信息安全专业攻读硕士学位研究生培养方案

（专业代码:070120 ）

一 培养目标

本专业培养的硕士生应为面向世界、面向未来、服务于信息社会，德智体全面发展的，能从事计算机网络、网络安全、其它形式信息安全技术的教学、科研、高科技工作的信息安全专业人才。具体要求如下:

1、较好地掌握马列主义、毛泽东思想和邓小平建设有中国特色的社会主义理论，坚持四项基本原则，树立正确的世界观、人生观、价值观，遵纪守法，热爱祖国，热爱社会主义。具有良好的道德品质和学术修养，有较强的事业心与责任感。

2、掌握信息安全专业的深厚而广泛的基础理论、独特的理论体系及系统的专业知识，了解本学科目前的学术研究进展与动向，具有独立从事科学研究、教学工作或担任信息安全专业技术工作的能力，服务于信息化社会。

3、掌握一门外国语，并能运用该门外国语比较熟练的阅读本专业的外文资料。

4、具有健康的体魄和心理素质。

二 研究方向

1、密码算法的分析技术与设计技术

2、密码协议的分析与设计

3、网络安全协议

4、PKI理论与实现技术

5、计算机网络攻击及防御技术

三 学习年限

全日制硕士研究生在校学习期限为二年至三年，基本学习年限掌握在三年。

四 应修总学分数

应修总学分：30，其中必修28学分。

五 课程设置（具体见课程设置一览表）

1 必修课

马克思主义理论课3学分

第一外国语4学分、专业外语1学分。

学位基础课、

2、学位基础课　　2门　　7学分

近世代数　3学分

算法数论　4学分

学位专业课　　2门　　7学分

密码算法设计与分析　3学分

网络攻击与防御 4学分

前沿讲座2学分。（具体要求）

3 选修课

指能使研究生拓宽知识面或加深某方面知识而开设的本专业或相关学科课程。鼓励跨学科选修1~2门课程，至多记2学分。

硕士生第二外国语，作为选修课，每周4学时，一学期，计2学分。

体育课作为选修课记1学分。

4 补修课　数论与代数结构

(未学过该课程的跨学科或同等学历的硕士生阶段的必修课)

具体课程设置详见本专业教学计划表。

5 前沿讲座 2学分

①讲座的目的和内容

前沿讲座旨在使硕士生了解本学科和本研究方向的重要学术问题、前沿性问题及这些问题的最新研究方法、技术及进展状况，提高学生参与学术研究的兴趣和学术交流能力。前沿讲座的内容主要包括国内外研究动态、国内外一些重大文献讲座、本领域中的新方法与新思路介绍等。

②前沿讲座的形式

一是硕士生本人做专题综述(讨论班)，二是听取国内外本学科或相关学科做出杰出成绩的专家作系列报告等。可以有讲授、讨论和对话等多种形式。力求生动、活泼。

③前沿讲座的次数

前沿讲座贯穿硕士生培养的全过程。

硕士生听取专家前沿系列报告不少于20学时。从二年级开始，硕士生每学期必须参加专业相关的学术讲座、学术报告和讨论班，提交书面专题综述报告或在讨论班做的学术报告。参加讨论班本人主讲不少于2次，主讲者要写出讲稿，讲稿内容要充实，并有个人见解，能够反映所研究领域最新学术进展情况。

④前沿讲座的考核要求和方式

个人主讲或书面前沿专题报告的考核由参加讲座的老师和指导教师共同进行，评定成绩，并写出评语，考核成绩按优、良、中、及格、不及格五级计分；听取学科或相关专业的前沿报告的考核，要自存个人下载的前沿讲座听课记录表，每次听专家讲学或听学院组织的学术报告时，请专家或学院的组织者签字，以备毕业时存入个人学籍档案。

硕士生满20学时的听专家讲座记录，个人主讲2次或书面报告2篇，考核成绩及格以上者记2学分。

六、中期筛选

硕士生实行中期筛选制度，筛选时间定于第四学期。筛选方式以硕士生作口头汇报，考核小组对该生入学以来的政治思想表现、课程学习情况、科研能力、外国语水平、专业外语水平、论文开题报告进行全面考核，并进行学科综合考试。考核小组对硕士生作出综合评价，给出成绩。

成绩合格者，继续攻读学位；中期筛选成绩不合格者，按《山东大学研究生学籍管理实施细则》有关规定处理。

七 科学研究与学位论文

撰写学位论文是对硕士生科研能力的全面训练，学位论文是衡量硕士生综合能力和能否获得学位的重要依据。硕士学位论文应对所研究的课题有新的见解，表明作者具有从事科学研究工作或独立承担专门技术工作的能力。

