《现代密码学》课程介绍

于红波

2023-2-22

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： 袁思同 博士研究生
- 课程
  - 时间：周三下午1:30-3:05(第3大节)

教师信息

- 于红波
  - 计算机系长聘副教授，博士生导师
  - 获得国家科技进步一等奖1次，2020年
  - 中国密码学会“优秀青年奖”2011
  - 获得国家自然科学二等奖1次, 2008
  - 研究方向：密码算法分析与设计
- 联系方式
  - Email: yuhongbo@mail.tsinghua.edu.cn
  - Phone: 15810117598
  - Room: 西主楼1区417

教师信息

- 袁思同　博士研究生
  - Email：yst20@mails.tsinghua.edu.cn
  - Room：西主楼1区417

周次	2023	2023年春季课程计划	备注
1	2月22日	课程介绍、密码学简介	
2	3月1日	古典密码	
3	3月8日	Enigma原理与破译	
4	3月15日	分组密码设计及分析	
5	3月22日	高级数据加密标准AES；分组密码工作模式	
6	3月29日	序列密码简介	
7	4月5日		清明节停课
8	4月12日	密码Hash函数	
9	4月19日	消息认证码	
10	4月26日	公钥密码学简介及其数学基础	
11	5月7日	公钥密码体制（1）	5.3的课程调到5.7
12	5月10日	公钥密码体制（2）	
13	5月17日	数字签名方案（1）	
14	5月24日	数字签名方案（2）	
15	5月31日	前沿讲座	
16	6月7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）
- 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
  - **公钥密码学的数学基础，王小云、王明强、孟宪萌**

    课程在中国大学慕课上分了两部分。上半部分主要是初等数论，链接：https://www.icourse163.org/course/SDU-1461587167

    下半部分包括代数结构基础，算法数论基础，格理论基础。链接：https://www.icourse163.org/course/SDU-1461641161
  - The Code Book，Simon Singh 密码故事

成绩评定

- 分数
  - 作业，通过网络学堂
    - 30分。共3次大作业（古典密码、对称密码、公钥密码）
  - 考勤+课堂小测
    - 10分。假设缺席n次，则
      - n<2, 考勤 10分
      - n>=2, 考勤 10-3*(n-1)
  - 考试（开卷）
    - 60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
- 利用微信群
- 面对面答疑（需要跟助教预约）

谢谢！