

国家网络安全学院

2016年6月，武汉大学国家网络安全学院依托原武汉大学计算机学院信息安全系、空天信息安全与可信计算教育部重点实验室、网络安全国家级虚拟仿真实验教学中心、网络空间安全智库正式成立。2017年9月在由中央宣传部、中央网络安全和信息化领导小组办公室主办的国家网络安全宣传周上，由第十八届中央政治局常委、中共书记处书记刘云山亲自向时任武汉大学校长窦贤康院士授牌——“一流网络安全学院建设示范项目高校”，充分肯定了武汉大学长期以来在网络空间安全人才培养方面的工作。

武汉大学国家网络安全学院秉承了一贯的网络空间安全学科优势，具有深厚的历史底蕴。2001年，武汉大学创建了全国第一个信息安全本科专业；2003年形成了全国第一个完整的信息安全专业本科、硕士、博士到博士后的人才培养体系；2004年，出版了全国第一套信息安全专业本科教材；2007年信息安全专业获批“国家特色专业建设点”，2008年获批“湖北省品牌专业”，同年获批“空天信息安全与可信计算教育部重点实验室”；2014年牵头11所高校制定的我国第一个“高等学校信息安全专业指导性专业规范”出版发行，同年信息安全专业建设成果获高等教育国家级教学成果奖一等奖，并获批“网络安全国家级虚拟仿真实验教学中心”；2015年成立了武汉大学网络空间安全研究院；2016年1月获批网络空间安全一级学科博士学位授权点，同年6月成立了武汉大学国家网络安全学院；2017年，武汉大学获批国家一流网络安全学院建设示范项目，并与武汉市临空港经济技术开发区签署战略合作协议，合作开展国家网络安全人才与创新基地建设。

武汉大学国家网络安全学院科教平台架构完整，学院下设信息安全系、网络空间安全系、密码科学与技术系；设有三个本科专业：信息安全专业、网络空间安全专业和密码科学与技术专业；拥有网络安全国家级虚拟仿真实验教学中心、空天信息安全与可信计算教育部重点实验室、网络空间国际治理研究基地、省部级平台14个、校企合作平台10余个。与此同时，武汉大学还发起创办了全国网络与信息安全防护峰会、中国信息安全与可信计算学术会议、可信云社区等交流合作平台。

截至2022年9月，学院拥有专职教师55人，其中教授26人，副教授25人，博士生导师29人；聘有中国科学院院士1人、国家级高层次青年人才6人，国家级教学名师1人，国家网络安全优秀个人1人，国家网络安全优秀教师3人，湖北省百人计划、楚天学者及黄鹤英才等入选者15人；为加强学科交叉融合，深入开展产学研合作育人与科研合作，学院建设了一支由校外知名学者与行业专家、企业导师组成的兼职教授队伍。

截至2022年9月，学院有本科生1192人、研究生791人。自2001年信息安全专业创办以来，已为国家输送近5000名网络空间安全各类人才，学生连续在“互联网+”、“挑战杯”、ACM数学建模、全国大学生信息安全竞赛等大赛中屡获大奖，培养的毕业生曾获全球网络安全技术领域国际大奖。

学院以总体国家安全观为指导，面向国家网络安全的中高端人才培养，打破现有学科界限，探索国家、地方、高校、企业合作育人以及协同创新的国际化开放培养模式。

一、计算机类（国家网络安全学院）培养方案

（一）大类

1. 大类名称

计算机类（国家网络安全学院）

2. 大类培养目标及分专业培养目标

本大类面向网络强国战略，立足党和国家对网络空间安全人才的重大战略需求，以“强政治、厚基础、宽口径、高素质、硬能力、重五育”为原则，培养掌握网络空间安全学科和计算机学科的基本理论、基本技术和基本应用，掌握网络空间安全学科的专业知识和专业实践能力，具有坚定民族精神和爱国主义信念、强烈的社会责任感和使命感、高度政治敏感度、开阔的国际视野和洞察力，人格健全、知识宽厚、能力全面，拥有较强的国际交流和沟通能力，未来能够胜任网络空间安全技术保障与治理的一流高素质专门人才。

学院坚持面向“服务总体国家安全观”的培养理念，设有三个本科专业：信息安全专业、网络空间安全专业和密码科学与技术专业，各专业的培养目标如下：

（1）信息安全专业培养目标

本专业瞄准中国公认、国际知名的一流专业建设目标，全面贯彻落实党的教育方针，坚持立德树人，培养学生德、智、体、美、劳全面发展；坚持以总体国家安全观为指导，面向网络强国战略，针对国内外复杂的网络对抗形势和国家网络安全技术保障需求，旨在培养拥有宽广系统的知识结构、扎实的专业基础理论知识与不断创新的素养和能力，掌握自然科学、人文科学、信息科学和相关法律法规基础知识，系统掌握网络空间安全学科和计算机学科的基本理论、技术、应用能力，系统掌握硬件安全、系统安全、软件安全、网络安全和数据安全等信息安全专业知识和专业技能，具有坚定民族精神和爱国主义信念、强烈的社会责任感和使命感、高度政治敏感度，人格健全、知识宽厚、能力全面，具有创新意识和解决复杂工程问题的能力，具备开阔国际视野、团队合作精神和组织管理能力的，“专技术、通攻防、强实战”的高素质专业技术型人才。

毕业生可以进入国内外知名 IT 企业、大型企事业单位和国家重要部门等，从事信息系统开发、信息系统安全设计与分析、信息安全技术咨询与评估、信息安全规划与管理、信息安全产品研发、信息安全攻防对抗等工作，也可以进一步在国内外高水平大学或科研院所读研深造，从事信息安全、网络空间安全、计算机学科相关领域的科学研究工作。

毕业五年后，学生将具有较强的技术开发、科研探索、项目管理和创新创业能力。能够在互联网企业或者信息安全企业从事相关技术研发、项目管理工作，并成为其所处部门的项目负责人、高级信息安全工程师，或安全创业者；在国内外知名高校或科研机构进一步深造成为优秀科研工作者，具备优良的科学探索和研究能力；在国家重要政府决策部门成为核心骨干，具备承担和参与信息安全技术研发和管理的能力。以其所具备的国际视野和洞察力，通过终身学习，未来成为引领信息安全领域的科技创新、产业引导的领军型人才。

