

《网络安全》期末速通

1. 引言

题型: 选择x1, 简答x1.

重点: 攻击的模式; 主动攻击和被动攻击的定义和例子.

[网络攻击的模式]

(1) 模式: 中断、窃听、篡改、伪造.

(2) 分类:

① 主动攻击:

(i) 定义: 更改数据流或发送假数据流.

(ii) 例: 中断、篡改、伪造、假冒、重放、拒绝服务.

② 被动攻击:

(i) 定义: 窃听和监视传输, 获得传输信息.

(ii) 例: 窃听、流量分析.

[CIA三元组] 机密性、完整性、可用性.

[例]

(1) 硬件:

① 可用性: 设备被偷盗或禁用, 因而拒绝提供服务.

② 机密性: 未加密的USB设备被盗.

(2) 软件:

① 可用性: 程序被删除拒绝用户访问.

② 机密性: 软件的非授权拷贝.

③ 完整性: 正在运行的程序被修改, 使其在执行过程中失败或执行一些非预期的任务.

(3) 数据:

① 可用性: 文件被删除, 拒绝用户访问.

② 机密性: 非授权读取数据, 分析统计数据来揭露潜在的深层次的数据.

③ 完整性: 修改已有的文件或伪造新文件.

(4) 通讯线路和网络:

- ① 可用性: 消息被破坏或删除, 通信线路或网络不可用.
- ② 机密性: 消息被读取, 消息流量模式被观察到.
- ③ 完整性: 消息被修改、延迟、重新排序或复制、伪造虚假消息.

[网络访问的安全实现]

- (1) 设计访问控制功能单元, 鉴别用户身份.
- (2) 实施安全控制, 只允许授权用户访问.

2. 对称加密

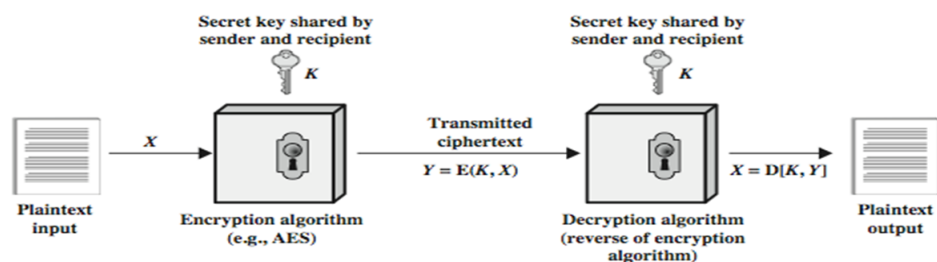
题型: 选择x1, 简答(猜测画图)x1.

重点: 解释分组密码运行模式; 画分组密码运行模式; 加密的步骤; 密码安全的要求; 密码分析的分类; DES和AES中的操作是否可逆; 流密码的步骤; RC4的弱密钥.

2.1 对称加密

[密码算法的强度的影响因素]

- (1) 因素: 算法强度、密钥保密性、密钥长度.
- (2) 加密算法公开, 密钥保密.

[对称加密模型]

(1) 数学表示: $C = E(K, M)$, $M = D(K, C)$, 其中 C 是密文, M 是明文, K 是私钥, E 是加密算法, D 是解密算法.

(2) 对称密码的安全要求:

- ① 一个强加密算法.
- ② 只有发送方和接收方知道私钥.
- ③ 存在安全的信道分发私钥.

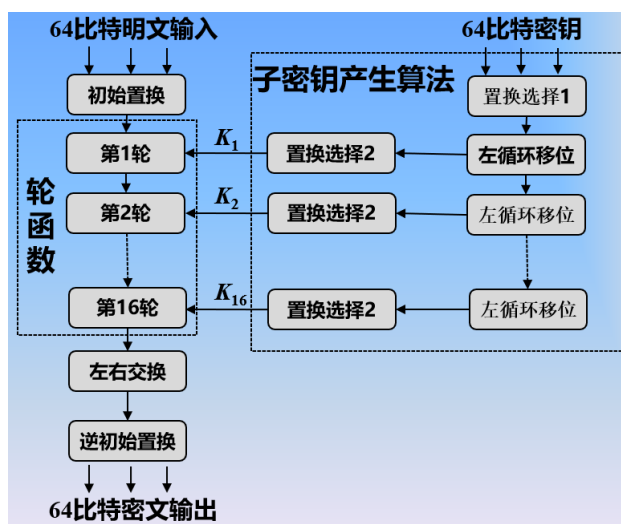
[密码分析的分类]

- (1) 唯密文攻击: ①加密算法; ②要解密的密文.
- (2) 已知明文攻击: ①加密算法; ②要解密的密文; ③用密钥产生的一个或多个明密文对.
- (3) 选择明文攻击: ①加密算法; ②要解密的密文; ③攻击者选定明文消息, 及使用密钥产生的对应密文.
- (4) 选择密文攻击: ①加密算法; ②要解密的密文; ③攻击者选定密文消息, 及使用密钥产生的对应明文.
- (5) 选择文本攻击: ①加密算法; ②要解密的密文; ③攻击者选定明文消息, 及使用密钥产生的对应密文; ④攻击者选定密文, 及使用密钥产生的对应解密密文.

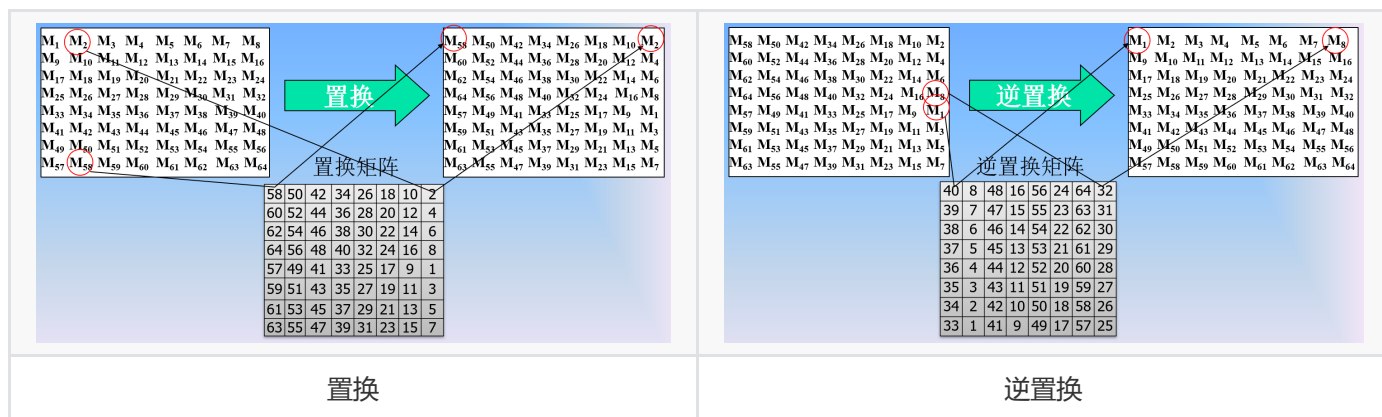
2.2 DES

[数据加密标准DES] DES的三个操作: ①初始置换; ②轮函数操作; ③子密钥产生算法.

