

# 中国科学技术大学

## 2024 年硕士研究生招生考试自命题科目 **考试大纲**

考试科目代码及名称	857 密码学与网络安全
<b>一、考试范围及要点</b>	
<b>1. 密码学基本理论</b> a) 现代密码学基本原则；密码学基本概念；香农密码理论 b) 典型代换/置乱加密技术；经典密码分析方法	
<b>2. 密码学数学基础</b> a) 有限域的计算；有限域一次/二次方程求解；中国剩余定理	
<b>3. 现代密码算法</b> a) 分组密码：Feistel 框架；DES 算法；AES 算法；分组密码工作模式；其它典型分组密码算法 b) 流密码：线性反馈移位寄存器；伪随机数发生器；其它典型流密码算法 c) 公钥密码：RSA 算法；ElGamal 算法 d) 消息认证的典型算法（如 MAC、HASH 等）和应用 e) RSA 签名算法；ElGamal 签名算法；数字签名的应用	
<b>4. 密钥管理与应用</b> a) 密钥协商和分配方案及协议 b) 密钥管理中的安全问题	
<b>5. 密码协议</b> a) 身份认证方案及协议 b) 盲签名协议；不经意传输协议	
<b>6. 现代密码分析</b> a) 现代密码算法的安全性分析 b) 差分攻击；线性攻击；中间相遇统计；相关攻击；生日攻击等密码算法分析方法 c) 中间人攻击；利用签名的攻击等基于密码协议的攻击	
<b>7. 网络安全基本概念</b> a) 网络安全特征；常见的不安全原因、因素；常见攻击手段 b) 网络安全模型、网络访问安全模型	
<b>8. PKI 体系</b> a) PKI 基本概念、组成和基本结构 b) PKI 基本功能、证书的生命周期、证书链、交叉认证	
<b>9. IPSec: AH、ESP 与 IKE</b> a) 熟悉 SA、SAD/SPD b) IKE：相关密钥的推导和作用；认证和密钥协商过程 c) AH/ESP 头标、保护范围 d) 工作模式：传输模式和隧道模式 e) VPN 的种类、功能 f) IPSec VPN 的处理流程	
<b>10. SSL/TLS</b>	

- a) SSL 的基本层次结构、安全服务
- b) SSL 协议的基本描述
- c) 安全操作流程：握手协议、会话重用
- d) 相关密钥的生成（派生方法）

**11. 防火墙和 NAT**

- a) 防火墙种类、功能
- b) 包过滤型防火墙和状态检测型防火墙之间的差异
- c) NAT 基本原理、作用；
- d) 数据访问 SNAT 和 DNAT 的处理流程和数据包的变化
- e) 基本组网原理：交换机、路由器等的基本功能

**12. 应用层安全和无线安全**

- a) PGP 的基本功能、安全服务
- b) SET 协议的基本概念、双重数字签名等
- c) WLAN 的基本概念，WEP 安全服务、增强方案举例

**二、考试形式与试卷结构**

**1. 考试形式：**

闭卷，考试时间 3 小时，试卷满分 150 分。

**2. 答题方式**

闭卷，不允许使用计数器。

**3. 试卷题型结构：**

- 单项选择题
- 填空题
- 简答与计算题

其中密码学约占 50%，网络安全约占 50%。

参考书目名称	作者	出版社	版次	年份
密码编码学与网络安全——原理与实践	William Stallings 著；唐明等译	电子工业出版社	第六版	2015
网络安全基础——应用与标准	William Stallings 著；白国强等译	清华大学出版社	第六版	2019