（2）网络空间安全专业培养目标

本专业瞄准中国公认、国际知名的一流专业建设目标，全面贯彻落实党的教育方针，坚持立德树人，培养学生德、智、体、美、劳全面发展。坚持以总体国家安全观为指导，面向网络强国战略，针对党和国家对网络空间安全技术及网络空间安全治理的重大战略需求，旨在培养拥有宽广系统的知识结构、扎实的专业基础理论知识与不断创新的素养和能力，掌握网络空间安全和计算机科学的基本理论、技术、应用能力，系统掌握网络空间中内容传播、安全检测与防御等技术，系统掌握网络内容采集、内容分析、社会计算、网络舆情分析和内容安全治理的专业知识和技能，具有坚定民族精神和爱国主义信念、强烈的社会责任感和使命感、高度政治敏感度与法律素养，人格健全、知识宽厚、能力全面，拥有较强的国际交流和沟通能力，具有网络空间安全管控能力的，“懂技术、通法律、善管理”的高素质复合型专业人才。

毕业生可以进入国内外知名 IT 企业、大型企事业单位和国家重要政府决策部门，从事应用系统开发、人工智能算法设计、网络空间安全治理、互联网大数据分析、网络空间安全法律法规建设等领域的系统开发、应用、管理、政策制定等工作，也可以进一步在国内外高水平大学或科研院所读研深造，从事信息安全、网络空间安全、计算机学科相关领域的科学研究工作。

毕业五年后，学生将具有较强的工程实践、科研探索、创新创业和管理协调能力。在 IT 企业中，能够成为其所处部门的项目负责人、高级算法工程师、IT 企业创业者；在国内外知名高校或科研机构进一步深造成为优秀科研工作者，具备优良的工程实践和科学研究能力；在国家重要政府决策部门成为核心骨干，具备承担和参与国家网络空间安全相关政策制定的能力。以其所具备的国际视野和洞察力，通过终身学习，未来成为引领网络空间安全领域的科技创新、产业引导或法律法规政策制定的领军型人才。

（3）密码科学与技术专业培养目标

本专业瞄准中国公认、国际知名的一流专业建设目标，全面贯彻党的教育方针，坚持立德树人，培养学生德、智、体、美、劳全面发展；坚持以总体国家安全观为指导，面向网络强国战略和国家密码发展战略，旨在培养拥有宽广系统的知识结构、扎实的专业基础理论知识与不断创新的素养和能力，掌握自然科学、人文科学、信息科学和相关法律法规的基础知识，系统掌握网络空间安全学科和计算机学科的基本理论、技术、应用能力，系统掌握密码科学与技术基础理论、专业知识和工程实践能力，具备密码科学与技术前沿领域的科研能力和创新意识，具有坚定民族精神和爱国主义信念、强烈的社会责任感和使命感、高度政治敏感度，人格健全、知识宽厚、能力全面，具有良好的团队合作精神和组织管理能力的密码科技高素质专业人才。

毕业生能在密码科学与技术相关的企业、科研部门、高等院校及国家密码管理相关的部门和机构中从事研究、应用、开发和管理等工作，也可进一步在国内外高水平大学或科研院所读研深造，从事网络空间安全、信息安全、计算机科学等相关领域的科学研究工作。

毕业五年后，学生将具有较强的工程实践、科研探索、创新创业和管理协调能力。能够在信息技术企业中从事技术研发和项目管理工作，能够成为其所处部门的项目负责人、密码高级工程师；在国内外知名高校或科研机构进一步深造成为优秀科研工作者，具备优良的工程实践和科学研究能力；能够面向国家重大战略需求，在国家重要政府决策部门成为核心骨干，具备承担和参与国家密码相关政策制定的能力；能够立足国民经济主战场，成为爱国进取和创新思辨的拔尖人才，成为在密码科学与技术相关领域具有国际视野的领军人才和行业骨干。

3. 大类平台课程

网络空间安全导论、网络安全政策与法律法规、数字逻辑与 EDA、数据结构、计算机组成原理、数据库系统及安全、操作系统原理及安全、计算机网络、网络安全。

4. 学制和学分要求

学制：四年。

学分要求：毕业生毕业时必须修满 160 学分。其中，

（1）通识教育课程不低于 12 学分；

（2）公共基础课程学分：信息安全专业不低于 68 学分，网络空间安全专业不低于 70 学分，密码科学与技术专业不低于 68 学分。其中，跨院公共基础课程不低于 4 学分（其中网络空间安全专业不低于 6 学分）；

（3）选修课程学分：信息安全专业不低于 47.5 学分，网络空间安全专业不低于 47.5 学分，密码科学与技术专业不低于 49.5 学分。其中，跨学院选修课学分不低于 6 学分；

（4）实践学分：信息安全专业不低于 46.5 学分，网络空间安全专业不低于 44 学分，密码科学与技术专业不低于 46.5 学分；

（5）创新创业实践学分不低于 2 学分；创新创业教育课程学分不低于 2 学分；

（6）各专业的具体毕业学分要求详见教学培养计划。

5. 学位授予：授予工学学士学位

6. 主要实验和实践性教学要求

学分要求：信息安全专业不低于 46.5 学分，网络空间安全专业不低于 44 学分，密码科学与技术专业不低于 46.5 学分。

平台实践课程：数据结构实验、安全创客实践、计算机设计实践、操作系统设计与实践、计算机网络实践、网络安全实验、毕业设计。

信息安全专业主要实践课程：编程能力综合训练、硬件设计基础、汇编语言与接口设计实验、密码学基础实验、系统安全基础能力实践、软件安全实验、嵌入式系统及安全实践、网络对抗演练、安全创新创业实践。

网络空间安全专业主要实践课程：编程能力综合训练、密码学基础实验、人工智能实验、自然语言处理实验、AI 程序设计实训、内容安全实验、数字取证实验、网络空间安全综合实训。

密码科学与技术专业主要实践课程：编程能力综合训练、密码学基础实验、密码攻防综合实践、哈希函数与对称密码学实验、公钥密码学实验、密码工程实验、密码应用系统设计与测评实验。