[DES流程图]



[置换与逆置换]



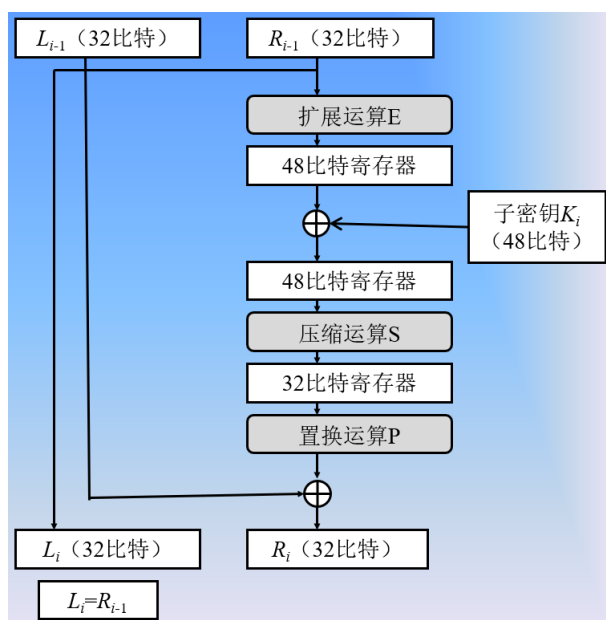
[例] 求置换矩阵 $\begin{bmatrix} 25 & 03 & 07 & 05 & 09 \\ 02 & 06 & 08 & 04 & 10 \\ 12 & 11 & 13 & 16 & 17 \\ 15 & 14 & 22 & 21 & 19 \\ 20 & 18 & 23 & 24 & 01 \end{bmatrix}$ 的逆置换矩阵.

[解] 逆置换矩阵中 01 处的值为置换矩阵中值 01 所在的位置, 即 25 ;

逆置换矩阵中 02 处的值为置换矩阵中值 02 所在的位置, 即 06 ;

故逆置换矩阵 $\begin{bmatrix} 25 & 06 & 02 & 09 & 04 \\ 07 & 03 & 08 & 05 & 10 \\ 12 & 11 & 13 & 17 & 16 \\ 14 & 15 & 22 & 20 & 21 \\ 19 & 18 & 23 & 24 & 01 \end{bmatrix}$.

[轮函数] 对右半数据 R_{i-1} 进行如下操作:



(1) 扩展运算: R_{i-1} 通过选择扩展运算 E 扩展成 48 - bit 的数据.

(2) 子密钥异或: 与子密钥 K_i 异或生成新的 48 - bit 数据.

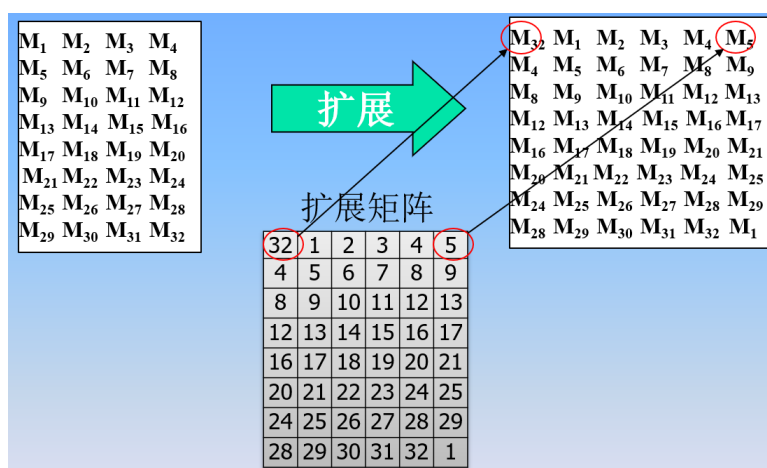
(3) 压缩运算: 经过压缩运算 S 变成 32 - bit 数据.

(4) 置换运算: 进行置换运算 P .

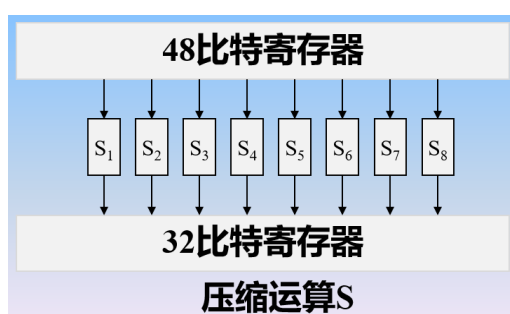
(5) 异或运算: 与左半部分数据 L_{i-1} 进行异或.

[注] 轮函数不可逆, 因为压缩运算不可逆.

[扩展运算]



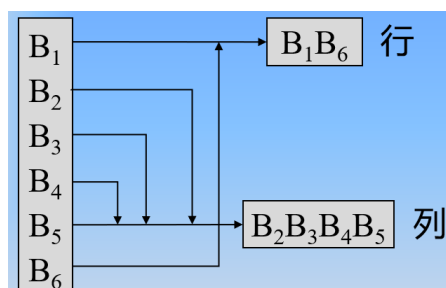
[压缩运算S-BOX]



(1) 压缩运算的特点:

- ① DES中的压缩运算 S 是非线性的, 其他运算都是线性的.
- ② 压缩运算 S 不可逆, 不易分析, 安全性高.

(2) 流程图:

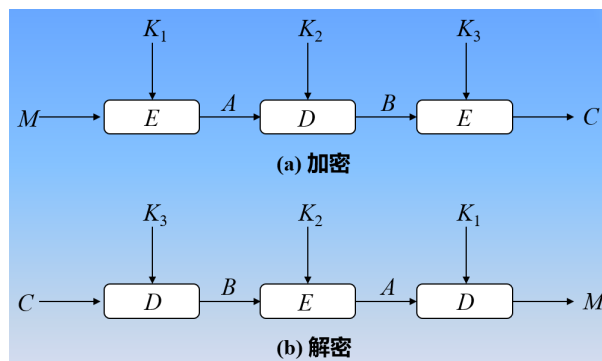


[例] 设DES中的S-BOX如下图所示:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

若输入数据 $b_1b_2b_3b_4b_5b_6 = (110011)_2$, 则行号 $b_1b_6 = (11)_2 = 3$, 列号 $b_2b_3b_4b_5 = (1001)_2 = 9$.

对应S-BOX的第3行第9列, 数据为14, 故输出为 $(1100)_2$.

[3重DES]

(1) (两个密钥的)3DES一般需 3 个不同的密钥, 但也可在 $E - D - E$ 序列下使用 2 个密钥, 即 $C = E_{K_1}(D_{K_2}(E_{K_1}(M)))$, 这样在安全上加密和解密等效. 特别地, $K_1 = K_2$ 时为DES.

(2) (三个密钥的)3DES加密 $C = E_{K_3}(D_{K_2}(E_{K_1}(M)))$, 解密 $M = D_{K_1}(E_{K_2}(D_{K_3}(C)))$.

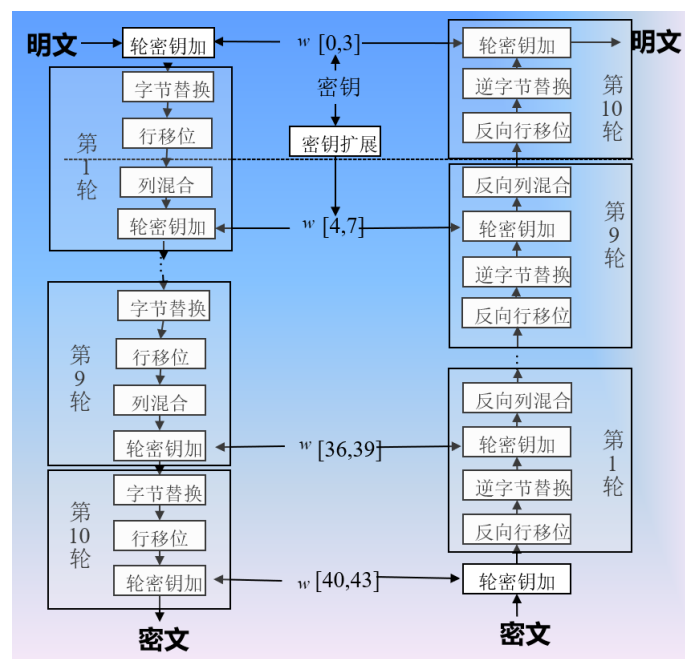
2.3 AES**[AES的流程]**

(1) 明文分组有 4 列字节方阵, 每列 4 个字节, 被复制到状态矩阵数组, 根据密钥行进行 9/11/13 轮运算, 包括:

- ① 字节替换: 对每个字节使用一个置换.
- ② 行移位: 对行做移位.
- ③ 列混合: 对列的每个字节做替换.
- ④ 轮密钥加: 将当前分组与一部分扩展密钥按位异或.

