注意看网络学堂的期末复习提纲

S-DES必考，而且很容易错

ACL好像不考

来自树洞：

网安的题目除了github上写的，我记得的似乎有：
一、
扩散和混淆，扩散是使密文和密钥的关系更加复杂
CIA包括保密性、继承性、可用性
HTTP的Basic认证和表单认证都要明文传输口令
IKE的两个阶段是协商IKE SA和协商IPsec SA
三、
解密8位的二进制串
六、
传输模式，认证前加密
隧道模式包含传输模式，认证后加密

重点：

Caesar、Playfair、S-DES、RSA、MD、Email Security、IPsec、Intrusion

易错点

IPsec SA

|原IPv4报头|TCP报头|数据|

Q: 隧道SA中包含传输SA，加密前认证：

理解为先认证（AH在里面）再加密（ESP在外面）

因此包变为：

|新IP头|ESP头|原IPv4报头|AH|TCP报头|数据|ESP尾|

Q: 隧道SA中包含传输SA，加密后认证：

理解为先加密（ESP在里面）再认证（AH在外面）

|新IP头|AH|原IPv4报头|ESP头|TCP报头|数据|ESP尾|

这两个都是隧道迭代的例子，通过隧道SA多层嵌套、应用多层安全协议。隧道里面嵌套了一个传输SA，使得一般情况下不能单个SA实现的AH和ESP，可以在这种情况下，同时实现AH和ESP，且一个内层，一个外层。

（传输模式只能做到传输邻接：`[IP1][AH][ESP][upper]`）

SSL

SSL工作在应用层和传输层之间

SSL握手协议是为SSL记录协议协商参数（密钥、加密算法等等）

认证相关

认证：要么摘要（这个无密钥）之后做加密

要么加密之后做一个带密钥的认证（这里就不能使用hash了）

MAC、hash都可以用来做摘要

注意画图怎么画：

M: 明文信息

H： hash函数

||: 拼接 （比如: $M||H(M), M||C_K(M)$）

E （带个K输入）：加密

认证+签名+保密：先算摘要$H(M)$，再签名$E_{KRa}(H(M))$，拼接原信息之后使用对称密钥加密$E_K[M||E_{KRa}(H(M))]$

入侵相关

判断恶意类型：

利用xx软件/系统漏洞： 陷门

在特定时间爆发：逻辑炸弹

伪装成其他程序：木马 （窃取信息、留下后门）

接管计算机发动攻击、不需要宿主的程序：zombie

单独的一个可感染系统软件、需要寄生的程序：病毒 （破坏系统、数据完整性、感染其它可执行文件或硬盘的某个区域）

在网络上自我复制传播（占用资源or破坏其他程序）：蠕虫

HTTP

HTTP的Basic认证和表单认证都要明文传输口令

HTTPS

https提供数据加密、完整性校验、对服务器的身份认证（对应加密机制、数据完整性机制、认证机制）

不能防止ARP欺骗（欺骗了也没用），能防止报文篡改

安全电子交易协议SET

用途：万能的答法：为**安全电子交易**提供了一个开放的**标准**，规定各方进行**安全电子交易**的具体**流程。**

双签名可以连接PI和OI两个报文，防止商家篡改信息，产生纠纷。

具体流程：$E_{KRc}[H(H(PI)||H(OI))]$

其他

明文传输的协议：SMTP(直接发邮件的那个)、DNS、HTTP