第一章

1. 网络信息系统安全（信息安全）的目标

(1) 保密性

① 定义：信息不泄露给非授权用户，即使非授权用户得到信息也无法知晓信息的内容。

② 实现：通过访问控制阻止非授权用户获得机密信息，通过加密技术阻止非授权用户获知信息内容。

(2) 完整性

① 定义：一方面指信息在生成、传输、存储和使用过程中不被篡改、丢失、缺损；另一方面指信息处理方法的正确性。

② 实现：通过访问控制阻止篡改行为，通过消息摘要算法检验信息是否被篡改。

(3) 可用性

① 定义：信息在授权人需要的时候可以随时获得

② 实现：攻击：切断线路、DDoS；防御：备份、冗余配置。

(4) 不可否认性

① 定义：保证用户无法在事后否认曾对信息进行的生成、签发、接受等行为。通信各方信息的真实同一性。

② 实现：数字签名、公证机制。

(5) 可控性

① 定义：可以控制授权范围内的信息流向及行为方式，对信

息的传播及内容具有控制能力。

② 实现：通过握手协议和认证对用户进行身份鉴别，通过访问控制列表来控制用户的访问方式，通过日志记录用户的所有活动以便于查询和审计。

2. 信息安全的主要内容 / 领域 / 组成部分

(1) 物理安全：环境安全、设备安全、媒体安全

(2) 运行安全

(3) 管理和策略

① 安全管理

1) 包含制度和教育两方面内容

2) 三项原则：多人负责、任期有限、职责分离

② 安全策略

3. 访问控制

(1) 定义：在身份识别的基础上，根据身份对提出的资源请求加以控制。访问控制机制决定用户能做什么，以及做到什么程度。

(2) 三元素

① 主体：访问的发起者

② 客体：各种资源

③ 保护规则：定义了主体与客体间可能的相互作用途径

(3) 两个过程：鉴别和授权

(4) 强制访问控制：所有主体和客体都被分配了安全标签，安全标签标识一个安全等级，访问控制执行时对主体和客体的安全级别进行比较，来决定是否可以访问。系统独立于用户行为，强制执行访问控制，用户不能更改安全标签。

(5) 自主访问控制：每个主体拥有一个用户名并属于一个组或具有一个角色；每个客体都拥有一个限定主体对其访问权限的访问控制列表（ACL）；每次访问发生时都会基于访问控制列表检查用户标志以实现对其访问权限的控制。用户可以针对被保护对象制定自己的保护策略。

