

目录

第一章 绪论.....	2
1. 网络信息安全问题的根源.....	2
2. 密码学的发展历史.....	2
3. 安全服务.....	4
4. 安全服务与安全机制之间的关系.....	6
5. 安全攻击的主要形式.....	7
6. 安全攻击形式的分类.....	9
7. 安全攻击形式的特点及防护.....	9
第二章 密码学基础.....	10
1. 密码概念.....	10
2. 五元组之间的关系图.....	11
3. 密码分析分类.....	11
4. 破译算法分级.....	12
5. 衡量攻击方法的复杂性.....	12
6. 一个密码系统实际安全的条件.....	12
7. 密码体制.....	13
8. 对称密码算法的优、缺点.....	13
9. 公开密钥密码体制的优、缺点.....	13
10. 公开密钥密码体制与常规密码体制的比较.....	14
第三章 古典密码.....	15
1. 隐写术的优缺点.....	15
2. 著名的 Caesar 密码举例.....	15
3. 代替密码的实现方法分类.....	16
4. 频率分析攻击的一般方法：.....	17
5. HILL 密码的加密和解密.....	17
6. Hill 密码的特点.....	18
7. 威胁代替密码的因素.....	18
第四章 密码学的数学引论.....	19
1. 密码学的数学基础（数论、群论、有限域理论）.....	19
2. 中国剩余定理（计算题）.....	22
第五章 对称密码体制.....	24
1. 分组密码模型.....	24
2. 分组密码原理.....	25
3. 雪崩效应.....	25
4. 分组密码的操作模式.....	26
5. DES 的加密处理略图.....	32
6. 3DES 的优、缺点.....	32
7. 高级加密标准（AES）.....	33
8. AES 的基本运算.....	34
第六章 公钥密码体制.....	34
1. 三种典型的公钥密码体制.....	34

2. 对公钥密码体制的要求.....	34
3. 陷门单向函数.....	35
4. 公钥密码系统的应用类型.....	35
5. DH 例子 (计算题)	35
6. RSA 数学基础.....	36
7. RSA 密码体制描述	36
8. RSA 算法实现的三个基本问题.....	37
9. 椭圆曲线密码体制 ECC	39
10. 椭圆曲线密码体制描述.....	40
11. 椭圆曲线密码体制与离散对数密码体制的比较	41
第七章 Hash 函数与消息认证	42
1. 安全 HASH 函数的一般结构	42
第八章 数字签名	42
1. 数字签名应具有的性质.....	42
2. 数字签名的要求	42
3. 数字签名方案描述	43
4. 两类数字签名函数 (分别举 1 例)	43
5. 直接数字签名的缺点	46
6. 可仲裁数字签名原理	47
7. 数字签名标准(DSS)的主要参数.....	47
第九章 密钥管理	48
1. 密钥管理的地位	48
2. 密钥管理的层次式结构.....	48
3. 层次式密钥管理的优势	49
4. 公开密钥的分发方式	49
开放性试题	49
1. 举例说明生活或工作中的密码技术.....	49

第一章 绪论

1. 网络信息安全问题的根源

网络自身的安全缺陷

- 协议不安全和业务不安全

网络的开放性

- 业务基于公开的协议
- 连接是基于主机上的社团彼此信任的原则
- 远程访问

人的因素

- 人为的无意失误
- 黑客攻击
- 管理不善

2. 密码学的发展历史

古代加密方法

- 大约起源于公元前 440 年出现在古希腊战争中的隐写术
- 斯巴达人于公元前 400 年应用 scytale
- 我国古代的藏头诗、藏尾诗、漏格诗以及绘画等
- Polybius 校验表
- 特点：主要基于手工的方式实现，简单

古典密码

- 阿拉伯人是第一个清晰地理解密码学原理的人：设计并且使用代替和换位加密，并发现了字母频率分布关系
- 欧洲的密码学起源于中世纪的罗马和意大利
- 1860 年，密码系统在外交通信中已得到普遍使用
- 一次世界大战期间，敌对双方使用加密系统用于战术通信
- 二十世纪 20 年代，转轮机的出现是密码学发展的重要标志之一
- 二次世界大战期间，转轮机得到广泛的使用
- 二次大战后，电子学开始被引入到密码机中

古典密码举例

- 单表代替密码：Caesar 密码
- 多表代替密码：Vigenere 密码、Hill 密码
- 转轮密码：Enigma 密码

古典密码特点

- 文字置换
- 保留手工实现方式，开始出现机械变换的实现方式
- 比古代加密方法更复杂，但其变化量仍然比较小
- 已经初步体现出近代密码系统的雏形
- 特别是转轮机的出现，大大提高了密码加密速度
- 在外交、军事领域得到过广泛应用

近代密码

- 1949 年 Claude Shannon 发表 The communication theory of secrecy systems
- 1976 年 W.Diffie 和 M.Hellman 发表了 New directions in cryptography，提出了适应网络上保密通信的公钥密码思想

- 1978 年 RSA 公钥密码体制的出现
- 1978 年美国批准批准 DES 用于政府等非机密单位及商业上的保密通信
- 二十世纪 70 年代，开始形成密码学科

🌈 近代密码特点

- 与计算机技术、电子通信技术紧密相关
- 密码理论蓬勃发展，密码算法设计与分析互相促进，出现了大量的密码算法和各种攻击方法
- 密码使用的范围也在不断扩张，出现了许多通用的加密标准，促进网络和技术的发展
- 出现了一些新的密码技术，如混沌密码、量子密码等

3. 安全服务

🌈 概念：加强数据处理系统和信息传输的安全性的一类服务

🌈 目的：利用一种或多种安全机制阻止安全攻击

🌈 机密性 (Confidentiality)

- 机密性是信息不泄露给非授权的用户、实体或过程，或供其利用的特性，是信息安全最基本的需求。机密性可保护数据免受被动攻击。
 - 对于消息内容的析出，机密性能够确定不同层次的保护，如广义保护可以防止一段时间内两个用户之间传输的所有用户数据被泄露，狭义保护可以保护单一消息中某个特定字段的内容。
 - 对于通信量分析，机密性要求一个攻击不能在通信设施上观察到通信量的源端和目的端、通信频度、通信量长度或其他特征。

🌈 完整性(Integrity)

- 完整性是数据未经授权不能进行改变的特性，即信息在存储或传输过程中不被修改、不被插入或删除的特性。它保证收到的数据确是授权实体所发出的数据。

- 完整性服务旨在防止以某种违反安全策略的方式改变数据的价值和存在的威胁。
- 违反完整性不一定是恶意行为的结果，系统的中断（如电力方面的浪涌）也可能造成某些信息意想不到的改变。对完整性的破坏通常只关注检测而不关注防止，一旦检测到完整性被破坏就报告并采取适当的恢复措施。

