

考试科目	825 密码学基础与网络安全	考试形式	笔试（闭卷）
考试时间	180 分钟	考试总分	150 分
<p>一、总体要求</p> <p>掌握密码学的基本理论、方法和应用技术，掌握网络安全的基本原理、知识体系结构以及保证网络安全的各种方法和技术，掌握信息安全工程基本概念和方法。</p> <p>二、内容</p> <p>1、信息安全基础</p> <ol style="list-style-type: none"> 1) 密码学的发展概况（了解） 2) 密码学的基本概念及其分类（掌握） <p>2、古典密码</p> <ol style="list-style-type: none"> 1) 古典密码中的基本加密运算（了解） 2) 几种典型的古典密码体制（了解） 3) 古典密码的统计分析（了解） <p>3、Shannon 理论</p> <ol style="list-style-type: none"> 1) 密码体制的数学模型（掌握） 2) 熵及其性质（了解） 3) 密码体制的完善保密性（了解） <p>4、分组密码</p> <ol style="list-style-type: none"> 1) 分组密码的基本原理（理解） 2) 数据加密标准 DES（掌握） 3) 多重 DES（掌握） 4) DES 的工作模式（掌握） 5) 高级加密标准 AES（理解） <p>5、公钥密码</p> <ol style="list-style-type: none"> 1) 初等数论基础知识（掌握） 2) 公钥密码的理论基础（理解） 3) RSA 公钥密码（掌握） 4) ElGamal 公钥密码（了解） 5) 椭圆曲线公钥密码理论及算法（掌握） <p>6、序列密码与移位寄存器</p> <ol style="list-style-type: none"> 1) 序列密码的基本原理（了解） 2) 移位寄存器与移位寄存器序列（理解） 3) 线性移位寄存器的表示（了解） 4) 线性移位寄存器序列的周期性（了解） 5) 线性移位寄存器的序列空间（了解） 6) RC4 算法及其在无线通信中的应用（掌握） 			

7、数字签名

- 1) 基于公钥密码的数字签名 (掌握)
- 2) ElGamal 签名方案 (理解)
- 3) 数字签名标准 DSS (掌握)

8、Hash 函数

- 1) Hash 函数的性质 (掌握)
- 2) 基于分组密码的 Hash 函数 (了解)
- 3) MD5Hash 函数算法 (掌握)
- 4) 安全 Hash 算法 (SHA-1) (掌握)

9、密码协议

- 1) 密钥建立协议 (掌握)
- 2) 秘密分割与共享技术 (理解)
- 3) 身份识别技术 (理解)
- 4) 零知识证明技术 (了解)
- 5) 密钥管理技术 (掌握)

10、网络与信息安全基础

- 1) 网络与信息安全基础 (理解)
- 2) TCP/IP 协议及其安全隐患 (理解)
- 3) 各种网络网络拓扑及网络互联设备与信息安全的关系 (掌握)
- 4) 无线通信网络及其网络威胁与防御技术 (掌握)

11、网络隔离与入侵检测技术

- 1) 安全策略技术 (了解)
- 2) 防火墙及其隔离技术 (掌握)
- 3) 网络地址转换技术 (掌握)
- 4) 网络设备隔离技术 (掌握)

12、网络安全防御与攻击

- 1) 网络扫描技术 (掌握)
- 2) 电子邮件、DNS 系统、WEB 系统等中的常见网络攻击及其防御方法 (掌握)
- 3) 各种网络威胁 (如 DDOS、僵尸网络、病毒、蠕虫、垃圾邮件等) 原理及其防护方法 (掌握)
- 4) 恶意软件 (如间谍软件、广告软件、网络钓鱼软件、后门及木马) 的原理及防御方法 (掌握)
- 5) 安全编码与缓冲区溢出的基本原理及防御方法 (掌握)
- 6) 蜜罐技术及其应用 (掌握)
- 7) 入侵检测技术 (掌握)

12、协议安全技术及其应用

- 1) 安全协议的基本概念 (理解)
- 2) 理解 PGP、S/MIME 及电子邮件安全

- 3) SSH 协议及其应用 (掌握)
- 4) SSL 协议及 WEB 安全 (掌握)
- 5) IPSec 协议 (理解)
- 6) Kerberos 和 X.509 协议 (掌握)

13、系统安全技术

- 1) 计算机系统物理安全 (掌握)
- 2) 系统可靠性技术 (掌握)
- 3) 访问控制技术 (掌握)
- 4) 多级安全与安全策略模型 (了解)
- 5) 多边安全技术 (了解)
- 6) UNIX 系统和 Windows 的访问控制技术 (掌握)
- 7) UNIX 系统和 Windows 系统的常用安全技术 (掌握)

14、电子战与信息战

- 1) 信息战 (掌握)
- 2) 信息对抗 (掌握)

15、电子商务安全

- 1) 电子商务的发展历史 (了解)
- 2) 网络欺骗 (掌握)
- 3) 安全电子事务 (SET) (掌握)

16、管理及操作安全

- 1) 安全管理方法论 (了解)
- 2) 安全需求工程 (了解)
- 3) 风险管理 (了解)
- 4) 计算机取证技术 (理解)
- 5) 快速响应、灾难备份与恢复技术 (理解)
- 6) 理解安全评估方法 (掌握)
- 7) 各种信息安全法律与法规 (了解)