南京邮电大学

信息安全考题

考试题型：填空题（1*20）　名词解释（4*6）　简答题（5*6）　综合题（3/26）

1. 网络攻击分为哪两类？各包括哪些具体的攻击行为？p6

答：被动攻击和主动攻击

被动攻击的两种形式：消息内泄漏攻击和流量分析攻击。

主动攻击划分为四类：假冒、重放、改写消息和拒绝服务。

2. 什么是不可抵赖性？P11 重放攻击？P7

答：不可抵赖性防止发送者或接收者否认一个已传输的消息。（因此，当消息发送之后，接受者能够证明宣称的发送者实际上发送了此条消息。同样，在消息接收之后，发送者也能证明宣称的接受者实际上接受了此条消息。

重放攻击：涉及被动获取数据单元并按照它之前的顺序重新传输，以此来产生一个非授权的效应。

3. 什么是传统加密技术？公钥加密技术？各自包括哪些加密算法？P24

答：传统加密技术即单钥加密，发送者和接收者都使用同一个密钥的技术。（*在该体制中，加密密钥和解密密钥是相同的（可互推算），系统的保密性取决于密钥的安全性。*）加密算法：数据加密标准（DES）、三重数据加密标准（3DES）、高级加密标准（AES）。

公钥加密技术：发送者和接收者使用不同的密钥。（*系统中，加密密钥称公开密钥（public key），可以公开发布（电话号码注册）；而解密密钥称私人密钥（private key,简称私钥）。加密：M=D(E(M,pub-key),private-key)认证：M=E(D(M,private-key),pub-key)。*）加密算法：RSA、Diffie-Hellman、DSS 和椭圆曲线加密术。

4. DES 和 3DES 的密钥长度？P27/p30

答：DES：56bit ；　3DES：168bit

5. 分组加密和流密码技术有何不同？P33 哪些加密技术属于分组加密或流密码？

答：分组加密是明文按组（含多个字符）加密。ECB、CBC、CFB

流密码技术是明文按位加密。RC4

6. 分组密码的工作模式有哪些？P37 有什么作用？哪些模式更安全？为什么？

答：工作模式：电子密码本(ECB)、密码分组链接（CBC）、密码反馈（CFB）。

ECB：明文一次被处理 64 比特，而且明文的每一个分组都使用同一个密钥加密。

CBC：加密算法的输入是当前明文分组与前一密文分组的异或；每个分组使用同一密钥。

CFB：将任意分组密码转化为流密码，流密码不需要将消息添加为分组的整数倍，他还能实时操作。

CBC 模式更安全，在此模式中，将明文分组序列的处理链接在一起，每个明文分组的加密函数的实际输入和明文分组之间的关系不固定，因此，64 比特的重复模式并不会被暴露。在 ECB 模式中，同一 64 比特的明文分组在消息中出现了不止一次，他总是产生相同的密文，因此，对于过长的消息，此模式不安全。

7. MAC 的含义？什么是散列函数？什么是哈希函数？作用？P51

答：MAC：消息认证码。即一种认证技术利用私钥产生一小块数据，并将其附在消息上。作用：验证消息的内容有没有被篡改和验证信源是否可信。
散列函数 H 必须具有下列性质：

① H 可适用于任意长度的数据块。

② H 能生成固定长度的输出。

③ 对于任意给定的 x，计算 H（x）相对容易，并且可以用软/硬件方式实现。

④ 对于任意给定值 h，找到满足 H（x）=h 的 x 在计算上不可行。（单向性）

⑤ 对于任意给定的数据块 x，找到满足 H（y）=H（x）的 y 不等于 x 在计算上是不可行的。（抗弱碰撞性）

⑥ 找到满足 H（x）=H（y）的任意一对(x，y）在计算上是不可行的。（抗强碰撞行）

作用:为文件、消息或其他数据块产生“指纹”

哈希（Hash）函数（*在中文中有很多译名，有些人根据 Hash 的英文原意译为“散列函数”或“杂凑函数”，有些人干脆把它音译为“哈希函数”，还有些人根据 Hash 函数的功能译为“压缩函数”、“消息摘要函数”、“指纹函数”、“单向散列函数”等等。*）

