附件 2

安徽理工大学
本科专业核心课程建设项目

申

报

书

推　荐　专　业　　信息安全

课　程　名　称　《现代密码学》

课 程 负 责 人　　方贤进

填 报 日 期 2016 年 07 月

安徽理工大学 教务处

二〇一六年五月

填 写 要 求

一、以 word 文档格式如实填写各项。

二、表格文本中外文名词第一次出现时，要写清全称和缩写，再次出现时可以使用缩写。

三、有可能涉密和不宜大范围公开的内容不可作为申报内容填写。

四、课程团队的每个成员都须在 “2．课程团队”表格中签字。

五、“11．承诺与责任”需要课程负责人本人签字.

1．课程负责人情况

<table>
<tr><td rowspan="6">基本情况</td><td>课程负责人</td><td>方贤进</td><td>性 别</td><td>男</td><td>出生年月</td><td>1968-11</td></tr>
<tr><td>最终学历</td><td>研究生</td><td colspan="2">专业技术职务</td><td colspan="2">教授</td></tr>
<tr><td>学 位</td><td>博士</td><td colspan="2">行政职务</td><td colspan="2">副院长</td></tr>
<tr><td colspan="2">所在院系及专业</td><td colspan="4">计算机科学与工程学院 信息安全专业</td></tr>
<tr><td>电子邮箱</td><td colspan="5">xjfang@aliyun.com</td></tr>
<tr><td>研究方向</td><td colspan="5">网络与信息安全，智能计算</td></tr>
<tr><td>教学情况</td><td colspan="6">主要从近五年本课程教学、实践；主要讲授的课程、承担的实践性教学任务；主持的教学研究课题；教学研究论文及编写教材几方面说明。
本课程教学、实践：自 2012 年起一直主讲《现代密码学》同时承担该课程的实验教学。
主讲课程及实践教学包括：《计算机科学导论》、《计算机安全与密码学》（研究生课程）、《Linux 操作系统服务器管理》、《人工智能导论》、《计算机网络》、《计算机网络安全》、《Linux 开发基础》、《Visual Foxpro 程序设计》、《服务器架构、配置与管理实训》，指导 40 余人次信息安全专业本科生毕业设计及毕业实习。
教学研究课题：
(1)基于 Linux 硬件防火墙实验仪器的研制（2010jyxm090），主持，201101~201212.
(2)信息安全专业综合改革试点项目（zy201418），主持，201401~201812.
教学研究论文：
(1)方贤进,潘地林. 建立高等学校计算机学科的教学、开发平台. 安徽理工大学学报(自然科学版), 2005, 25(3): 53~56.
(2)方贤进. 再谈基于 Open source 技术的网络安全实验专题设计 . 计算机教育, 2008(18): 6~7.
(3)方贤进，郑诚. TCP/IP 网络综合实验室建设方案. 安庆师范学院学报(自然科学版),2005, 11(2): 75-78.
(4)何礼富，方贤进. 计算机专业本科毕业设计(论文)存在的问题及思考. 巢湖学院学报, 2007,9(6): 151~153.
(5)张柱，方贤进. 网络实践自学平台的设计与搭建. 计算机时代, 2009,12: 47~49.
(6)吴艳婷，方贤进. 计算机基础课程中信息系统安全实验专题的设计. 安庆师范学院学报(自然科学版), 2013, 19(1): 120-122.
(7)吴艳婷，方贤进. Linux 系统中的口令加密函数及其应用. 电脑知识与技术, 2015, 11(35): 48~49.
(8)吴艳婷，方贤进. 《计算机导论》实验设计——数据在计算机内存中的存储形式. 安庆师范大学学报（已录用）.
主编教材：
(1)《Linux 服务器管理与配置》, 2009.8, 国防科技大学出版社, ISBN: 978-7-81099-863-9
(2)《数据结构(C 语言描述)》，2010.9，国防科技大学出版社, ISBN: 978-7-81099-803-1</td></tr>
</table>