4. 信息安全的模型

(1) 多级安全模型：划分多个安全级别

① BLP 保密性模型（不可上读、下写）

1) 提供分级别数据机密性保障的多级安全模型

2) 五个安全等级：公开、受限、秘密、机密、高密

3) 规则 1　上读：主体不可读安全级别高于它的数据

4) 规则 2　下写：主体不可写安全级别低于它的数据

② BIBA 完整性模型（不可上写、下读）

1) 信息在系统中只能自上而下流动

2) 五个安全等级：公开、受限、秘密、机密、高密

3) 规则 1　下读：主体不能读取安全级别低于它的数据

4) 规则 2　上写：主体不能写入安全级别高于它的数据

③ Clark-Wilson 完整性模型

(2) 多边安全模型：划分安全边界

① Lattice 安全模型

② Chinese Wall 模型

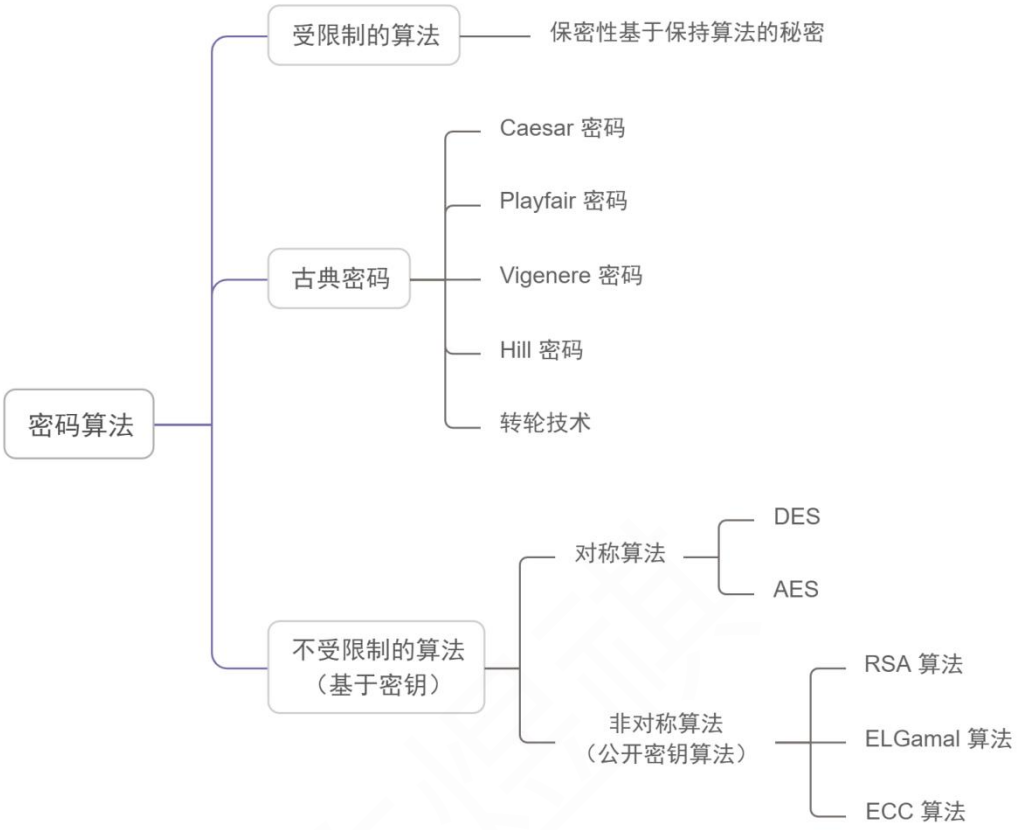
5. 信息安全标准分类

(1) 互操作标准

(2) 技术与工程标准

(3) 网络与信息安全管理标准

第二章



1. 密码分析攻击

(1) 唯密文攻击

(2) 已知明文攻击

(3) 选择明文攻击

(4) 选择密文攻击