(2) 上述过程可看作交替异或密钥和扰乱消息字节.

(3) 最后一轮不完整, 只有①②④操作.

[AES的流程图]

(1) 128 比特密钥长度的AES执行 9 轮完整运算和 1 轮不完整运算.

(2) 原始密钥扩展为 44 个字(一个字为 32 bit)的子密钥, 用于每轮的运算.

[AES的解密过程] AES轮运算中的四个操作都可逆, 它们的逆操作即解密过程:

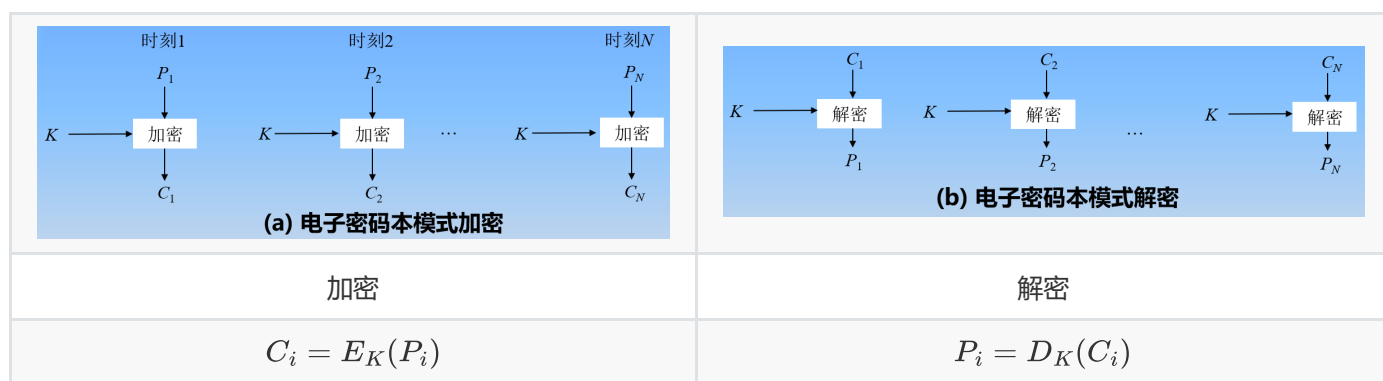
- (1) 逆字节替换: 查找逆S盒.
- (2) 反向行移位: 相应执行右移操作.
- (3) 反向列混合: 乘逆矩阵恢复.
- (4) 轮密钥加: 异或操作.

[DES与AES的区别]

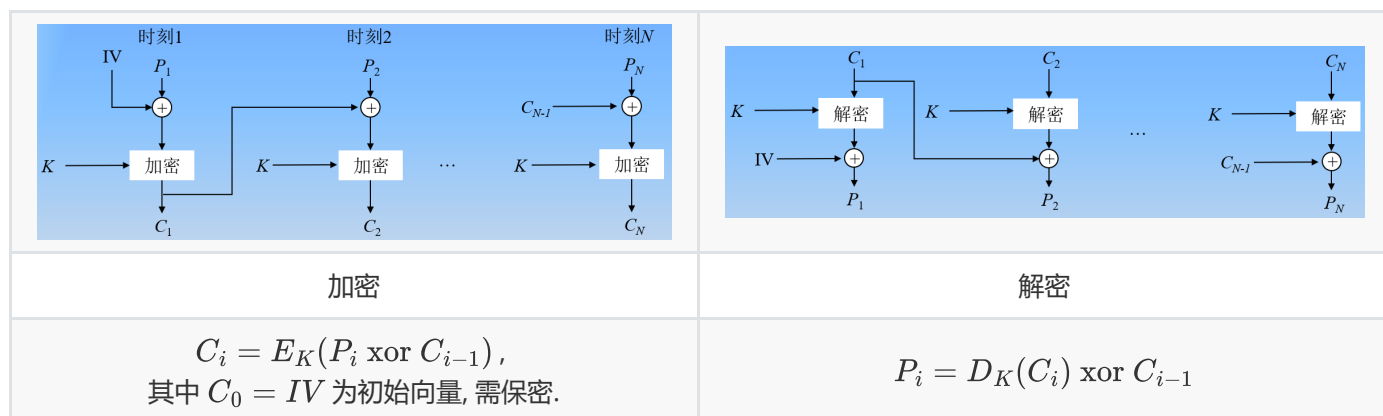
- (1) DES的分组分左右迭代, 存在不可逆操作.
- (2) AES整个分组迭代, 所有操作都可逆.

2.4 分组密码的运行模式

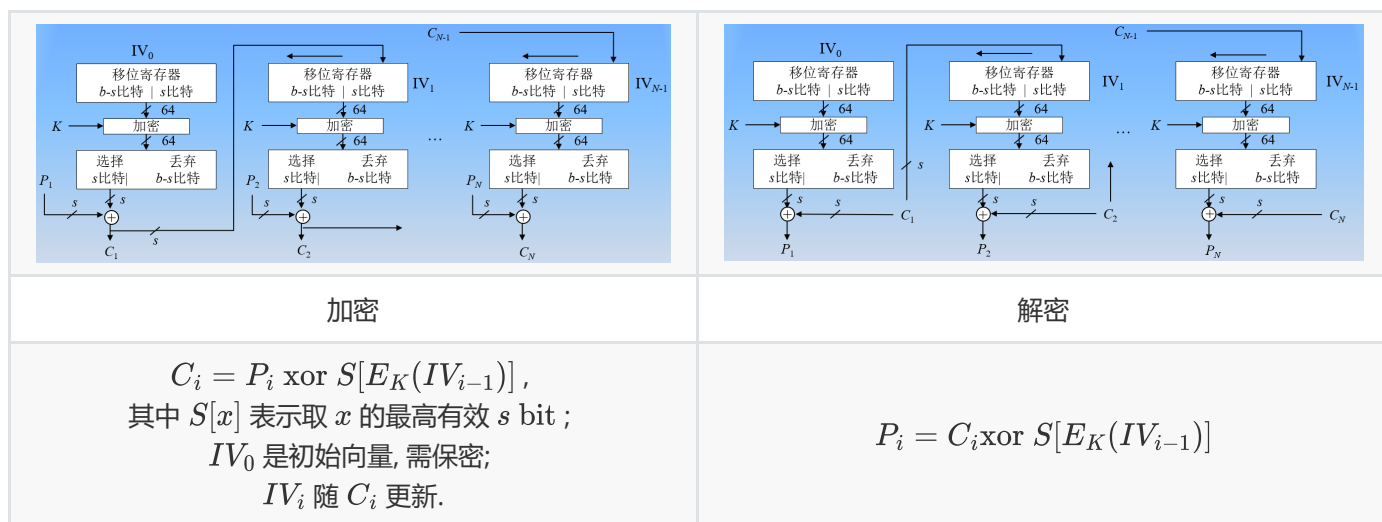
[电子密码本模式] 消息被独立分组进行加密, 每个分组是一个值, 将会被替换, 像一个密码本一样.