鉴别(Authentication)

- 也叫认证，用于确保一个消息的来源或消息本身被正确地标识，同时确保该标识没有被伪造。
- 鉴别服务关注确保一个通信是真实可信的，分为实体认证和数据源认证。
 - 对于单个消息而言，鉴别服务要求能向接收方保证该消息确实来自于它所宣称的源，即数据源认证。数据源认证主要用于无连接的通信。
 - 实体认证是指对于通信的双方而言，鉴别服务则要求在连接发起时能确保这两个实体是可信的，即每个实体的确是它宣称的那个实体。实体认证主要用于面向连接的通信。

非否认性(Non-repudiation)

- 也叫不可抵赖性。非否认是防止发送方或接收方抵赖所传输的消息，要求无论发送方还是接收方都不能抵赖所进行的传输。
 - 当发送一个消息时，接收方能够提供源方证据以证实该消息的确是由所宣称的发送方发来的（源非否认性）。
 - 当接收方收到一个消息时，发送方能够提供投递证据以证实该消息的确送到了指定的接收方（宿非否认性）。

访问控制(Access Control)

- 在网络环境中，访问控制是限制或控制经通信链路对主机系统和应用程序等系统资源进行访问的能力。防止对任何资源（如计算资源、通信资源或信息资源）进行未授权的访问。
- 访问控制直接支持机密性、完整性以及合法使用等安全目标。访问控制是实施授权的一种方法。

- 通常有两种方法用来阻止非授权用户访问目标：
 - (1)访问请求过滤：当一个发起者试图访问一个目标时，需要检查发起者是否被准予访问目标（由控制策略决定）。
 - (2)隔离：从物理上防止非授权用户有机会访问到敏感的目标。
- 访问控制策略的具体类型：·基于身份的策略、·基于规则的策略和基于角色的策略

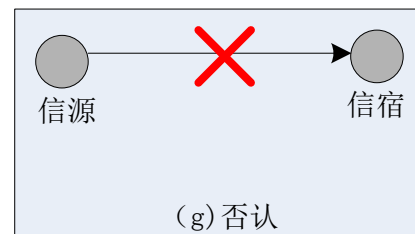
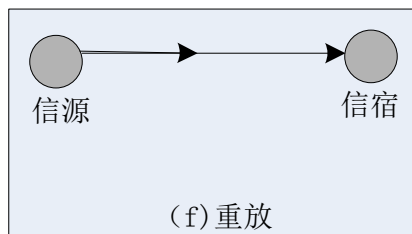
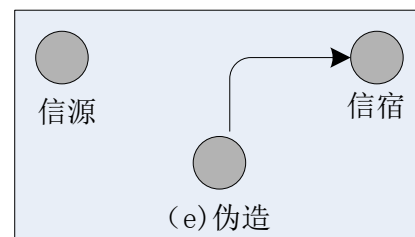
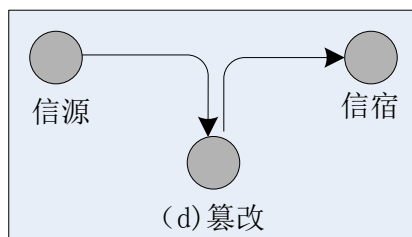
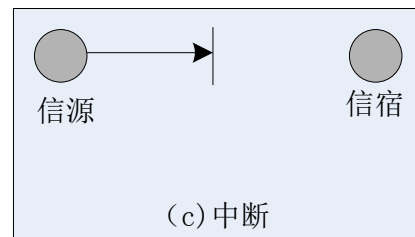
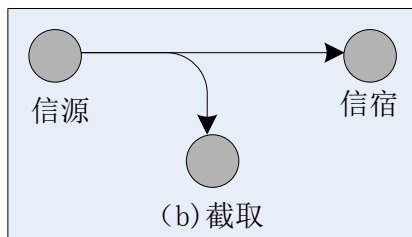
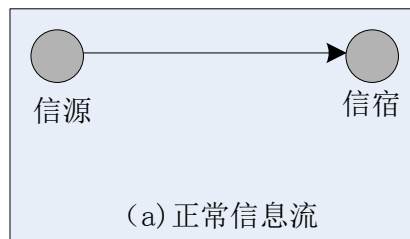
可用性(Availability)

- 可用性是可被授权实体访问并按需求使用的特性，要求网络信息系统的有用资源在需要时可为授权各方使用，保证合法用户对信息和资源的使用不会被不正当地拒绝

4. 安全服务与安全机制之间的关系

安全服务	安全机制
机密性	加密和路由控制
完整性	加密、数字签名和数据完整性
鉴别	加密、数字签名和认证交换
非否认性	数字签名、数据完整性和公证
访问控制	访问控制
可用性	访问控制和路由控制

5. 安全攻击的主要形式



截取 (Interception or Eavesdropping)

- 即未获授权地通过对传输进行窃听和监测，从而获取对某个资源的访问，这是对机密性的攻击，分为两种情况：
 - 析出消息内容 (Snooping)
 - 当人们通过网络进行通信或传输文件时，如果不采取任何保密措施，攻击者就有可能在网络中搭线窃听，以获取他们通信的内容。

- 通信量分析(Traffic analysis)
 - 假定用某种方法（如加密）屏蔽了消息内容，这使得即使攻击者获取了该消息也无法从消息中提取有用信息。
 - 但即使我们已用加密进行保护，攻击者也许还能观察这些消息的结构模式，即他还能够测定通信主机的位置和标识，能够观察被交换消息的频率和长度，这些信息对猜测正在发生的通信的性质或许是有用的。

中断(Interruption)

- 即拒绝服务（Denial of Service，DoS）。是指防止或禁止通信设施的正常使用或管理，从而达到减慢或中断系统服务的目的，这是对可用性的攻击。
- 这种攻击通常有两种形式：
 - 一种是攻击者删除通过某一连接的所有协议数据单元(Protocol Data Unit，PDU)，从而抑制所有的消息指向某个特殊的目的地(如安全审计服务)；
 - 另一种是使整个网络性能降低或崩溃，可能采取的手段是使网络不能工作，或者滥发消息使之过载。

篡改(Modification)

- 即更改报文流，它是对通过连接的协议数据单元 PDU 的完整性的攻击，意味着一个合法消息的某些部分被改变，或消息被延迟、删除或改变顺序，以产生一个未经授权的效果

伪造 (Fabrication or Masquerading)

- 伪造是一个非法实体假装成一个合法的实体。伪造通常与其他攻击形式结合在一起才具有攻击性效果

重放 (Replaying)