(5) 自适应选择明文攻击

2. Caesar 凯撒密码

(1) 循环移位密码，加密时向后移动 K 位

3. Playfair 密码

(1) 构造 5×5 字母矩阵：先按顺序填入关键词（去除重复字母），再填入其余字母，I/J 填一起。

(2) 明文分组：明文按两个字母为一组分组；相同字母同一组时插入填充字母 k，最后一组落单时插入填充字母 k。

(3) 加密分组

① 同行：循环取右

② 同列：循环取下

③ 不同行不同列：取同行且和另一个字母同列的对角

(4) 优点：改变了单字母替代密码的频率分布；双字母组合多

4. Vigenere 密码

(1) 用单词作密钥，a ~ z → 0 ~ 25

(2) 将密钥逐一循环加到明文上

(3) 强度在于每个明文字母有多个密文字母对应

5. Hill 密码

(1) 矩阵乘 $C = KP \mod 26$

(2) 强度在于完全隐藏了单字母的频率

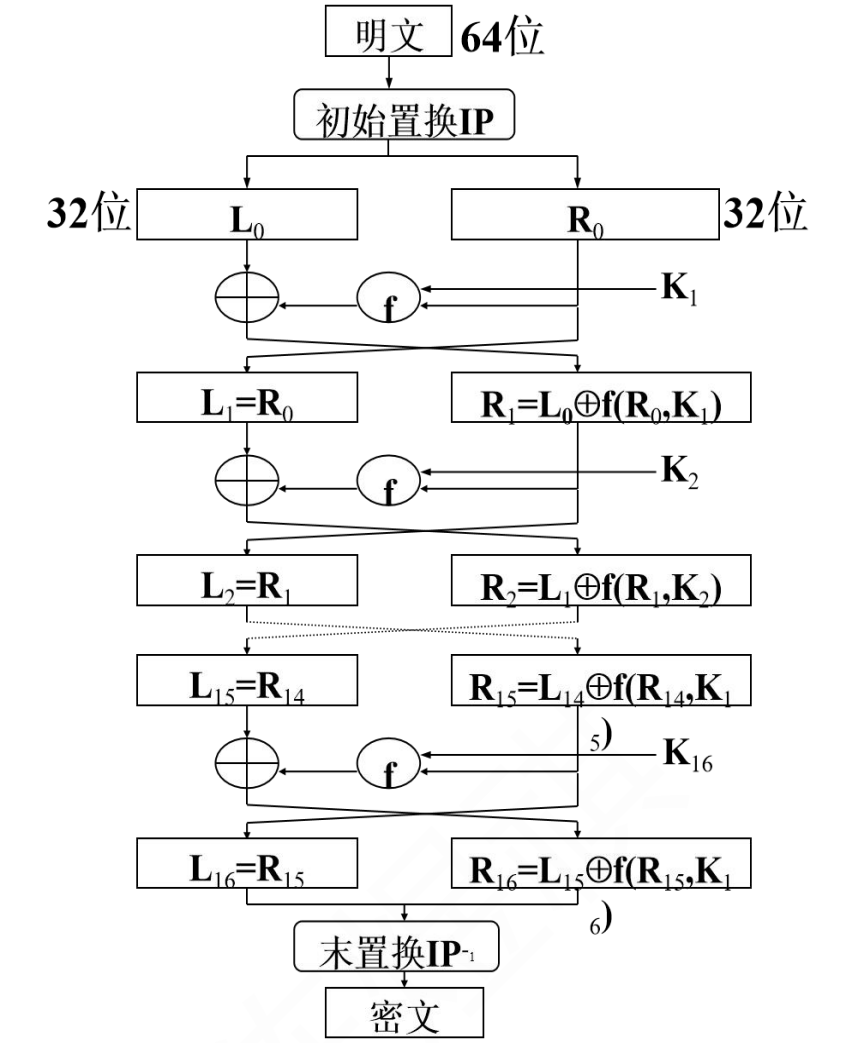
6. DES

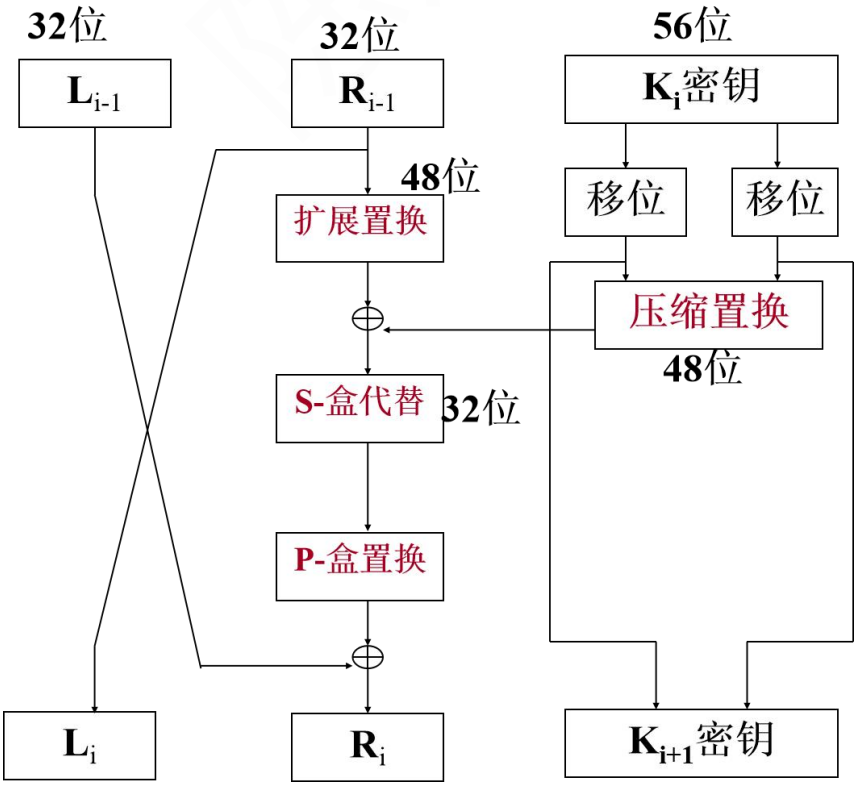
(1) 给定置换 p，a[i]=a[p[i]]