7. 毕业条件及其它必要说明

学生毕业时必须修满 160 学分，并完成学校要求的学习实习任务方可颁发本科毕业文凭，成绩符合武汉大学学位授予条件，方可获得工学学士学位证书。

（二）专业

1. 信息安全专业

专业代码：080904K

专业名称：信息安全（Information Security）

专业必修课程：离散数学、汇编语言与接口设计、算法设计与分析、编译原理、密码学、软件安全、系统安全与可信计算、嵌入式系统及安全。

毕业要求：

（1）工程知识

具备坚实的信息安全专业知识体系，包括从事信息及信息安全类工程工作所需的相关数学、自然科学、工程实践和专业知识，有系统的信息安全专业相关的工程实践学习经历，熟悉信息安全的发展现状和趋势，并能够将各类知识应用于解决复杂信息及信息安全类工程问题。

（2）问题分析

掌握信息安全基础理论知识和核心知识，并对本信息安全专业领域新知识、新技术有较敏锐的洞察力；能够应用数学、自然科学和工程科学的基本原理，对复杂工程问题进行识别、分析、归类和表达，掌握文献检索及运用现代信息技术对复杂工程问题进行综合分析与抽象表示和数学建模的能力，以获得有效分析结论。

（3）设计/开发解决方案

掌握综合运用专业基础理论知识、技术方法和实践技巧分析并解决实际的复杂工程问题的能力，具体包括信息系统安全需求分析能力、信息系统安全设计与研发能力、信息系统安全分析与评价能力。

（4）科学研究

掌握基本的科学研究方法与技能，具有探索前沿问题的意识，掌握科研探索的方法，能够针对网络空间安全学科相关的科学问题开展研究，具备对相关复杂问题的分析与解决能力。

（5）使用现代工具

针对信息安全中所涉及的复杂工程问题，合理利用已有的资源和技术，自主开发、选择与使用恰当的技术方法、工程工具，辅助复杂工程问题的预测与模拟、分析建模以及解决方案的设计等、提高复杂工程问题解决的效率，并同时能理解这些预测模拟的局限性。

（6）工程与社会

能够基于信息安全相关工程背景知识进行合理分析，评价专业工程实践和复杂工程问题解决方案对社会、健康、安全、法律以及文化的影响，并理解应承担的责任。能够在设计与开发环节中体现创新性

识，综合考虑社会、健康、安全、法律、文化以及环境等制约因素。

(7) 环境和可持续发展

能够理解和评价针对复杂工程问题的专业工程实践对环境、社会可持续发展的影响。

(8) 职业规范

具有人文社会科学素养、社会责任感，能够在工程实践中理解并遵守工程职业道德和规范，履行责任。

(9) 个人和团队

具有较强的团队合作能力、组织管理能力；能够在多学科背景下的团队中承担个体、团队成员以及领导的角色。

(10) 沟通

能够就信息系统安全复杂工程问题与业界同行及社会公众进行有效沟通和交流，包括撰写报告和设计文稿、陈述发言、清晰表达或回应指令。并具备一定的国际视野，能够在跨文化背景下进行沟通和交流。

(11) 项目管理

理解并掌握基本的管理原理和一般的项目管理方法，具备一定的工程项目规划与管理能力，能够在多约束条件下进行经济高效的管理决策，并进一步在多学科环境中应用。

(12) 终身学习

能够持续关注本专业的前沿发展现状和趋势，学习最新出现的方法与技术，具有自主学习和终身学习的意识，具有不断学习和适应发展的能力。

2. 网络空间安全专业

专业代码：080911TK

专业名称：网络空间安全（Cyberspace Security）

专业必修课程：离散数学、密码学引论、算法设计与分析、人工智能、自然语言处理、社会计算、内容安全、数字取证、法理学、信息安全管理。

毕业要求：

(1) 工程知识

具备坚实的知识体系，包括从事工程工作所需的相关数学、自然科学、工程实践和专业知识，有系统的专业相关的工程实践学习经历，熟悉网络空间安全的发展现状和趋势，并能够将各类知识应用于解决复杂工程问题。

(2) 问题分析

掌握网络空间安全基础理论知识和核心知识，并对本专业新知识、新技术有较敏锐的洞察力；能够应用数学、自然科学和工程科学的基本原理，对复杂工程问题进行识别、分析、归类和表达，掌握文献检索及运用现代信息技术对复杂工程问题进行综合分析与抽象表示和数学建模的能力，以获得有效结论。

(3) 设计/开发解决方案

掌握综合运用专业基础理论知识、技术方法和实践技巧分析并解决实际的复杂工程问题的能力，具体包括网络空间安全系统需求分析能力、网络空间安全设计与研发能力、网络空间安全系统分析与评价能力。能够在设计与开发环节中体现创新意识，综合考虑社会、健康、安全、法律、文化以及环境等制约因素。

(4) 研究

掌握基本的科学研究方法与技能，具有探索前沿问题的意识，能够针对网络空间安全学科相关的科学问题开展研究，具备对相关复杂问题的分析与解决能力。

(5) 使用现代工具

针对网络空间安全中所涉及的复杂工程问题，合理利用已有的资源和技术，自主开发、选择与使用

恰当的技术方法、工程工具，辅助复杂工程问题的预测与模拟、分析建模以及解决方案的设计等、提高复杂工程问题解决的效率，并同时能理解这些预测模拟的局限性。

（6）工程与社会

能够基于网络空间安全相关工程背景知识进行合理分析，评价专业工程实践和复杂工程问题解决方案对社会、健康、安全、法律以及文化的影响，并理解应承担的责任。

（7）环境和可持续发展

能够理解和评价针对复杂工程问题的专业工程实践对环境、社会可持续发展的影响。

（8）职业规范

具有人文社会科学素养、社会责任感，能够在工程实践中理解并遵守工程职业道德和规范，履行责任。

（9）个人和团队

具有较强的团队合作能力、组织管理能力；能够在多学科背景下的团队中承担个体、团队成员以及领导的角色。

（10）沟通

能够就网络空间安全复杂工程问题与业界同行及社会公众进行有效沟通和交流，包括撰写报告和设计文稿、陈述发言、清晰表达或回应指令。并具备一定的国际视野，能够在跨文化背景下进行沟通和交流。

