**《密码分析学》课程教学大纲**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **课程代码** |  | **课程性质** | | **专业选修** |
| **课程名称：** | **密码分析学** | | | |
| **英文名称** | Cryptanalysis of cryptography | | | |
| **学时/学分** | **36/2** | **其中实验/实践学时** |  | |
| **开课单位** | **软件工程学院** | **适用专业：** | **软件工程** | |
| **先修课程** | **无** | | | |
| **大纲撰写人** | **王高丽** | **大纲审核人** |  | |
| **课程网址** |  | **授课语言** | **中文** | |

一、课程说明

《密码分析学》是密码与网络安全专业学生的重要选修课。本课程从安全性分析的角度，评估密码算法的安全性，较全面地介绍对称密码算法的主流分析技术。该课程注重数学模型的构建与编程测试技术的结合，以测试算例CipherFour、高级加密标准AES、数据加密标准DES、哈希函数MD5等对称密码算法为研究对象，系统介绍经典分析技术的数学原理，构造数学模型，并讨论影响复杂度的因素。主要分析方法包括生日攻击、差分分析、线性分析、积分分析、中间相遇攻击、比特追踪法等。每种分析方法以缩减轮数的算法或小版本的算法为例，结合数学原理进行具体分析，并可对小规模算法分析进行编程实现，测试理论模型的合理性，启发学生发现问题，解决问题。

二、课程目标

目标1：能够掌握典型密码分析技术，并对密码算法的安全性进行初步分析与评估。（支撑毕业要求2）

目标2：能够根据复杂应用的安全性需求，综合基础密码算法，提出增强算法安全性的建议。（支撑毕业要求2）

目标3：了解密码与网络安全法律法规的相关知识，能够严格遵守密码与网络安全行业法律法规与职业道德规范、具备强烈社会责任感、爱国精神及团队协作精神。（支撑毕业要求6,8）

二、课程目标与毕业要求的对应关系

|  |  |  |
| --- | --- | --- |
| 毕业要求 | 指标点 | 课程目标 |
| 毕业要求2：问题分析 | 观测点2-1：能够运用数学、自然科学的基本原理及专业工程基础知识，识别和判断软件工程领域中复杂工程问题的关键环节； | 目标1 |
| 观测点2-2：能够运用数学、自然科学和专业工程基础知识的科学原理和数学模型方法，正确表达软件工程领域的复杂工程问题。 |
| 毕业要求2：问题分析 | 观测点2-3：能够借助文献研究，寻求解决专业领域复杂工程问题的多种方案，能够运用本专业知识的基本原理，分析过程的影响因素，并进行方案比较，得出有效结论。 | 目标2 |
| 毕业要求6：工程与社会 | 观测点6-1：了解专业相关领域的技术标准体系、知识产权、产业政策和法律法规，理解不同社会文化对工程活动的影响，树立全面客观的工程社会意识观。 | 目标3 |
| 毕业要求8：职业规范 | 观测点8-1：树立和践行社会主义核心价值观，理解个人与社会的关系，了解中国国情，具有人文社会科学素养和社会责任感、社会主义事业建设者和接班人所肩负的使命感； | 目标3 |
| 观测点8-2：具有科学、严谨、公正的工程职业道德，理解诚实公正、诚信守则的工程职业道德和规范，并能在专业实践中自觉遵守。 | 目标3 |

三、教学内容与学时安排

第一章 现代密码分析学概述（支撑课程目标1,3）

学时：2学时

1.密码算法安全性的概念

2.Kerckhoffs假设

3.常见的攻击模型和攻击思想

要求学生：概述密码分析学的研究对象、密码算法安全性基本含义、分析中常见的假设和原则如Kerckhoffs假设等；概述四种常见的攻击类型、三类攻击方法、密钥恢复攻击的一般模型和攻击思想。

第二章 差分分析的原理与实例分析（支撑课程目标1,2）

学时：6学时

1.差分分析的原理及实例分析

2.DES算法的差分分析

要求学生：理解差分分析相关的基本概念、攻击原理和区分器的一般模型，掌握差分在各个部件的传播特性、S盒差分分布表的定义及程序求解方式。了解对DES的差分分析过程，讨论采样、去噪、恢复密钥各阶段的流程及复杂度分析，结合信噪比，求解成功率。

第三章 哈希函数的典型分析技术（支撑课程目标1,2）

学时：10学时

1.比特追踪法

2.对哈希函数MD5、SHA-1的碰撞攻击

要求学生：理解哈希函数结构的常见攻击及比特追踪法的主要思路。理解对哈希函数MD5、SHA-1的碰撞攻击方法。

第四章 哈希函数SHA-3的碰撞攻击和原像攻击（支撑课程目标1,2）

学时：8学时

1.对哈希函数SHA-3的碰撞攻击

2. 对哈希函数SHA-3的原像攻击

要求学生：理解对新一代哈希函数国际标准SHA-3的碰撞攻击和原像攻击方法。

第五章 截断差分分析的原理及实例分析（支撑课程目标1,2）

学时：2学时

1. 截断差分的基本概念

  2. CipherFour算法的截断差分分析

要求学生：掌握截断差分的基本概念和原理，理解截断差分分析定义形式的缘由，明确截断差分和差分的关系，以CipherFour算法为例，构造4轮截断差分区分器，并进行密钥恢复攻击。