- 重放涉及一个数据单元被获取以后的后继重传，以产生一个未授权的效果

否认 (Repudiation)

- 否认不同于上述任何一种攻击形式，因为它的执行者（即攻击者）不是来源于通信参与双方之外，而是通信的发送方或接收方
- 即消息的发送方可能事后否认他曾发送过该消息，或消息接收方可能事后否认他曾收到过该消息

6. 安全攻击形式的分类

攻击类别	攻击形式	受威胁的数据性质
被动攻击	析出消息内容	机密性
	通信量分析	
主动攻击	中断	可用性
	篡改	机密性、完整性
	伪造	
	重放	
	否认	

7. 安全攻击形式的特点及防护

被动攻击

- 攻击者只是观察通过一个连接的协议数据单元 PDU，以便了解与交换相关的信息，并不修改数据或危害系统；这种消息的泄露可能会危害消息的发送方与接收方，但对系统本身不会造成任何影响，系统能够正常工作
- 难以检测
- 重点是防止，提供机密性

主动攻击

- 指攻击者对连接中通过的 PDU 进行各种处理，这些攻击涉及某些数据流的篡改或一个虚假流的产生
- 难以防止

- 重点是检测，发现并恢复

第二章 密码学基础

1. 密码概念

明文

- 作为加密输入的原始信息，即消息的原始形式

密文

- 明文经加密变换后的结果，即消息被加密处理后的形式

密钥

- 是参与密码变换的参数

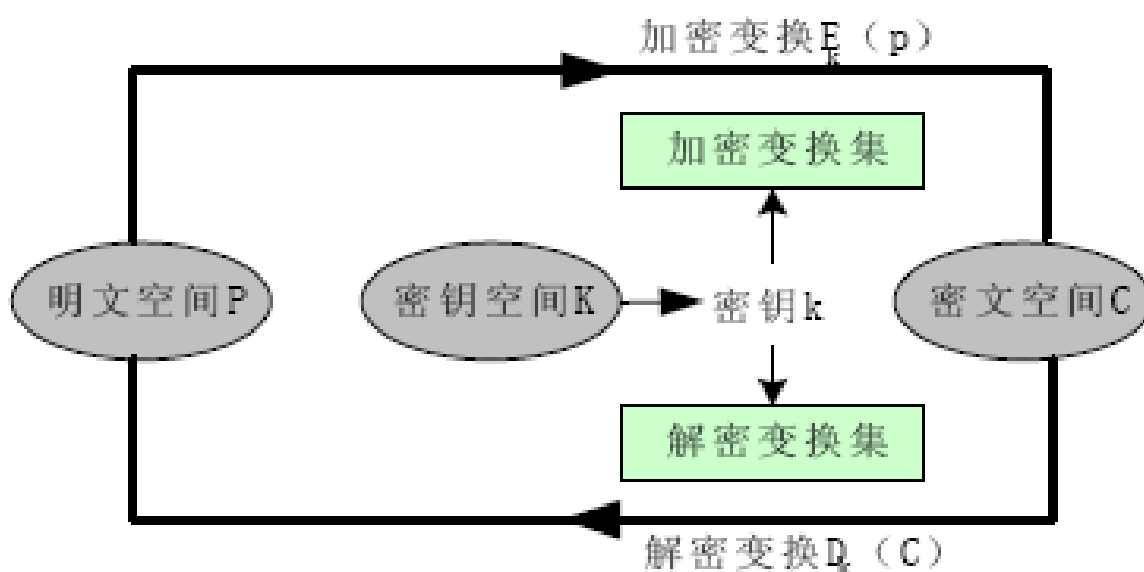
加密算法

- 是将明文变换为密文的变换函数，相应的变换过程称为加密，即编码的过程

解密算法

- 是将密文恢复为明文的变换函数，相应的变换过程称为解密

2. 五元组之间的关系图



$$\forall k \in K, \forall p \in P, \text{有 } D_k(E_k(p)) = p$$

图2-1 密码体制的组成

3. 密码分析分类

🚩 唯密文攻击 (Ciphertext only)

- 破译者已知：加密算法、待破译的密文

🚩 已知明文攻击 (Known plaintext)

- 破译者已知：加密算法、一定数量的密文和对应的明文

🚩 选择明文攻击 (Chosen plaintext)

- 破译者已知：加密算法、选定的明文和对应的密文

🚩 选择密文攻击 (Chosen ciphertext)

- 破译者已知：加密算法、选定的密文和对应的明文


🚩 选择文本攻击 (Chosen text)

- 破译者已知：加密算法、选定的明文和对应的密文、选定的密文和对应的明文

分析

- 唯密文攻击是最困难的
- 上述攻击的强度是递增的
- 一个密码体制是安全的，通常是指在前三种攻击下的安全性

4. 破译算法分级


 全部破译 (total break)

 全部推导 (global deduction)

 实例推导 (instance deduction)

 信息推导 (information deduction)


5. 衡量攻击方法的复杂性

 数据复杂性 (data complexity)


 处理复杂性 (processing complexity)

 存储需求 (storage requirement)

6. 一个密码系统实际安全的条件

 每一个加密函数和每一个解密函数 都能有效地计算

 破译者取得密文后将不能在有效的时间或成本范围内破解出密钥或明文

 一个密码系统是安全的必要条件：穷举密钥搜索将是不可行的

7. 密码体制

- 🌈 对称密码体制
- 🌈 非对称密码体制（公开密钥密码体制）

8. 对称密码算法的优、缺点

- 🌈 优点：加/解密处理速度快、保密度高等。
- 🌈 缺点：
 - 如何把密钥安全地送到收信方，是对称密码算法的突出问题。对称密码算法的密钥分发过程十分复杂，所花代价高
 - 多人通信时密钥组合的数量会出现爆炸性膨胀，使密钥分发更加复杂化
 - 通信双方必须统一密钥，如果发信者与收信人素不相识，这就无法向对方发送秘密信息了
 - 存在数字签名困难问题

9. 公开密钥密码体制的优、缺点

- 🌈 优点：
 - 网络中的每一个用户只需要保存自己的私有密钥。密钥少，便于管理
 - 密钥分配简单，不需要秘密的通道和复杂的协议来传送密钥
 - 可实现数字签名
- 🌈 缺点：加密、解密处理速度相对较慢，同等安全强度下所要求的密钥位数多一些