学术研究 工程研究 工程实践情况	主要从近五年学术研究 ；工程研究； 工程实践情况几方面说明。 **承担的科研项目：** (1)国家自然科学基金面上项目，差分隐私高维数据发布理论与方法研究(61572034)，2016/01~2019/12、在研、主持. (2)国家自然科学基金青年基金项目，基于树突细胞行为模型的僵尸程序检测方法研究(61402012)、2015/01-2017/12、在研、参与(第二承担人). (3)国家自然科学基金科学部主任基金项目，基于生物免疫学中危险理论的入侵检测研究(61240023)、2013/01-2013/12、已结题、主持. (4)安徽省高等学校省级自然科学基金重点项目，集成智能算法的入侵检测/防御系统研究（KJ2010A095）、2010/01-2011/12、已结题、主持. **近 5 年发表的主要学术论文：** (1)王丽，**方贤进**，刘佳. 树突细胞算法的运行时间属性分析. 计算机应用研究，2016，33(1): 17~30. (CSCD) (2)Li Wang, **Xianjin Fang**. *The Detection of P2P Bots Using the Dendritic Cells Algorithm*. Proc. of 2015 International Conference on Estimation, Detection and Information Fusion (ICEDIF2015), 299-302, Haerbin, China, 2015.01.10-2015.01.12. (EI) (3)**Fang Xianjin**, Wang Li. *Theoretical investigation on the dendritic cells algorithm*. Journal of Beijing Institute of Technology(English Edition), 2014, 23（3）: 401-406. (EI) (4)**Fang Xianjin**, Song Danjie. *Dendritic Cells Algorithm and Its Application to Nmap Portscan Detection*. China Communications, 2012, 9(3): 145-152. (SCI) (5)**Xianjin Fang**, Jia Liu. *Input Data Preprocessing for Bots Detection Using the Dendritic Cells Algorithm*. Proc. of 2013 6th International Congress on Image and Signal Processing, CISP2013, 1362-1366, Hangzhou, China, 2013.12.16-2013.12.18. (EI) (6)**Xianjin Fang**, Lingbing Liu. *Integrating artificial intelligence into Snort IDS*. Proc. of 2011 3rd International Workshop on Intelligent Systems and Applications, ISA2011, 1-4, Wuhan, 2011.05.28-2011.05.29. (EI) (7)**方贤进**，蔡妙琪，基于人工免疫系统的入侵检测研究，计算机工程，2013，39(11): 136-138. (CSCD) (8)杨高明，**方贤进**，陆奎，王静. 面向函数依赖的隐私保护研究. 计算机工程与科学，2015, 37(11): 2154~2161. (CSCD) (9)党华箏，**方贤进**. DCA 自动数据预处理技术研究. 计算机工程与应用，2014，50(19): 85-88. (CSCD) (10)**方贤进**，刘凌冰，慕学海，王兴旺. 一般克隆选择算法的概率性收敛研究. 计算机应用研究, 2011, 28(1): 121~123. (CSCD) (11)**方贤进**，李龙澍，钱海. 一种基于接种疫苗的克隆选择算法. 计算机工程，2011，37(9): 190~192. (CSCD)