（11）项目管理

理解并掌握基本的管理原理和一般的项目管理方法，具备一定的工程项目规划与管理能力，能够在多约束条件下进行经济高效的管理决策，并进一步在多学科环境中应用。

（12）终身学习

能够持续关注本专业的前沿发展现状和趋势，学习最新出现的方法与技术，具有自主学习和终身学习的意识，具有不断学习和适应发展的能力。

3. 密码科学与技术

专业代码：080918TK

专业名称：密码科学与技术（Cryptographic Science and Technology）

专业必修课程：离散数学、密码学引论、信息安全数学基础、哈希函数与对称密码学、公钥密码学、算法设计与分析、密码算法实现与分析、密码应用系统设计与测评。

毕业要求：

（1）工程知识

能够将数学、自然科学、工程实践和专业密码理论和技术知识用于解决复杂密码工程问题。

（2）问题分析

能够应用数学、自然科学和工程科学的基本原理，识别、表达、并通过文献研究分析复杂密码工程问题，以获得有效结论。。

（3）设计/开发解决方案

能够设计针对复杂工程问题的解决方案，设计满足特点需求的密码系统、密码单元（部件）或软硬件设计工艺流程，并能够在设计与开发环节中体现创新意识，综合考虑社会、健康、安全、法律、文化以及环境等因素。

（4）研究

能够基于科学原理，并采用科学方法对复杂密码工程问题进行研究，包括设计实验、分析与解释数据、并通过信息综合得到合理有效的结论。

（5）使用现代工具

能够针对复杂密码工程问题，开发、选择与使用恰当的技术资源、现代工程工具和信息技术工具，包括对复杂密码工程问题的预测与模拟，并能够理解其局限性。

(6) 工程与社会

能够基于密码工程背景知识进行合理分析，评价专业密码工程实践和复杂密码工程问题解决方案对社会、健康、安全、法律以及文化的影响，并理解应承担的责任。

(7) 环境和可持续发展

能够理解和评价针对复杂密码工程问题的工程实践对环境、社会可持续发展的影响。

(8) 职业规范

具有人文社会科学素养、社会责任感，能够在密码工程实践中理解并遵守密码工程职业道德和规范，履行责任。

(9) 个人和团队

能够在多学科背景下的团队中承担个体、团队成员以及领导的角色。

(10) 沟通

能够就复杂密码工程问题与业界同行及社会公众进行有效沟通和交流，包括撰写报告和设计文稿、陈述发言、清晰表达或回应指令。并具备一定的国际视野，能够在跨文化背景下进行沟通和交流。

(11) 项目管理

理解并掌握密码工程管理原理和经济决策方法，并能在多学科环境中应用。

(12) 终身学习

具有自主学习和终身学习的意识，具有不断学习和适应发展的能力。

计算机类（国家网络安全学院）教学计划

课程类别			课程名称	学分数			学时数			修读学期	备注
				总学分	理论学分	实践学分	总学时	理论学时	实践学时		
通识教育课程	通识必修课程	必修6	人文社科经典导引	2	2	0	32	32	0	1-2	1. 所有学生必须修读《人文社科经典导引》《自然科学经典导引》《中国精神导引》。 2. 所有学生必须选修“中华文化与世界文明”和“艺术体验与审美鉴赏”模块课程，其中“艺术体验与审美鉴赏”模块课程至少选修2学分。 3. 所有学生必须至少修满12学分通识教育课程。
			自然科学经典导引	2	2	0	32	32	0	1-2	
			中国精神导引	2	2	0	32	32	0	1-2	
	通识选修课程	选修6	中华文化与世界文明模块								
			科学精神与生命关怀模块								
			社会科学与现代社会模块								
			艺术体验与审美鉴赏模块								
公共基础课程	公共基础必修课程	必修37	马克思主义基本原理	3	2.5	0.5	52	40	12	2	1. “四史”教育模块包括《党史》《新中国史》《改革开放史》和《社会主义发展史》，要求至少选修1门课程。 2. 带*号课程为同一大类指定选修。
			毛泽东思想和中国特色社会主义理论体系概论	3	2.5	0.5	52	40	12	3	
			中国近现代史纲要	3	2.5	0.5	52	40	12	4	
			思想道德与法治	3	2.5	0.5	52	40	12	1	
			习近平新时代中国特色社会主义思想概论	3	3	0	48	48	0	4	
			形势与政策	2	2	0	32	32	0	1-4	
			体育	4	0	4	128	16	112	1-4	
			大学英语	6	6	0	96	96	0	1-2	
			军事理论与技能	4	2	2	200	32	168	1-2	
			新时代中国特色社会主义劳动教育	2	0.5	1.5	44	8	36	3-4	
			大学生心理健康	2	2	0	32	32	0	1-2(三)	
			国家安全教育	1	1	0	16	16	0	1	
			“四史”教育模块	1	1	0	16	16	0	1-2	
	公共基础选修课程	选修27	高等数学 A1*	6	6	0	96	96	0	1	
			高等数学 A2*	6	6	0	96	96	0	2	
			线性代数 A*	3	3	0	48	48	0	2	
			概率论与数理统计 A*	3	3	0	48	48	0	3	
			大学物理 B*	7	7	0	112	112	0	2-3	
			大学物理实验*	2	0	2	48	0	48	2-3	
	跨学院公共基础课程	必修4/6	程序设计 A	4	2	2	80	32	48	1	1. 跨学院公共基础课程为必修课程，信息安全和密码专业不低于4学分，网络空间专业不低于6学分。 2. 信安和密码专业必修课程：程序设计 A；网安专业必修课程：程序设计 A 和法理学。
			法理学	2	2	0	32	32	0	4	