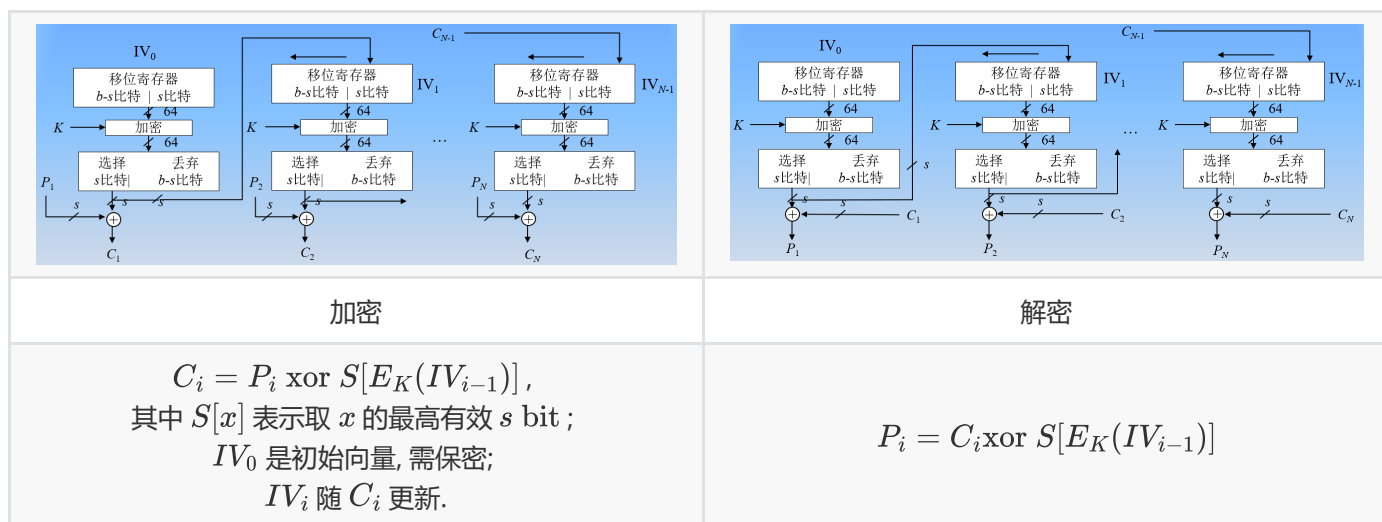
[密码分组链接模式] 消息被切分为多个分组, 加密时每个明文分组与前面的密文分组相链接, 使得同一明文分组将会产生不同的密文分组.



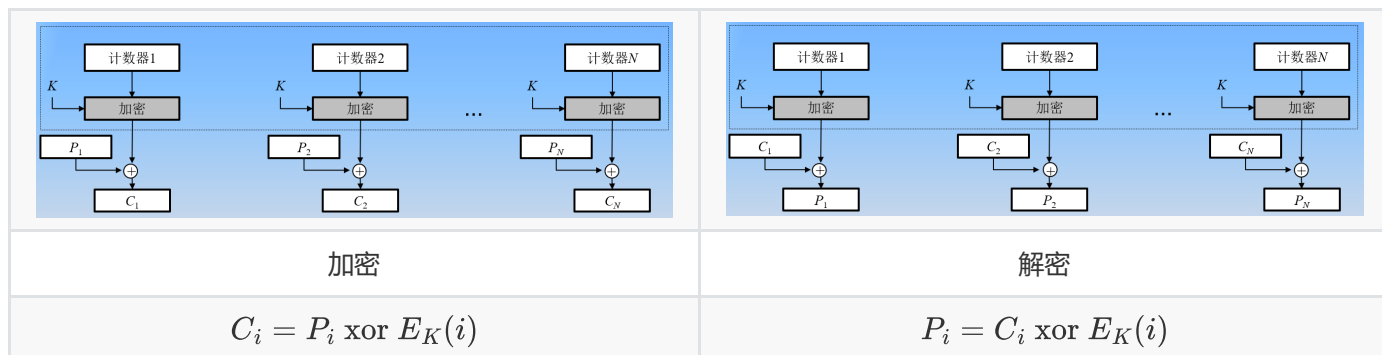
[密码反馈模式] 将分组密码转化为流密码, 无需将消息填充为分组长度的整数倍, 还可实时操作, 充分利用传输信道.



[输出反馈模式] 类似于密码反馈模式, 区别在于反馈的内容是加密器输出的随机数而非密文, 故不具有错误传播特性.



[计数器模式] 计数器模式应用于ATM(异步传输模式)、网络安全和IPSec中. 它类似于密码反馈模式, 但不是加密反馈值, 而是加密每个计数值, 再对明文分组进行异或操作. 每个明文分组需有不同的密钥和计数值, 且不重复使用.



[不同运行模式的对比]

(1) 需实现解密操作: 电子密码本模式、密码分组连接模式.

无需实现解密操作: 密码反馈模式、输出反馈模式、计数器模式.

(2) 无需实现解密操作的原因: 只对分组密码加密操作生成的密钥流做异或.

2.5 流密码

[分组密码和流密码的区别]

(1) 分组密码一次处理一个输入分组, 产生与之对应长度的输出分组.

(2) 流密码在运行过程中连续地处理输入元素, 每次输出一个元素.

(3) 例子:

① 分组密码: DES、3DES、AES.

② 流密码: RC4.

[RC4弱密钥的推导]

RC4的密钥调试为:

```

1  for i = 0 to 255:
2      S[i] = i
3      T[i] = K[i % keylen]
4      j = 0
5
6  for i = 0 to 255:
7      j = (j + S[i] + T[i]) % 256
8      swap(S[i], S[j])

```

只需保证 $j = (j + S[i] + T[i]) \pmod{256}$, 则:

(1) $i = 0$ 时, $(0 + S[0] + T[0]) = 0 \pmod{256}$, 即 $T[0] = 0$.

(2) $i > 0$ 时, $(i - 1 + S[i] + T[i]) = i \pmod{256}$, 即 $T[i] = 1 - S[i] = 257 - S[i] \pmod{256}$.

3. 公钥密码

题型: 选择x1, 计算x2.

重点: RSA和D-H密钥交换的计算; 散列函数; 消息认证码; HMAC、CMAC、CCM在何处应用; 数字签名与证书的关系.

3.1 RSA

[公钥密码系统的应用]

- ① 加解密: 发送者用接收者的公钥加密消息.
- ② 数字签名: 发送者用自己的私钥签名消息.
- ③ 密钥交换: 通信双方用公钥密码交换会话密钥.

[RSA算法] RSA属于分组密码, 基于大整数运算. 对某个 n , 明文与密文都是 $[0, n - 1]$ 范围内的整数, 则加密过程: $C = M^e \bmod n$, 其中 $M \in [0, n - 1]$, 解密过程: $M = C^d \bmod n = M^{ed} \bmod n$, 其中公钥 $PU = \{e, n\}$, 私钥 $PR = \{d, n\}$.

[RSA的密钥设置]

- (1) 随机选择两个大素数 p, q , 求它们的乘积 $n = p \times q$ 作为模数.
- (2) 求 n 的Euler函数 $\varphi(n) = (p - 1)(q - 1)$.
- (3) 选择一个与 n 互素的加密密钥 e , 使得 $1 < e < \varphi(n)$, 且 $\gcd(e, \varphi(n)) = 1$.
- (4) 求 e 模 $\varphi(n)$ 的乘法逆元 d 作为解密密钥.
- (5) 公布公钥 $PU = \{e, n\}$, 保留私钥 $PR = \{d, n\}$.

[例] RSA的密钥设置.

- ① 选择素数 $p = 17, q = 11$, 计算 $n = p \times q = 17 \times 11 = 187$.
- ② 求Euler函数 $\varphi(n) = (p - 1)(q - 1) = 16 \times 10 = 160$.
- ③ 取 $e = 7$ 使得 $\gcd(e, \varphi(n)) = \gcd(7, 160) = 1$.
- ④ 因 $23 \times 7 = 161$, 取 $d = 23 < 160$, 则 $de \equiv 1 \pmod{160}$.
- ⑤ 公布公钥 $PU = \{7, 187\}$, 保留私钥 $PR = \{23, 187\}$.

[例] RSA的加密和解密.

消息 $M = 88$, 公钥 $\{7, 187\}$, 私钥 $\{23, 187\}$.

- (1) 加密: $C = M^e \bmod n = 88^7 \bmod 187 = 11$.
- (2) 解密: $M = C^d \bmod n = 11^{23} \bmod 187 = 88$.

[例] 设RSA中截获了发给其他用户的密文 $C = 10$, 该用户的公钥 $e = 7$, RSA的参数 $n = 77$. 求明文 M .