2、课程团队

<table>
<tr><td rowspan="4">团队基本情况</td><td>姓 名</td><td>性别</td><td>出身年月</td><td>专业技术职务</td><td>在本课程中承担的工作</td><td>签字</td></tr>
<tr><td>葛斌</td><td>男</td><td>197505</td><td>教授</td><td>承担《密码学》先修课程《信息论与编码》教学</td><td></td></tr>
<tr><td>赵宝</td><td>男</td><td>198206</td><td>讲师</td><td>承担《密码学》先修课程《信息安全的数学基础》教学</td><td></td></tr>
<tr><td>周强</td><td>男</td><td>197706</td><td>讲师</td><td>承担《计算机网络安全》教学</td><td></td></tr>
<tr><td>课程团队整体情况</td><td colspan="6">主要从近五年本课程教学、实践；主要讲授的课程、承担的实践性教学任务；主持的教学研究课题；教学研究论文及编写教材；学术研究 ；工程研究； 工程实践情况几方面说明。
本课程教学、实践：团队中的葛斌教授承担本课程的先修课程《信息论与编码》教学，同时承担本课程的后续课程《计算机网络》、《网络安全协议理论与技术》的教学工作。赵宝讲师自 2012 年起一直主讲《现代密码学》的先修课程《信息安全的数学基础》。
课程团队主讲课程及实践教学包括:《数据库系统概论》、《C 语言程序设计》、《专业方向课程设计》、《计算机网络实训》、《物联网技术》。《入侵检测与防范技术》、《TCP/IP 网络编程》、《虚拟现实技术》、《Oracle 数据库》、《计算机导论》、《Linux 系统开发基础》、《计算机网络安全》、《数据库应用系统开发》、《操作系统》、《网络安全协议与标准》、《算法分析与设计》、《Android 系统程序设计》、《Linux 服务器配置与管理》、《数据结构》、《数据仓库与数据挖掘》、《编译原理》、《计算机文化基础》、《VFP 程序设计》和《C 语言程序设计》等课程。指导 70 余人次信息安全专业本科生毕业设计及毕业实习。
教学研究课题：
(1)葛斌主持，计算机专业网络方向课程项目驱动法教学改革研究与实践（2015jyxm133），201601~201812.
教学研究论文：
(1)葛斌，张友能，石文兵. 新形势下高校信息安全专业教学改革探讨. 通化师范学院学报，2015, 36(4):94-96
(2)葛斌，孟祥瑞. 高校计算机基础课程教学改革与创新. 安徽理工大学学报(社会科学版), 2005, (6): 88-90.
(3)葛斌，潘地林.《计算机文化基础》课程教学的实践与探讨. 黑龙江科技信息, 2009, 21:210-211.
(4)石文兵，葛斌.数字化校园网站群管理平台下数据传输序列化模型的研究.2014,29(09):82-84
(5)李慧宗,王向前，何叶荣,葛斌.高校经管类专业第二课堂教学体系研究.淮南师范学院学报, 2014,16(05):138-142.
主编、参编教材：</td></tr>
</table>

	(1)**葛斌主编**，《计算机网络》，2008.9，中国科学技术大学出版社，ISBN: 978-7-31202-385-9 (2)**葛斌主编**，《数据结构(C 语言描述)》，2004.4，华东理工大学出版社，ISBN: 978-7-56281-553-2 (3)**赵宝参编**，《Linux 服务器管理与配置》，2009.8，国防科技大学出版社，ISBN: 978-7-81099-863-9 (4)**赵宝参编**，《道路工程 CAD 基础与实例》，2015.12，国防工业出版社，ISBN: 978-7-118-10510-0 **学术研究（科研项目）：** (1)安徽省自然科学基金面上项目，矿山物联网自主组网模型与低耗自组方法研究(1408085ME110)．2014/01~2015/12、在研、**主持人葛斌**. (2)安徽省高等学校省级自然科学研究重大项目，面向矿井电机车无人驾驶系统的机车精确定位技术的研究(KJ2013ZD09)．2013/01~2014/12、结题、**主持人葛斌**. (3)安徽省高等学校省级自然科学研究重点项目，Zigbee 技术在矿井安全监控系统中的应用研究(KJ2012A096)．2012/01~2013/12、结题、**主持人葛斌.** (4)国家自然科学基金项目，煤矿井下物联网感知层感控异构融合理论与技术基础研究(61170060)．2011/01~2015/12、结题、参与(**葛斌为第三承担人**). (5)教育部人文社会科学研究项目，社会化标注环境下的标签层次关系发现方法研究(13YJCZH077). 2013/01~2014/12、结题、参与(**葛斌为第二承担人**). **学术研究（发表的学术论文）：** (1)**Bin Ge**, Kai,Wang, Jianghong Han. Improved RSSI positioning algorithm for coal mine underground locomotive, Journal of Electrical and Computer Engineering , 2015，38（2）：145-152. (EI) (2)**Ge Bin**, Wang Kai and Han Jianghong. Research of Underground Mine Locomotive Positioning Algorithm Based on RSSI, Journal of Software Engineering，2015 ,9（3）:598-609. (EI) (3)**Ge Bin**, Han Jianghong,. Ant Colony Optimization Algorithm for vehicle routing problem with simultaneous delivery and pickup. Frontiers of Information Technology & Electronic Engineering, 2017, 18(1). (SCI 录用) (4)**Bin Ge**. Detect and Reuse Redundant Nodes for MAC Address Assignment Algorithm in Wireless Sensor Networks. Journal of computers(Taiwan), 2015, 26(3):102-1083. (EI) (5)**Bin Ge**，Kai Wang, Yue Han. A Design for Simulation Model and Algorithm of Rail Transport of Molten Iron in Steel Enterprise，computer modeling & new technologies，2014,18(11):1056-1061. (EI) (6) **GE Bin**, HAN Yue, Bian Chen. Hybrid Ant Colony Optimization Algorithm for Solving the Open Vehicle Routing Problem. Journal of computers(Taiwan), 2015, 26(4):143-150. (EI) (7)**Ge Bin**. Research on Low Consumption Ad Hoc Network Method of Mine