课程类别				课程名称	学分数			学时数			修读学期	备注
					总学分	理论学分	实践学分	总学时	理论学时	实践学时		
专业教育课程	专业准出课程	大类平台课程	必修19.5	网络空间安全导论	0.5	0.5	0	8	8	0	1	
				网络安全政策与法律法规	0.5	0.5	0	8	8	0	1	
				数字逻辑与EDA	2.5	2	0.5	44	32	12	2	
				数据结构	2	1.5	0.5	36	24	12	2	
				计算机组成原理	3	2.5	0.5	52	40	12	3	
				数据库系统与安全	2.5	2	0.5	44	32	12	3	
				操作系统原理及安全	3	3	0	48	48	0	4	
				计算机网络	3	2.5	0.5	52	40	12	5	
				网络安全	2.5	2	0.5	44	32	12	6	
		专业核心课程	信安专业必修19	离散数学	2.5	2	0.5	44	32	12	2	
				汇编语言与接口设计	2	2	0	32	32	0	3	
				算法设计与分析	2.5	2	0.5	44	32	12	3	
				编译原理	2	1.5	0.5	36	24	12	4	
				密码学	2	1.5	0.5	36	24	12	4	
				软件安全	3	3	0	48	48	0	5	
				系统安全与可信计算	3	2.5	0.5	52	40	12	5	
				嵌入式系统及安全	2	1.5	0.5	36	24	12	5	
			网安专业必修18	离散数学	2.5	2	0.5	44	32	12	2	
				密码学引论	2	1.5	0.5	36	24	12	3	
				算法设计与分析	2.5	2	0.5	44	32	12	3	
				人工智能	2	2	0	32	32	0	4	
				自然语言处理	2	2	0	32	32	0	4	
				社会计算	2	2	0	32	32	0	5	
				信息安全管理	1	1	0	16	16	0	5	
				内容安全	2	2	0	32	32	0	6	
				数字取证	2	2	0	32	32	0	6	
			密码专业必修18	离散数学	2.5	2	0.5	44	32	12	2	
				密码学引论	2	1.5	0.5	36	24	12	3	
				信息安全数学基础	3	2.5	0.5	52	40	12	3	
				哈希函数与对称密码学	2	1.5	0.5	36	24	12	4	
				公钥密码学	2	1.5	0.5	36	24	12	4	
				算法设计与分析	2.5	2	0.5	44	32	12	5	
				密码算法实现与分析	2	1.5	0.5	36	24	12	5	
				密码应用系统设计与测评	2	1.5	0.5	36	24	12	6	
		专业必修实践17		数据结构实验	2	0	2	48	0	48	2	所有专业必修
				安全创客实践③	2	0	2	48	0	48	2 (三)	
				计算机设计实践	1	0	1	24	0	24	4	
				操作系统设计与实践	2	0	2	48	0	48	5	
				计算机网络实践	2	0	2	48	0	48	6	
				网络安全实验	2	0	2	48	0	48	6	
				毕业设计	6	0	6	144	0	144	7-8	

课程类别				课程名称	学分数			学时数			修读学期	备注
					总学分	理论学分	实践学分	总学时	理论学时	实践学时		
专业教育课程	专业准入课程	专业核心课程	信安专业必修实践10	编程能力综合训练	1	0	1	24	0	24	2-5	
				硬件设计基础 ^②	1	0	1	24	0	24	2 (三)	
				汇编语言与接口设计实验	1	0	1	24	0	24	3	
				密码学基础实验	1	0	1	24	0	24	4	
				系统安全基础能力实践 ^②	2	0	2	48	0	48	4 (三)	
				软件安全实验	1	0	1	24	0	24	5	
				嵌入式系统及安全实践	1	0	1	24	0	24	5	
				安全创新创业实践 ^③	2	0	2	48	0	48	7	
			网安专业必修实践9	编程能力综合训练	1	0	1	24	0	24	2-5	
				密码学基础实验	1	0	1	24	0	24	3	
				人工智能实验	1	0	1	24	0	24	4	
				自然语言处理实验	1	0	1	24	0	24	4	
				AI 程序设计实训 ^②	2	0	2	48	0	48	4 (三)	
				内容安全实验	1	0	1	24	0	24	6	
				数字取证实验	2	0	2	48	0	48	6	
			密码专业必修实践9	编程能力综合训练	1	0	1	24	0	24	2-5	
				密码学基础实验	1	0	1	24	0	24	3	
				密码攻防综合实践 ^③	2	0	2	48	0	0	4 (三)	
				哈希函数与对称密码学实验	1	0	1	24	0	24	4	
				公钥密码学实验	1	0	1	24	0	24	4	
				密码工程实验	2	0	2	48	0	48	5	
				密码应用系统设计与测评实验	1	0	1	24	0	24	6	
	专业选修课程	学院内选修课程	信安专业选修	电路与电子技术	2	1.5	0.5	36	24	12	2	1. 信息安全专业推荐选修; 2. 带*课程为特定专业的必修课程, 可以作为其它专业选修课。
				硬件安全综合设计	2	0	2	48	0	48	6	
				智能移动操作系统设计与应用开发 ^②	2	1.5	0.5	36	24	12	4 (三)	
				软件工程	2	1.5	0.5	36	24	12	5	
				软件逆向分析	2	1.5	0.5	36	24	12	6	
				Linux 内核分析与实践	2	1.5	0.5	36	24	12	6	
				移动操作系统安全及应用	2	1.5	0.5	36	24	12	6	
				云计算安全	2	2	0	32	32	0	7	
				信息安全数学基础*	3	2.5	0.5	52	40	12	3	
				信息内容安全	2	2	0	32	32	0	6	
				信息安全前沿技术讲座 ^②	2	2	0	32	32	0	4(三)	
				网络对抗演练	2	0	2	48	0	48	6(下)	

课程类别				课程名称	学分数			学时数			修读学期	备注
					总学分	理论学分	实践学分	总学时	理论学时	实践学时		
专业教育课程	专业选修课程	学院内选修课程	网安专业选修	网络空间安全前沿技术③	1	1	0	16	16	0	4(三)	网络空间安全专业推荐选修
				信息检索技术	2	2	0	32	32	0	5	
				多媒体分析技术	2	1.5	0.5	36	24	12	5	
				新闻安全分析	2	2	0	32	32	0	5	
				大数据处理技术	2	2	0	32	32	0	6	
				网络认知计算	2	2	0	32	32	0	6	
				人工智能安全	2	2	0	32	32	0	6	
				网络空间安全综合实训④	2	0	2	48	0	48	6(下)	
			密码专业选修	可证明安全理论与方法	2	2	0	32	32	0	4	密码理论方向推荐选修课程
				密码协议设计与分析	2	2	0	32	32	0	5	
				后量子密码	2	2	0	32	32	0	6	
				数据安全与隐私保护	2	2	0	32	32	0	6	
				编译原理*	2	1.5	0.5	36	24	12	4	1. 密码应用方向推荐选修课程 2. 带*课程为特定专业的必修课程，可以作为其它专业选修课。
				系统安全与可信计算*	2	2	0	32	32	0	5	
				区块链技术与应用	2	2	0	32	32	0	6	
				密钥管理	2	2	0	32	32	0	6	
		公共专业选修	汇编语言与接口设计*	2	2	0	32	32	0	3	1. 自主选修课程； 2. 带*课程为特定专业的必修课程，可以作为其它专业选修课。	
			汇编语言与接口设计实验*	1	0	1	24	0	24	3		
			人工智能*	2	2	0	32	32	0	4		
			人工智能实验*	1	0	1	24	0	24	4		
			软件安全*	3	3	0	48	48	0	5		
			软件安全实验*	1	0	1	24	0	24	5		
			信息隐藏技术	2	1.5	0.5	36	24	12	5		
			通信原理	2	2	0	32	32	0	6		
			数字取证*	2	2	0	32	32	0	6		
			数字取证实验*	2	0	2	48	0	48	6		
			嵌入式系统及安全*	2	1.5	0.5	36	24	12	5		
			嵌入式系统及安全实践*	1	0	1	24	0	24	5		
			科技论文写作	1	0	1	24	0	24	7		
			专业学习引导与前沿系列讲座	1	1	0	16	16	0	1-6		
			安全创新创业实践④	2	0	2	48	0	48	7		
			互联网创业思维④	2	2	0	32	32	0	7		
	跨学院选修课程	跨学院选修	网络空间安全法⑤	3	2	1	56	32	24	4	1. 至少选修6学分； 2. 推荐选修计算机学院、电子信息学院、遥感信息工程学院的专业选修课； 3. 网安专业推荐选修网络空间安全法与面向对象程序设计；信安专业推荐选修面向对象程序设计。	
			面向对象程序设计	2	2	0	32	32	0	3		