[解] $n = 77 = 7 \times 11$, 取 $p = 7, q = 11$, 则 $\varphi(n) = (p-1)(q-1) = 60$.

私钥 $d = e^{-1} \bmod 60 = 43$, 则 $M = C^d \bmod n = 10^{43} \bmod 77 = 10$.

[数字签名与数字证书的区别和联系]

(1) 区别:

① 数字签名是使用数字证书和信息加密技术, 用于鉴别电子数据信息.

② 数字证书是由权威公证的第三方认证机构(Certificate Authority, CA)负责签发和管理的、个人或企业的网络数字身份证明.

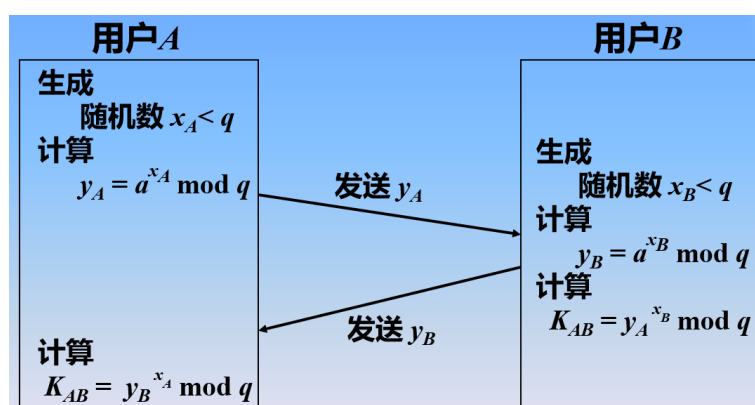
(2) 联系:

① 数字签名是用数字证书对文件签名后在文件上保留的签署结果, 用于证明签署人的签署意愿.

② 数字证书是数字签名的基础, 数字签名是数字证书的一种应用.

3.2 D-H密钥交换

[Diffie-Hellman密钥交换过程]



(1) 用户 A 和用户 B 都同意以下全局参数: 大素数或多项式 q 、模 q 下的原根 a .

(2) 每个用户产生自己的密钥: 分别选择一个数字 $x_A < q, x_B < q$, 计算公开密钥 $y_A = a^{x_A} \bmod q, y_B = a^{x_B} \bmod q$.

(3) 公开密钥 y_A 和 y_B , 保留私钥 x_A 和 x_B .

(4) 用户 A 和用户 B 共享会话密钥 $K_{AB} = a^{x_A x_B} \bmod q = y_A^{x_B} \bmod q = y_B^{x_A} \bmod q$.

K_{AB} 作为会话密钥, 可在用户 A 和用户 B 间采用私钥加密方案中使用.

(5) 若用户 A 和用户 B 接着通信, 他们会采用同样的密钥, 除非他们选择新的公钥.

[例] 假设用户 A 和用户 B 交换会话密钥, 同意素数 $q = 353$ 和 $a = 3$.

(1) 用户 A 选择随机私钥 $x_A = 97$, 用户 B 选择随机私钥 $x_B = 233$.

(2) 用户 A 计算公钥 $y_A = a^{x_A} \bmod q = 3^{97} \bmod 353 = 40$, 发送给用户 B .

用户 B 计算公钥 $y_B = a^{x_B} \bmod q = 3^{233} \bmod 353 = 248$, 发送给用户 A .

(3) 收到公钥后, 双方分别计算会话密钥:

A 计算 $K_{AB} = y_B^{x_A} \bmod q = 248^{97} \bmod 353 = 160$.

B 计算 $K_{AB} = y_A^{x_B} \bmod q = 40^{233} \bmod 353 = 160$.

(4) 攻击者已知 $q = 353, a = 3, y_A = 40, y_B = 248$.

攻击者可用穷举搜索的方法推出会话密钥, 求解方程 $3^{x_A} \bmod 353 = 40$ 或 $3^{x_B} \bmod 353 = 248$.

一直搜索直至等式成立, 可求得 $x_A = 97, x_B = 233$. 只有数值很大时穷举法才不切实际.

4. 密钥管理与分发

题型: 选择x1.

重点: 了解Kerberos.

[Kerberos的概述]

(1) 有一个基本的第三方认证策略.

(2) 有一个认证服务(AS).

① 用户开始与AS交涉, 验证自己.

② AS提供一个认证凭证(票据).

(3) 用户基于自己的票据, 请求进入票据的其他服务.

(4) 在一个复杂协议中用DES.

[PKIX的协议]

(1) 证书管理协议(CMP).

(2) 证书管理消息(CMC).

浏览一遍课件即可.

5. 传输层安全

题型: 选择x1.

重点: 传输层安全的协议; 每一层的功能; HTTPS; SSL、TLS、SSH; 提供的服务.

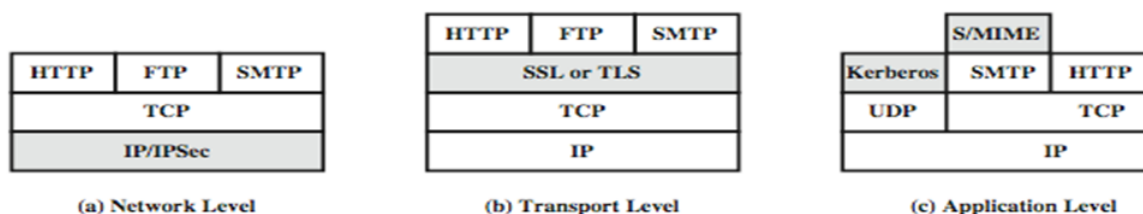
[传输层安全] 传输层安全(Transport Layer Security, TLS)采用的IETF标准RFC2246非常接近于SSLv3,但有如下不同点:

- (1) 记录规格版本号.
- (2) 使用HMAC.
- (3) 一个伪随机函数扩展密钥: 基于HMAC使用SHA-1或MD5.
- (4) 有额外的警告码.
- (6) 支持的密钥套件有改变.
- (7) 证书类型和握手信息有改变.
- (8) 加密计算和填充有改变.

[安全套接层] 安全套接层(SSL, Secure Sockets Layer)提供传输层安全服务.

- (1) SSL采用TCP提供一种可靠的端对端的安全服务.
- (2) SSL由两层协议组成.

[Web流量安全方法]



- (1) 应用层: Kerberos和S/MIME.
- (2) 传输层: SSL和TLS.
- (3) 网络层: IPSec.

[HTTPS] HTTPS(HTTP over SSL).

- (1) 用HTTP和SSL/TLS的结合来实现网络浏览器和服务器间的安全通信. SSL或TLS上的HTTP无根本性区别.
- (2) 使用"https://"而不是"http://", 使用端口 443 而非 80 .
- (3) 加密URL、文件内容、表单内容、cookies、HTTP报头.

[Secure Shell] Secure Shell(SSH).

- (1) 网络信息安全通信协议: 相对简单和经济.
- (2) SSH1提供安全的远程登录装置:
 - ① 替换TELNET和其他不安全的远程登陆机制.
 - ② 提供客户端/服务器功能.
- (3) SSH2修补了一些安全缺陷.
- (4) 记录在标准FECs 4250到4254中.
- (5) SSH客户端和服务端随处可见.
- (6) 是远程登陆/X隧道选择的方法.

[端口转发]

- (1) 将任何不安全的TCP连接转换成安全的SSH连接:
 - ① SSH传输层协议在SSH客户端和服务端建立一个TCP连接.
 - ② 客户端流量重定向到本地SSH, 通过隧道转发, 接着远程SSH传送到服务器.
- (2) 支持两种类型的端口转发:
 - ① 本地转发.
 - ② 远程转发.

6. IPSec

题型: 选择x1, 简答x1.

重点: IPSec的用途、优点、架构、模式; EPS.