10. 公开密钥密码体制与常规密码体制的比较

分类	对称密码体制	非对称密码体制
运行条件	加密和解密使用同一个密钥和同一个算法	用同一个算法进行加密和解密，而密钥有一对，其中一个用于加密，另一个用于解密
	发送方和接收方必须共享密钥和算法	发送方和接收方每个使用一对相互匹配、而又彼此互异的密钥中的一个
安全条件	密钥必须保密	密钥对中的私钥必须保密
	如果不掌握其他信息，要想解密报文是不可能或至少是不现实的	如果不掌握其他信息，要想解密报文是不可能或者至少是不现实的
	知道所用的算法加上密文的样本必须不足以确定密钥	知道所用的算法、公钥和密文的样本必须不足以确定私钥
保密方式	基于发送方和接收方共享的秘密（密钥）	基于接收方个人的秘密（私钥）
基本变换	面向符号（字符或位）的代替或换位	面向数字的数学函数的变换
适用范围	消息的保密	主要用于短消息的保密（如对称密码算法中所使用密钥的交换）或认证、数字签名等

第三章 古典密码

1. 隐写术的优缺点

🌈 优点：

- 能够被某些人使用而不容易被发现他们间在进行秘密通信
- 加密则很容易被发现谁与谁在进行秘密通信，这种发现本身可能具有某种意义或作用

🌈 缺点：

- 形式简单但构造费时，要求有大量的开销来隐藏相对较少的信息
- 一旦该系统的构造方法被发现，就会变得完全没有价值
- 隐写术一般无稳健性

2. 著名的 Caesar 密码举例

🌈 设明文为：China，对应的数字为：2 7 8 13 0。

🌈 加密：C：对应着字母 F；

h：对应着字母 K；

i：对应着字母 L；

n：对应着字母 Q；

a：对应着字母 D。

🌈 所以明文“China”基于 Caesar 密码被加密为“FKLQD”。

Coding characters into numbers

A \Leftrightarrow 0	N \Leftrightarrow 13
B \Leftrightarrow 1	O \Leftrightarrow 14
C \Leftrightarrow 2	P \Leftrightarrow 15
D \Leftrightarrow 3	Q \Leftrightarrow 16
E \Leftrightarrow 4	R \Leftrightarrow 17
F \Leftrightarrow 5	S \Leftrightarrow 18
G \Leftrightarrow 6	T \Leftrightarrow 19
H \Leftrightarrow 7	U \Leftrightarrow 20
I \Leftrightarrow 8	V \Leftrightarrow 21
J \Leftrightarrow 9	W \Leftrightarrow 22
K \Leftrightarrow 10	X \Leftrightarrow 23
L \Leftrightarrow 11	Y \Leftrightarrow 24
M \Leftrightarrow 12	Z \Leftrightarrow 25

解密：

F：对应着 C；

K：对应着 H；

L：对应着 I；

Q：对应着 N；

D：对应着 A。

即“FKLQD”经 Caesar 密码解密恢复为“CHINA”(不区分大小写)

3. 代替密码的实现方法分类

单表代替密码

- 使用密钥的单表代替加密
- 仿射加密

多表代替密码

- Playfair 密码

- Hill 密码
- Vigenere 密码

4. 频率分析攻击的一般方法：

- 第一步：对密文中出现的各个字母进行出现的频率统计
- 第二步：根据密文中出现的各个字母的频率，和英语字母标准频率进行对比分析，做出假设，推论加密所用的公式
- 第三步：证实上述假设或继续作其他假设

5. HILL 密码的加密和解密

- P = HILL，对应：7, 8, 11, 11。

- 密钥：

$$K = \begin{bmatrix} 8 & 6 & 9 & 5 \\ 6 & 9 & 5 & 10 \\ 5 & 8 & 4 & 9 \\ 10 & 6 & 11 & 4 \end{bmatrix}$$

- 加密：
$$C = (7 \ 8 \ 11 \ 11) \cdot \begin{bmatrix} 8 & 6 & 9 & 5 \\ 6 & 9 & 5 & 10 \\ 5 & 8 & 4 & 9 \\ 10 & 6 & 11 & 4 \end{bmatrix} \bmod 26$$

$$= (9, 8, 8, 24)$$

$$= (\mathbf{JIY})$$

解密：

$$K^{-1} = \begin{bmatrix} 23 & 20 & 5 & 1 \\ 2 & 11 & 18 & 1 \\ 2 & 20 & 6 & 25 \\ 25 & 2 & 22 & 25 \end{bmatrix}$$

$$P = CK^{-1} = (9 \ 8 \ 8 \ 24) \cdot \begin{bmatrix} 23 & 20 & 5 & 1 \\ 2 & 11 & 18 & 1 \\ 2 & 20 & 6 & 25 \\ 25 & 2 & 22 & 25 \end{bmatrix} \bmod 26$$

$$= (7, 8, 11, 11)$$

$$= (\text{HILL})$$

6. Hill 密码的特点

- 🚩 Hill 密码完全隐藏了单字母的频率
- 🚩 字母和数字的对应可以改成其它方案，使得更不容易攻击成功
- 🚩 能比较好地抵抗频率法的分析，对抗仅有密文的攻击强度较高
- 🚩 易受已知明文攻击

7. 威胁代替密码的因素

- 🚩 频率分析
- 🚩 考虑最可能的字母及单词
- 🚩 重复结构分析
- 🚩 持久性、组织性、创造性和运气
- 🚩 明文已知且易于识别

第四章 密码学的数学引论

1. 密码学的数学基础（数论、群论、有限域理论）

数论

1、除数(因子)的概念：

设 Z 为由全体整数而构成的集合，若 $b \neq 0$ 且 $a, b, m \in Z$ 使得 $a = mb$ ，此时称 b 整除 a 。记为 $b \mid a$ ，还称 b 为 a 的**除数(因子)**。

注：若 $a = mb + r$ 且 $0 < r < b$ ，此时 b 不整除 a ，记为 $b \nmid a$

2、素数(质数)的概念：

整数 $p > 1$ 被称为素数是指 p 的因子仅有 $1, -1, p, -p$ 。

§算术基本定理：

任何一个不等于 0 的正整数 a 都可以写成唯一的表达式 $a = P_1^{a_1} P_2^{a_2} \dots P_t^{a_t}$ ，这里 $P_1 < P_2 < P_3 \dots < P_t$ 是素数，其中 $a_i > 0$

§最大公约数：

若 $a, b, c \in Z$ ，如果 $c \mid a$ ， $c \mid b$ ，称 c 是 a 和 b 的公约数。正整数 d 称为 a 和 b 的最大公约数，如果它满足