课程类别	课程名称	学分数			学时数			修读学期	备注
		总学分	理论学分	实践学分	总学时	理论学时	实践学时		
毕业应取得 总学分：160 分	信息安全专业：								
	通识教育课程：12 学分；公共基础课程学分：68 学分；专业教育课程学分：80 学分，其中大类平台课程学分：19.5 学分；								
	实践教学学分：46.5 学分，占总学分的：29.063% ；								
	（实践教学学时:1116 学时，占总学时的：38.06%）；								
	选修课程学分：47.5 学分，占总学分的：29.69%；								
	网络空间安全专业：								
	通识教育课程：12 学分；公共基础课程学分：70 学分；专业教育课程学分：78 学分，其中大类平台课程学分：19.5 学分。								
	实践教学学分：44 学分，占总学分的：27.5%								
	（实践教学学时：1056 学时，占总学时的：36.01%）								
	选修课教学学分：47.5 学分，占总学分的：29.69%；								
	密码科学与技术专业：								
	通识教育课程：12 学分；公共基础课程学分：68 学分；专业教育课程学分：80 学分，其中大类平台课程学分 19.5 学分。								
	实践教学学分：46.5 学分，占总学分的：29.063%								
	选修课教学学分：49.5 学分，占总学分的：30.93%								

备注：

1. 带 ④ 字的课程为创新创业类课程。
2. 带 ③ 字的课程为第三学期开设课程。
3. 带 ② 字的课程为跨学院课程。
4. 学生应修读创新创业教育课程（理论）不低于 2 学分，创新创业实践学分不低于 2 学分。
5. 专业选修课程：信安专业专业选修课程不低于 14.5 学分，网安专业专业选修课程不低于 14.5 学分，密码专业专业选修课程不低于 16.5 学分。

二、网络安全试验班培养方案

（一）大类

1. 大类名称

计算机类（国家网络安全学院）

2. 大类培养目标及专业培养目标

本大类面向网络强国战略，立足党和国家对网络空间安全人才的重大战略需求，以“强政治、厚基础、宽口径、高素质、硬能力、重五育”为原则，培养掌握网络空间安全学科的基本理论、基本技术和基本应用，掌握网络空间安全学科的专业知识和专业实践能力，具有坚定民族精神和爱国主义信念、强烈的社会责任感和使命感、高度政治敏感度、完备的法律素养、开阔的国际视野和洞察力，人格健全、知识宽厚、能力全面，拥有较强的国际交流和沟通能力，未来能够胜任网络空间安全治理与技术保障的一流高素质专门人才。

学院坚持面向“服务总体国家安全观”的培养理念，设立网络安全试验班，网络安全试验班的培养目标是对接网络强国战略，采取“新工科”建设思路，依托全国唯一的国家网络安全人才与创新基地，定位高端网络空间安全后备人才培养；以综合性大学多学科交叉融合背景为优势，采取适应网络空间安全拔尖人才培养要求的分阶段本-硕-博衔接式培养、进阶式专业实训、小班教学、导师管理、科教协同、国际交流等特色培养方法；通过试验班建设，探索适应国际化高等教育发展趋势、国家战略发展和网络空间安全学科发展需求、具有武大特色的拔尖人才培养模式。

本试验班依托网络空间安全专业建设基础，培养体系以培养网络空间安全综合分析和设计能力为目标，涉及计算机、通信、数学等专业方向的多学科交叉专业，人才培养的专业知识体系，包括程序设计、计算机系统、网络空间安全学科专业知识、交叉复合型知识、科研创新、校企协同实训等贯通式实践课程。课程设置包括通识教育课、公共基础课、专业大类平台课、专业核心准出课、专业选修课、集中实践环节、综合能力素质拓展模块等课程。

本试验班提供四年制本科教育，授予工学学士学位，实行学分制小班培养模式，在完成专业必修课程后，可根据学生兴趣并结合发展规划，制定个性化专业课程选修方案（包括系统安全、网络安全、内容安全三类特色方向）。同时，注重国际化交流能力培养，支持学生参加各类国际名校访学、交换等计划，组织学术交流活动，指导和鼓励学生积极参加国外学者讲授的暑期课程、国内外优质 MOOC 课程等。

本试验班贯彻落实为党育人、为国育才的教育方针，坚持立德树人，培养德、智、体、美、劳全面发展的建设者；践行新工科教育理念，培养学生掌握和运用自然科学、人文科学和信息科学技术知识的能力，系统掌握网络空间安全学科和计算机学科的基本理论、基本方法、专业技能及应用技术；培养学生探索网络空间安全前沿科技的自主学习能力和解决复杂问题的能力，形成面向总体国家安全观的综合创新能力。

本试验班毕业生能够从事信息系统安全设计与分析、信息安全技术咨询与评估、信息安全规划与管理、网络空间治理、网络内容监管等领域的开发、应用及管理工作；同时可继续攻读信息安全、网络空间安全、计算机科学与技术等相关学科及相关交叉学科的硕士/博士学位。旨在培养毕业生成为具备国际竞争力的网络空间安全领域科学研究、工程技术、行业发展的未来领导者。

