《信息安全概论》考试大纲

（一）信息安全概述

1、信息安全、网络安全概念、信息安全特征；

2、信息安全的威胁；

3、主要安全措施；

4、信息安全的一般模型；

5、信息安全研究的主要内容。

单钥密码体制

1、传统密码、序列密码、分组密码；

2、Feistel 密码结构；

3、数据加密标准（DES）。

公钥密码体制

1、数论基础；

2、计算复杂度；

3、RSA 算法。

（四）密钥管理

1、单钥加密体制的密钥分配；

2、公钥加密体制的密钥管理。

（五）消息认证

1、消息认证基本概念；

2、进行消息认证的方式。

（六）数字签字

1、数字签字的含义和过程；

2、数字签字体制；

3、数字签字标准 DSS。

（七）网络的安全与保密

1、网络安全的威胁；

2、网络安全服务；

3、网络安全对策；

4、网络通信中的一般加密方式。

（八）身份认证技术

1、身份认证概念；

2、Kerberos 认证系统。

（九）协议安全

1、Web 的安全要求；

2、安全套接字层。

（十）防火墙技术

1、基本知识；

2、防火墙设计的准则；

3、包过滤防火墙；

4、应用层网关、线路层网关；

5、构建防火墙系统。

参考教材：《信息安全概论》，段云所等编著，高等教育出版社，2003 年 9 月版。