**中山大学研究生课程教学大纲**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 中文名称 | | 密码学前沿技术 | | | 课程编号 | | DCS5242 | |
| 英文名称 | | Advanced Cryptography | | | | | | |
| 总学时 | | 36学时 其中实验课： 0学时 | | | | | 学分 | 2 |
| 开课院系 | | 计算机学院 | 课程负责人 | 张方国 | 课程性质 | | □必修 ✓选修 | |
| 授课团队 | | 张方国，田海博 | | | | | | |
| 课程类别 | | □公共课 □专业基础课 □专业方向课  □专业技术实践课 ✓选修课 | | | | | | |
| 授课方式 | | 面授课程 | | 授课语言 | | 中文 | | |
| 考核方式 | | 课程设计（大作业） | | | | | | |
| 先修课程要求 | | 密码学 | | | | | | |
| 教学目标（100字以内）  了解现代密码学的研究现状，研究问题和面临的挑战，以及在人工智能、区块链、隐私保护等领域的应用。为保密管理和计算机科学技术，特别是对密码学方向感兴趣的研究生开阔视野。 | | | | | | | | |
| 课程简介（教学内容及基本要求）  本课程主要涉及和讲述如下内容：   * 可证明安全性（3次课） * 椭圆曲线密码体制及其安全性（2次课） * 量子计算对ECC的威胁（1次课） * 后量子密码体制研究现状介绍，基于格的，基于纠错码的，基于同源的，基于多变量方程组的等（4次课） * 区块链原理，共识算法研究，门限密码（签名）等（2次课） * 隐私信息提取（2次课） * 隐私保护的联邦学习（4次课）   在上述内容的讲述中，会涉及到国内密码算法及其研究进展，使同学们充分体会到国内密码研究人员在密码领域的卓越贡献和突出成果，增加同学们对国内密码领域的兴趣，增强保密意识，增加爱国情怀。 | | | | | | | | |
| 教材及主要参考书目、文献与资料 | 近几年的三大密码会（美密，欧密和亚密）及一些主流密码和安全会议上的论文。 | | | | | | | |

注：每门课程都应填写此表。