- d 是 a 和 b 的公约数。
- 对 a 和 b 的任何一个公约数 c 有 $c \mid d$ 。
-

注：1*. 等价的定义形式是：

$$\gcd(a, b) = \max\{k \mid k \mid a \text{ 且 } k \mid b\}$$

2*. 若 $\gcd(a, b) = 1$ ，称 a 与 b 是**互素的**。

群论

群的概念

- 是由一个非空集合 G 组成，在集合 G 中定义了一个二元运算符 “ \cdot ”，并满足以下性质的代数系统，记为 $\{G, \cdot\}$

- (1) 封闭性：对任意的 $a, b \in G$ ，有： $a \cdot b \in G$ ；
- (2) 结合律：对任何的 $a, b, c \in G$ ，有： $a \cdot b \cdot c = (a \cdot b) \cdot c = a \cdot (b \cdot c)$ ；
- (3) 单位元：存在一个元素 $1 \in G$ （称为单位元），对任意元素，有： $a \cdot 1 = 1 \cdot a = a$ ；
- (4) 逆元：对任意 $a \in G$ ，存在一个元素 $a^{-1} \in G$ （称为逆元），使得： $a \cdot a^{-1} = a^{-1} \cdot a = 1$ ；

交换群：

- (5) 交换律：对任意的 $a, b \in G$ ，有： $a \cdot b = b \cdot a$

有限群

无限群

有限群的阶

循环群

循环群的生成元

定义： $a^3 = a \cdot a \cdot a$ ， $a^0 = 1$ ， $a^{-n} = (a^{-1})^n$ 。

群的性质

- 群中的单位元是唯一的
- 群中每一个元素的逆元是唯一的
- (消去律) 对任意的 $a, b, c \in G$ ，如果 $a \cdot b = a \cdot c$ ，或 $b \cdot a = c \cdot a$ ，则 $b = c$

有限域理论

域的概念

- 域是由一个非空集合 F 组成，在集合 F 中定义了两个二元运算符：“+”和“ \cdot ”，并满足：

F 关于加法“+”是一个交换群；其单位元为“0”， a 的逆元为 $-a$

F 关于乘法“ \cdot ”是一个交换群；其单位元为“1”， a 的逆元为 a^{-1}

(分配律)对任何的 $a, b, c \in F$ ，有： $a \cdot (b + c) = (b + c) \cdot a = a \cdot b + a \cdot c$

(无零因子)对任意的 $a, b \in F$ ，如果 $a \cdot b = 0$ ，则 $a = 0$ 或 $b = 0$

域记为 $\{F, +, \cdot\}$

两个定义：

减法： $a - b = a + (-b)$

除法： $a / b = a \cdot (b^{-1})$

域的实质：

域是一个可以在其上进行加法、减法、乘法和除法运算而结果不会超出域的集合。如有理数集合、实数集合、复数集合都是域，但整数集合不是

有限域

有限域的阶

有限域的两个定理

定理 1：每个有限域的阶必为素数的幂

定理 2：对任意素数 p 与正整数 n ，存在 p^n 阶域。记为 $GF(p^n)$ ，当 $n=1$ 时，有限域 $GF(p)$ 也称为素域

密码学常用素域 $GF(p)$ 或阶为 2^m 的域 $GF(2^m)$

2. 中国剩余定理 (计算题)

例子：

(孙子算经) 今有物不知其数。三三数之余二；五五数之余三；七七数之余二。问物几何？

答曰：二十三。

$$23 \equiv 2 \cdot 70 + 3 \cdot 21 + 2 \cdot 15 \pmod{105}$$

(口诀：三人同行七十稀，五树梅花廿一枝，七子团圆月正半，除百零五便得知。)

问，70，21，15 如何得到的？

原问题为：

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

求解同余方程组

注意：若 x_0 为上述同余方程组的解，则 $x_0' = x_0 + 105 \cdot k (k \in \mathbb{Z})$ 也为上述同余方程组的解。有意义的是，解题口诀提示我们先解下面三个特殊的同余方程组

$$(1) \begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 0 \pmod{5} \\ x \equiv 0 \pmod{7} \end{cases} \quad (2) \begin{cases} x \equiv 0 \pmod{3} \\ x \equiv 1 \pmod{5} \\ x \equiv 0 \pmod{7} \end{cases} \quad (3) \begin{cases} x \equiv 0 \pmod{3} \\ x \equiv 0 \pmod{5} \\ x \equiv 1 \pmod{7} \end{cases}$$

的特殊解

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = ? \quad \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = ? \quad \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = ?$$

以方程 (1) 为对象，相当于解一个这样的同余方程 $35y \equiv 1 \pmod{3}$ ，为什么呢？

原因是，从 (1) 的模数及条件知， x 应同时是 5 和 7 的倍数，即应是 35 的倍数，于是可以假设 $x = 35y$ 有：

$$35y \equiv 1 \pmod{3} \text{ 相当于 } 2y \equiv 1 \pmod{3} \text{ 解出 } y \equiv 2 \pmod{3}$$

$$\text{于是 } x \equiv 35 \cdot 2 \equiv 70 \pmod{105}$$


类似地得到 (2)、(3) 方程的模 105 的解 21、15。

于是有：

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = 70 \qquad \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = 21 \qquad \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = 15$$

得

$$\begin{bmatrix} 2 \\ 3 \\ 2 \end{bmatrix} = 2 \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + 3 \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + 2 \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \\ = 2 * 70 + 3 * 21 + 2 * 15 \equiv 23 \pmod{105}$$

 中国剩余定理：

设自然数 m_1, m_2, \dots, m_r 两两互素，并记 $M = m_1 m_2 \dots m_r$ ， b_1, \dots, b_r 表示 r 个整数，则同余方程组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \dots\dots\dots \\ \dots\dots\dots \\ x \equiv b_r \pmod{m_r} \end{cases} \quad (A)$$

在模 M 同余的意义下有唯一解。

证明： $M = m_1 m_2 \dots m_r$ ，

令 $M_j = M/m_j = m_1 m_2 \dots m_{j-1} m_{j+1} \dots m_r$

求 y_j 使： $M_j y_j \equiv 1 \pmod{m_j}$ $j=1, 2, \dots, r$

由于 $(M_j, m_j) = 1$ ，所以 y_j 是存在的。

令： $x_0 \equiv b_1 M_1 y_1 + b_2 M_2 y_2 + \dots + b_r M_r y_r \pmod{M}$ (B)

可证明 x_0 便是 (A) 式的解。为证明这一点，注意 $j = h$ 时 $m_h | M_j$ 。故 $M_j \equiv 0 \pmod{m_h}$ ，即 x_0 中各项除第 h 项外，其余都模 m_h 同余 0。又 $M_h y_h \equiv 1 \pmod{m_h}$ ，所以：

