2006:

尹霞老师很厚道的...总体比较简单，感觉考试时间稍有点紧（因为可以带电脑开卷，开始时不够紧张，我浪费了不少时间）。原定75分钟收卷，延时10分。
没记题，这是凭印象写的。第7题不太确定，其他应该相差不多。

1.用Caesar,解密，答案是tsinghua。
2.Playfair，密钥词是tsinghua，加密computer。 uroqhsfw
3.使用简化DES，加密。（这题耗时长...应该考前练练）（15分）
注：（与作业一形式一样数据不同）
4.RSA，p=17，q=31，e=7 ，M=2，加密。
5.RSA，公钥e=5，n=35，C=10，求明文M。
6.如何同时提供MAC认证、数字签名和保密性。画图并作简要说明。（12分?）
2.1 30页
希望保证保密性又希望有数字签名的,先用发送方的私钥对hash码进行加密,再用对称密码中的密钥对消息和上述加密结果进行加密

7.IPsec，画出图表。（15分）
l原IPv4报头lTCP报头l数据l
(1)隧道SA中包含传输SA，加密前认证。
(2)隧道SA中包含传输SA，加密后认证。

8-12，问答题,各5分，大概是：
8.Secure Electronic Transactions的用途；双签名机制在哪一阶段，其原理是什么?
1.SET协议为在Internet上进行安全的电子商务提供了一个开放的标准,规定了交易各方进行安全交易的具体流程。
2.SET协议为持卡人、商家、银行提供了一个多方参与的安全通信信道。
3.SET协议基于X.509v3证书的身份认证,保证交易信息的私密性、保密性、完整性、抗抵赖。

购买请求阶段和支付授权阶段

PI(payment information)和OI(orderinformation)必须分开加密和签名,以保证用户的隐私不被泄漏。
PI 和OI必须有联系,以防止商家篡改信息,产生纠纷

?

9.统计异常检测和基于规则入侵检测的区别。
基于统计的方法试图定义正常的、期望的行为,基于规则的方法定义正确的行为。

统计异常行为的入侵检测:收集一段时间内合法用户的行为,
用统计测试来观测其行为,判定该行为是否是合法用户行为

基于规则的入侵检测系统是通过观察系统中的事件,运用规
则集判定一个给定的活动模式是否可疑

基于规则的渗透鉴别建立在专家系统之上,关键在于使用规

则去鉴别已知的渗透或利用已知弱点的渗透。
10.什么是蜜罐技术。

蜜罐是诱导潜在攻击者远离重要系统的一个圈套。

任何对蜜罐的攻击,系统都会给出攻击成功的假相。所以系统管理员可以在不暴露真正在工作的系统条件下,有时间转移、记录、跟踪攻击者

蜜罐系统充满合法用户无法访问、但表面看起来有价值的虚假信息。因此,任何对蜜罐的访问都是可疑的

11.防火墙是什么，作用，分类。

防火墙是在被保护网络和其他网络之间限制访问的一种设备
@ 由软件和硬件设备组成、在内部网和外部网之间、专用网与公共网之间的界面上构造的保护屏障

防火墙的作用
@ 隐藏内部网络结构及资源
@ 保护不安全的网络服务
@ 执行网络间的访问控制策略
@ 统一集中的安全管理
@ 记录并统计网络使用情况
@ 监视和预警

防火墙有多种分类方式
@ 结构、性能、应用部署位置、技术
@ 从防火墙结构上划分
@ 单一主机防火墙
@ 路由器集成式防火墙
@ 分布式防火墙
@ 从防火墙性能上划分
@ 百兆级防火墙
@ 千兆级防火墙
@ 万兆级防火墙

从防火墙应用部署的位置上划分
@ 个人防火墙
@ 安装于单台主机中,防护的也只是单台主机
@ 主要应用于个人用户,通常为软件防火墙,价格最便宜,性能也最差
@ 边界防火墙
@ 最为传统的防火墙,对内、外部网络实施隔离,保护边界内部网络
@ 一般都是硬件类型的,价格较贵,性能较好
@ 芯片级防火墙
@ 使用专有的ASIC(专用集成电路)芯片处理能力强,性能高,价格也最贵
@ 比较知名的厂商有NetScreen、FortiNet、Cisco等

从防火墙技术上划分为四类
@ 包过滤技术(Packet filtering/screening)
@ 地址转换(NAT)
@ 电路层网关(Circuit Gateway)
@ 应用层代理(Proxy)

12.入侵技术的两类是什么；病毒、蠕虫属于那种，这两者区别。
用户入侵
软件入侵

软件入侵
4.3 P28

附：三次作业
作业一：使用S-DES，用密钥(01 11 11 11 01)手工解密二进制串 (1010 0010)。要求说明执行过程，以及执行了IP、Fk、SW、Fk、IP-1后的中间值。

作业二
问题1：用RSA算法对下面数据实现加密和解密。
p=3 ； q=11 ； e=7 ； M=5
p=17 ； q=31 ； e=7 ； M=2
问题2：在使用RSA的公钥体制中，已经截获发给某个用户的密文C=10，该用户的公钥是e=5，n=35，那么明文M等于多少呢?

