**南开大学本科课程教学大纲**

**一、课程信息**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **课程名称** | | 数据安全 | | | | | | | | | |
| **英文名称** | | Data Security | | | | | | | | | |
| **课程代码** | | COMP0187 | | | | | | | | | |
| **课程类别** | | □通识必修课 □通识选修课  □专业必修课 █专业选修课 | | | | | | | | | |
| **学分** | | 2.5 | | **主讲学时** | **32** | **实践学时** | 32 | | **总学时** | | 64 |
| **授课语言** | | █中文 □全英文 □双语 □外语语言类 （单选） | | | | | | | | | |
| **成绩类型** | | █百分制 □等级制（通过/不通过）（单选） | | | | | | | | | |
| **开课单位** | | 网络空间安全学院 | | | | | | | | | |
| **先修课程** | | 密码学 | | | | | | | | | |
| **课程负责人** | | 刘哲理 | | | | | | | | | |
| **课程教材与参考资料** | | | | | | | | | | | |
| **教**  **材** | **作者** | | **名称** | | | **出版社** | | **ISBN** | | **出版时间** | |
|  | |  | | |  | |  | |  | |
| **参**  **考**  **资**  **料** | **作者** | | **名称** | | | **出版社** | | **ISBN** | | **出版时间** | |
|  | |  | | |  | |  | |  | |
|  | |  | | |  | |  | |  | |
|  | |  | | |  | |  | |  | |
|  | |  | | |  | |  | |  | |

**二、中文课程简介**

|  |
| --- |
| （简要介绍课程的目标、主要授课内容、授课对象以及在学生培养中的作用，150—500字。）  面向大三学生，融合密码学基础、安全多方计算、差分隐私、数据库加密系统、密文查询算法、不经意随机存取模型、机密计算等内容于一体，配合一定的实践案例（有配套的视频教程），激发学生对于数据安全的专业兴趣。  通过本课程的学习，将让学生掌握数据安全的基本知识，学会如何从隐私保护和数据合规利用的角度去发现和解决数据安全有关的问题，能够在算法设计和开发过程考虑安全、法律、环境等制约因素，培养信息安全工程师的职业道德和规范，了解国家相关法律法规，不得利用所学技术手段损害公众和国家利益。 |

**三、英文课程简介**

|  |
| --- |
| （中文课程简介的英文翻译版。）  Software security integrates software vulnerabilities, vulnerability analysis, vulnerability exploitation, penetration testing, WEB security, etc., and cooperates with a large number of rich practical cases (with supporting video tutorials) to stimulate students' interest in information security. Through the study of this course, students will develop the basic knowledge of information security attack and defense and practical ability, learn how to discover and solve software security, system security and WEB security related issues from the perspective of vulnerability exploitation, and learn how to use penetration testing tools to evaluate the security of the system. |

**四、课程目标**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| （需根据课程性质，描述课程教学在培养学生在知识、能力、素质等方面的贡献，以及课程思政相关目标。）  目标1：掌握数据脱敏、差分隐私的基本理论与方法，能够设计满足特定安全目标的数据脱敏或者数据合成算法，理解差分攻击等带来的安全风险和危害，能够在算法设计和开发过程考虑安全、法律、环境等制约因素。  目标2：具备动手实践能力，掌握安全多方计算、密文集合运算、联邦学习的理论知识，并能完成相关数据安全分析类项目的实验，能够正确分析实验数据、解释实验过程和实验结果背后的原理。  目标3：理解可证明安全的概念，掌握密码学基本原语、可搜索加密、保留顺序加密、不经意随机存取模型等原理，能够阅读相关前沿学术论文并进行展示，具有一定终身学习和自主学习的能力。  **课程目标与毕业要求对应关系**   |  |  | | --- | --- | | **课程目标** | **毕业要求指标点** | | **目标1** | **3.4在计算机工程项目设计中能够考虑安全、健康、法律、文化及环境等制约因素。** | | **目标2** | **4.4能对实验结果进行分析和解释，并能通过信息综合得到合理有效的结论。** | | **目标3** | **12.2具有自主学习的能力，包括对技术问题的理解能力，归纳总结的能力和提出问题的能力等。** |   注：课程目标可填写对应相应序号，如“目标2”。课程目标不一定与毕业要求一一对应。 |