	The Internet of Things，2nd International Conference on Computer Science and Network Technology，2012，pp699-702．December 29-31. (EI) (8)**Ge Bin**、Zhang Shaoxin. Research on Precise Positioning Technology of Mine Locomotive Unmanned Systems，Applied Mechanics and Materials，2013, v397-400 ,pp1602-1605 (EI) (9)**Ge Bin**, Han Jianghong, Wei Zhen, Cheng Lei. A Design of Model and Algorithm of Intelligent Preparation System in Enterprise Railway Shunting Plan, Applied Mechanics and Materials，2013, pp1617-1621 (EI) (10)**Ge Bin**, LI Huizong. The Research on ZigBee-Based Mine Safety Monitoring System，2011 International Conference on Electric Information and Control Engineering，2011，pp1837-1840． (EI) (11)**Bin Ge**, Zhen Wei. The Research on key technologies of Internet of Things on Sensing Mine，2011 International Conference on Consumer Electronics Communications and Networks，2011，pp4555-4558． (EI) (12)**葛斌**，韩江洪，魏臻，程磊，韩越．求解带时间窗车辆路径问题的动态混合蚁群优化算法．模式识别与人工智能．2015，28（7）：641-650. (CSCD) (13)**葛斌**，韩江洪，魏臻，程磊，韩越．最小最大车辆路径问题的动态自适应蚁群优化算法．模式识别与人工智能．2015，28（10）：930-938. (CSCD) (14)**葛斌**，郑建宝，韩江洪．RSSI 辅助三维空间坐标四面体质心定位算法．计算机科学, 2015, 42(4):81-84. (CSCD) (15)**葛斌**，王凯，韩江洪．基于 TDOA 改进的矿山井下机车定位方法．计算机工程与应用， 2015，51(07):244-248. (CSCD)

3、本专业培养目标

培养系统掌握网络及网络安全、系统安全、计算机平台安全、计算机应用软件开发等信息安全理论与信息安全工程的较宽基本理论、基础知识和基本技能，具备在信息系统安全分析、安全方案制定、系统安全评估、安全技术开发等方面从事科学研究和教学、技术开发和管理方面的能力。

