**网络空间安全** **2025** **年硕士研究生** **入学考试专业课考研大纲**

一、考试内容组成

网络空间安全专业综合共包括两部分内容：（ 1 ）密码学理论；（2）网络安全 技术。两部分内容合计为 150 分。

二、“密码学理论”部分考试大纲

**（** **一）整体要求**

1．掌握密码学所涉及的数论、有限域等基本数学理论；

2. 掌握密码学的基本概念、常用密码算法原理和密码协议设计方法。

**（二）** **知识要点**

1．数论基础

（ 1 ）整除性和带余除法；

（2）欧几里得算法，扩展欧几里得算法；

（3）模运算；

（4）素数，素性测试；

（5 ）欧拉定理，费马小定理；

（6）中国剩余定理；

（7）离散对数。

2．有限域

（ 1 ）群的概念及性质；

（2）环的概念及性质；

（3）域的概念及性质；

（4）有限域的概念及性质；

（5 ）有限域 GF（p）和 GF（2n ）；

（6）多项式运算。

3．单钥密码体制

（ 1 ）密码体制的定义；

（2）对称密码基本概念，分组密码常见结构；

（3 ）DES/AES/SM4 算法；

（4）流密码的基本概念，RC4、祖冲之算法；

（5）分组密码的工作模式及特点；

（6）伪随机数发生器和伪随机函数。

4．双钥密码体制

（ 1 ）双钥密码体制的基本概念；

（2）RSA 公钥密码算法；

（3 ）ElGamal 公钥密码算法；

（4）椭圆曲线密码算法；

（5 ）中国 SM2 公钥密码算法。

5．消息认证与杂凑函数

（ 1 ）杂凑函数的概念、性质及基本结构；

（2）常用杂凑函数算法（MD5 、SHA 、SM3 等）；

（3 ）消息认证码（MAC）与消息检测码（MDC）的构造方法与安全功能；

（4）迭代杂凑函数的构造方法；

（5 ）应用杂凑函数的基本方式。

6．数字签名

（ 1 ）数字签名算法基本概念；

（2）RSA 数字签名算法；

（3 ）ElGamal 数字签名算法；

（4）Schnorr 数字签名算法；

（5 ）DSS 数字签名标准；

（6）椭圆曲线数字签名算法；

（7）中国 SM2 签名算法；

（8 ）具有特殊功能的签名算法。

三、“网络安全技术”部分考试大纲

**（** **一）整体要求**

1．掌握网络安全的基本概念；

2. 掌握计算机网络的基础知识；

3. 掌握常用 Internet 协议的安全性；

3．掌握网络安全技术与应用。

**（二）** **知识要点**

1. 网络安全的基本概念

（ 1 ）网络安全的需求；

（2）安全威胁与防护措施；

（3 ）网络安全策略；

（4）安全攻击的分类；

（5 ）网络攻击的常见形式；

（6）开放系统互连安全体系结构；

（7）网络安全模型。

2．计算机网络基础

（ 1 ）计算机网络的定义；

（2）计算机网络体系的结构；

（3 ）分组交换技术；

（4）Internet 的基本知识，包括：Internet 的构成、服务类别、IPv4 地址、 IPv6 地址、端口的概念等。

3. Internet 协议的安全性

（ 1 ）HTTP、FTP、TELNET、POP3、SMTP、SSH、DNS、DHCP 等常用网 络协议的功能、使用的端口及安全性；

（2）网络地址转换（NAT）的作用及安全性；

（3 ）UDP 协议的安全性及优缺点；

（4）TCP 协议的安全性及优缺点。

4．密码协议

（ 1 ）协议的基本概念；

（2）密码协议分类及基本密码协议；

（3 ）Diffie-Hellman 协议；

（4）Kerberos 协议；

（5）秘密分拆协议；

（6）会议密钥分配和秘密广播协议；

（7）密码协议的安全性分析。

5．数字证书与公钥基础设施

（ 1 ）PKI 的定义、组成及应用；

（2）数字证书的概念；

（3）数字证书的结构；

（4）数字证书的生成、签名及验证；

（5 ）X.509 证书格式。

6． 网络加密与密钥管理

（ 1 ）四种网络加密模式的原理、特点；

（2）密钥管理的基本概念；

（3）密钥的生成与分配方法；

（4）密钥的保护、存储与备份；

（5 ）层次化密钥管理方法；

（6）密钥管理系统组成。

7．无线网络安全

（ 1 ）无线网络面临哪些安全威胁；

（2）GSM/CDMA /3G 系统的认证过程及主要安全缺陷；

（3 ）WCDMA 蜂窝系统的认证过程及安全性改进。

8． 防火墙

（ 1 ）防火墙的类型和结构；

（2）静态包过滤器工作原理；

（3）动态包过滤器工作原理；

（4）电路级网关工作原理；

（5）应用级网关工作原理。

9．入侵检测技术

（ 1 ）入侵检测概述；

（2）入侵检测原理及主要方法；

（3 ）IDS 的分类及优缺点；

（4）NIDS 工作原理；

（5 ）HIDS 工作原理；

（6）IDS 在网络中的部署（所处的位置）。

10．VPN

（ 1 ）VPN 的基本概念；

（2）VPN 的分类及优缺点；

（3 ）IPSec VPN 的工作原理；

（4）SSL/TLS VPN 的工作原理；

（5 ）VPN 在网络中的部署（所处的位置）。

**（三）** **参考书目**

1.《网络安全——技术与实践》（第 3 版），刘建伟，王育民编，清华大学出 版社，2017。

2.《密码编码学与网络安全——原理与实践（第七版）》，William Stallings 著， 王后珍等译，电子工业出版社，2017。