(2) S-盒替代

① 共 8 个盒，每个 6 位输入，4 位输出

② $b_{1\sim6}$ 输入，b_1b_6 确定行，$b_2b_3b_4b_5$ 确定列（从 0 开始计数）


明文
64位
初始置换IP
32位
L0
R0
32位
K1
f
L1=R0
R1=L0⊕f(R0,K1)
K2
L2=R1
R2=L1⊕f(R1,K2)
L15=R14
R15=L14⊕f(R14,K1
5)
K16
L16=R15
R16=L15⊕f(R15,K1
6)
末置换IP-1
密文


32位
Li-1
32位
Ri-1
56位
Ki密钥
48位
扩展置换
移位
移位
压缩置换
48位
S-盒代替
32位
P-盒置换
Li
Ri
Ki+1密钥

7. RSA 算法

(1) 密钥生成

① 选择$n = p \times q$

② $\varphi(n) = (p-1) \times (q-1)$

③ 选择公钥e，计算$d = e^{-1} \bmod \varphi(n)$

④ 逆元存在的条件是两数互质

⑤ 互质数数量$\varphi(n) = n \times \prod_i (1 - \frac{1}{p_i})$

(2) 加密

① 公钥e, n

② $C = m^e \bmod n$

(3) 解密

① 私钥d, n

② $m = C^d \bmod n$

8. ELGamal 算法

(1) 密钥生成

① 选择 g, x, p，计算 $y = g^x \bmod p$

(2) 加密

① 公钥 y, g, p

② 选择临时随机数 r

③ 计算 $C = (m \times y^r) \bmod p$，发送 C，g^r

(3) 解密

① 私钥 x, p

② $m = C \times (y^r)^{-1} \bmod p = C \times \left((g^r)^x\right)^{-1} \bmod p$

9. ECC 算法

(1) 方程定义 $E_p(a,b) \Rightarrow y^2 = x^3 + ax + b(\mathrm{mod}\, p)$

(2) 求点数

① 对于每个 $y \in [0, p)$，计算 $(y^2) \bmod p$

② 对于每个 $x \in [0, p)$，计算 $(x^3 + ax + b) \bmod p$

③ 对 x 的结算结果，统计匹配的 y 数量

④ 最后加上无穷远点 O

(3) 基本法则

① $P + O = P$

② $P + (-P) = O$，$-P = (x, -y)$

(4) 计算法则

① $x_3 = \lambda^2 - x_1 - x_2 \bmod p$

② $y_3 = \lambda(x_1 - x_3) - y_1 \bmod p$

③ $P \neq Q$：$\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$

④ $P = Q$：$\lambda = \dfrac{3x_1^2 + a}{2y_1}$

(5) 加密过程

① 选择私钥 r_a，计算 $P_a = r_a G$

② 公开公钥 p, a, b, G, P_a

③ 选择随机数 k，计算密文：$\{\ kG,\ \ P_m + kP_a\ \}$

④ 明文 $P_m = (P_m + kP_a) - r_a(kG)$

第三章

1. 报文鉴别

(1) 定义：通信的接收方能够鉴别验证所收到的报文的真伪

(2) 报文源的鉴别：利用报文加密解密对身份进行鉴别

(3) 报文宿的鉴别：收方标识符 IDB、收方通行字 PWB

(4) 报文时间性的鉴别

① 定义：确认报文是否保持正确的顺序，有无断漏和重复

② 方法：初始向量法、时间参数法、随机数法（抗重放）