$x_0 \equiv b_h M_h y_h \pmod{m_h} \equiv b_h \pmod{m_h}$ 。即满足(A)式， x_0 是其解。

下面证明 x_0 是模 M 的唯一解。如若不然，设 x_1 和 x_2 是 (A) 式模 M 的两个解，则有： $x_1 \equiv x_2 \equiv b_j \pmod{m_j} (j=1\dots r)$

那么， $x_1 - x_2 \equiv 0 \pmod{m_j}$ ，即 $m_j \mid (x_1 - x_2) (j=1\dots r)$

因此， $M \mid (x_1 - x_2)$ ，即 $x_1 - x_2 \equiv 0 \pmod{M}$

所以 x_1, x_2 是模 M 的相同解，从而证明了对于模 M 式 (A) 的解是唯一的。

例如：

$$x \equiv 1 \pmod{2}$$

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

解：

$$M = 2 \times 3 \times 5 = 30$$

$$M_1 = 15, M_2 = 10, M_3 = 6$$

$$15y_1 \equiv 1 \pmod{2}, y_1 = 1$$

$$10y_2 \equiv 1 \pmod{3}, y_2 = 1$$

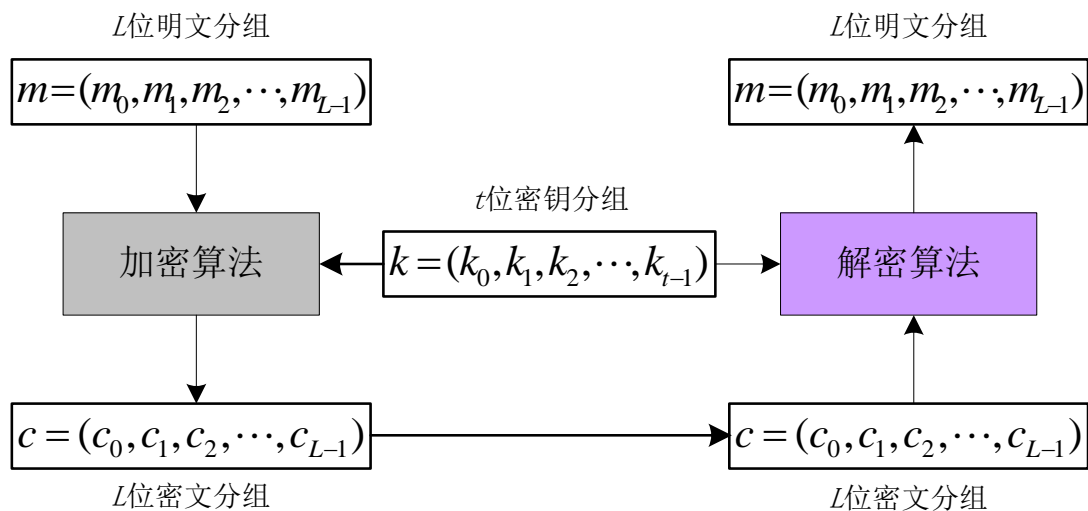
$$6y_3 \equiv 1 \pmod{5}, y_3 = 1$$

$$\text{所以, } x = 1 \times 15 \times 1 + 2 \times 10 \times 1 + 3 \times 6 \times 1 = 53 \equiv 23 \pmod{30}$$

第五章 对称密码体制

1. 分组密码模型

 分组密码模型



2. 分组密码原理

扩散

- 就是将每一位明文的影响尽可能迅速地作用到较多的输出密文位中去，以便隐藏明文的统计特性。

混乱

- 是指密文和明文之间的统计特性关系尽可能地复杂化。

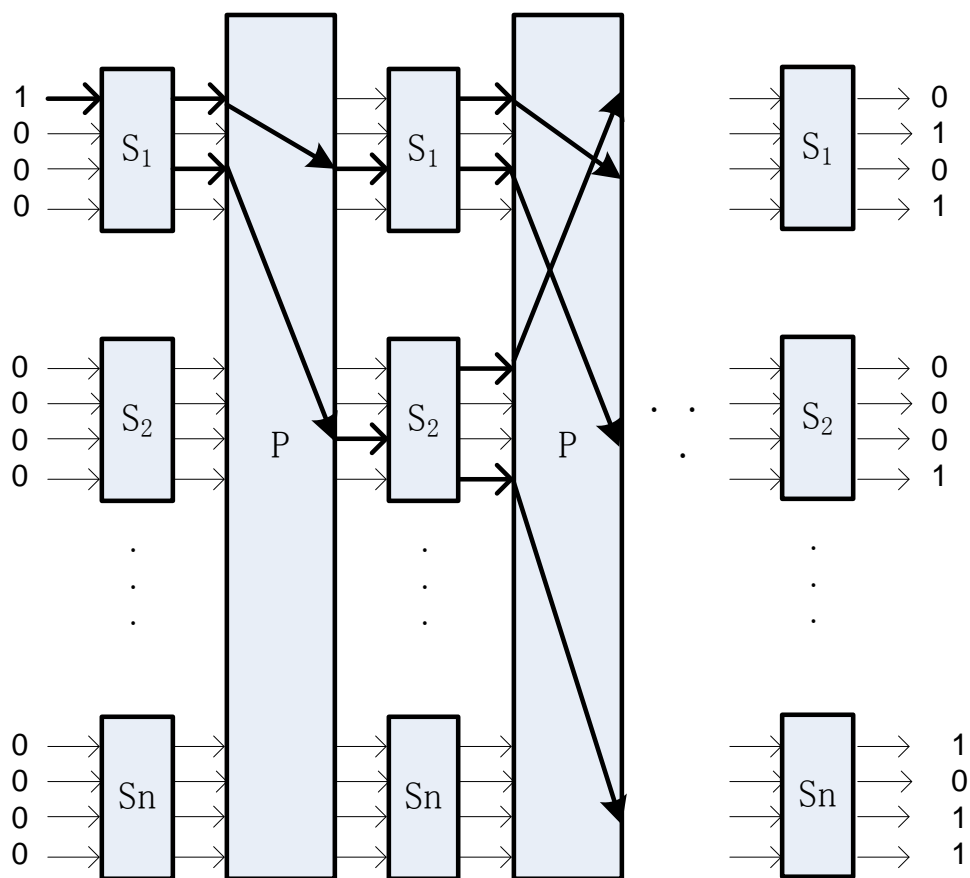
乘积密码

- 指依次使用两个或两个以上的基本密码，所得结果的密码强度将强于所有单个密码的强度

3. 雪崩效应

- 雪崩效应：输入（明文或密钥）即使只有很小的变化，也会导致输出发生巨大变化的现象

- 输入位有很少的变化，经过多轮变换以后导致多位发生变化。即明文的一个比特的变化应该引起密文许多比特的改变



4. 分组密码的操作模式

- 电子密码本 (ECB) 模式
- 密码分组链接 (CBC) 模式
- 计数器 (CRT) 模式
- 输出反馈 (OFB) 模式
- 密码反馈 (CFB) 模式
- ECB 模式