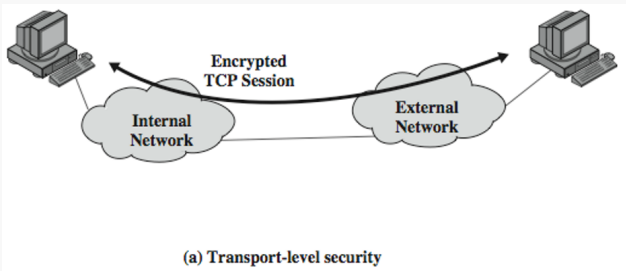
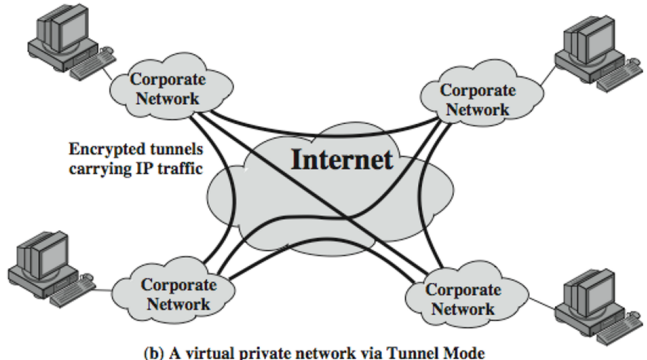
[IPSec的用途]

- (1) 通过互联网安全分支机构接入.
- (2) 通过互联网进行安全远程访问.
- (3) 与合作者建立企业间联网和企业内联网接入.
- (4) 加强电子商务的安全性.
- (5) 加密或认证流量, 保护分布式应用(如远程登录、文件传输、Web访问).

[IPSec的优点]

- (1) 在防火墙/路由器中, 为跨越周边的流量提供安全性.
- (2) 在防火墙/路由器中抵抗旁路流量.
- (3) 在传输层以下, 对应用程序透明.
- (4) 可对最终用户透明.
- (5) 可为个人用户提供安全保障.
- (6) 保证路由架构安全.

[模式]

 <p>(a) Transport-level security</p>	 <p>(b) A virtual private network via Tunnel Mode</p>
运输模式	隧道模式
<ul style="list-style-type: none">① 加密、验证(可选)IP数据.② 可做流量分析, 效率高.③ 适用于ESP主机对主机的流量.	<ul style="list-style-type: none">① 加密整个IP包.② 为下一跳添加新外部IP报头.③ 沿途的路由器不可检查内部IP头.④ 适用于VPN,网关到网关安全.

[封装安全载荷]

- (1) 封装安全载荷(Encapsulate Security Payload, ESP).
- (2) 特点:
 - ① 服务依赖于建立安全关联(SA)和网络位置.
 - ② 可使用各种加密和认证算法.
- (3) 功能: 提供消息内容的机密性、数据源认证, 无连接完整性, 反重播服务, 受限的流量机密性.

7. 无线网络安全

- 题型: 选择x1.
- 重点: 步骤; 指出提供安全在哪一段.

无线网络安全是无线端到路由端.

Wi-Fi网络安全存取(Wi-Fi Protected Access, WPA).

强健安全网络(Robust Security Network, RSN).

计数器模式CBC MAC协议(CCMP).

浏览一遍课件即可.

8. 电子邮件安全

题型: 简答(猜测画图)x1.

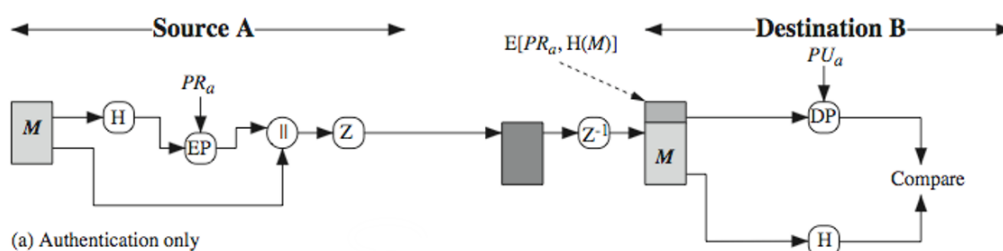
重点: 协议; 功能; 框架; 结合公钥.

[电子邮件安全涉及到的方面]

- (1) 保密性: 防止邮件泄露.
- (2) 认证性: 发送方身份认证.
- (3) 邮件完整性: 防止邮件被修改.
- (4) 不可否认性: 防止发送方否认曾发送过邮件.

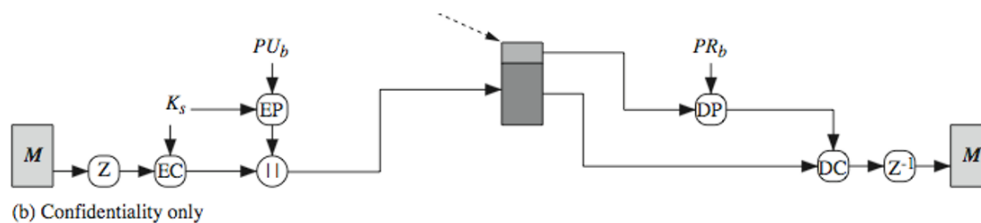
[PGP协议]

- (1) Pretty Good Privacy(PGP)协议是使用广泛、事实上的邮件安全标准, 使用当前最好的密码算法.
- (2) 功能: 消息认证、消息加密、压缩、邮件兼容性.
- (3) 消息认证:



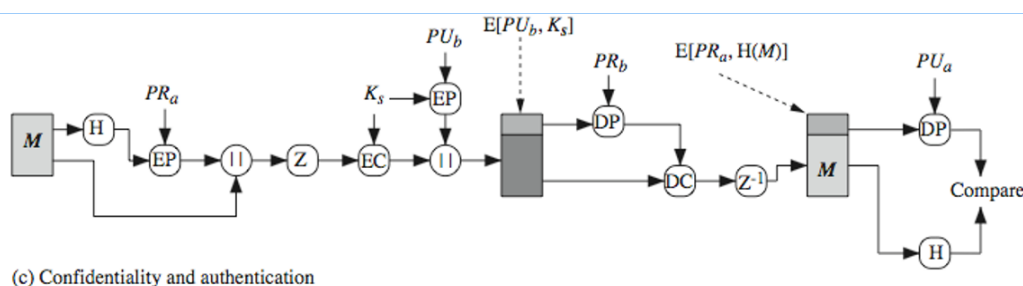
- ① 发送方准备待发送消息.
- ② 计算消息摘要(SHA-1160-bit).
- ③ 用RSA签名消息摘要.
- ④ 接收方使用签名算法验证消息摘要的正确性.
- ⑤ 接收方使用加密算法和摘要,验证消息的正确性.

(4) 消息保密:



- ① 发送方生成128 bit的随机会话密钥.
- ② 用会话密钥加密消息.
- ③ 用RSA加密会话密钥,附加于消息.
- ④ 接收方解密会话密钥.
- ⑤ 接收方解密消息.

(5) 消息认证和保密: 同时使用认证和保密功能.



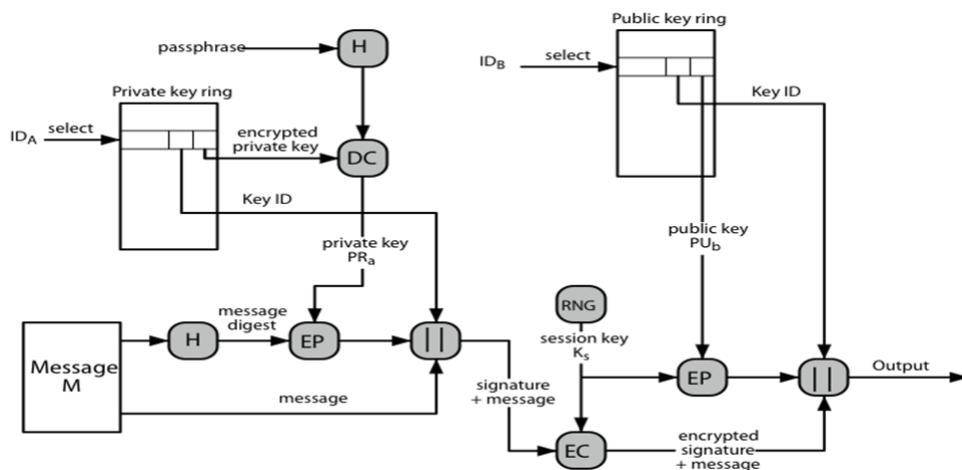
- ① 生成签名, 附加于消息.
- ② 同时加密消息和签名.
- ③ 附加会话密钥.

