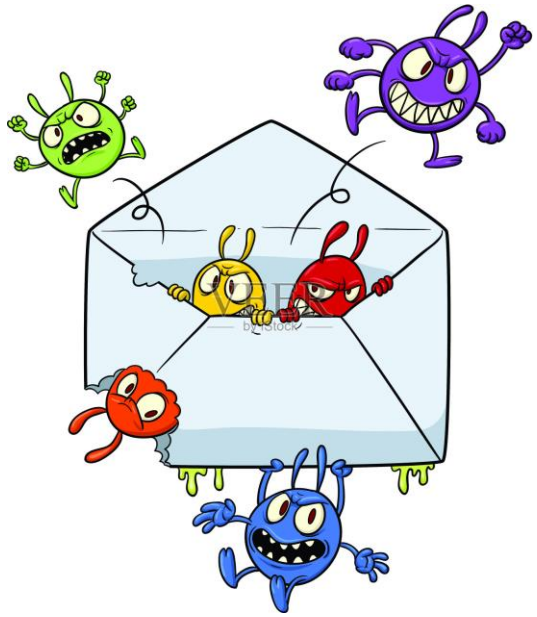
现代密码学

廖永建
信息与软件工程学院
网络空间安全实验室
电子科技大学

学习密码学之前，请想一想。。。

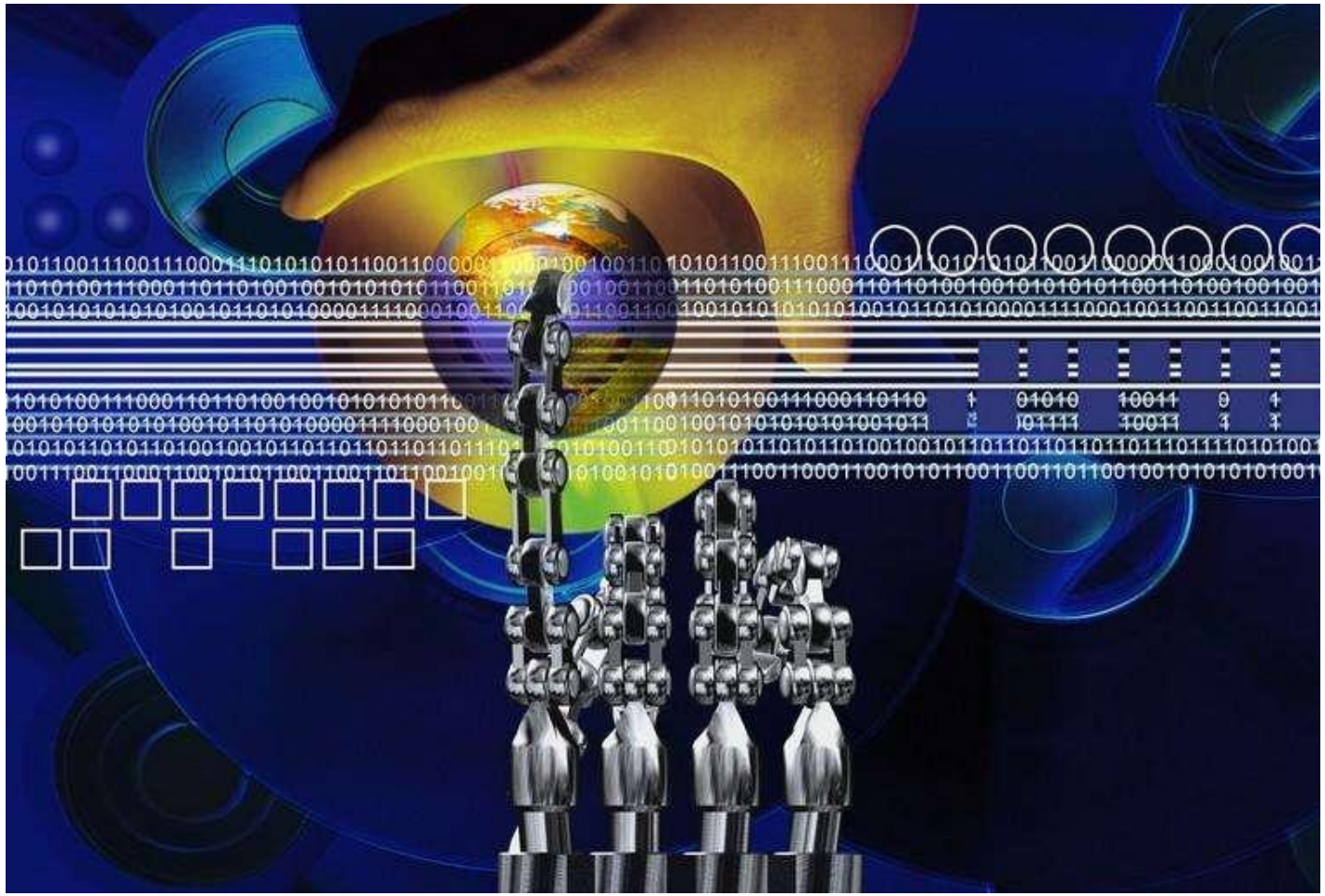
- 你相信网络吗？
  - 网络好比筋斗云，一翻十万八千里，让我们不出门也能知天下事
  - 现代人生活、工作中的一切几乎全面仰赖计算机及网络，不容易察觉其中的危机
- 不设防的便利之下，潜藏着危机