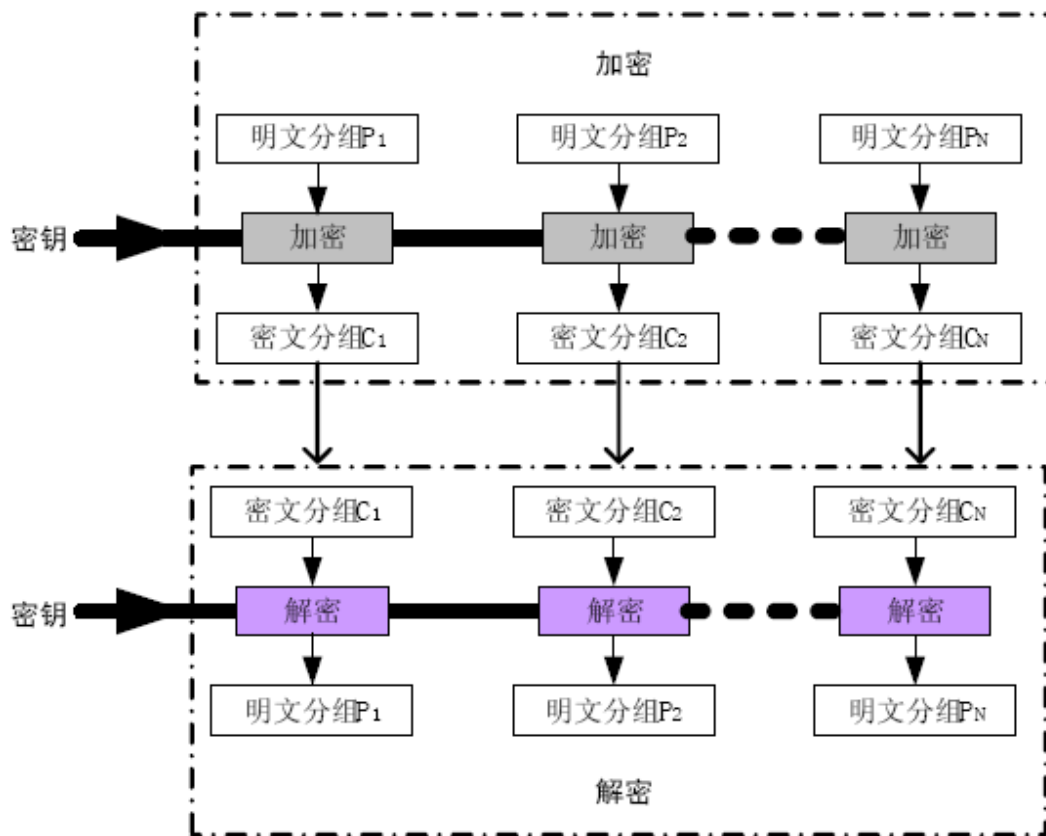


图5-9 电子密码本模式

ECB 模式的优缺点

- 模式操作简单
- 明文中的重复内容将在密文中表现出来，特别对于图像数据和明文变化较少的数据
- 适于短报文的加密传递

CBC 模式

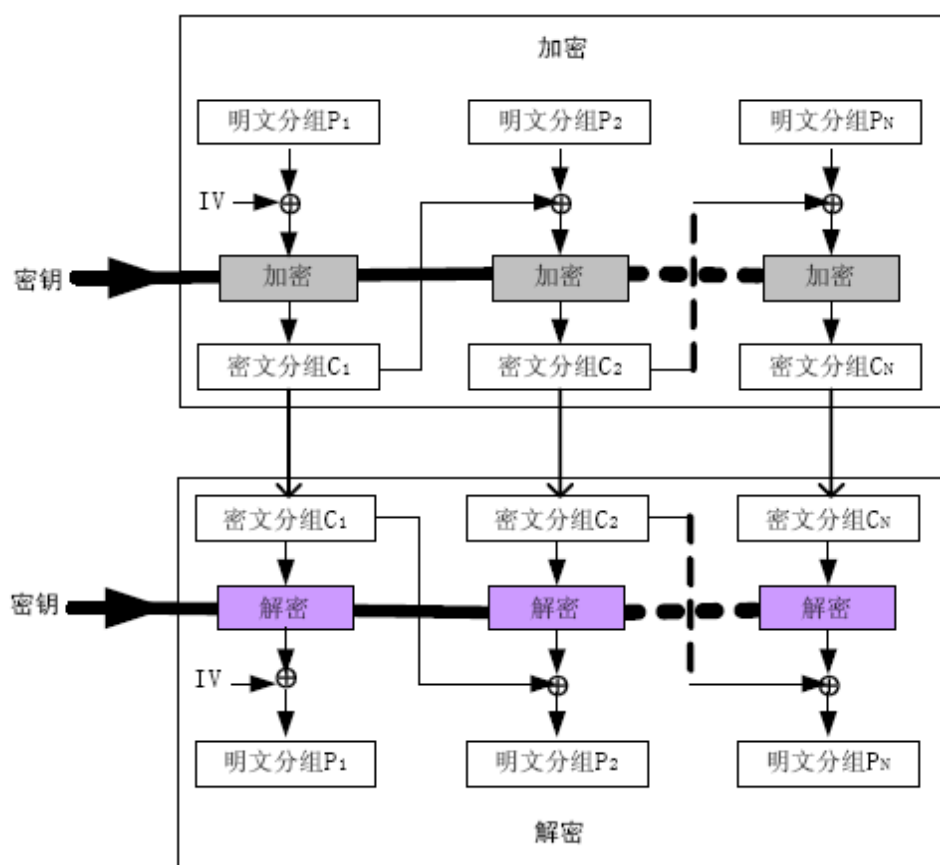


图5-10 密码分组链接模式

🌈 CBC 模式的特点

- 同一个明文分组重复出现时产生不同的密文分组
- 加密函数的输入是当前的明文分组和前一个密文分组的异或；对每个分组使用相同的密钥。
- 将明文分组序列的处理连接起来了。每个明文分组的加密函数的输入与明文分组之间不再有固定的关系
- 有助于将 CBC 模式用于加密长消息