(6) 压缩:

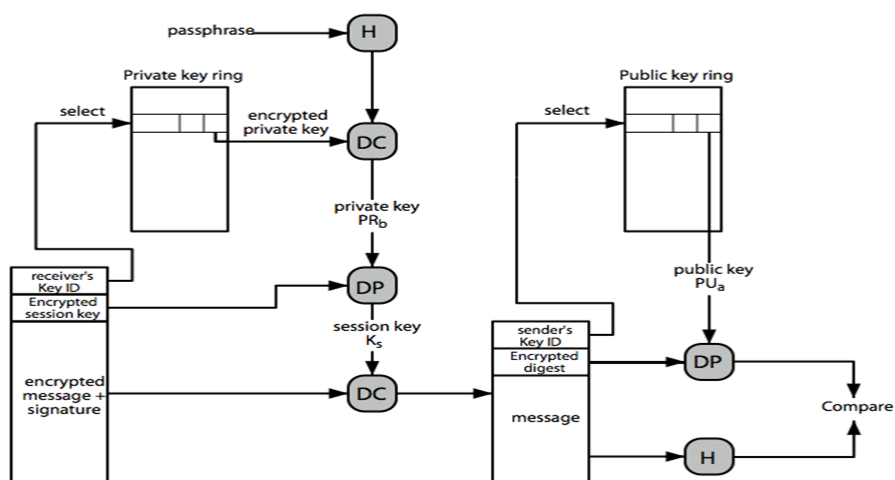
- ① 默认情况下, PGP签名后、加密前压缩待加密消息, 故可先存储消息, 验证可延后.
- ② 使用ZIP压缩算法.
- ③ 压缩是非确定性的.

(7) 邮件兼容性: 邮件发送协议只支持文本. 对任意二进制数据, 先转化为ASCII字符, 使用radix-64编码算法, 将 3 字节映射为 4 个可打印的ASCII字符. 若消息过大, PGP会分割消息.

[PGP消息发送]



[PGP消息接收]



[S/MIME协议]

(1) Secure/Multipurpose Internet Mail Extensions对MIME协议做了安全性增强.

(2) 功能:

- ① 数据保密: 加密内容和密钥.
- ② 数据签名: 消息编码 + 摘要签名.
- ③ 仅签名消息: 未编码消息 + 编码后摘要签名.
- ④ 数据保密和签名: 保密和签名功能嵌套.

[DKIM协议] Domain Key Identified Mail协议描述了如何由邮件服务提供商使用密码学工具对消息进行安全保护, 消息接收方对消息进行验证.

9. 恶意软件

题型: 选择x1, 简答x2.

重点: 恶意软件的定义; DDOS的定义; DDOS的分类.

[恶意软件的定义] 隐蔽植入另一程序的程序, 企图破坏数据、运行破坏性程序或入侵性程序、破坏应用程序或操作系统的机密性、完整性和可用性的软件.

[病毒]

(1) 定义: 一种能感染程序的软件, 可修改软件使它们包含复制的病毒, 在运行主机程序时秘密执行.

(2) 阶段:

- ① 休眠: 不执行操作并等待被某些事件激活.
- ② 传播: 将副本植入其它程序或磁盘的某些系统区域.
- ③ 触发: 病毒被激活以执行其预设功能.
- ④ 执行: 病毒执行预设功能.

(3) 组件:

- ① 感染机制: 病毒散布或传播的方法, 能使病毒复制.
- ② 触发: 使有效载荷激活的事件.
- ③ 有效载荷: 除传播外病毒所做的事, 恶意或良性.

(4) 分类:

- ① 目标型病毒: 企图感染的病毒.
 - (i) 引导扇区: 从包含病毒的磁盘启动, 病毒将传开.
 - (ii) 文件病毒: 感染被操作系统认为是可执行的文件.
 - (iii) 宏病毒: 一个应用程序解释宏代码或脚本代码时感染.
 - (iv) 混合体病毒: 以上多种方法感染文件.
- ② 方法型病毒: 病毒隐藏自己的方法.
 - (i) 加密病毒: 病毒的一部分进行加密并存储密钥.
 - (ii) 隐形飞机式病毒: 隐蔽性较好, 逃避检测.
 - (iii) 多态病毒: 感染时表现为不同形态.
 - (iv) 变形病毒: 反复感染时会改写自己的代码.

(5) 应对措施: 反病毒软件.

[蠕虫]

- (1) 定义: 主动感染其他机器并变成攻击的源头, 可伪装成一个系统进程, 不易察觉.
- (2) 借助网络连接或共享媒介传播.
- (3) 有像病毒一样的阶段: 休眠、传播、触发、执行.
- (4) 传播阶段: 扫描目标宿主, 找到合适的访问机制.
- (5) 防御方法:
 - ① 基于签名的蠕虫扫描过滤.
 - ② 基于过滤的蠕虫控制.
 - ③ 基于有效载荷分类的蠕虫控制.
 - ④ 阈值随机游走扫描检测.
 - ⑤ 速率限制和速率停止.

[恶意移动代码]

- (1) 定义: 能不变地植入各种不同平台, 执行有相同语义的程序.
- (2) 从远程系统传输到本地系统, 在本地系统上执行.
- (3) 常注射病毒、蠕虫或特洛伊木马.
- (4) 常利用漏洞执行自身操作, 如未经授权的数据访问, 获得根用户权限.

[电子邮件病毒]

- (1) 在附件doc中使用Word宏, 若附件打开, 宏激发并发送电子邮件到所有用户, 造成本地伤害.
- (2) 附件是特洛伊木马或脚本代码, 自动安装恶意软件.
- (3) 钓鱼攻击, 引导用户输入用户名和密码.

[特洛伊木马]

- (1) 定义: 一种有用的或表明有用的程序或使用工具, 包含隐藏代码, 被调用将执行不想要或有害的功能.
- (2) 执行时间接完成攻击者无法直接完成的功能.
- (3) 常用于传播病毒、蠕虫或安装后门, 或只为了破坏数据.
- (4) 模式:
 - ① 执行原程序功能外执行一个独立的恶意动作.
 - ② 继续执行源程序功能, 但修改某些功能以便能执行恶意动作.
 - ③ 执行恶意功能并完全代替原程序的功能.

[载荷]

(1) 系统破坏:

- ① 目的: 传播, 携带空载荷或无功能的载荷.
- ② 触发条件满足时, 毁坏受感染系统的数据.
- ③ 加密用户数据后勒索.

(2) 攻击代理: 恶意软件破坏已感染系统的计算和网络资源, 以被攻击者使用, 这类系统被称为机器人或僵尸.

(3) 信息窃取: 攻击目标是登录用户银行、游戏和相关站点的用户名和密码证书.

(4) 隐身:

- ① 陷门是进入程序的秘密入口点, 允许绕过正常的安全访问机制而直接访问程序.
- ② 隐匿程序是安装在系统上的一组程序, 用管理员特权隐蔽连接到该系统的访问路径, 同时最大程度地掩盖自己的存在.

[恶意软件的防护措施]

(1) 预防措施:

- ① 确保所有系统尽可能都是最新的, 打完补丁.
- ② 为应用程序和数据设置合适的访问权限.
- ③ 通过合适的用户觉悟和训练应对传播机制.

(2) 预防措施失败:

- ① 检测: 决定是否感染并定位恶意软件.
- ② 鉴定: 检测完成, 鉴定感染系统的恶意软件.
- ③ 删除: 移除所有感染软件中病毒的痕迹.

