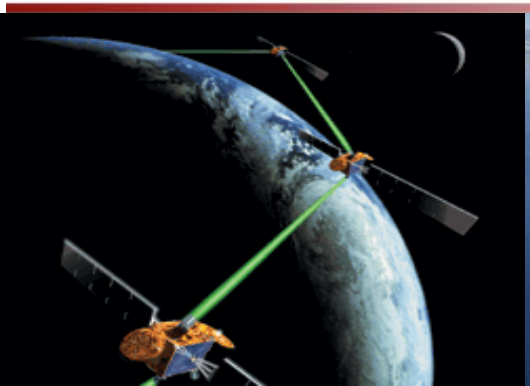
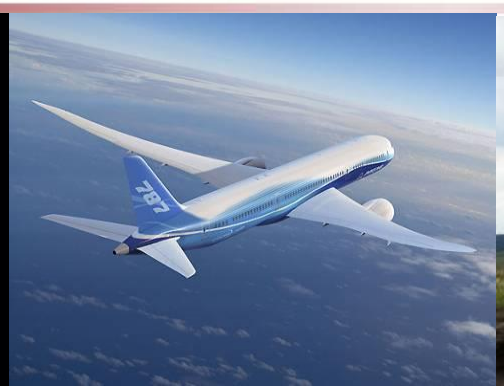
普通高等教育“十一五”国家级规划教材
“信息化与信息社会”系列丛书

复习中要求掌握的知识点

刘建伟

2016年11月08日

第1章　引言

1. 掌握信息安全的四个目标
2. 信息系统中常见的威胁有哪些？
3. 安全攻击的分几大类？有何区别？
4. 掌握OSI的七层参考模型和Internet四层参考模型
5. 熟记X.800标准中的5类安全服务和8种特定安全机制，并简述安全服务和安全机制之间的关系。
6. 能够画出网络安全参考模型和网络访问参考模型

第2-3章　TCP/IP协议族的安全性

1. 必须知道IPv4及IPv6地址的格式及长度
2. 必须知道MAC地址的长度
3. 必须熟记http/ftp/telnet/pop3/smtp/ssh/dns等常用通信协议的端口号及功能
4. 为什么要进行网络地址转换（NAT）？
5. ARP协议的作用是什么？
6. 为什么UDP比TCP协议更加容易遭到攻击？

第4章 单钥密码体制

1. 按照对明文消息的处理方式不同，单钥体制可分为分组密码和流密码。
2. DES的分组长度是多少位？密钥长度是多少位？
3. AES的分组长度是多少位？密钥长度是多少位？
4. 分组密码算法都含有扩散和混淆两个过程。
5. 加密的安全性只取决于密钥的保密，而算法可以公开
6. 加密轮数是否越多越好？密钥是否越长越好？
7. 一条明文经过2个算法串联加密，是否一定更安全？
8. 分组密码的5种工作模式是什么？请画图说明。

第5章 双钥密码体制

1. 双钥密码体制是基于数学难题构造的，请列举出目前存在的数学难题。
2. RSA是基于何种数学难题构造的？Diffie-Hellman是基于何种数学难题构造的？
3. 请写出RSA加密和解密的数学表达式，并指出什么是公钥，什么是私钥？并能做简单的加密和解密计算。
4. RSA是否可以看成是分组密码体制？为什么？
5. 必须知道，用双钥体制加密时采用谁的公钥？解密时采用谁的私钥？

第6章 消息认证与杂凑函数

1. 请说明Hash函数与加密函数有何不同？
2. 杂凑函数具有哪些性质？
3. 什么是消息认证码MAC？如何构造？
4. 什么是消息检测码MDC？简述MDC与MAC的异同。
5. MD5的输出长度是多少位？
6. SHA-1的输出长度是多少位？
7. 熟悉P165页的图6-6的几个图所能够提供的安全功能

第7章 数字签名

1. 数字签名应该具有哪些性质？
2. 数字签名可以分为哪几类？
3. RSA签名是基于何种数学难题？
4. ElGamal签名是基于何种数学难题？
5. 数字签名时，签名者用的是谁的何种密钥？验证时，验证者用的是谁的何种密钥？
6. Diffie-Hellman能用来做数字签名吗？
7. 单钥体制能用来做数字签名吗？
8. 试比较数字签名与双钥加密的区别。

第8章 密码协议

1. 协议的三个要素是什么？
2. 如果按照密码协议的功能分类，密码协议可以分为哪几类？
3. 什么是中间人攻击？如何对Diffie-Hellman协议进行中间人攻击？请画图说明。
4. 请用数学表达式写出DIffie-Hellman协议的密钥交换过程？
5. Diffie-Hellman能用来做数字签名吗？
6. 掌握大嘴青蛙协议和Yahalom安全协议设计的思想。

第9章　数字证书与公钥基础设施

1. 什么是PKI？PKI由哪几部分组成？每个组成部分的作用是什么？
2. 什么是数字证书？X.509证书的格式是什么？
3. 实际中，由谁来签发证书？
4. 签发证书时，是由CA的何种密钥（私钥还是公钥）进行签名？验证证书时，是用谁的公钥来验证？
5. 数字证书的作用是什么？它本质上是为了解决网络安全中的何种问题？

第10章　网络加密与密钥管理

1. 熟记网络加密的4种方式
2. 密钥有哪些种类？它们各自有什么用途？
3. 按照协议的功能分类，密码协议可以分成哪3类？
4. 写出Diffie-Hellman协议的数学表达式
5. 简述为何Diffie-Hellman协议不能抵抗中间人攻击？并画图说明中间人攻击的过程。
6. 一个好的密钥应具备哪些特性？
7. 软件加密和硬件加密有何区别？

第11章　无线网络安全

1. 无线网络面临哪些安全威胁？请写出5种以上。
2. GSM的主要安全缺陷有哪些？
3. 请简要描述GSM蜂窝系统的认证过程。为何挑战值是一个随机数而不能是常数？（画图分析说明）
4. 为何3G系统比2.5G系统更安全？3G系统在提高安全性上作了哪些改进？

谢谢！