章节	内容	考试重点
1	物联网基础知识	物联网特点和定义、物联网的“云-管-边-端”架构、物联网区分于互联网的特点（感知、控制）、关键技术尤其是和传感器、AI 相关的特有的技术、RFID 的系统原理及组成、应用场景如车联网等。
2	信息安全基础知识——古典密码学	古典：古典密码学的特点和哲学思想（置换和替换）、信息安全的几个内涵、常见的古典密码学加密方法、安全性分析、密码安全攻击的分类及特点、攻击手段尤其是仿射加密（词频统计攻击）； 现代：现代密码学的哲学思想（混淆和扩散），对称加密的原理、区别及使用场景、如何一起使用，DES 的加密过程、AES 的四个阶段、S 盒等细节的计算过程，公钥加密的原理及和对称加密的区别，公钥私钥加密如何结合使用、RSA 算法的计算过程、DH 协议推导过程及安全分析，哈希函数、数字签名的基本原理
3	信息安全基础知识——现代密码学	
4	终端安全：设备认证	认证的定义、物联网认证的特殊性、3M 框架（尤其是 device free 和 non-device based）、设备硬件指纹的原理、来源及举例、生物认证的定义、举例，物联网场景认证、场景指纹等。
5	终端安全：传感器安全	传感器的组成结构及其和安全相关的特性、感知（测量）安全的定义、换能攻击定义和原理、通用传感器模型和感知安全（换能攻击）模型并能结合常见的换能攻击如海豚音、ghostalk、walnut 对其进行分析，换能攻击的攻击步骤，常见的可利用的攻击原理，换能攻击如海豚音的攻击防护方法（思考），传感器和隐私安全的关系、执行器安全的定义
6	终端安全：芯片安全	芯片/SoC 的定义、芯片制造流程、IP 等，芯片安全问题来源、重要安全事件、硬件木马的定义、基于 FSM 图的攻击分析，物理侧信道如功耗、电磁、缓存的攻击，ROWHAMMER 攻击例子、TrustZone 等防护机制的概念等
7	终端安全：软件安全	物联网的固件的内涵、特殊性，固件、软件、驱动的区别，常见的物联网固件/操作系统，固件或者软件安全漏洞如弱口令、SQL 注入等的攻击原理，结合代码会分析缓存区溢出、格式化字符串等常见的软件漏洞

9	协议流量安全	协议定义、作用，物联网协议的特殊性，物联网协议举例如 COAP、MQTT 及其区别，管道安全的内涵，从五层架构来看每层的风险，安全协议如 IPSEC（传输模式、隧道模式区别），SSL 及其握手过程、HTTPS 等等、流量测信道如摄像头检测
10	物联网云安全	物联网云的内涵和传统云端区别，物联网云计算的安全挑战；
11	物联网业务安全	掌握物联网业务及业务安全的定义，了解物联网也的常见特性；业务安全分析方法，尤其是控制不变量分析法
12	专题 1：语音安全	物联网里面语音处理的相关技术应用，物联网智能语音设备安全的几个层面和脆弱点的来源，语音安全攻击的分类，海豚音攻击原理及过程（如何利用器件非线性作用推导、时频域信号流图、如何防护等等（结合 HW、实验 1 相关）； 声纹识别安全，说话人辨认、确认的区别，方法的不同（文本相关、无关）、基于声场的方法原理。
13	专题 2：边缘计算及其安全	边缘计算定义（尤其是对于边缘这个概念的理解）、历史发展技术（尤其是 CDN）、边缘计算的必要性及其和云计算、雾计算的区分，边缘计算的关键技术如计算迁移、负载均衡、5G 等的定义内涵，边缘计算场景分析（如智能城市摄像头，分析功能如何实现、安全隐私保护等等）
14	专题 3：AI 安全	AI 安全的内涵和影响因素，AI 安全的攻击入口（以自动驾驶为例），AI 的工作机理流程和 AI 模型的 3 个分类，AI 攻击目标分类、手段分类、攻击入口分类、CIA 分类、攻击者分类，数据中毒攻击定义、原理、例子（DNN 后门），对抗样本攻击定义、原理、模型、例子，尤其是 real-world 对抗样本攻击的特殊性，逆向工程攻击的定义、分类、方法，三种攻击手段的详细对比。