标 题: 计算机网络安全技术(2010.1.5，期末)

// 基本差不多，考试时间由一个半小时增加到了两个小时。

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|TCP头|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

标 题: [网络安全]08年期末（08年12月31日）

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|TCP报头|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。

标 题: 计算机网络安全(2007秋)

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

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。

标 题: 计算机网络安全技术(2006秋)

1.用Caesar,解密，答案是tsinghua。

2.Playfair，密钥词是tsinghua，加密computer。

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?）

7.IPsec，画出图表。（15分）

|原IPv4报头|TCP报头|数据|

(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？

9.统计异常检测和基于规则入侵检测的区别。

10.什么是蜜罐技术。

11.防火墙是什么，作用，分类。

12.入侵技术的两类是什么；病毒、蠕虫属于那种，这两者区别。

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）

(1) 安全目标 CIA 是什么含义？（2分）

(2) Block cipher 和 Stream cipher 的区。别是什么？

S-DES 算法属于上述哪种密码？（2分）

(3) 请说明 Substitution Cipher 和 Transposition Cipher 的工作原理？（3分）

(4) 请用 Caesar 密码加密 TSINGHUA，再用 Caesar 密码解密 TSINGHUA。（3分）

(1) IPSec的工作原理是什么？IPSec文档由哪些部分组成。（3分）

(2) 什么是安全关联SA？什么是SA选择子？（2分）

(3) 传输模式和隧道模式的区别是什么？AH和ESP各自使用了哪种模式？（2分）

(4) IKE使用的ISAKMP框架的两个阶段都完成了什么功能？（3分）

(1) 什么是蜜罐技术？有哪些重要的功能？（5分）

(2) 什么是陷门？（2分）

(3) 蠕虫、木马和病毒哪些属于依赖宿主程序的，哪些属于不依赖宿主程序的。（3分）