作业三
简要说明SSL连接和SSL会话的区别是什么？（2分）
简要说明SSL如何防止重放攻击和IP欺骗这两种WEB安全性威胁（3分）
重放攻击：重放先前的SSL连接
IP欺骗：使用伪造的IP地址使主机接收伪造的数据
请分析统计异常检测和基于规则入侵检测的区别。（3分）
蜜罐的含义是什么。（2分）
简述特洛伊木马、病毒、蠕虫的工作原理。（5分）

2007:
2007.秋

2008.1.2 13:30-15:05

各题目考察内容及分值：

1	Caesar	3
2	Playfair	7
3	S-DES	15
4	RSA	10
5	RSA	10
6	MD	10

7 Email Security 5
8 IPsec 15
9 Intrusion 10
10 Intrusion 15

1 Caesar, 解密 wVLqJKxD tsinghua

2 Playfair, 密钥 COMPUTER 加密 TSINGHUA

3 S-DES, 密钥 0111011101, 加密 00101010. 写出详细过程，包括IP, Fk, SW, Fk, IP-1等步骤的结果

4 RSA, p=17 q=31 e=7. 明文M=2, 求密文C=?

5 RSA, C=10 e=5 n=35. 明文M=?

6 请用图形表示一个能够支持消息认证（使用MAC认证）、数字签名和保密性功能的加密解密过程，并简要解释。

7 简要说明RFC821, RFC822, MIME, S/MIME功能上面的区别和联系

8 IPSec, 两台主机之间进行端对端的加密盒认证。
原有的格式：
+----------+-------+----+
|原IPv4报头|TCP报头|数据|
+----------+-------+----+

（1）要求一个隧道SA中有一个传输SA，认证前加密。画图
（2）要求一个隧道SA中有一个传输SA，加密前认证。画图

9 基于统计、基于规则的入侵检测的差别是什么?
什么是蜜罐技术?

10 入侵技术两种类型是什么?
病毒和蠕虫属于哪种，区别
简要说明宏病毒的工作原理。

可以带笔记本。

2008:

一 用Caesar解密 vLOHqwGHOdB
二 用Playfire以PEKING为密钥加密TSINGHUA
三 D-H分发密钥，参数q=19，a=3（本原根），Xa=6，Xb=4
之后用分发的密钥使用S-DES加密（1110 0010），参数
S0=[1,0,3,2;3,1,3,2;0,2,1,3;3,2,1,0];
S1=[3,0,1,0;2,1,0,3;0,1,2,3;2,0,1,3];
四 RSA算法，参数p=17，q=31，e=7，加密2
五 RSA算法，参数n=35，e=5，解密10
六 用图形表示支持消息认证（使用MAC认证）、数字签名和

保密性功能的加密解密过程，并加以解释。
七 IPSec协议，两主机间端到端的加密和认证
要加密的IPv4数据如下
原IPv4头ITCP报头l数据
1. 一个隧道SA中有一个传输SA，认证前加密，画图表示
2. 一个隧道SA中有一个传输SA，加密前认证，画图表示
八 解释防火墙配置结构中的屏蔽子网结构
九 入侵技术有哪两种？什么是蜜罐?
十 病毒和蠕虫属于哪种类型，区别是什么？简要说明宏病毒的工作原理。

2010:
一、用Caesar加密Tsinghua两次，用得到的串作为Playfire的密钥解密某一个串。
二、用图形表示支持消息认证（使用MAC认证）、数字签名和保密性功能的加密解密过程，并加以解释。
三、基于统计的异常检测和基于规则的入侵检测的区别；什么是密罐技术。
四、(1)木马、病毒、蠕虫、Zombie是否要宿主、是否能自我复制，它们的工作原理是什么。
(2)解释引导病毒的工作原理
(3)Morris Worm是因为什么程序错误而诞生的
五、SSL的工作原理；SSL Record Protocol、SSL Handshake Protocol的作用。
六、(1)解释IPSec中密钥交换的工作原理
(2)原始数据 [原IPv4头ITCP头l数据]，画图表示：
传输邻接，先认证后加密
隧道迭代，先加密后认证
七、为什么要用双签名，它的工作原理是什么。
八、已知ALICE、BOB的RSA的p,q,e，发布公钥；他们用D-H来产生会话密钥（已知其p,a,Xa,Xb）；现在ALICE要发给BOB一个消息(8 bits的串)，首先ALICE使用数字签名，然后用会话密钥S-DES加密，发送给BOB。
(1)用图表示此过程，指明所用的密钥
(2)求BOB收到的密文，要求写出详细过程以中间结果