具体目标：

1、掌握信息安全领域的基本理论和专业知识；

2、掌握信息安全的基本方法与技能；

3、具有从事信息安全工作的基本能力；

4、了解信息安全技术发展的前沿，具有设计安全网络系统、从事安全产品集成与信息安全产品开发的基本能力，以及较强的知识更新能力；

5、掌握文献检索、资料查询及应用现代信息技术获取相关信息的基本方法；

6、了解相近专业的一般原理和知识；

7、熟悉国家信息产业政策及国内外有关信息安全和知识产权的法律法规。

4、本专业的毕业要求（参考工程教育毕业要求）

一级指标	二级指标
1、基本素质	1.1 思想品德素质：热爱祖国，拥护中国共产党的领导，树立科学的世界观、人生观和价值观；具有责任心和社会责任感；具有法律意识，自觉遵纪守法；具有诚信意识，注重职业道德修养；具有合作精神和团队精神。 1.2 文化素质：具有一定的文化修养，既要具有一定的中华民族传 1.1 函数、极限、微积分等基本的概念、公式及其运算、推理和数学应用能力统优秀文化的修养，也要具有一定的近现代世界文化的修养。 1.3 专业素质：掌握科学思维方法和科学研究方法，具有一定的创新和创业意识，具有较强的事业心和严谨求实的实干精神。 1.4 身心素质：具有良好的身体素质和心理素质。
2、知识要求	2.1 人文社会科学知识：文学、外语、哲学、政治学、社会学、法学、管理学、教育学、心理学、艺术等方面的常识或基本知识。 2.2 自然科学知识：较扎实的数学基础知识和一定的物理学、生物学等基础知识。 2.3 专业知识：专业基础知识：扎实的信息安全数学基础、信息科学基础、信息安全基础知识。专业知识：系统扎实的密码学、网络安全、信息系统安全的基础知识，并在某一方面有所侧重。
3、能力要求	3.1 学习能力：具有自学能力，知识和技术的获取能力。 3.2 分析和解决问题的能力：具有通过理论分析、仿真计算、实验等方法分析和解决信息安全实际问题的能力，即具有信息安全领域的一定的科学研究能力或科技开发能力或服务应用能力。 3.3 创新能力：具有创新意识，具有一定的创造性思维能力和创新实验能力。

5、本课程培养目标

通过密码学理论与方法的讲授，总结出一般原则、思想方法及基本工具，使学生明确密码体制的安全性必须建立在严格的理论基础上，以建立清晰的密码学概念、掌握相应的原理及应用，培养学生利用密码学的基本原理分析和解决实际问题的能力，为今后进行更深入的研究奠定良好的理论基础。贯彻以学生为主体、以教师为主导及“理工融合”的教育理念，注重基础理论，使学生获取一种可以在工程实践中终身受益的理论功底、科学素养和发展后劲；联系实际应用，使学生能够用理论指导实践。将科学方法论和工程方法论以及时代发展对密码学提出的新要求融入教学，结合信息安全实验、课程设计和基地实习，针对不同学生特点，培养灵活思维、科研创新能力以及社会适应能力。

学校一直将本课程列为信息安全专业的核心课程，大力扶植本课程的建设，形成了一支稳定的高水平的教师队伍，不断运用新的教学理念进行教学改革。具体目标为：

课程培养目标	本专业毕业要求	支撑情况
目标 1、掌握现代密码学概念	(1)掌握密码技术的基本思想；	高
	(2)熟悉密码体制的组成结构；	高
	(3)熟悉置换、代替和代数等基本古典密码的原理；	高
	(4)掌握密码体制的分类；	高

	(5)掌握密码安全性的概念。	高
目标 2、掌握分组密码算法及应用	(1)掌握分组密码的基本概念;	高
	(2)掌握 DES 或 AES 或 SMS4 等分组密码算法;	高
	(3)掌握分组密码常用工作模式及其特点;	高
	(4)了解 DES、AES、SMS4 密码的安全性。	中
目标 3、掌握流密码及分析	(1)掌握序列密码的基本概念;	高
	(2)掌握线性移位寄存器序列产生器的结构与序列的伪随机性;	高
	(3)熟悉非线性序列的概念与产生方法;	高
	(4)了解常用伪随机性评价方法;	中
	(5)掌握一种典型序列密码（如 RC4）。	高
目标 4、掌握 HASH 函数及应用	(1)掌握 Hash 函数的基本概念和安全性要求;	高
	(2)掌握 MD5、SHA-1 的算法结构;	高
	(3)掌握 HMAC 的算法结构与应用;	高
	(4)了解 MD5、SHA-1 的安全性。	中
目标 5、掌握公钥密码算法及应用	(1)掌握公钥密码的概念;	高
	(2)熟悉公钥密码基本工作方式;	高
	(3)掌握 RSA 密码、ElGamal 密码和椭圆曲线密码的原理与算法;	高
	(4)了解 RSA 密码、ElGamal 密码和椭圆曲线密码的安全性。	中
目标 6、掌握各种数字签名方案原理及应用	(1)掌握数字签名的概念;	高
	(2)掌握基于 RSA 密码、基于 ElGamal 密码和基于椭圆曲线密码的数字签名方法;	高
	(3)熟悉盲签名的原理，了解盲签名的应用;	高
	(4)了解基于 RSA 密码、基于 ElGamal 密码和基于椭圆曲线密码的数字签名的安全性	中
目标 7、掌握各种认证技术及应用	(1)掌握认证的基本概念;	高
	(2)掌握站点认证、报文源认证、报文宿认证、报文顺序认证、报文内容认证的概念与方法;	高
	(3)了解密码协议的基本概念;	中
目标 8、掌握各种秘钥管理技术及 PKI	(1)掌握密钥管理的基本概念;	高
	(2)熟悉传统密码体制的密钥管理技术;	高
	(3)熟悉公钥密码的密钥管理技术;	高
	(4)了解公钥基础设施 PKI 的概念和应用。	中