**五、课程内容与教学安排**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **教学内容** | **学时** | **教学方式** | **对应课程目标** |
| 1 | 第一章 密码技术  1.1 术语符号  1.1.1 常见符号  1.1.2 算法复杂度  1.1.3 P问题和NP问题  1.2 密码技术  1.2.1 基本概念  1.2.2 对称密码  1.2.3 公钥密码  1.2.4 哈希函数  1.2.5 同态加密  1.3 密码应用实践 | 4 | 讲授 | 3 |
| 2 | 第二章 可证明安全性  2.1 可证明安全性  2.1.1 基本概念  2.1.2 敌手能力  2.1.3 安全性定义  2.1.4 安全性证明  2.1.5 安全性模型  2.2 通用可组合安全  2.2.1 基本概念  2.2.2 半诚实安全性  2.2.3 恶意安全性\*  2.2.4 组合性 | 2 | 讲授 | 3 |
| 3 | 第三章 典型密码原语  3.1 承诺  3.2 茫然传输  3.2.1 基本概念  3.2.2 基础构造  3.3 零知识证明  3.4 秘密共享  3.4.1 定义  3.4.2 Shamir秘密共享 | 4 | 讲授 | 3 |
| 4 | 第四章 数据脱敏  4.1 数据脱敏  4.2 可逆脱敏  4.2.1 Prefix算法  4.2.2 Cycle-walking  4.2.3 FPE算法  4.3 数据发布  4.3.1 准标识符  4.3.2 K匿名  4.4 应用实践 | 2 | 讲授 | 1 |
| 5 | 第五章 差分隐私  5.1 基本概念  5.1.1 基本定义  5.1.2 灵敏度  5.1.3 度量指标  5.1.4 安全性  5.2 算法性质  5.3 差分隐私机制  5.3.1 中心化差分隐私  5.3.2 本地化差分隐私  5.4 差分隐私模型  5.4.1 数据收集模型  5.4.2 数据发布模型  5.4.3 分布式数据收集模型  5.5 应用实践 | 2 | 讲授 | 1 |
| 6 | 第六章 密文查询  6.1 可搜索加密  6.2 保留顺序加密  6.3 顺序揭示加密  6.4 应用实践 | 4 | 讲授 | 1 |
| 7 | 第七章 安全多方计算  7.1 基本概念  7.2 姚氏百万富翁问题  7.3 姚氏混淆电路  7.3.1 基本思想  7.3.2 构造方法  7.3.3 执行过程  7.4 混淆电路示例  7.4.1 电路生成  7.4.2 电路求解  7.5 基础MPC协议  7.5.1 BGW协议  7.5.2 GMW协议  7.5.3 Beaver三元组  7.6 MPC应用实践 | 6 | 讲授 | 1 |
| 8 | 第八章 密文集合运算  8.1 基本概念  8.1.1 定义及分类  8.1.2 可交换加密  8.1.3 布隆过滤器  8.1.4 不经意PRF  8.2 密文集合交集运算  8.2.1 基于朴素哈希的PSI  8.2.2 Google PSI方案  8.2.2 低通信非平衡PSI  8.2.3 基于不经意PRF的构造  8.3 OT扩展及高效OPRF构造 \*  8.3.1 预计算技术  8.3.2 OT-扩展  8.3.3 高效OPRF的构造  8.4 密文集合基数运算\* | 4 | 讲授 | 1 |
| 9 | 第九章 隐私保护机器学习  9.1 基本原理  9.2 联邦学习  9.3 安全聚合策略 | 2 | 讲授 | 1 |
| 10 | 第十章 不经意随机存取模型  10.1 典型ORAM模型  10.2 高效ORAM模型设计 | 2 | 讲授 | 1 |
| 11 | 实验一：密码技术应用  内容：同态加密库与代码实现。  性质：验证性  类别：必做  分组：无 | 2 | 上机/实验 | 3 |
| 12 | 实验二：数据脱敏应用实践  内容：可逆数据脱敏。  性质：验证性  类别：必做  分组：无 | 4 | 上机/实验 | 1 |
| 13 | 实验三：数据合成应用实践  内容：基于差分隐私的数据合成算法设计。  性质：验证性  类别：必做  分组：无 | 8 | 上机/实验 | 1 |
| 14 | 实验四：密态数据库应用实践  内容：按照密态数据库，并完成查询算法设计。  性质：综合性  类别：必做  分组：无 | 8 | 上机/实验 | 3 |
| 15 | 实验五：安全多方计算应用实践  内容：基于安全多方计算实现联合分析。  性质：验证性  类别：必做  分组：无 | 8 | 上机/实验 | 3 |
| 16 | 顶级会议论文心得汇报 | 2 | 研讨 | 3 |

注：1.对应的课程目标可填写大纲中第四部分课程目标的相应序号。

2.教学方式填写：讲授、研讨、上机、实验、习题课等内容。

3.实验课程要在教学内容中详细列出每个实验的名称、内容、实验性质（验证性、综合性、设计性）、实验类别（选做、必做）和实验的分组情况等。实践教学课程要写出相应的时间、地点、方式、教学内容等。

**5.1讲授课实施**

课堂授课采用雨课堂工具实施，基于雨课堂进行点名签到、每个知识点实时考核、随机点名问答，活跃课堂气氛。

部分课程内容以学生自学、期末试卷考核为主，学生自学方式以学堂在线慕课学习和录制的视频材料学习为主。

**5.2 上机/实验课实施**

培养学生动手能力，以复现实验、解释实验过程和实验原理为主要目标。

定期抽查学生在实验课堂进行翻转，讲解已做完的实验，引发讨论，加强对知识的理解程度和认知程度。

**5.3 研讨内容实施**

目标：阅读顶会论文，分组研讨分享。

**六、课程考核**

|  |
| --- |
| 请简述本课程考核方案：  （我校推行课程的过程化考核，鼓励采用平时多次考核的方式。过程化考核包括课后书面作业、实践、上机、课堂讨论、课堂作业表现及考试等等。）  课程的考核采用平时成绩考核的形式。  平时成绩占总评成绩100%，包括：   1. 课堂表现：通过雨课堂工具实时答题进行考核，占总评成绩30%，支撑课程目标1、2和3。 2. 点名签到：通过雨课堂工具进行点名签到，占总评成绩的5%，支撑课程目标3。 3. 实验报告：通过对实验课堂展示汇报、实验报告评分等方式完成考核，占总评成绩50%，支撑课程目标1、2和3。 4. 顶会论文分享：通过对课堂研讨表现、思政作业评分等方式完成考核，占总评成绩15%，支撑课程目标3。 |

**七、审批意见**

|  |
| --- |
| **开课单位学术委员会或本科教学指导委员会意见：**  **负责人签字： 日期：** |
| **开课单位分管负责人意见：**  **负责人签字： （单位公章）**  **日期：** |
| **教务处意见：**  **负责人签字： （公章）**  **日期：** |