[分布式拒绝服务攻击]

(1) 定义: 分布式拒绝服务(DDoS)试图阻止某种服务的合法用户使用该服务, 构成严重安全威胁.

(2) 分类: 直接DDoS攻击、反射DDoS攻击.

(3) 应对措施(三大防线):

- ① 攻击前: 预防攻击和先占.
 - ② 攻击时: 攻击检测和过滤.
 - ③ 攻击后: 攻击源回溯与鉴定.
-
-

10. 入侵者

题型: 选择x1, 简答x1.

重点: 各种入侵者的定义和区别; 入侵检测.

[入侵者的分类]

- (1) 假冒用户: 潜入系统的访问控制以获取合法用户的账户.
- (2) 违法用户: 合法用户访问未授权的数据、程序或资源.
- (3) 隐秘用户: 夺取系统的管理控制权限, 躲避审计机制.

[计算机安全应急响应组]

- (1) 计算机安全应急响应组(Computer Incident Response Team, CERT).
- (2) 功能:
 - ① 收集攻击信息.
 - ② 传送系统管理者.
 - ③ 对漏洞打补丁.

[内部攻击] 内部攻击最难检测和防护.

[入侵技术]

- (1) 目的: 获得系统的访问权限或提升权限级别.
- (2) 常利用系统或软件的弱点.
- (3) 关键是获取用户口令.

[入侵检测]

- (1) 目的:
 - ① 足够快检测到的入侵行为.
 - ② 作为威慑.
 - ③ 收集信息以提高安全性.
- (2) 分类:
 - ① 统计异常检测: 尝试定义正常或期望的行为.
 - (i) 阈值检测: 对各种事件的出现频率定义阈值.
 - (ii) 基于行为曲线: 为每个用户建立行为曲线.

② 基于规则检测: 尝试定义特有的行为.

(i) 异常: 定义一个规则集.

(ii) 渗透检测: 建立一个用于搜索可疑行为的专用系统.

[统计异常检测]

(1) 阈值检测:

① 随着时间的推移, 若特定时间发生次数超过合理的值则认为入侵.

② 效率低下、粗糙.

(2) 基于行为曲线:

① 以用户过去的行为特征, 检测概要文件的显著偏差.

② 行为曲线常多参数.

[基于规则检测]

(1) 观察系统上的事件和应用规则判断活动是否可疑.

(2) 分类:

① 基于规则的异常检测.

② 基于规则的渗透检测.

[分布式入侵检测] 通过网络使单机入侵检测系统进行协同操作.

[蜜罐]

(1) 定义: 引诱攻击者的诱饵系统.

(2) 目的:

① 使攻击者不去访问关键系统.

② 收集攻击者活动信息.

③ 鼓励攻击者停留在系统上以便管理者回应.

[口令]

- (1) 防御入侵者的第一道防线.
 - (2) 选择策略:
 - ① 使用政策和良好的用户教育.
 - ② 计算机生成.
 - ③ 后验口令检查: 周期性运行口令破解程序, 被破解的口令将不被允许.
 - ④ 先验口令检查.
 - (i) 最认可的提高口令安全的方法.
 - (ii) 允许用户选择自己的口令, 系统判断是否可接受.
-
-

11. 防火墙

题型: 选择x1, 简答x1.

重点: 防火墙的分类; 防护墙的作用; 防火墙的局限性.

[防火墙的设计目标]

- (1) 出入站流量需经防火墙.
- (2) 经授权的网络流量才可通过.
- (3) 防火墙本身不可攻破.

[防火墙提供的机制]

- (1) 服务控制: 确定可访问的互联网服务类型.
- (2) 方向控制: 确定特定服务请求发起和通过的方向.
- (3) 用户控制: 根据用户控制服务器的访问权限.
- (4) 行为控制: 控制特定服务的使用方法.

[防火墙的功能]

- (1) 将未授权的用户阻止在受保护的网路之外.
- (2) 提供监视安全事件的场所, 执行审计和警告功能.
- (3) 用于与安全不相关的互联网功能的便利平台.
- (4) 作为IPSec的平台.

[防火墙的局限性]

- (1) 不能阻止绕过防火墙的攻击, 如拨号连接ISP.
- (2) 不能完全防止内部威胁.
- (3) 安全性不当的无线局域网可能受系统外的访问.
- (4) 移动设备可能被网络外部利用、感染, 再接入内网.

[防火墙的分类]

(1) 按采用的技术分类:

- ① 包过滤型防火墙.
- ② 代理防火墙.
- ③ 状态检测防火墙.

(2) 按实现形态分类:

- ① 软件防火墙.
- ② 硬件防火墙.

(3) 按部署位置分类:

- ① 边界防火墙.
- ② 个人防火墙.
- ③ 混合防火墙.

[包过滤型防火墙]

(1) 功能:

① 检查每个IP数据包(源IP地址、目的IP地址、源端和目的端的传输层地址、IP协议域、接口), 并按规则允许或拒绝, 以此限制对服务或端口的访问.

② 有两种可能的默认策略:

- (i) 丢弃: 无明确准许的将被阻止.
- (ii) 传递: 无明确阻止的将被准许.

(2) 是最简单、最快的防火墙组件, 是任何防火墙系统的基础.

(3) 弱点:

- ① 不检查更高层的数据, 不能阻止特定攻击.
- ② 防火墙可利用的信息有限, 日志有限.
- ③ 大多数不支持高级的用户认证机制.
- ④ 对用TCP/IP规范和协议栈的攻击无应对方法.
- ⑤ 只根据几个变量做访问决策控制, 易受到安全威胁.

(4) 攻击与防范方法:

① IP地址假冒攻击:

- (i) 攻击: 信任一个假地址.
- (ii) 防范方法: 在路由器上添加过滤器以阻止.

② 源路由攻击:

- (i) 攻击: 攻击者设置默认路由.
- (ii) 防范方法: 阻止源路由的数据包.

③ 细小帧攻击.

- (i) 攻击: 在很小的数据帧上分割TCP字头信息.
- (ii) 过滤路由只检查第一个帧, 其余通过.

[状态检测防火墙的功能]

- (1) 在上下文语境检查每个IP包, 跟踪客户端-服务器会话, 建立出站TCP连接目录, 检查每个包是否有效.
- (2) 在上下文中检测伪造包, 甚至可检查有限的应用程序数据.

[代理防火墙]

(1) 应用层网关或代理:

① 完全访问协议:

- (i) 用户请求来自代理的服务, 代理将请求验证为合法后返回结果给用户.
- (ii) 可在应用程序级别记录、审核流量.

② 每个服务需单独的代理.

- (i) 检查和传送所有的双向流量.
- (ii) 对每个连接的额外处理带来开销.

(2) 链路层网关或代理:

① 不允许点对点的TCP连接, 而是建立自身与内部主机、自身与外部主机的两个TCP连接.

创建后, 网关在两连接间传播TCP段时不检查其内容.

② 常用于受信任的内部用户建立出去的连接.

③ 链路层网关实现套接字连接.

[主机防火墙]

(1) 定义: 主机防火墙是用来保护个人计算机的软件模块.

(2) 特点:

- ① 可在多个操作系统中使用, 或作为附加包提供.
- ② 一般用于服务器.

(3) 优势:

- ① 可根据主机环境定制过滤规则.
- ② 保护的提供独立于拓扑结构.
- ③ 与独立防火墙一起使用, 提供额外的层保护.

[个人防火墙]

(1) 定义: 个人防火墙是个人计算机上的软件模块, 控制一边是电脑/工作站、另一边是因特网或企业网络的通信.

(2) 特点:

- ① 可防止在路由器中, 将所有计算机连接到DSL或调制解调器或其他网络接口.
- ② 常比其他防火墙类型简单.

(3) 作用:

- ① 拒绝未经授权的远程访问计算机.
 - ② 监测有检测功能的活动, 阻止蠕虫和其他病毒.
-
-