|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 曲 阜 师 范 大 学 教 学 日 历 2015--2016 学年第 1学期 | | | | | | | | | | |  |  |  |  |
|  | 开课单位\_\_\_\_\_\_\_\_\_\_信息学院\_\_\_\_\_\_\_任课教师单位\_\_信息学院\_\_\_\_\_\_\_课程名称:\_\_\_\_密码学\_\_\_\_\_\_ 课程性质\_\_\_\_\_限选\_\_\_\_\_\_ | | | | | | | | | | |  |  |  |  |
|  | 任课教师：\_\_\_胡越梅\_\_\_\_\_职称：\_\_\_\_讲师\_\_\_\_授课专业\_\_网络工程卓越班\_\_年级\_\_2013\_\_人数\_\_50\_\_本学期行课周数：18\_\_周学时\_\_3\_\_ | | | | | | | | | | |  |  |  |  |
|  | 课程总学时\_\_\_54\_\_\_本学期学时\_54\_讲授使用课时\_\_\_54\_实验（练习、实习见习、课堂讨论、测验或其他）使用课时\_\_\_\_填表日期：\_\_9.10\_\_\_ | | | | | | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 周次 | 日期 | 节次 | 课堂讲授 | | | | | 实验（练习、实习见习、课堂讨论、社会实践或其他） | | 备注 |  |  |  |  |
|  | 讲授内容 | | | 教学方式方法手段 | 时数 | 题目或内容 | 时数 |  |  |  |  |
|  |  |  |  |  |  |  |  | | | |  |  | |  | **时** |
|  |  |  |  |  | **数** |
|  | 1 | 9.6 | 1—3 | 密码学概述，发展 | | |  | 3 |  |  |  |  |  |  |  |
|  | 2 | 9.8 | 1—3 | 密码学的基本概念 | | |  | 3 |  |  |  |  |  |  |  |
|  | 3 | 9.15 | 1—3 | 古典密码技术 | | |  | 3 | 利用替代密码，置换密码加解密 |  |  |  |  |  |  |
|  | 4 | 9.22 | 1—3 | 古典密码的统计分析 | | |  | 3 | 古典密码器的设计实现 |  |  |  |  |  |  |
|  | 5 | 9.29 | 1—3 | 分组密码概述，设计原则，设计方法。DES | | |  | 3 | DES的安全性分析 |  |  |  |  |  |  |
|  | 6 | 10.13 | 1—3 | AES及分组密码的工作模式 | | |  | 3 | RC6算法的设计实现 |  |  |  |  |  |  |
|  | 7 | 10.2 | 1—3 | 数论基础 | | |  | 3 | 求逆，平方乘运算的练习 |  |  |  |  |  |  |
|  | 8 | 10.27 | 1—3 | 公钥密码体制概述，RSA | | |  | 3 | 利用RSA进行加解密 |  |  |  |  |  |  |
|  | 9 | 11.3 | 1—3 | Elgamal、ECC | | |  | 3 | 利用ECC加解密 |  |  |  |  |  |  |
|  | 10 | 11.1 | 1—3 | 散列函数的概念及构造与设计 | | |  | 3 |  |  |  |  |  |  |  |
|  | 11 | 11.17 | 1—3 | 安全散列函数SHA-1，MD5 | | |  | 3 | SHA-1算法的分析 |  |  |  |  |  |  |
|  | 12 | 11.24 | 1—3 | 对散列函数的攻击；消息鉴别 | | |  | 3 |  |  |  |  |  |  |  |
|  | 13 | 12.1 | 1—3 | 数字签名概述及典型的公钥签名方案 | | |  | 3 | 基于RSA的数字签名方案的分析应用 |  |  |  |  |  |  |
|  | 14 | 12.8 | 1—3 | 特殊的数字签名方案 | | |  | 3 |  |  |  |  |  |  |  |
|  | 15 | 12.15 | 1—3 | 密钥管理技术 | | |  | 3 | PKI |  |  |  |  |  |  |
|  | 16 | 12.22 | 1—3 | 身份鉴别技术 | | |  | 3 |  |  |  |  |  |  |  |
|  | 17 | 12.29 | 1—3 | 序列密码 | | |  | 3 | RC4算法的设计实现 |  |  |  |  |  |  |
|  | 18 | 1.5 | 1—3 | 密码技术的应用 | |  |  | 3 | PGP技术的应用 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 说明：1、开课单位为课程所属单位，可填多个单位。公共课（必修、选修）填“全校”； 2、备注：填写本学期课程讲授期间的答疑、考查、作业内容及有关教学活动地点等 | | | | | | | | | | |  |  |  |  |
|  |  | | | | | | | | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |