2019 年秋季《计算机网络安全技术》期末复习提纲

期末考试范围请以课程讲义为准。本复习提纲仅列出课程核心内容，仅供参考。

一、必会密码学算法：

- Enigma 加解密
- Casear 密码、Playfair 密码、Hill 密码、Vigenere 密码
- S-DES、DES、3DES　计算题别丢分
- RSA 算法、Diffie-Hellman 密钥交换算法

二、密码学基础

- 密码学基本概念　基本概念
- 古典密码、近代密码（对称）、现代密码（非对称）的各自技术特点
- 流密码和分组密码、混淆与扩展、Feistel 密码结构的基本概念
- 密钥分配的三种情况、密钥分配中心 KDC 模式

三、认证技术　区别是什么？：是否需要Key

- 消息认证基本概念，MAC 码和 Hash 码的工作原理　结合加解密：认证+签名？+加解密？
- 安全 Hash 函数的一般结构、了解 MD5/SHA-1/RIPEMD160 的基本步骤　算法细节并不需要
- 对于网站身份认证，基于 Basic 认证和基于表单认证的工作原理和各自特点

缺陷？各自有什么？第三方认证

四、访问控制技术

- 防火墙的设计目标和局限性、防火墙屏蔽子网结构以及对防火墙的争论　防外不防内

做过作业的内容都不考，ACL不出现，IPSec会出现的

五、互联网安全协议

- CIA 基本概念
- IPsec：工作原理、AH/ESP、安全关联、模式、安全关联组合　每年都考。两种模式放在一起
- IKE：工作阶段和工作模式、IPsec 和 IKE 的工作过程

建立通道+传输，轻载+快速。重点是IPsec，IKE协作过程。：数据库。SADB。。。

- SSL：SSL 体系结构、记录协议和握手协议的工作原理
- HTTPS：基本工作原理，以及防范 ARP 欺骗、报文篡改的技术保障　是如何被防范的？
- SET：电子交易工作原理，双签名机制的设计目标和工作过程

关联和区别

六、无线网安全：

- 802.11 网络连接过程和安全弱点是什么；WiFi 的加密方式有哪些

七、软件入侵　核心概念，会考描述一段恶意软件的行为，分析具有哪些属性。

- 陷门、逻辑炸弹、特洛伊木马、Zombie、病毒和蠕虫各类恶意行为的基本属性

2019 年 12 月 15 日