1、用Caesar解密wvlqjkxd。

解：tsinghua。

2、Playfair加密computer，密钥词是tsinghua。

解：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| T | S | I/J | N | G |
| H | U | A | B | C |
| D | E | F | K | L |
| M | O | P | Q | R |
| V | W | X | Y | Z |

解：分词co mp ut er。加密co->UR，mp->OQ，ut->HS，er->LO。答案UROQHSLO。

3、使用S-DES加密二进制串(1010 0010)，密钥(01 11 11 11 01)。

解：

计算子密钥：

P10(01 11 11 11 01)=(11 11 11 00 11)

LS-1(11 11 1)=(11 11 1)

LS-1(1 00 11)=(00 11 1)

P8(11 11 10 01 11)=(01 01 11 11) = **K1**

LS-2(11 11 1)=(11 11 1)

LS-2(00 11 1)=(11 10 0)

P8(11 11 11 11 00)=(11 11 11 00) = **K2**

计算初始置换IP：

IP(10 10 00 10)=(00 11 00 01)

L4=(00 11)

R4=(00 01)

计算第一个Fk函数：

对R4扩展置换E/P(00 01)=(10 00 00 10)

与子密钥K1异或(10 00 00 10)⊕(01 01 11 11)=(11 01 11 01)

前4位查找S0表，第(11)=3行第(10)=2列，即3=(11)

后4位查找S1表，第(11)=3行第(10)=2列，即0=(00)

置换P4(11 00)=(10 01)

与L4异或(10 01)⊕(00 11)=(10 10)

输出(10 10 00 01)

计算交换函数SW：

SW(10 10 00 01)= (00 01 10 10)

L4=(00 01)

R4=(10 10)

计算第二个Fk函数：

对R4扩展置换E/P(10 10)=( 01 01 01 01)

与子密钥K2异或(01 01 01 01)⊕(11 11 11 00)=(10 10 10 01)

前4位查找S0表，第(10)=2行第(01)=1列，即2=(10)

后4位查找S1表，第(11)=3行第(00)=0列，即2=(10)

置换P4(10 10)=(00 11)

与L4异或(00 11)⊕(00 01)=(00 10)

输出(00 10 10 10)

计算末尾置换IP-1：

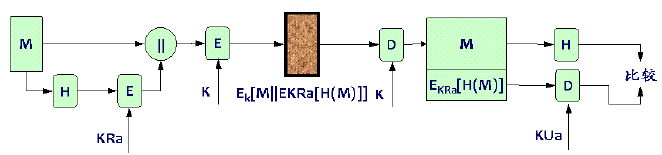
IP-1(00 10 10 10)=(00 11 10 00)