学习密码学之前，请想一想。。。

- 网络真的免费吗？
  - 一个陌生人需要付多少钱，你会给他看你的日记？
  - 免费用网络与家人联络、视频通话、看新闻看影片、收发电子邮件、使用搜索引擎。只有少数人知道我们真正的付费方式
  - 每一天我们用个人隐私作为货币，来换取网络的“免费服务”

密码学——保护信息安全的第一道防线



2014年2月27日　　2015年6月11日

国务院学位委员会 教育部关于增设网络空间安全一级学科的通知

学位〔2015〕11号

各省、自治区、直辖市学位委员会、教育厅（教委），新疆生产建设兵团教育局，有关部门（单位）教育（人事）司（局），中国人民解放军学位委员会，中共中央党校学位评定委员会，各学位授予单位：

为实施国家安全战略，加快网络空间安全高层次人才培养，根据《学位授予和人才培养学科目录设置与管理办法》的规定和程序，经专家论证，国务院学位委员会学科评议组评议，报国务院学位委员会批准，决定在“工学”门类下增设“网络空间安全”一级学科，学科代码为“0839”，授予“工学”学位。请各单位加强“网络空间安全”的学科建设，做好人才培养工作。

国务院学位委员会 教育部

手机端　微博　微信
邮箱

国家密码管理局
WWW.SCA.GOV.CN

请输入关键字

热门搜索：商用密码　电子认证　电子签名

首页 | 机构概况 | 新闻动态 | 信息公开 | 在线服务 | 互动交流 | 专题专栏

首页 > 信息公开 > 政策法规 > 法律法规

中华人民共和国密码法

发布日期：2019-10-27　来源：中国人大网

【字体：大 中 小】　打印

目　录

第一章　总　　则
第二章　核心密码、普通密码
第三章　商用密码
第四章　法律责任
第五章　附　　则

最新标准公布

当前位置：检测标准 > 最新标准公布

GM/T 0054-2018 信息系统密码应用基本要求	[2019-02-25]
GM/T 0053-2016 密码设备管理 远程监控与合规性检验接..	[2019-02-25]
GM/T 0052-2016 密码设备管理 VPN设备监察管理规范	[2019-02-25]
GM/T 0051-2016 密码设备管理 对称密钥管理技术规范	[2019-02-25]
GM/T 0050-2016 密码设备管理 设备管理技术规范	[2019-02-25]
GM/T 0049-2016 密码键盘密码检测规范	[2019-02-25]
GM/T 0048-2016 智能密码钥匙密码检测规范	[2019-02-25]
GM/T 0047-2016 安全电子签章密码检测规范	[2019-02-25]
GM/T 0046-2016 金融数据密码机检测规范	[2019-02-25]
GM/T 0045-2016 金融数据密码机技术规范	[2019-02-25]

共 7 页 67 条记录 [1] [2] [3] [4] [5] [6] [7]

《中华人民共和国密码法》


深入学习贯彻密码法　奋力开创新时代密码工作新局面
中华人民共和国
密码法
法律出版社
中华人民共和国主席令
第三十五号
《中华人民共和国密码法》已由中华人民共和国第十三届全国人民代表大会常务委员会第十四次会议于2019年10月26日通过，现予公布，自2020年1月1日起施行。
中华人民共和国主席　习近平
2019年10月26日
Baidu 百科


《中华人民共和国密码法》的主要内容
日前，全国人大常委会审议通过《中华人民共和国密码法》，自2020年1月1日起施行
密码法是总体国家安全观框架下，国家安全法律体系的重要组成部分，也是一部技术性、专业性较强的专门法律
密码法共五章四十四条，重点规范了以下内容：
第一章 总则部分
规定了本法的立法目的、密码工作的基本原则、领导和管理体制，以及密码发展促进和保障措施
第二章 核心密码、普通密码部分
规定了核心密码、普通密码使用要求、安全管理制度以及国家加强核心密码、普通密码工作的一系列特殊保障制度和措施
第三章 商用密码部分
规定了商用密码标准化制度、检测认证制度、市场准入管理制度、使用要求、进出口管理制度、电子政务电子认证服务管理制度以及商用密码事中事后监管制度
第四章 法律责任部分
规定了违反本法相关规定应当承担的相应的法律后果
第五章 附则部分
规定了国家密码管理部门的规章制定权，解放军和武警部队密码立法事宜以及本法的施行日期
新华社记者 孟丽静 编制

新增专业（2021.2.10）

2020年度普通高等学校本科专业备案和审批结果

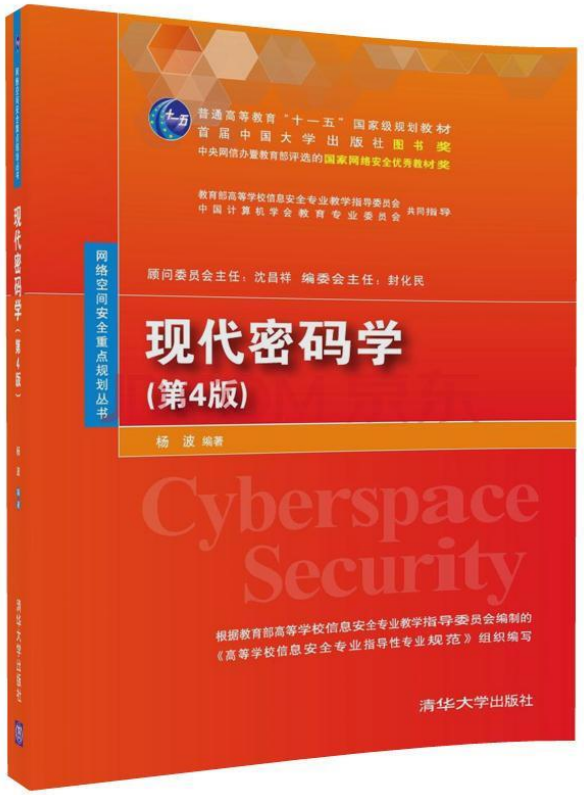
二、新增审批本科专业名单

序号	主管部门、学校名称	专业名称	专业代码	学位授予门类	修业年限	备注
教育部						
9	南开大学	密码科学与技术	080918TK	工学	四年	新专业
13	山东大学	密码科学与技术	080918TK	工学	四年	新专业
15	华中科技大学	密码科学与技术	080919TK	工学	四年	新专业
19	西安电子科技大学	密码科学与技术	080918TK	工学	四年	新专业
中央办公厅						
21	北京电子科技学院	密码科学与技术	080918TK	工学	四年	新专业
工业和信息化部						
26	北京理工大学	密码科学与技术	080918TK	工学	四年	新专业
海南省						
152	海南大学	密码科学与技术	080918TK	工学	四年	新专业

