《现代密码学》课程介绍

于红波

2020-2-19

课程信息

- 课程名称：现代密码学
- 课程代号：40240892
- 学时：2学时
- 教师
  - 授课：于红波 副教授
  - 助教： 陈怡 博士研究生
- 课程
  - 时间：周三下午1:30-3:05(第3大节), 6A205

教师信息

- 于红波 副教授
  - Email: yuhongbo@mail.tsinghua.edu.cn
  - Phone: 62788631, 18519692780
  - Room: 西主楼1区404
- 陈怡 博士研究生
  - Email：chenyi19@mails.tsinghua.edu.cn
  - Phone：13163234706
  - Room：西主楼1区407

周次	2020年	2020年春季课程计划	备注
1	2月19日	密码学简介	
2	2月26日	古典密码	
3	3月4日	分组密码设计及算法	对称密码
4	3月11日	分组密码工作模式	
5	3月18日	分组密码的分析	
6	3月25日	序列密码简介	
7	4月1日	密码Hash函数	
8	4月8日	消息认证码简介	
9	4月15日	Hash函数和消息认证码的分析	
10	4月22日	作业讲解； 量子密码讲座	
11	4月29日	公钥密码学简介及其数学基础	公钥密码
12	5月6日	RSA、ECC密码体制	
13	5月13日	数字签名方案	
14	5月20日	其他公钥密码体制	
15	5月27日	作业讲解，课程总结	
16	6月3日	考试	

课程教材

- 教材
  - Cryptography Theory and Practice（Third Edition）密码学原理与实践（第三版, 第二版）
  - Cryptography and Network Security, William Stallings

    密码编码学与网络安全-原理与实践（第5版）

课程参考书

- 参考书目：
  - HandBook of Applied Cryptography. A. J. Menezes, P. C. van Oorschot, S. A. Vanstone
  - Applied Cryptography: Protocols, Algorithms and Source Code in C. Bruce Schneier
  - 密码学导引，冯登国等
  - 图解密码技术，[日] 结城浩 著， 周自恒 译
  - 公钥密码学的数学基础，王小云、王明强、孟宪萌
  - The Code Book，Simon Singh 密码故事
  - 量子计算与量子信息（10周年版），Michael A. Nielsen, Isaac L. Chuang

成绩评定

- 分数
  - 作业，通过网络学堂
    - 30分。共3次大作业
  - 考勤+课堂小测
    - 10分+5分。假设缺席n次，则
      - n<2， 考勤 10分；n>=2， 考勤 10-3*(n-1)
      - 课堂表现5分
  - 考试（开卷）
    - 55分

课程交流方式

- 利用网络学堂
  - 课程公告：教师通知
  - 课程文件：课件、教材电子版等
  - 课程作业：作业布置、提交与批改
  - 课程答疑：一对一答疑
  - 课程讨论：欢迎同学们讨论
- 微信群+雨课堂+腾讯会议+Zoom等

谢谢！

投票 最多可选1项

设置

你的网络状态好吗？

A 好

B 不好

C 此处添加选项内容

D 此处添加选项内容

提交