# 安全试题

1. **分组密码和流密码的区别**

分组密码是将明文分成若干个固定长度的组(不够用规定的字符填充)，在用相同的秘钥对每一组加密。

而流密码是具有固定开始段，没有固定的结束段，逐位加密长度不定的明文数据流

1. **网络安全漏洞有哪些**

计算机网络安全漏洞是在硬件、软件和协议的具体实现或系统安全策略 存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统  
1.软件漏洞  
2.结构漏洞  
3.配置漏洞  
4.管理漏洞

1. **解释名词VPN**

Virtual Private Network，简称虚拟专用网络

1. 利用密码技术和访问控制技术在公共网络建立的专用通信网络
2. 任意两个节点之间的连接并没有传统专用网络所需的端到端的物理链路，而是利用某种公众网络的资源动态组成
3. 对用户透明，用户好像使用一条专用路线进行通信
4. **网络攻击与防御方法有哪些？**
5. 被动攻击：流量分析、消息内容泄露，防御方法：加密
6. 主动攻击：假冒、重放、改写、拒绝服务，防御方法：认证、数字签名
7. **写出防护墙的基本功能**
8. 防止阻断服务攻击
9. 防止对内部数据的非法盗用和篡改
10. 只允许合法连接通过防火墙进入内网
11. **简述X.509的特点与作用**
12. X.509 是国际电信联盟制定的关于数字证书和认证协议的一种重要标准
13. 解决“在公用网络提供用户目录信息服务”的问题
14. X.059 是基于公钥密码体制和数字签名的服务。其标准中未规定使用摸个特定的算法，但推荐使用RSA；其数字签名需要用到散列函数，但未规定具体的散列算法。
15. **名词解释机密性、完整性、可认证性？**

机密性：确保只有经过授权的人才能访问信息

完整性：保护信息和信息的处理方法准确而完整。

可认证性：能保障用户无法再事后否认曾经对信息进行的生成、签发、接收行为，是针对通信各方信息真实的安全要求

1. **什么是理论安全？什么是实际安全？**

理论安全：攻击者无论截获多少密文，都无法得到足够的信息来唯一的确定明文。

实际安全：如果攻击者拥有无限资源，任何系统都是可以破译的，但是在有限的范围内，攻击者都不能通过系统地分析方法来破解系统，则称这个系统是计算机上安全的或破译这个系统是计算上不可行的

1. **物理安全包括哪些？**

主要包含的内容有：机房环境安全、通信线路安全、设备安全和电源安全。

1. **WPA用了什么办法加强了无线局域网的安全**
2. 802,1x认证(使用了独立的radius服务器)
3. TKIP协议(临时密钥完整协议)：每个包生成不同的加密密钥，增大破解难度
4. 更强的数据完整性检验算法
5. **电子商务SET系统双重签名**

SET 为 Secure Electronic Transaction 的缩写

SET协议也是一个基于可信的第三方认证中心的方案，采用公钥密码体制和X.509数字证书标准，主要应用于B2C模式中保障支付信息的安全性。

1. **DNS缓存中毒？**

DNS缓存中毒，也称为DNS欺骗，是一种利用域名系统（DNS）中的漏洞将攻击者从合法服务器转移到假冒系统的攻击

1. **RSA加密与解密**

公钥：KU = {e, n}

私钥：KR = {d, n}

M 是明文，C是密文，n预先给出

加密：C =

解密：M =

1. **Hill加密与解密**

M 是模 q 的矩阵，对字母加密，q=26，M 要满足 GCD(det M, 26) = 1

其中：M是加密用的矩阵，X代明文，Y是密文

1. **Diffe-Hellman 加密与解密**

安全书P67和密码书p68

两个用户A，B，协商一个素数q以及一个本原根p，且p<q

A生成私钥a，B生成私钥b

A生成公钥，B生成公钥

获取共享秘钥：