北京信息科技大学
2020年硕士研究生招生考试大纲

考试科目名称：《网络空间安全专业基础综合（计算机网络+密码学）》　　考试科目代码：812

《计算机网络》考试大纲

一、考查目标

1、掌握计算机网络的基本概念、基本原理和基本方法。

2、掌握计算机网络的体系结构和典型网络协议，了解典型网络设备的组成和特点，理解典型网络设备的工作原理。

3、掌握各层协议的基本原理和具体工作流程。

4、能够运用计算机网络的基本概念、基本原理和基本方法进行网络系统的分析、设计和应用。

二、考查内容

（一）计算机网络概述

1、计算机网络的概念、分类、发展和标准化工作

2、计算机网络的组成

3、计算机网络的性能

4、计算机网络的体系结构

（二）物理层

1、物理层的基本概念及主要任务

2、数据通信的基础知识

3、计算机网络的拓扑结构及传输媒体

4、信道复用技术

（三）数据链路层

1、数据链路层的基本概念：数据链路层的基本信道类型和链路层协议要解决的基本问题

2、使用点对点信道的数据链路层：点对点协议 PPP

3、使用广播信道的数据链路层：局域网

4、以太网在不同层上的扩展及虚拟局域网

5、物理层设备（中继器、集线器）与数据链路层设备（以太网交换机）原理及特点

（四）网络层

1、网络层的基本概念：虚电路服务与数据报服务，虚拟互连概念

2、三种 IPv4 地址编址方式：

（1）分类的 IP 地址

（2）划分子网

（3）构造超网（CIDR）

3、互联网的路由选择协议：

（1）路由算法概念

（2）路由选择协议分类：静态路由与动态路由、内部网关协议与外部网关协议

（3）RIP 协议

（4）OSPF 协议

（5）BGP 协议

4、路由表的基本概念和形式：与不同网络编址方式和路由协议对应下的路由表

5、网络层的分组转发

6、IP 数据报格式

7、网络层配套协议：基本作用、与 IP 协议关系及其应用

（1）ARP 协议

（2）ICMP 协议

8、IPv6

9、路由器的构成及基本原理

（五）运输层

1、运输层协议概述

2、用户数据报协议 UDP

3、传输控制协议 TCP 概述

4、TCP 的基本工作原理：

（1）可靠传输原理：滑动窗口机制、超时重传时间的选择

（2）连接管理原理：连接建立与连接释放

（3）流量控制原理：利用滑动窗口实现流量控制

（4）拥塞控制原理

5、TCP 报文段格式

（六）应用层

1、域名系统 DNS

2、文件传送协议 FTP

3、电子邮件

4、远程终端协议 TELNET

5、万维网 WWW

6、动态主机配置协议 DHCP

三、参考书目

计算机网络(第七版). 谢希仁编著，电子工业出版社，2017 年。

《密码学》考试大纲

一、考查目标

1、掌握密码学的基本概念、基本原理和基本方法。

2、理解密码体制的组成和分类，掌握不同密码体制的基本原理。

3、掌握典型密码算法的基本原理和工作流程。

4、能够运用密码学的基本概念、基本原理和基本方法对网络安全问题进行分析、设计和应用。

二、考查内容

（一）密码学概论

1、 密码体制的组成

2、 密码体制分类

3、 古典密码算法的基本原理

(1) 替代密码算法

(2) 置换密码算法

4. 密码系统的基本攻击类型

(1) 唯密文攻击

(2) 已知明文攻击

(3) 选择明文攻击

(4) 选择密文攻击

（二）流密码

1、线性反馈移位寄存器的数学模型

(1) 生成线性反馈移位寄存器序列的特征多项式

(2) 输出序列的周期

2、m 序列的伪随机性

3、m 序列密码的破译

4、非线性序列的生成

（三）分组密码

1、分组密码的基本原理

2、DES 算法的密钥生成及加密轮结构

3、AES 算法的密钥生成及加密轮结构

4、分组密码的基本工作模式

(1) 电子密码本工作模式

(2) 密码链接本工作模式

(3) 密文反馈工作模式

(4) 输出反馈工作模式

5、三重 DES 的工作原理

（四）公钥密码

1、公钥密码的基本原理

2、RSA 算法的基本原理和计算问题

3、RSA 算法的安全性分析

4、其他公钥密码算法的基本原理

(1) Rabin 密码算法

(2) ElGamal 密码算法

(3) 椭圆曲线密码算法

（五）密钥分配与密钥管理

1、密钥分配的基本方法

(1) 分组密码体制的密钥分配

(2) 用公钥加密分配分组密码体制的密钥

2、Diffie-Hellman 密钥交换

3、秘密分割门限方案：Shamir 门限方案、基于中国剩余定理的门限方案

（六）消息认证和哈希函数

1、消息认证码的定义及使用方式，应满足的条件

2、哈希函数的定义及使用方式，应满足的条件

3、迭代型哈希函数的一般结构

4、MD5 哈希算法的工作流程

5、安全哈希算法的工作流程

（七）数字签名和认证协议

1、数字签名的基本原理

(1) 数字签名应满足的要求

(2) 数字签名的执行方式

(3) 数字签名的产生方式

2、数字签名方案

(1) 基于离散对数问题的数字签名体制：ElGamal 签名方案、Schnorr 签名方案

(2) 基于大数分解问题的数字签名体制：Fiat-Shamir 签名方案、Guillou-Quisquater 签名方案

3、认证协议

(1) 相互认证

(2) 单向认证

（八）网络加密与认证

1、网络加密基本方式

2、X.509 认证业务

(1) 证书的格式、获取和吊销

(2) 认证过程

3、Kerberos 系统的认证流程

三、参考书目

现代密码学(第 4 版). 杨波编著. 清华大学出版社, 2017 年。