1、Hash 算法是把任意长度的输入数据经过算法压缩，输出一个尺寸小了很多的固定长度的数据，即哈

希值。哈希值也称为输入数据的数字指纹（Digital Fingerprint）或消息摘要（Message Digest）等。

Hash 函数具备以下的性质：

2、给定输入数据，很容易计算出它的哈希值；

3、反过来，给定哈希值，倒推出输入数据则很难，计算上不可行。这就是哈希函数的单向性，在技术

上称为抗原像攻击性；

4、给定哈希值，想要找出能够产生同样的哈希值的两个不同的输入数据，（这种情况称为碰撞，

Collision），这很难，计算上不可行，在技术上称为抗碰撞攻击性；

5、哈希值不表达任何关于输入数据的信息。

作用:保证信息的真实性、完整性和不可否认性。

8. 什么是 SHA?p53HMAC?p57

答:SHA：安全散列函数；

HMAC 的设计目标:

1）不改动即可使用散列函数。

2）嵌入式散列函数要有很多的可移植性，以便开发更快或更安全的散列函数。

3）保持散列函数的原有性能,不发生显著退化。

4）使用和处理密钥简单。

5）基于嵌入式散列函数的合理假设，能够很好地理解和分析认证机制的密码强度。

9. MD5 消息摘要的长度？P56 几种 SHA 消息摘要的长度？P53

答:MD5：128bit；

SHA-1：160bit、SHA-256：256bit、SHA-384：384bit、SHA-512：512bit。

10、什么是碰撞？什么是抗强碰撞性？抗弱碰撞性？ P51

答： 若 key1≠key2，有 h(key1)=h(key2)，这种现象称为碰撞。

抗弱碰撞性：对于任意给定的数据块 x，找到满足 H（y）=H（x）的 y 不等于 x 在计算上是不可行的。

抗强碰撞行：找到满足 H（x）=H（y）的任意一对(x，y）在计算上是不可行的。

10. Diffie-Hellman 算法的主要用途？P63

答:使得两个用户能够安全地交换密钥，供以后加密消息时使用。(*该算法仅局限于密钥交换*。)

11. Diffie-Hellman 密钥交换的中间人攻击流程？P65

答：假设 Alice 和 Bob 希望交换密钥，Darth 是攻击者。中间人攻击按如下步骤进行：

1） 为了进行攻击,Darth 首先生成两个密钥 X_{D1} 和 X_{D2},然后计算相应的公钥 Y_{D1} 和 Y_{D2}。

2） Alice 向 Bob 发送 Y_A。

3） Darth 截取 Y_A 并且向 Bob 发送 Y_{D1}。Darth 也计算 $K2 = (Y_A)^{X_{D2}} \bmod q$。

4） Bob 接收 Y_{D1}，计算 $K1 = (Y_{D1})^{X_B} \bmod q$。

5） Bob 向 Alice 发送 X_A。

6） Darth 截取 X_A 并且向 Alice 发送 Y_{D2}。Darth 计算 $K1 = (Y_B)^{X_{D1}} \bmod q$。

7） Alice 接收 Y_{D2}，计算 $K2 = (Y_{D2})^{X_A} \bmod q$。

这时，Bob 和 Alice 认为他们之间共享了一个密钥。但实际上 Bob 和 Darth 共享密钥 K1，而 Alice 和 Darth 共享密钥 K2。将来，Bob 和 Alice 之间的所有通信都以如下的方式受到威胁：

① Alice 发送加密消息 M：E（K2，M)。

② Darth 截取加密的消息并且解密，恢复出消息 M。

③ Darth 向 Bob 发送 E（K1，M）或者发送 E（M'），这里 M'可以是任何消息。

在第一种情况下，Darth 只是想偷听通信内容却不篡改它。在第二种情况下，Darth 想要篡改发送给 Bob 的消息。

12. 什么是数字签名？数字签名的流程？P67

答：假设 Bob 想给 Alice 发送消息。虽然这条消息的保密性并不重要，但是他想给 Alice 能够确认这条消息确实来自于他。当 Alice 收到密文时，她发现能够用 Bob 的公钥进行解密，从而证明这条消息确实是 Bob 加密的。因为没有其他人拥有 Bob 的私钥,所有其他任何人都不能创建由 Bob 的公钥能够解密的密文。因此，整个加密的消息就成为一个数字签名。