新增职业（2021.1.5）

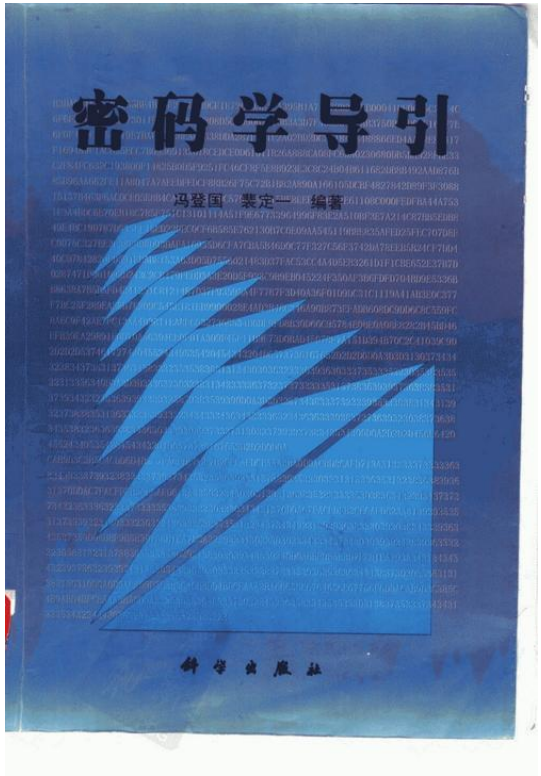
- 4-07-05-06 密码技术应用员
- 定义：运用密码技术，从事信息系统安全密码保障的架构设计、系统集成、检测评估、运维管理、密码咨询等相关密码服务的人员。
- 主要工作任务：
- 1.分析信息系统安全威胁和业务应用场景的密码应用需求；
- 2.设计密码保障应用规划和实施方案；
- 3.从事信息系统的密码资源融合部署实施工作；
- 4.依据标准和规范，开展信息系统密码应用安全性评估工作；
- 5.从事密钥资产安全管理与使用工作；
- 6.应急处置密码应用安全突发事件；
- 7.从事信息系统密码应用态势监控与运维工作；
- 8.提供密码应用技术咨询、密码职业技能培训、密码科普等相关服务。

