**应用密码学与网络安全知识点**

1. 第一章

保密性、完整性、可用性、真实性、可追溯性

安全攻击、安全机制、安全服务

2. 第二章

密码编码学、密码分析学基本概念、保护密码算法还是密钥？

凯撒密码、单表代替密码、playfair密码、Hill密码、维吉尼亚密码、置换密码

3. 第三章

Feistel密码结构、扩散、混淆、DES加解密、雪崩效应

4. 第四章

模运算性质、欧几里得算法、求逆元

群环域基本概念、基于多项式的有限域构造及运算、密码学中为什么用GF(2m)

5. 第五章AES加密

AES加解密过程：字节代替、行移位、列混合、轮密钥加

AES密钥生成过程

6. 分组密码工作模式

2DES、中间相遇攻击基本过程、3DES

为什么需要分组密码工作模式、五种工作模式的具体构造及特点

7. 随机数与流密码

随机数基本概念、基于密码学的随机数生成、流密码的基本原理

8. 数论基础

素数基本概念、费马小定理、欧拉定理、素性检测概率算法、离散对数的基本概念

9. 公钥密码

对称密码弱点、公钥密码基本原理、RSA公钥密码基本原理及计算

10. 其他公钥密码体制

Diffie-Hellman密钥交换、中间人攻击、ElGamal密码体制

11. 密码学哈希函数

哈希函数基本概念、密码学哈希函数及其基本结构、生日攻击基本原理

12. 消息认证码

消息认证的基本需求、消息认证码、HMAC

13. 数字签名

数字签名基本概念、RSA数字签名、ElGamal数字签名

14. 密钥管理与分发

对称加密的对称密钥分发机制、基于公钥加密的对称密钥分发机制

公钥分发机制、X.509证书、PKI基本概念

15. 用户认证

Needham-Schroeder认证协议、Kerberos基本原理及步骤、基于公钥的远程认证步骤

16. 传输层安全

SSL协议设计思路、SSL握手协议过程以及其能对抗攻击的原因

17. IP安全

IPSec基本原理、AH、ESP、传输模式、隧道模式、密钥管理基本思路