从而可得，所求密文为(00 11 10 00)。

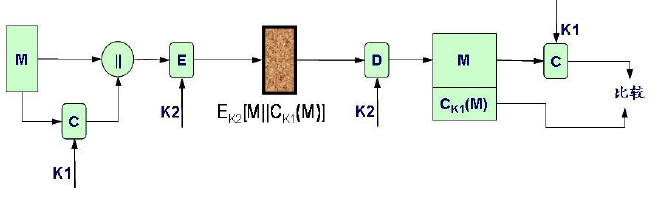
4、RSA，p=17，q=31，e=7 ，M=2，加密。

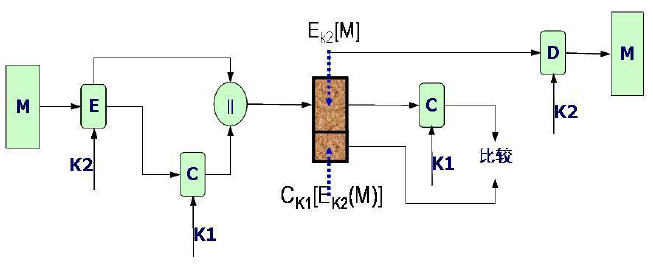
5、RSA，公钥e=5，n=35，C=10，求明文M。

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。**PPT2.1**



认证+保密：





7、IPsec，画出图表。**PPT4.1**

|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。

解：

(1)新IP头 | ESP头 | 原IP头 | AH | TCP头 | 数据 | ESP尾

(2)新IP头 | AH | 原IP头 | ESP | TCP头 | 数据 | ESP尾



8、Secure Electronic Transactions(安全电子交易SET)的用途；双签名机制在哪一阶段，其原理是什么？ **PPT4.3**

解：

SET的用途：参照ppt简介部分。

双签名机制：在支付处理过程的第一阶段。原理参照ppt双签名部分。

9、统计异常检测和基于规则入侵检测的区别。PPT5.1

解：

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定义一个规则集，用于判定给定行为是否为入侵者行为。规则不是由分析审计记录得到的，而是专家系统定义的，可用来识别可疑行为。

统计方法能有效对付假冒者，因为假冒者不可能模仿他们盗用帐号的行为模式，但不能防范合法者。对于合法者的攻击，基于规则的方法可以识别攻击事件和顺序，从而发现入侵。

与基于统计的异常检测一样，基于规则的异常检测无需知道系统内部的安全脆弱性。

10、什么是蜜罐技术。参照PPT5.1

11、防火墙是什么，作用，分类。

防火墙：就是一个位于计算机和它所连接的网络之间的软件。该计算机流入流出的所有网络通信均要经过此防火墙。

防火墙是一项协助确保信息安全的设备，会依照特定的规则，允许或是限制传输的数据通过。防火墙可以是一台专属的硬件也可以是架设在一般硬件上的一套软件

防火墙：一种位于内部网络与外部网络之间的网络安全系统。

防火墙的功能：防火墙对流经它的网络通信进行扫描，这样能够过滤掉一些攻击，以免其在目标计算机上被执行。防火墙还可以关闭不使用的端口。而且它还能禁止特定端口的流出通信，封锁特洛伊木马。最后，它可以禁止来自特殊站点的访问，从而防止来自不明入侵者的所有通信。

从结构上来分，防火墙有两种：即代理主机结构和路由器+过滤器结构，后一种结构如下所示：内部网络过滤器(Filter)路由器(Router)Internet

从原理上来分，防火墙则可以分成4种类型：特殊设计的硬件防火墙、数据包过滤型、电路层网关和应用级网关。安全性能高的防火墙系统都是组合运用多种类型防火墙，构筑多道防火墙“防御工事”。

1. 从软、硬件形式上分为 软件防火墙和硬件防火墙以及芯片级防火墙。 2. 从防火墙技术分为 “包过滤型”和“应用代理型”两大类。 3. 从防火墙结构分为 单一主机防火墙、路由器集成式防火墙和分布式防火墙三种。 4. 按防火墙的应用部署位置分为 边界防火墙、个人防火墙和混合防火墙三大类。 5. 按防火墙性能分为 百兆级防火墙和千兆级防火墙两类。 6.按防火墙使用方法分为 网络层防火墙，物理层防火墙和链路层防火墙三类。

12、入侵技术的两类是什么；病毒、蠕虫属于那种，这两者区别。参照ppt5.1

13、简要说明宏病毒的工作原理。

宏病毒的产生，是利用了一些数据处理系统内置宏命令编程语言的特性而形成的。这些数据处理系统内置宏编程语言的存在使得宏病毒有机可乘，病毒可以把特定的宏命令代码附加在指定文件上，通过文件的打开或关闭来获取控制权，实现宏命令在不同文件之间的共享和传递，从而在未经使用者许可的情况下获取控制权，达到传染目的。

最后,以普通WORD宏病毒为例,看一下它是如何工作的。

WORD使用一种叫做word basic的宏语言,它同时支持一系列的自动宏.当某些事件发生时，word将自动执行文档中包含的有特殊名称的宏.这类操作会独立发生，不论正在使用的可疑文档是否来自磁盘。

