022101 | 王润青 | 2 | 题目2： 多功能数字签名系统 |
| B19030701 | 丁瑾艳 | 3 | 题目3：Hash算法的设计与实现 |
| B19030702 | 冯世玲 | 4 | 题目4： U盘加密系统 |
| B19030703 | 严妍 | 5 | 题目5：网络监控与管理软件设计 |
| B19030704 | 吴则怡 | 6 | 题目6：CA系统 |
| B19030705 | 张承红 | 7 | 题目1：密钥管理系统 |
| B19030706 | 荀文清 | 8 | 题目2： 多功能数字签名系统 |
| B19030707 | 钱徐琨 | 9 | 题目3：Hash算法的设计与实现 |
| B19030708 | 蒋昕怡 | 10 | 题目4： U盘加密系统 |
| B19030709 | 万力桐 | 11 | 题目5：网络监控与管理软件设计 |
| B19030711 | 王嘉政 | 12 | 题目6：CA系统 |
| B19030712 | 田金翌 | 1 | 题目1：密钥管理系统 |
| B19030713 | 朱世涛 | 2 | 题目2： 多功能数字签名系统 |
| B19030714 | 刘海波 | 3 | 题目3：Hash算法的设计与实现 |
| B19030715 | 李成 | 4 | 题目4： U盘加密系统 |
| B19030716 | 李博 | 5 | 题目5：网络监控与管理软件设计 |
| B19030717 | 杨博淳 | 6 | 题目6：CA系统 |
| B19030718 | 汪行健 | 7 | 题目1：密钥管理系统 |
| B19030719 | 张泉林 | 8 | 题目2： 多功能数字签名系统 |
| B19030720 | 陈纪闿 | 9 | 题目3：Hash算法的设计与实现 |
| B19030721 | 陈瑾瑜 | 10 | 题目4： U盘加密系统 |
| B19030722 | 林翔宇 | 11 | 题目5：网络监控与管理软件设计 |
| B19030723 | 郑友恒 | 12 | 题目6：CA系统 |
| B19030724 | 胡志豪 | 1 | 题目1：密钥管理系统 |
| B19030725 | 施蒋帅 | 2 | 题目2： 多功能数字签名系统 |
| B19030726 | 顾雨涛 | 3 | 题目3：Hash算法的设计与实现 |
| B19030727 | 徐方泽 | 4 | 题目4： U盘加密系统 |
| B19030728 | 凌腾飞 | 5 | 题目5：网络监控与管理软件设计 |
| B19030729 | 郭稼逸 | 6 | 题目6：CA系统 |
| B19030730 | 梁其 | 7 | 题目1：密钥管理系统 |
| B19030731 | 蒋璐 | 8 | 题目2： 多功能数字签名系统 |
| B19030732 | 雷昊麟 | 9 | 题目3：Hash算法的设计与实现 |
| B19031614 | 任远哲 | 10 | 题目4： U盘加密系统 |
| B19080419 | 赵仁杰 | 11 | 题目5：网络监控与管理软件设计 |
| B19080422 | 胡东博 | 12 | 题目6：CA系统 |
| B19111509 | 徐子琴 | 12 | 题目6：CA系统 |

**特别说明：**

1. 同一组别为一组，一起完成规定的课题，每组选一名组长负责课题任务分工和统筹；
2. 每位同学的设计报告重点写自己的工作，不可分工不明，不可报告内容相似，课题答辩以组为单位；
3. 报优的同学需要在课题基础上有拓展，或者申请其他适合的课题。
4. 如果有课题变更，请务必在第一次课下课前和老师沟通确认，过期不候。

**四、考核及报告要求**

**1、考核标准：**根据学生平时的上机出勤情况、为上机所作的准备情况、上机时的表现、实验课程完成情况、课题设计程序的完成情况、报告的完成情况、验收答辩时的表现等综合打分。等级为：优秀、良好、中等、及格、不及格。

**2、报告要求：**请参考《专业课程设计报告内容与格式建议版本》

**3、验收答辩考核内容：**

(1) 功能演示（界面友好性和功能完备性）；

(2) 程序结构描述（如：选用的数据结构、功能模块结构关系、类与类之间的关系、函数调用关系、输入输出文件属性描述等）；

(3) 测试数据的准备情况；

(4) 编程过程中遇到的典型问题及解决方案。

**五、参考资料**

[1]陈伟. 网络安全原理与实践[M].北京：清华大学出版社，2014

[2] 谷利泽. 现代密码学教程[M]. 北京：北京邮电大学出版社 ，2009．

[3] 费翔林. 操作系统教程(第五版)[M].北京：高等教育出版社，2014.

[4] 殷肖川．网络编程与开发技术（21世纪大学计算机专业教材）[M]．西安交通大学出版社，2009.

[5]杨庚．《计算机通信与网络》（第2版）[M]．北京：清华大学出版社，2014