13. Nonce 是什么？作用？P97

答：Nonce 是现时，作用：用来检测重放攻击。

14. AAA 是何意？
答：
15. Kerberos 和 X.509 证书是基于什么加密技术的认证标准？P75/p93
答：Kerberos 基于传统加密方法（对称加密体制）的认证协议。
X.509 证书基于公钥加密体制和数字签名的使用。
16. Kerberos 系统结构中含有哪几个主要部分？它们的作用分别是什么？认证的流程？P83
答；1)用于获取票据授权票据的认证服务交换；
2）用于获取服务授权票据的票据授权服务交换；
3）用于获取服务的客户端/服务器认证交换
17. Kerberos 中的票据的作用？票据是如何发放的？P80
答：检查用户是否提了对于这个用户 ID 的正确口令，并检测这个用户是否被允许访问服务器。
AS 创建一个票据，这个票据包括用户 ID、用户网络地址和服务器 ID。
18. 什么是 CA？作用？P100
答：CA 是认证中心。作用：证书的发放者，通常也是撤销证书列表（CRL）的发放者。它还可能支持很多管理功能，虽然这些一般是由一个或多个注册中心代理的。
19. X.509 证书中有哪些内容？P94 它们的作用是什么？P94 使用 X.509 证书进行认证的过程？P97 什么是 CRL？CRL 的作用？P95-96
答：（参考）版本：识别用于该证书的 X.509 标准的版本。
序列号：发放证书的实体有责任为证书指定序列号，以使其区别于该实体发放的其它证书。此信息用途很多。例如，如果某一证书被撤消，其序列号将放到证书撤消清单（CRL）中。 签名算法标识符：用于识别 CA 签写证书时所用的算法。

签发人姓名：签写证书的实体的 X.500 名称。它通常为一个 CA。 使用该证书意味着信任签写该证书的实体（注意：有些情况下（例如根或顶层 CA 证书），签发人会签写自己的证书）。
有效期：每个证书均只能在一个有限的时间段内有效。该有效期以起始日期和时间及终止日期和时间表示，可以短至几秒或长至一世纪。所选有效期取决于许多因素，例如用于签写证书的私钥的使用频率及愿为证书支付的金钱等。它是在没有危及相关私钥的条件下，实体可以依赖公钥值的预计时间。
主体名：证书可以识别其公钥的实体名。此名称使用 X.500 标准，因此在 Internet 中应是唯一的。它是实体的特征名（DN），例如， CN=Java Duke，OU=Java Software Division，O=Sun Microsystems Inc，C=US （这些指主体的通用名、组织单位、组织和国家）。
主体公钥信息：这是被命名实体的公钥，同时包括指定该密钥所属公钥密码系统的算法标识符及所有相关的密钥参数。
证书注销列表(Certificate Revocation List，简称 CRL)，是一种包含注销的证书列表的签名数据结构。 （*CRL 是 Certificate Revocation List 的缩写，中文翻译为证书废弃列表，*）主要功能是保存废除证书序列号和废除的原因
20. X.509 证书的目的是什么？为达到这个目的，采取了那些措施？
答：目的：可以让用户获得公钥证书，以便用户团体可以确信公钥的有效性。