只要编制一个含有 autoopen宏的文档，就可自动引发病毒。在word打开这个文档时宏会接管计算机，然后将自己感染到其他文档,或直接删除文件等等。

WORD宏和其他样式储存在模板.dot文件中，因此总是把文档转换成模板再储存他们的宏,这样的结果是默写WORD版本回强制将感染的文档储存在模板中。

14、D-H分发密钥，参数q=19，a=3（本原根），Xa=6，Xb=4。**PPT1.4**

后用密钥使用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];

15、解释防火墙配置结构中的屏蔽子网结构。

这种方法是在内部网络和外部网络之间建立一个被隔离的子网，用两台分组过滤路由器将这一子网分别与内部网络和外部网络分开。

如果攻击者试图完全破坏防火墙，他必须重新配置连接三个网的路由器，既不切断连接又不要把自己锁在外面，同时又不使自己被发现，这样也还是可能的。但若禁止网络访问路由器或只允许内网中的某些主机访问它，则攻击会变得很困难。在这种情况下，攻击者得先侵入堡垒主机，然后进入内网主机，再返回来破坏屏蔽路由器，整个过程中不能引发警报。

屏蔽子网防火墙能够帮助建立一个非防护区，这种类型防火墙利用堡垒主机夹在两个路由器中间是最安全的防火墙系统。

屏蔽子网体系结构添加额外的安全层到屏蔽主机体系结构，即通过添加周边网络更进一步的把内部网络和外部网络（通常是Internet）隔离开。

屏蔽子网体系结构的最简单的形式为，两个屏蔽路由器，每一个都连接到周边网。一个位于周边网与内部网络之间，另一个位于周边网与外部网络（通常为Internet）之间。这样就在内部网络与外部网络之间形成了一个“隔离带”。为了侵入用这种体系结构构筑的内部网络，侵袭者必须通过两个路由器。即使侵袭者侵入堡垒主机，他将仍然必须通过内部路由器。

16、安全目标 CIA 是什么含义？**PPT0.3**

17、Block cipher 和 Stream cipher 的区别是什么？**PPT1.1第12页**

18、Substitution Cipher(代换密码) 和 Transposition Cipher(置换密码)的工作原理。

把明文中的字母重新排列，字母本身不变，但其位置改变了，这样编成的密码称为置换密码。

代换密码则是将明文中的字符替代成其他字符。

19、什么是陷门？

如果一个登陆处理系统允许一个特定的用户识别码,通过该识别码可以绕过通常的口令检查,直观的理解就是可以通过一个特殊的用户名和密码登陆进行修改等操作。这种安全危险称为陷门,又称为非授权访问。

陷门是在某个系统或某个文件中设置的"机关"，使得在提供特定的输入数据时，允许违反安全策略。例如，一个登录处理子系统允许处理一个特定的用户识别码，以绕过通常的口令检查。

**陷门**：计算机操作的陷门设置是指进入程序的秘密入口,它使得知道陷门的人可以不经过通常的安全检查访问过程而获得访问。程序员为了进行调试和测试程序,已经合法地使用了很多年的陷门技术。当陷门被无所顾忌的程序员用来获得非授权访问时,陷门就变成了威胁。对陷门进行操作系统的控制是困难的,必须将安全测量集中在程序开发和软件更新的行为上才能更好地避免这类攻击。

20、解释引导病毒的工作原理

引导型病毒寄生在主引导区、引导区，病毒利用操作系统的引导模块放在某个固定的位置， 并且控制权的转交方式是以物理位置为依据，而不是以操作系统引导区的内容为依据，因而病毒占据该物理位置即可获得控制权，而将真正的引导区内容搬家转移，待病毒程序执行后，将控制权交给真正的引导区内容，使得这个带病毒的系统看似正常运转，而病毒已隐藏在系统中并伺机传染、发作。

引导型病毒进入系统，一定要通过启动过程。在无病毒环境下使用的软盘或硬盘，即使它已感染引导区病毒，也不会进入系统并进行传染，但是，只要用感染引导区病毒的磁盘引导系统，就会使病毒程序进入内存，形成病毒环境。

21、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