3. 大类平台课程

网络空间安全导论、网络安全政策与法律法规、数字逻辑与 EDA、数据结构、计算机组成原理、数据库系统及安全、操作系统原理及安全、计算机网络、网络安全。

4. 学制和学分要求

学制：四年。

学分要求：毕业生毕业时必须修满 160 学分。其中，

（1）通识教育课程不低于 12 学分；

（2）公共基础课程不低于 68 学分；跨院公共基础课程不低于 4 学分；

(3) 实践学分不低于 46.5 学分;

(4) 选修课学分不低于 47.5 学分; 跨学院选修课学分不低于 6 学分;

(5) 创新创业实践学分不低于 2 学分; 创新创业教育课程学分不低于 2 学分;

具体学分要求详见教学培养计划。

5. 学位授予: 授予工学学士学位

6. 主要实验和实践性教学要求

专业实践学分不低于 46.5 学分。

平台实践课程: 数据结构实验、安全创客实践、计算机设计实践、操作系统设计与实践、计算机网络实践、网络安全实验、毕业设计。

主要实践课程: 软件安全实验、密码学基础实验、人工智能实验、内容安全实验、硬件设计基础、系统安全基础能力实践、网络空间安全综合实训、科研创新实训 I&II。

7. 毕业条件及其它必要说明

学生毕业时必须修满 160 学分, 并完成学校要求的学习实习任务方可颁发本科毕业文凭, 成绩符合武汉大学学位授予条件, 方可获得工学学士学位证书。

(二) 专业

网络安全试验班

专业代码: 080911TK

专业名称: 网络空间安全 (Cyberspace Security)

专业必修课程: 软件安全、人工智能、内容安全、系统安全与可信计算、密码学引论、离散数学、算法设计与分析、信息安全管理。

毕业要求:

(1) 工程知识

具备坚实的知识体系, 包括从事工程工作所需的相关数学、自然科学、工程实践和专业知识, 有系统的专业相关的工程实践学习经历, 熟悉网络空间安全的发展现状和趋势, 并能够将各类知识应用于解决复杂工程问题及科学研究问题。

(2) 问题分析

掌握网络空间安全基础理论知识和核心知识, 并对本专业新知识、新技术有较敏锐的洞察力; 能够应用数学、自然科学和工程科学的基本原理, 对复杂工程问题进行识别、分析、归类 and 表达, 掌握文献检索及运用现代信息技术对复杂工程问题进行综合分析与抽象表示和数学建模的能力, 以获得有效结论。

(3) 设计/开发解决方案

掌握综合运用专业基础理论知识、技术方法和实践技巧分析并解决实际的复杂工程问题的能力, 具体包括网络空间安全系统需求分析能力、网络空间安全设计与研发能力、网络空间安全系统分析与评价能力。能够在设计与开发环节中体现创新意识, 综合考虑社会、健康、安全、法律、文化以及环境等制约因素。

(4) 研究

掌握基本的科学研究方法与技能, 具有探索前沿问题的意识, 能够针对网络空间安全学科相关的科学问题开展持续研究, 具备对相关复杂问题的深入分析与有效解决能力。

(5) 使用现代工具

针对网络空间安全中所涉及的复杂工程问题, 合理利用已有的资源和技术, 自主开发、选择与使用恰当的技术方法、工程工具, 辅助复杂工程问题的预测与模拟、分析建模以及解决方案的设计等、提高复杂工程问题解决的效率, 并同时能理解这些预测模拟的局限性。

(6) 工程与社会

能够基于网络空间安全相关工程背景知识进行合理分析, 评价专业工程实践和复杂工程问题解决方

案对社会、健康、安全、法律以及文化的影响，并理解应承担的责任。

（7）环境和可持续发展

能够理解和评价针对复杂工程问题的专业工程实践对环境、社会可持续发展的影响。

（8）职业规范

具有人文社会科学素养、社会责任感，能够在工程实践中理解并遵守工程职业道德和规范，履行责任。

（9）个人和团队

具有较强的团队合作能力、组织管理能力；能够在多学科背景下的团队中承担个体、团队成员以及领导的角色。

（10）沟通

能够就网络空间安全复杂工程问题与业界同行及社会公众进行有效沟通和交流，包括撰写报告和设计文稿、陈述发言、清晰表达或回应指令。并具备一定的国际视野，能够在跨文化背景下进行沟通和交流。