硕士生应在导师的指导下，至少用一年左右的时间参加科学研究及撰写学位论文。

1、选题和开题报告

硕士生在导师指导下，于第三学期初完成论文选题工作。研究课题必须具备科学性、创新性和可行性，应强调与国家重大研究项目（如863等）、国家自然科学基金项目、博士点基金项目、省部级以上的重点科研项目、该学科国家重点科研项目等相结合。硕士生应于第四学期初中期筛选时提交论文撰写计划，并向教研室或指导小组做开题报告，经过讨论认为选题合适，计划切实可行，方能正式开展论文撰写工作。

2、定期检查学位论文进展情况

学位论文应在导师的指导下由研究生独立完成。在论文撰写期间，根据论文的进度及研究进展，硕士生应定期报告论文进展情况，导师、指导小组及有关人员参加，帮助硕士生分析论文工作进展中的难点，及时给予指导，促进论文研究工作的顺利进展。

学位论文应在介绍本领域已有成果的基础上有所发展和创新，要求命题正确、论证严谨、数据可靠、文字流畅。

3、认真进行学位论文的全面审查

硕士生应在申请学位论文答辩前3-5个月向本专业和相关专业有关教师、导师、指导小组成员全面地报告学位论文进展情况及取得的成果，广泛征求意见，进一步修改和完善学位论文。

4、严格执行各项规章制度，保证学位授予质量

硕士学位论文完成后，导师、指导小组及院、总(所)学位评定分委员会主席和主管院、主任，按照《山东大学授予硕士、博士学位工作细则》认真组织做好学位论文的审阅和答辩的各项工作，保证学位授予质量。

八 实践环节

学院将提供硕士研究生教学实践、科研实践和社会实践的岗位供研究生选择和锻炼，参加实践不少于32个学时。各岗位负责人要对实践者写出考核评语，合格者记入研究生学籍档案。

1 教学实践 与山东大学数学与系统科学学院信息安全专业的课程、习题、试验课程的安排，适当安排硕士生的教学实践。

2 根据硕士生所作研究论文的研究方向，一般围绕信息安全专业所承担的国家自然科学基金等重要研究项目，鼓励自己选择研究课题的原则。相关的科研实践在山东大学信息安全专业实验室或者在省科学院的山东省计算机网络重点实验室完成。

3 信息社会实践的实验主要围绕IT业公司的信息安全技术与产品开发工作。

附：需阅读的主要经典著作和专业学术期刊目录

（一）专业学术刊物

中国科学	科学通报
计算机学报	软件学报
通信学报	通信技术
密码学进展-CHINACRTPT	电子学报

Journal of Cryptology

Advances in Cryptology_EUROCRYPT

Advances in Cryptology_CRYPTO

Advances in Cryptology_AUSCRYPT

Advances in Cryptologu-ASIACRYPT

Public Key Cryptography (PKC)

Workshop on Selected Area in Cryptography(SAC)

IEEE Transactions on Information Theory

IEEE Symposium on Foundations of Computer Science(FOCS)

ACM Conference on Computer and Communications Security

ACM Symposium on Theory of Computing

Communications of ACM

SIAM Journal on Computing

另外全国性学术会刊、国家重点大学学报及其它相关学科的一级学术刊物，皆在此范围内。

（二）主要经典著作

1 B. Schneier， Applied Cryptography.

2 A. J.Menezes， Handbook of Applied Cryptography.

附：信息安全专业硕士研究生教学计划表

类别		序号	课程编号	课程名称	开课学期	总学时数	学分	授课教师	考核方式
必修课	学位公共课	1	MP09001	科学社会主义理论与实践	1	30	1	马列教学部	考试
		2	MP91001	第一外国语	1-2	216	4	外国语学院	考试
		3	M019002	专业外语			1	数学与系统科学学院	考试
	学位基础课	1	M019003	近世代数	1or2	48	3	数学与系统科学学院	考试
		2	M019107	算法数论	1or3	64	4	展涛、王明强	考试
	学位专业课	1	C019103	密码算法分析与设计	1-2	64	4	王小云	考试
		2	C019112	网络攻击与防御	2	48	3	王美琴	考试
		3	M019001	前沿讲座	2-6		2		考查
选修课		1	M019034	对称密码	2	48	3	王小云	考试
		2	M019035	椭圆曲线基础	2	48	3	王明强	考试
		3	C019104	密码协议	2	48	3	孙秋梅	考试
		4	C019113	公钥密码学	3	8	3	秦静	考试
		5	C019105	PKI原理与关键技术	3	32	2	王明强	考试
		6	C019114	VC-开发	3	48	3	王美琴	考试
		8	C019106	密码实现技术	3	32	2	孙秋梅	考试
		9	M019108	新一代网络安全计算	3	32	2	王美琴	考试
		11	C019115	防火墙原理与配置	3	32	2	王美琴	考试
		12	MP91022	第二外国语	3	72	2	外国语学院	考试
		13	C019116	电子商务	4	48	3	秦静	考查
		14	M019037	信息安全标准与法律法规	4	32	2	孙秋梅	考查

	15	C019108	布尔函数与流密码	4	32	2	王小云	考试
补修课		C019109	数论与代数结构	1	64		王明强	考试