(5) 报文内容的鉴别

① 报文鉴别码 MAC：用密钥生成小的数据块，追加在报文的后面

② 报文加密：用完整的报文的密文作为对报文的认证

③ 报文摘要 MD：将可变长度的报文作为单向散列函数的输入，得出固定长度的报文摘要。最广泛使用的是 MD5 算法。

2. 散列函数

(1) 定义：把任意长度的报文 M 通过函数变换为一个固定的散列码 h，散列函数表示为 h=H(M)。它生成报文所独有的“指纹”，唯一地对应原始报文。

(2) 用途：验证报文完整性、密钥认证

(3) 单向散列函数的性质

① 广泛适用性：适用于任何大小的数据分组

② 码长固定性：产生定长的输出

③ 易计算性：对任何数据都容易计算

④ 单向不可逆性：无法根据散列码倒推原文

⑤ 弱单向性：对于任意给定的数据 X，找到另一个属于 Y 使得 H(X)=H(Y)，在计算上是不可行的。

⑥ 强单向性：要寻找任意一对数据(X,Y)，使得 H(X)=H(Y)，在计算上是不可行的。即对于所有不同的报文都不能产生相同的散列码。

3. 数字签名

(1) 确认信息确实是由签名者发送的

确认信息自签发后到收到为止未曾作过任何修改

(2) 解决的问题

① 接收者能够核实发送者

② 发送者事后不能抵赖对报文的签名

③ 接收者不能伪造对报文的签名

(3) RSA 数字签名

① 用私钥 d 签名，用公钥 e 验证

② 缺点：产生密钥很麻烦，受到素数产生技术的限制，很难做到一次一密；为保证安全性，n 要 600bit 以上，运算代价高，速度慢。

(4) ELGamal 数字签名

① 全局参数 g, p，私钥 x，公钥 y

② 签名过程

1) 选择随机数 k

2) 计算 $r = g^k \bmod p$

3) 计算 $s = (H(M) - xr)k^{-1} \bmod (p-1)$

4) 发送消息和签名结果 (M, r, s)

③ 认证过程

1) 获取公钥 y

2) 预查合法性：$r \in [1, p-1]$

3) 计算 $u_1 = y^r r^s \bmod p$

4) 计算 $u_2 = g^{H(M)} \bmod p$

5) 如果 $u_1 = u_2$，表示签名有效

4. 课后习题

第四章

1. SSL 协议

(1) SSL 主要采用公开密钥体制和 X.509 数字证书技术，其目标是保证两个应用间通信的保密性、完整性和可靠性，可在服务器和客户端两端同时实现支持。

(2) SSL 介于可靠的传输层协议 TCP 和应用层协议如 HTTP 之间。

(3) SSL 使用公钥密码系统和技术进行客户端和服务器通信实体间的身份认证和会话密钥协商；使用对称密码算法对 SSL 连接上传输的敏感数据进行加密。

(4) 四个子协议

① SSL 握手协议

② SSL 告警协议

③ SSL 修改密文规约协议

④ SSL 记录协议

(5) 通信过程包括两个状态

① 连接状态

② 会话状态

(6) 通信步骤

① 建立 TCP 连接

② SSL 握手，建立 SSL 会话

③ 通过会话传送加密数据包

④ 释放连接，会话过期

(7) SSL 连接的特性

① 连接是私有的。握手协议商量一个会话密钥，然后用对称的加密算法对数据加密。

② 连接的标识符用非对称算法加密。

③ 连接是可靠的。消息的传送过程包含了消息完整性检查。

2. SET 协议 - 双向签名

(1) 允许将两种数据连接在一起，并交给两个不同的实体处理

(2) 目的：为了连接两个发送给不同接收者的报文

(3) 消费者想要将订购信息(OI)发送给商家，将支付信息(PI)发送给银行。商家不必知道消费者的信用卡号码；银行不必知道消费者订单的细节；消费者可以证明这个支付是用于这次订购而不是用于其他某种货物或服务。