（11）项目管理

理解并掌握基本的管理原理和一般的项目管理方法，具备一定的工程项目规划与管理能力，能够在多约束条件下进行经济高效的管理决策，并进一步在多学科环境中应用。

（12）终身学习

能够持续关注本专业的前沿发展现状和趋势，学习最新出现的方法与技术，具有自主学习和终身学习的意识，具有不断学习和适应发展的研究与研发能力。

网络安全试验班教学计划

课程类别			课程名称	学分数			学时数			修读学期	备注
				总学分	理论学分	实践学分	总学时	理论学时	实践学时		
通识教育课程	通识必修课程	必修6	人文社科经典导引	2	2	0	32	32	0	1-2	1. 所有学生必须修读《人文社科经典导引》《自然科学经典导引》《中国精神导引》。 2. 所有学生必须选修“中华文化与世界文明”和“艺术体验与审美鉴赏”模块课程，其中“艺术体验与审美鉴赏”模块课程至少选修2学分。 3. 所有学生必须至少修满12学分通识教育课程。
			自然科学经典导引	2	2	0	32	32	0	1-2	
			中国精神导引	2	2	0	32	32	0	1-2	
	通识选修课程	选修6	中华文化与世界文明模块								
			科学精神与生命关怀模块								
			社会科学与现代社会模块								
			艺术体验与审美鉴赏模块								
公共基础课程	公共基础必修课程	必修37	马克思主义基本原理	3	2.5	0.5	52	40	12	2	1. “四史”教育模块包括《党史》《新中国史》《改革开放史》和《社会主义发展史》，要求至少选修1门课程。 2. 带*号课程是同一大类指定选修。
			毛泽东思想和中国特色社会主义理论体系概论	3	2.5	0.5	52	40	12	3	
			中国近现代史纲要	3	2.5	0.5	52	40	12	4	
			思想道德与法治	3	2.5	0.5	52	40	12	1	
			习近平新时代中国特色社会主义思想概论	3	3	0	48	48	0	4	
			形势与政策	2	2	0	32	32	0	1-4	
			体育	4	0	4	128	16	112	1-4	
			大学英语	6	6	0	96	96	0	1-2	
			军事理论与技能	4	2	2	200	32	168	1-2	
			新时代中国特色社会主义劳动教育	2	0.5	1.5	44	8	36	3-4	
			大学生心理健康	2	2	0	32	32	0	1-2 (三)	
			国家安全教育	1	1	0	16	16	0	1	
			“四史”教育模块	1	1	0	16	16	0	1-2	
	公共基础选修课程	选修27	高等数学 A1*	6	6	0	96	96	0	1	
			高等数学 A2*	6	6	0	96	96	0	2	
			线性代数 A*	3	3	0	48	48	0	2	
			概率论与数理统计 A*	3	3	0	48	48	0	3	
			大学物理 B*	7	7	0	112	112	0	2-3	
			大学物理实验*	2	0	2	48	0	48	2-3	
	跨学院公共基础课程	必修4	程序设计 A	4	2	2	80	32	48	1	跨学院公共基础课程为必修课程，具体必修课程门数及内容根据专业需要决定。
专业准入课程	大类平台必修课程	必修19.5	网络空间安全导论	0.5	0.5	0	8	8	0	1	
			网络安全政策与法律法规	0.5	0.5	0	8	8	0	1	
			数字逻辑与 EDA	2.5	2	0.5	44	32	12	2	
			数据结构	2	1.5	0.5	36	24	12	2	
			计算机组成原理	3	2.5	0.5	52	40	12	3	
			数据库系统及安全	2.5	2	0.5	44	32	12	3	

课程类别				课程名称	学分数			学时数			修读学期	备注
					总学分	理论学分	实践学分	总学时	理论学时	实践学时		
专业教育课程	专业准出课程	专业核心课程	必修46	操作系统原理及安全	3	3	0	48	48	0	4	
				计算机网络	3	2.5	0.5	52	40	12	5	
				网络安全	2.5	2	0.5	44	32	12	6	
				软件安全	3	3	0	48	48	0	5	
				人工智能	2	2	0	32	32	0	4	
				内容安全	2	2	0	32	32	0	6	
				系统安全与可信计算	3	2.5	0.5	52	40	12	5	
				密码学引论	2	1.5	0.5	36	24	12	3	
				离散数学	2.5	2	0.5	44	32	12	2	
				算法设计与分析	2.5	2	0.5	44	32	12	3	
				信息安全管理	1	1	0	16	16	0	5	
				数据结构实验	2	0	2	48	0	48	2	
				计算机设计实践	1	0	1	24	0	24	4	
				操作系统设计与实践	2	0	2	48	0	48	5	
				计算机网络实践	2	0	2	48	0	48	5	
				网络安全实验	2	0	2	48	0	48	6	
				安全创客实践③	2	0	2	48	0	48	2（三）	
				毕业设计	6	0	6	144	0	144	7-8	
				软件安全实验	1	0	1	24	0	24	5	
				密码学基础实验	1	0	1	24	0	24	3	
				人工智能实验	1	0	1	24	0	24	4	
				内容安全实验	1	0	1	24	0	24	6	
				硬件设计基础③	1	0	1	24	0	24	2（三）	
				系统安全基础能力实践③	2	0	2	48	0	48	4（三）	
				网络空间安全综合实训④	2	0	2	48	0	48	6（下）	
				科研创新实训 I ④	1	0	1	24	0	24	5	
				科研创新实训 II ④	1	0	1	24	0	24	6	
	专业选修课程	学院内选修课程	选修14.5	编译原理	2	1.5	0.5	36	24	12	4	系统安全特色模块
				嵌入式系统及安全	2	1.5	0.5	36	24	12	5	
				嵌入式系统及安全实践	1	0	1	24	0	24	5	
				数字取证	2	2	0	32	32	0	6	网络安全特色模块
				数字取证实验	2	0	2	48	0	48	6	
				通信原理	2	2	0	32	32	0	6	
				社会计算	2	2	0	32	32	0	5	内容安全特色模块
				自然语言处理	2	2	0	32	32	0	4	
				自然语言处理实验	1	0	1	24	0	24	4	
				互联网创业思维④	2	2	0	32	32	0	7	创新创业教育课程
				网络空间安全前沿技术③	1	1	0	16	16	0	4（三）	
				电路与电子技术	2	1.5	0.5	36	24	12	2	
				硬件安全综合设计	2	0	2	48	0	48	6	
				汇编语言与接口设计	2	2	0	32	32	0	3	

课程类别				课程名称	学分数			学时数			修读学期	备注
					总学分	理论学分	实践学分	总学时	理论学时	实践学时		
专业教育课程	专业选修课程	学院内选修课程	14.5	汇编语言与接口设计实验	1	0	1	24	0	24	3	
				软件逆向分析	2	1.5	0.5	36	24	12	6	
				云计算安全	2	2	0	32	32	0	7	
				数据安全与隐私保护	2	2	0	32	32	0	6	
				多媒体分析技术	2	1.5	0.5	36	24	12	5	
				人工智能安全	2	2	0	32	32	0	6	
				大数据处理技术	2	2	0	32	32	0	6	
				网络认知计算	2	2	0	32	32	0	6	
				信息检索技术	2	2	0	32	32	0	5	
	跨学院课程	面向对象程序设计	2	2	0	32	32	0	3	1. 至少选修6学分 2. 推荐选修计算机学院、电子信息学院、遥感信息工程学院的专业选修课		
		网络空间安全法 ^④	3	2	1	56	32	24	4			
毕业应取得 总学分：160分 总学时：2920学时				其中，通识教育课程学分：12；公共基础课程学分：68； 专业教育课程学分：80；大类平台课程：19.5学分 实践教学学分：46.5，占总学分的：29.063 % （实践教学学时：1116，占总学时的：38.22 %） 选修课程学分：47.5，占总学分的：29.688 % （选修课程学时：760，占总学时的：26.027 %）								

备注：

1. 带^④字的课程为创新创业类课程。
2. 带^③字的课程为第三学期开设课程。
3. 带^②字的课程为跨学院课程。
4. 学生应修读创新创业教育课程（理论）不低于2学分，创新创业实践学分不低于2学分。
5. 专业选修课程不低于14.5学分。