6、教学改革与研究

近五年来教学改革、教学研究成果及其解决的问题（不超过十项）

（1）本科生的毕业设计课题来源于《现代密码学》课程建设，2015 届信息安全专业学生辛韵完成了毕业设计课题“DES 算法加解密教学演示系统”，贾倩倩完成了“RSA 算法加解密教学演示系统”。2016 届信息安全专业学生许嘉璐完成了“椭圆曲线加密算法教学演示系统的设计”等课题。

（2）2015 年使用红亚网络试验平台进行信息安全学科竞赛训练。

（3）2015 年购置了一套网络攻防实验教学系统（非实战）。

（4）2016 年免费使用西普的实验吧在线网络攻防教学系统进行信息安全学科竞赛训练，我院注册学生数为 303 人。

（5）学科竞赛取得了较好成绩：2012 年获全国大学生信息安全竞赛优胜奖； 2015 年在合肥工业大学举行的“蓝盾杯”网络安全攻防大赛，获得二等奖；2015 年“智胜杯”网络与信息安全大赛二等奖。

（6）在《安徽理工大学学报》、《计算机教育》、《安庆师范大学学报》、《淮南师范学院学报》发表与本课程相关的教学研究论文 5 篇。

7、课程建设

详细介绍课程持续建设和更新情况

(1)适时更换了《现代密码学》教材。将原来的教材《现代密码学》（杨波编著，清华大学出版社）更换为由谷利泽、郑世慧、杨义先编著的《现代密码学教程》（北京邮电大学出版社，普通高等教育‘十五’国家级教材规划）。

(2)开发了一系列加密、解密算法的演示程序，如 DES 加密、解密、弱秘钥、算法对称性演示系统、Virginia 加密算法的破解程序、大数幂模运算、有限域上大数逆元计算等函数库。

(3)教学课件及教学网站每年更新，参见申报者个人 web 站点：
http://star.aust.edu.cn/~xjfang/crypto

(4)购置了信息安全试验教学系统一套（2011 年）

(5)购置了网络攻防实验教学系统一套（2015 年）

(6)本科生的毕业设计课题来源于《现代密码学》课程建设，2015 届信息安全专业学生辛韵完成了毕业设计课题“DES 算法加解密教学演示系统”，贾倩倩完成了“RSA 算法加解密教学演示系统”。2016 届信息安全专业学生许嘉璐完成了“椭圆曲线加密算法教学演示系统的设计”等课题。

(7)利用学科竞赛促进教学。2012 年获全国大学生信息安全竞赛优胜奖； 2015 年在合肥工业大学举行的“蓝盾杯”网络安全攻防大赛，获得二等奖；2015 年“智胜杯”网络与信息安全大赛二等奖。