(4) 商家收到 PIMD、OI、DS，计算 H(PIMD||H(OI))和 D_{KUc}[DS]，验证该签名。购买请求报文中与订购相关的信息。

(5) 银行收到 OIMD、PI、DS，计算 H(OIMD||H(PI))和 D_{KUc}[DS]，验证该签名。购买请求报文中与购买相关的信息。

(6) 消费者将 OI 和 PI 连接起来并且能够证明这个连接关系。

第五章

- 第三，对于WWW服务
  - 允许内部网用户访问Internet上任何网络和站点
  - 但只允许一个公司的网络98.120.7.0访问内部WWW服务器，内部WWW服务器的IP址为116.111.4.5

116.111.4.0:应用程序端口 ⟶ ⟵ 其它站点:80

规则	方向	源地址	目的地址	协议	源端口	目的端口	ACK设置	动作
I	出	116.111.4.0	任意	TCP	>1023	80	任意	允许
J	入	任意	116.111.4.0	TCP	80	>1023	是	允许

116.111.4.5:80 ⟵ ⟶ 98.120.7.0 :应用程序端口

规则	方向	源地址	目的地址	协议	源端口	目的端口	ACK设置	动作
K	入	98.120.7.0	116.111.4.5	TCP	>1023	80	任意	允许
L	出	116.111.4.5	98.120.7.0	TCP	80	>1023	任意	允许

- 第二，邮件服务
  - 允许SMTP出站入站服务，邮件服务器是IP地址为116.111.4.1

116.111.4.1:应用程序端口 ⟶ ⟵ 其它站点:25

规则	方向	源地址	目的地址	协议	源端口	目的端口	ACK设置	动作
E	出	116.111.4.1	任意	TCP	>1023	25	任意	允许
F	入	任意	116.111.4.1	TCP	25	>1023	是	允许

116.111.4.1:25 ⟵ ⟶ 其它站点:应用程序端口

规则	方向	源地址	目的地址	协议	源端口	目的端口	ACK设置	动作
G	入	任意	116.111.4.1	TCP	>1023	25	任意	允许
H	出	116.111.4.1	任意	TCP	25	>1023	任意	允许

116.111.4.0:应用程序端口 ⟷ 202.208.5.6:23

规则	方向	源地址	目的地址	协议	源端口	目的端口	ACK设置	动作
A	出	116.111.4.0	202.208.5.6	TCP	>1023	23	任意	拒绝
B	入	202.208.5.6	116.111.4.0	TCP	23	>1023	是	拒绝

- 对于Internet的其他站点，允许内部网用户通过Telnet方式访问。

116.111.4.0:应用程序端口 ⟷ 其它站点:23

规则	方向	源地址	目的地址	协议	源端口	目的端口	ACK设置	动作
C	出	116.111.4.0	任意	TCP	>1023	23	任意	允许
D	入	任意	116.111.4.0	TCP	23	>1023	是	允许

规则	方向	源地址	目标地址	协议	源端口	目标端口	ACK 设置	动作
A	出	116.111.4.0	202.108.5.6	TCP	>1023	23	任意	拒绝
B	入	202.108.5.6	116.111.4.0	TCP	23	>1023	是	任意
C	出	116.111.4.0	任意	TCP	>1023	23	任意	允许
D	入	任意	116.111.4.0	TCP	23	>1023	是	允许
E	出	116.111.4.1	任意	TCP	>1023	25	任意	允许
F	入	任意	116.111.4.1	TCP	25	>1023	是	允许
G	入	任意	116.111.4.1	TCP	>1023	25	任意	允许
H	出	116.111.4.1	任意	TCP	25	>1023	任意	允许
I	出	116.111.4.0	任意	TCP	>1023	80	任意	允许
J	入	任意	116.111.4.0	TCP	80	>1023	是	允许
K	入	98.120.7.0	116.111.4.5	TCP	>1023	80	任意	允许
L	出	116.111.4.5	98.120.7.0	TCP	80	>1023	任意	允许
M	双向	任意	任意	任意	任意	任意	任意	任意

表 5.3 过滤规则示例