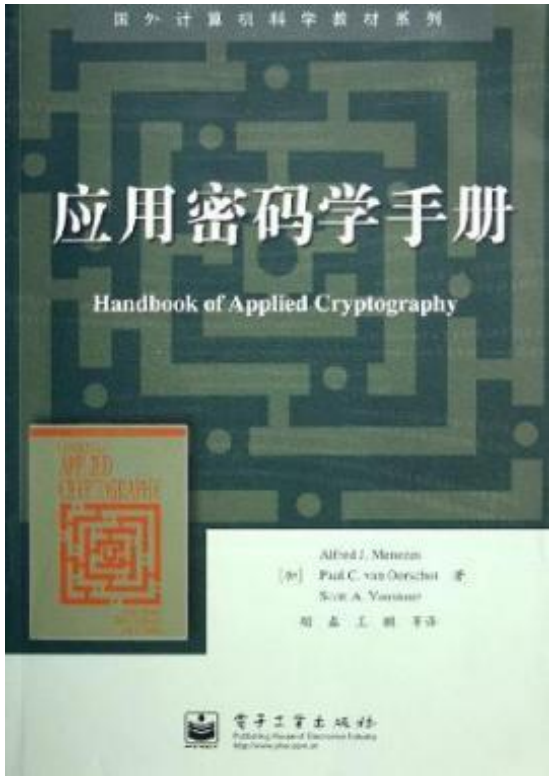
现代密码学（第4版），杨波，清华大学出版社，2017

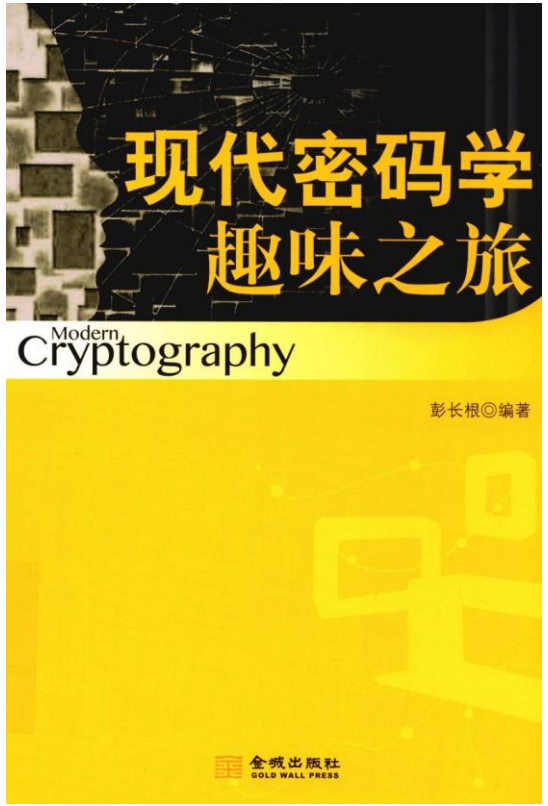


参考书目

- 密码学导引，冯登国，裴定一，科学出版社，**1999**。
- 应用密码学手册，**[**加拿大**]** 梅尼斯（**Menezes**） 等著；胡磊，王鹏等译，电子工业出版社，**2005**。
- 彭长根**.** 现代密码学趣味之旅**.** 金城出版社**, 2015.**







目的

毕业要求指标点：

- **GR3.1** 能够根据用户需求，分析和确定设计目标
- **GR3.2** 能够在社会、健康、安全、法律、文化以及环境等约束条件下，通过技术经济评价对设计方案的可行性进行研究
- **GR6.1**掌握至少一个应用领域中软件工程技术的应用方法和工程实践
- **GR10.1**能够撰写报告和设计文稿，清晰阐述复杂工程问题

课程目标

- **CO1**：掌握分析保密通信系统中安全需求的方法
- **CO2**：理解密码学的基本概念、基本原理和一些典型的密码算法的原理
- **CO3**：理解各类密码算法的应用场景和相关的安全需求
- **CO4**：掌握常用密码算法的实现

学习方法——自主学习

- 基础：信息安全数学基础、信息安全导论
- 核心：算法和协议，掌握算法和协议的流程、合理性、安全性基础和设计方法。
- 阅读文献，了解密码学最新进展
- 密码学顶级会议：**CRYPTO**、**Eurocrypt**、**Asiacrypt**……
- 密码学期刊：**Journal of Cryptology** 、密码学报
- 相关网址：
  - 国际密码协会：**http://www.iacr.org/**
  - 数缘社区：http://www.mathmagic.cn/bbs/
- 微信公众号：密码头条，中国密码学会，数缘信安社区。。。

《现代密码学》慕课

- 现代密码学_电子科技大学_中国大学MOOC(慕课)
  https://www.icourse163.org/course/UESTC-1003046001
- 现代密码学_SPOC
  https://www.icourse163.org/spoc/course/UESTC-1450239182
- 课程密码：nxylyjwyy

现代密码学

主讲人：聂旭云 熊虎 廖永建 陈大江 王煜宇

电子科技大学信息与软件工程学院

考核方式

- 平时**50% +**期末**50%**
- 平时成绩主要来源于**SPOC**（**30%**）和课程研讨（**20%**）
  - **SPOC**：单元测试**20%**、单元作业**20%**、线上讨论**10%**、期末考试占**50%**。
  - 课程研讨：个人评分**10%**，课程研讨小论文**60%**，结题汇报**30%**

课程研讨的考核

- 每6人一组
- 自主选题，明确分工
- 课外作业以小论文形式提交
- 结题汇报：
  - 结题汇报时每人上台陈述自己所做工作（1-2分钟）
- 个人评分10%，课程研讨小论文60%，结题汇报30%

课外作业选题（均为算法实现）

- 分组密码：**AES**、**SM4**
- 序列密码：祖冲之算法、**A5**
- 公钥密码：**SM2**，多变量公钥密码，**NTRU**
- 杂凑函数：**SM3**，**SHA-3**
- 数字签名：**DSS**，**SM2**
- 密码协议：**Diffie-Hellman**密钥交换协议，**Shamir**秘密分享
- 密码分析：大整数分解，求解离散对数
- 新型密码算法或协议实现（自拟或与老师协商）

目录

感 谢 聆 听!

liaoyj@uestc.edu.cn