8、课程内容

介绍课程内容及各章节对课程培养目标的支撑关系

1、Chapt1, 密码学的概念。包括：（1）密码体制（2）古典密码（3）密码安全性。

2、Chapt2, 分组密码。内容包括：（1）分组密码概念（2）DES 算法（3）AES 算法（4）SMS4 算法(5)分组密码工作模式。

3、Chapt3, 流密码。内容包括：（1）序列密码概念（2）线性移位寄存器序列（3）非线性序列（4）伪随机序列评价（5）典型序列密码介绍。

4、Chapt4, Hash 函数。内容包括：(1)Hash 函数概念(2)MD5、SHA 系列算法：SHA-1，SHA-2（3）HMAC

5、Chapt5, 公钥密码。内容包括：（1）公钥密码概念（2）RSA 密码（3）ElGamal 密码（4）椭圆曲线密码。

6、Chapt6, 数字签名。内容包括：（1）数字签名概念（2）RSA 数字签名（3）ElGamal 数字签名（4）椭圆曲线密码数字签名（5）盲签名

7、Chapt7, 认证。内容包括：（1）认证概念（2）站点认证（3）报文认证（4）密码协议概念

8、Chapt8, 密钥管理。（1）密钥管理概念（2）对称密码的密钥管理（3）公钥密码的密钥管理（4）公钥基础设施 PKI

各章节内容对应于课程培养目标的支撑关系见“毕业要求支撑情况表”。

9、课程资源

介绍课程采用教材及参考书、实践实验器材设备等

教材：谷利泽，郑世慧，杨义先. 现代密码学教程. 北京邮电大学出版社，2015.03.

主要参考书：

(1). Menezes A J. 应用密码学手册. 胡磊等译. 科学出版社，2005.

(2). B. Schneier. Applied cryptograghy second edition: protocols, algorithms, and source code in C. NewYork: John Wiley & Sons, 1996. 中译本：吴世忠，祝世雄，张文政译，

(3). 马春光. 现代密码学教程, 哈尔滨工程大学自编讲义.

(4). 马春光, 武朋. 现代密码学实验教程, 哈尔滨工程大学自编讲义.

实践实验器材设备:

(1) 购置了“信息安全实验教学系统”一套（2011 年）

(2) 购置了“网络攻防实验教学系统”(非实战演练)一套（2015 年）

10、课程评价

自我评价：

“密码学”是信息安全的核心和基础，它不仅与保密性密切相关，而且也与完整性、身份认证与访问控制、数字签名、信息隐藏、审计与追踪、网络安全协议密切相关。申请者通过密码学理论与方法的讲授，总结出一般原则、思想方法及基本工具，使学生明确密码体制的安全性必须建立在严格的理论基础上，以建立清晰的密码学概念、掌握相应的原理及应用，培养学生利用密码学的基本原理分析和解决实际问题的能力，为今后进行更深入的研究奠定良好的理论基础。贯彻以学生为主体、以教师为主导及“理工融合”的教育理念，注重基础理论，使学生获取一种可以在工程实践中终身受益的理论功底、科学素养和发展后劲；联系实际应用，使学生能够用理论指导实践。将科学方法论和工程方法论以及时代发展对密码学提出的新要求融入教学，结合信息安全实验系统，针对不同学生特点，培养灵活思维、科研创新能力以及社会适应能力。

校外同行专家评价：

安徽师范大学数学与计算机学院副院长罗永龙教授评价：“安徽理工大学信息安全本科专业招生在全国高校当中是比较早的，所开设的《现代密码学》课程时间较长，教学内容充实，教学方式灵活，教学效果良好，对全省其他高等院校有示范使用。”

安徽大学计算机科学与技术学院常务副院长仲红教授评价：“安徽理工大学《现代密码学》教学团队，在密码学、网络与信息安全等方面取得了一些教学、科研成果。同时培养了一批具有较高水平的密码、信息安全领域的研究生、本科生。”

11、承诺与责任

申请者及其教学团队郑重承诺，将严格按照《安徽理工大学专业核心课程建设标准》的要求进行课程建设，按照各项考核指标开展课程教学研究与改革、网络资源建设，提升教学质量。

课题组负责人：

二〇一六年七月十日

12、院（部）推荐意见

公章

负责人：

年　　月　　日