第六章 不可能差分分析的原理及实例分析（支撑课程目标1,2）

学时：2学时

1. 不可能差分分析的基本原理

2. 可能差分路线的自动化搜索

要求学生：掌握不可能差分分析的基本原理和概率模型，综合现有的不可能差分特征的形式，介绍自动化搜索不可能差分路线的主要思路。

第七章 线性分析的原理与实例分析（支撑课程目标1,2）

学时：4学时

1. 线性分析的原理及实例分析

2. 差分-线性分析的原理及实例分析

要求学生：理解线性分析定义形式的缘由，发现S盒输入输出线性分布表的不均匀特性，理解掩码在各个部件的传播特性和线性分析的模型，能编程求解S盒线性分布表。以缩减轮数的DES算法为例，分析如何连接3轮的差分特征和3轮的线性特征得到6轮的差分-线性特征，并结合堆积引理进行偏差计算。

第八章 广义生日攻击的原理（支撑课程目标1,2）

学时：2学时

1. 广义生日攻击

2.4-tree算法

要求学生：理解生日攻击、广义生日攻击的原理，阐述对*n*比特数据分别计算异或和的分割思想，理解4-tree算法。

四、教学方法

首先介绍密码分析学的内涵，向学生全面讲解密码分析学具体包含哪些内容，然后重点介绍其中若干部分的内容，而不是对每个知识点平均分配学时。这门课需要理解的原理偏多，通过实例来讲解概念，来提高学生的学习兴趣。

加大学生在教学中的参与度，提高学生的自主学习能力，使学生从被动学习变为主动学习。在每次课讲解新课之前，由事先指定的学生总结上次课的授课内容，在讲授完新的知识点之后，组织学生进行讨论，教师再点评和总结，教师不直接回答问题，而是以启发和引导为主。鼓励学生课下多查阅资料，提高学生的独立思考能力和终身学习能力。

五、考核方式

1. 课程考核方式

课程成绩由两部分组成：平时成绩50%和考试成绩50%。其中，平时成绩具体包括：上课提问10%、作业10%、随堂测试20%、课上展示10%。

1. 课程目标与考核方式对应关系

| **考核方式**  **课程目标** | **期末考试** | **上课提问** | **作业** | **随堂测试** | **课上展示** |
| --- | --- | --- | --- | --- | --- |
| **课程目标1** | √ | √ | √ | √ | √ |
| **课程目标2** | √ | √ | √ | √ | √ |
| **课程目标3** | √ | √ |  |  |  |

六、推荐教材和参考资料

1. 推荐教材：

《密码分析学》，主编：王美琴，科学出版社，2024年。

2. 参考书目：

（1） 《分组密码的攻击方法与实例分析》，李超、孙兵、李瑞林著，科学出版社，2010年。

（2） 《A Salad of Block Ciphers》, Roberto Avanzi, 2017.08。

（3） 《The Block Cipher Companion》, Lars R. Knudsen, Matthew J. B. Robshaw, 2011年。

（4） 在密码学顶级会议正式发表的论文等。

## 七、评分标准【请按照本门课程采用的课程考核方式选择下表之一填写】（具体分段可以根据实际情况调整）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **课程目标** | **评分标准** | | | | |
| **90-100** | **80-89** | **70-79** | **60-69** | **0-59** |
| **课程目标1**  **（占70%）** | 非常熟练掌握差分分析、线性分析原理和区分器的一般模型，非常熟练掌握差分、掩码在各个部件的传播特性，能编程求出S盒的差分分布表和线性分布表，非常熟练掌握截断差分分析、不可能差分分析的原理，非常熟练掌握比特追踪法和对MD5、SHA-1的碰撞攻击方法、对SHA-3的碰撞攻击和原像攻击方法，非常熟练掌握广义生日攻击的原理。 | 熟练掌握差分分析、线性分析原理和区分器的一般模型，熟练掌握差分、掩码在各个部件的传播特性，能编程求出S盒的差分分布表和线性分布表，熟练掌握截断差分分析、不可能差分分析的原理，熟练掌握比特追踪法和对MD5、SHA-1的碰撞攻击方法、对SHA-3的碰撞攻击和原像攻击方法，熟练掌握广义生日攻击的原理。 | 掌握差分分析、线性分析原理和区分器的一般模型，掌握差分、掩码在各个部件的传播特性，能编程求出S盒的差分分布表和线性分布表，掌握比特追踪法和对MD5的碰撞攻击方法、对SHA-3的碰撞攻击和原像攻击方法。 | 了解差分分析、线性分析原理和区分器的一般模型，了解差分、掩码在各个部件的传播特性，了解比特追踪法和对MD5、SHA-3的碰撞攻击方法。 | 缺乏对差分分析、线性分析原理的了解，缺乏对差分、掩码在各个部件的传播特性的了解，缺乏对比特追踪法等技术的了解。 |
| **课程目标2**  **（占25%）** | 能够提出增强密码算法安全性的四个建议。 | 能够提出增强密码算法安全性的三个建议。 | 能够提出增强密码算法安全性的两个建议。 | 能够提出增强密码算法安全性的一个建议。 | 不能提出增强密码算法安全性的建议。 |
| **课程目标3**  **（占5%）** | 非常熟悉密码学与网络安全方面的法律法规和主要制度。 | 熟悉密码学与网络安全方面的法律法规和主要制度。 | 部分熟悉密码学与网络安全方面的法律法规和主要制度。 | 了解密码学与网络安全方面的法律法规和主要制度。 | 对密码学与网络安全方面的法律法规和主要制度缺乏了解。 |