21. 什么是证书链？作用？P96
答：数字证书由颁发该证书的 CA 签名。多个证书可以绑定到一个信息或交易上形成证书链，证书链中每一个证书都由其前面的数字证书进行鉴别。最高级的 CA 必须是受接受者信任的、独立的机构。
作用：沿着一条路径得到另一个用户的公钥证书。
22. 什么是零知识认证？作用是什么？
答：所谓零知识证明，指的是示证者在证明自己身份时不泄露任何信息，验证者得不到示证者的任何私有信息，但又能有效证明对方身份的一种方法。
23. 什么是 IPSec？目的是什么？P142 有哪两种封装模式？P147 哪种模式支持端到端、端到网关、网关到网关的隧道？哪种模式只支持端到端？P141
答：“Internet 协议安全性（IPSec）”是一种开放标准的框架结构，通过使用加密的安全服务以确保在 Internet 协议（IP）网络上进行保密而安全的通讯。
目的：提供了在 LAN、专用和公用 WAN 以及互联网中安全通信的性能。
传输模式和隧道模式。隧道模式。阐述模式。
24. IPSec 中 AH 和 ESP 分别有什么作用？有何不同？P148/p152
答：AH（认证报头）给数据完整性和 IP 包认证提供支持。
ESP（封装安全载荷）提供保密服务，包括报文内容保密和流量限制保密。
AH：认证报头。
ESP：封装安全载荷。
1、AH 没有 ESP 的加密特性
2、AH 的认证是对整个数据包做出的，包括 IP 头部分，因为 IP 头部分包含很多变量，比如 type of service（TOS），flags，fragment offset，TTL 以及 header checksum.所以这些值在进行认证前要全部清零。否则 hash 会 mismatch 导致丢包。
相反，ESP 是对部分数据包做认证，不包括 IP 头部分。
25. 什么是 SA？作用？P145
答：安全关联（Security Association，SA）是两个应用 IPsec 实体（主机、路由器）间的一个单向逻辑连接，决定保护什么、如何保护以及谁来保护通信数据。SA 用一个三元组（安全参数索引 SPI、目的 IP 地址、安全协议）唯一标识。 SA 提供安全服务。
26. SSL 中有哪两大协议？分别有何作用？P178
答：（参考）SSL 记录协议，提供两种服务：机密性，消息完整性。
SSL 密码变更规格协议，使得延迟状态改变为当前状态，更新连接上应用的密码机制
SSL 报警协议，将与 SSL 相关的报警传达给对等实体
SSL 握手协议，允许客户端和服务器相互认证，并协商加密和 MAC 算法，以及用于保护 SSL 记录中所发送数据加密密钥
27. 保证网络支付安全的协议是什么协议？P197
答:SET.
28. 什么是双重签名？作用是什么？双重签名的过程？P196
答：双重数字签名 定义：有的场合需要寄出两个相关信息给接收者，接收者只能打开一个，而另一个只需转送，不能打开看其内容。
把要发送给不同接受者的两条消息连接起来。
过程：1）商家收到 OI 并验证签名。2）银行收到 PI 并验证签名。3）消费者把

OI 和 PI 联系起来并能够证明这种联系。
29. 防火墙有哪几种类型？P286
答：包过滤器、应用级网关、电路级网关。
30. 屏蔽主机防火墙和屏蔽子网防火墙有何不同？P292
答:屏蔽主机防火墙配置中，防火墙包含两个系统：包过滤路由器和堡垒主机。此配置同样支持在提供直接互联网访问时的灵活性，提供的双层安全机制在本配置中得到保障。
屏蔽子网防火墙配置中，使用了两个包过滤路由器，其中一个在堡垒主机和互联网之间，另一个在堡垒主机和内部网络之间。此配置创建了一个独立的子网，它可能只包含堡垒主机，但也可能包含一个或多个信息服务器和实现拨入能力的调制解调器。
31. 有哪两种入侵检测的方法？P240
答：统计异常检测、基于规则的检测。
32. 什么是蜜罐？作用？P248
答：蜜罐是一个诱惑系统，用来把潜在的攻击者从重要系统中引诱开。
作用：转移攻击者对重要系统的访问；收集关于攻击者活动的信息；鼓励攻击者停留在系统中足够长的时间以便管理员作出反应。
补充：
(1)WEP 中主要存在哪些缺陷？
答:没有反重放机制；
CRC32 是很简陋的完整性校验算法，攻击者在不知密钥情况下就能修改数据而不被发现；
WEP 中直接将共享密钥和 IV 一起作为 RC4 的种子，当 IV 相同时，密钥流就会一样，存在密钥重用问题，容易被统计破解；
(2)针对这些缺陷，TKIP 做了怎样的改进？
答：为避免重放攻击，对 MPDU 采用了 TSC，发现重复的 TSC 就认为受到重放攻击；
采用更加完善的 MIC 算法对 MSDU 进行完整性校验，计算散列值时使用了密钥(TK 的一部分)；
采用层次结构的密钥管理，TK（部分)、发送方的 MAC 地址、TSC、IV 以及相应的密钥混合函数共同生成 RC4 的种子，并且 TK 也是定期更新，提高了加密的安全性。
(3)在 WPA2 中，哪个加密机制安全性最高？该机制中采用什么加密算法？
答:CCMP，AES
(4)基于 PSK 的认证和基于 802.1x 的认证分别适合在什么场合应用？为什么？
答:基于 PSK 认证适合个人家庭用户使用，基于 802.1x 的认证适合企业用户。
因为企业用户众多，如果采用 PSK，每个用户都必须维护公有的 PSK，一旦某个用户的 PSK 泄露了，那么整个网络的密钥层次结构就能被攻破。而 802.1x 采用认证服务器的集中化管理，简化同时也加强了安全管理。
另外，由于基于 802.1x 认证需要有专门的认证服务器，所以不适合家庭用户采用。
BALABALABALA