🌈 CTR 模式

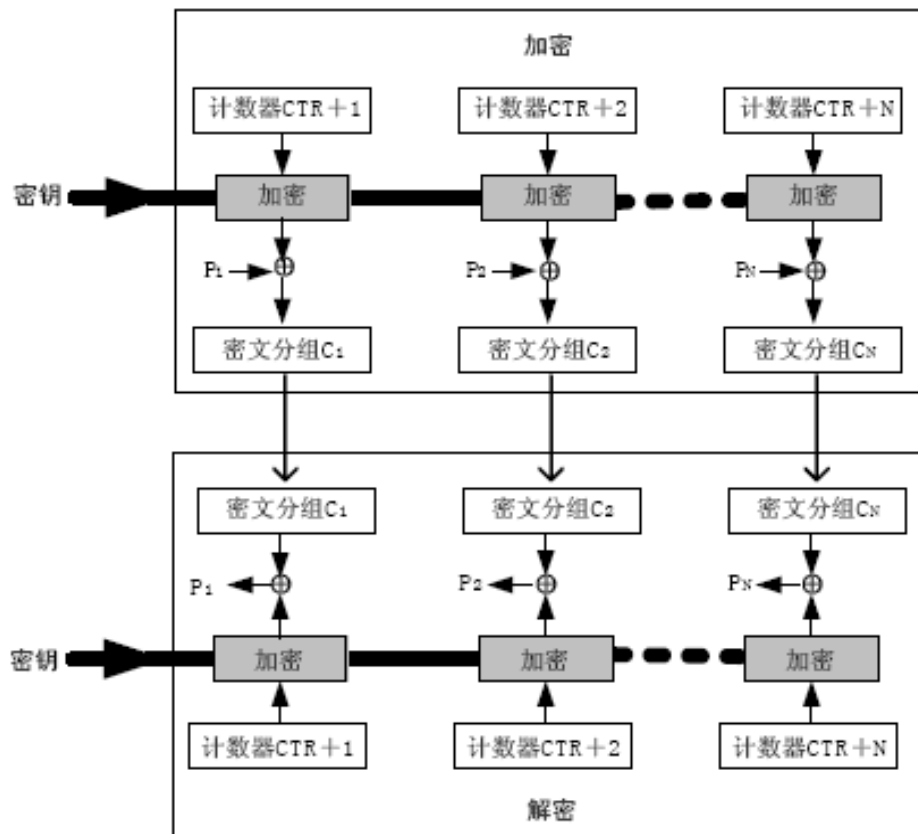


图5-11 计数器模式

CTR 模式的特点

- 使用与明文分组规模相同的计数器长度
- 处理效率高（并行处理）
- 预处理可以极大地提高吞吐量
- 可以随机地对任意一个密文分组进行解密处理，对该密文分组的处理与其它密文无关
- 实现的简单性
- 适于对实时性和速度要求较高的场合

OFB 模式

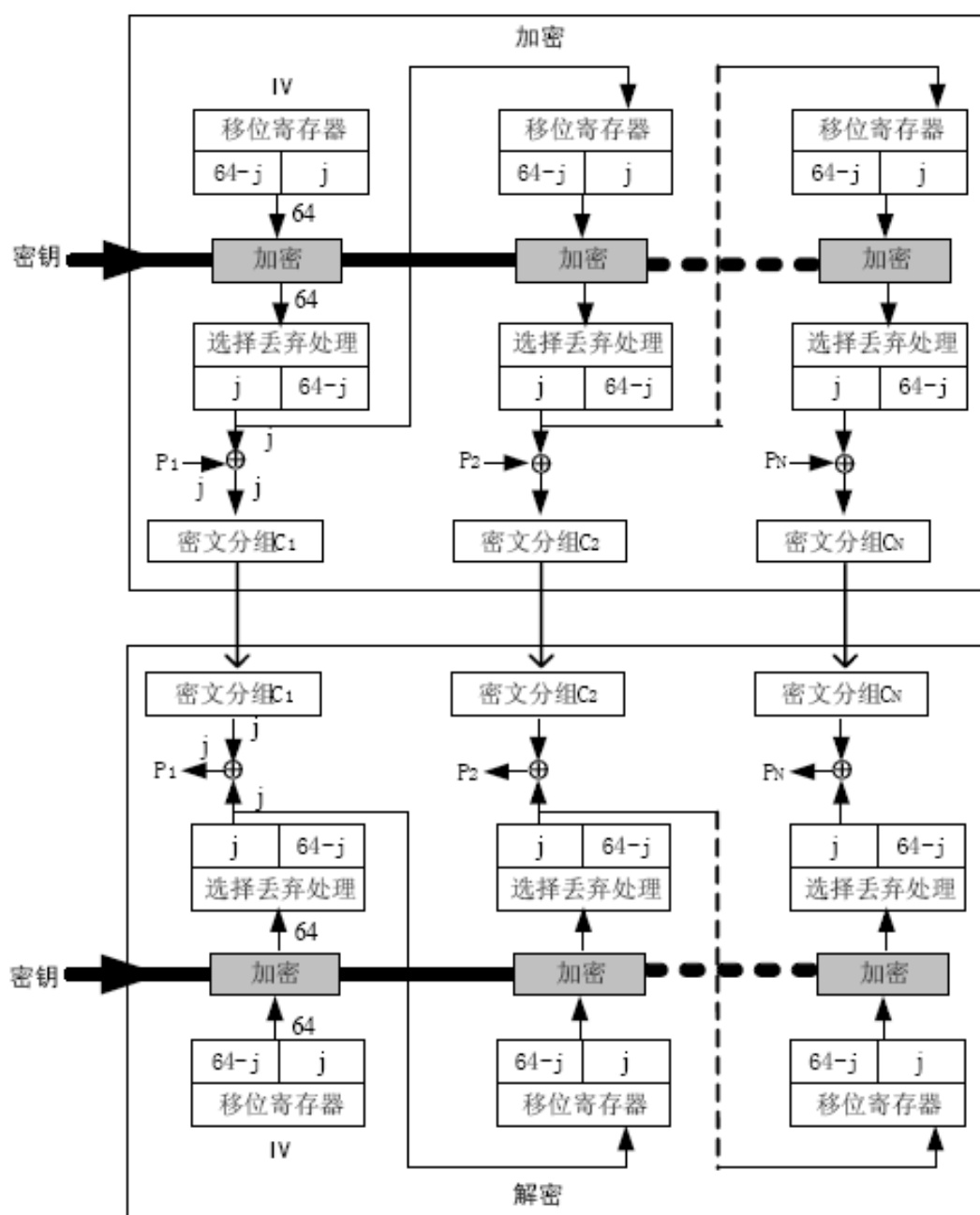


图5-12 输出反馈模式

CFB 模式

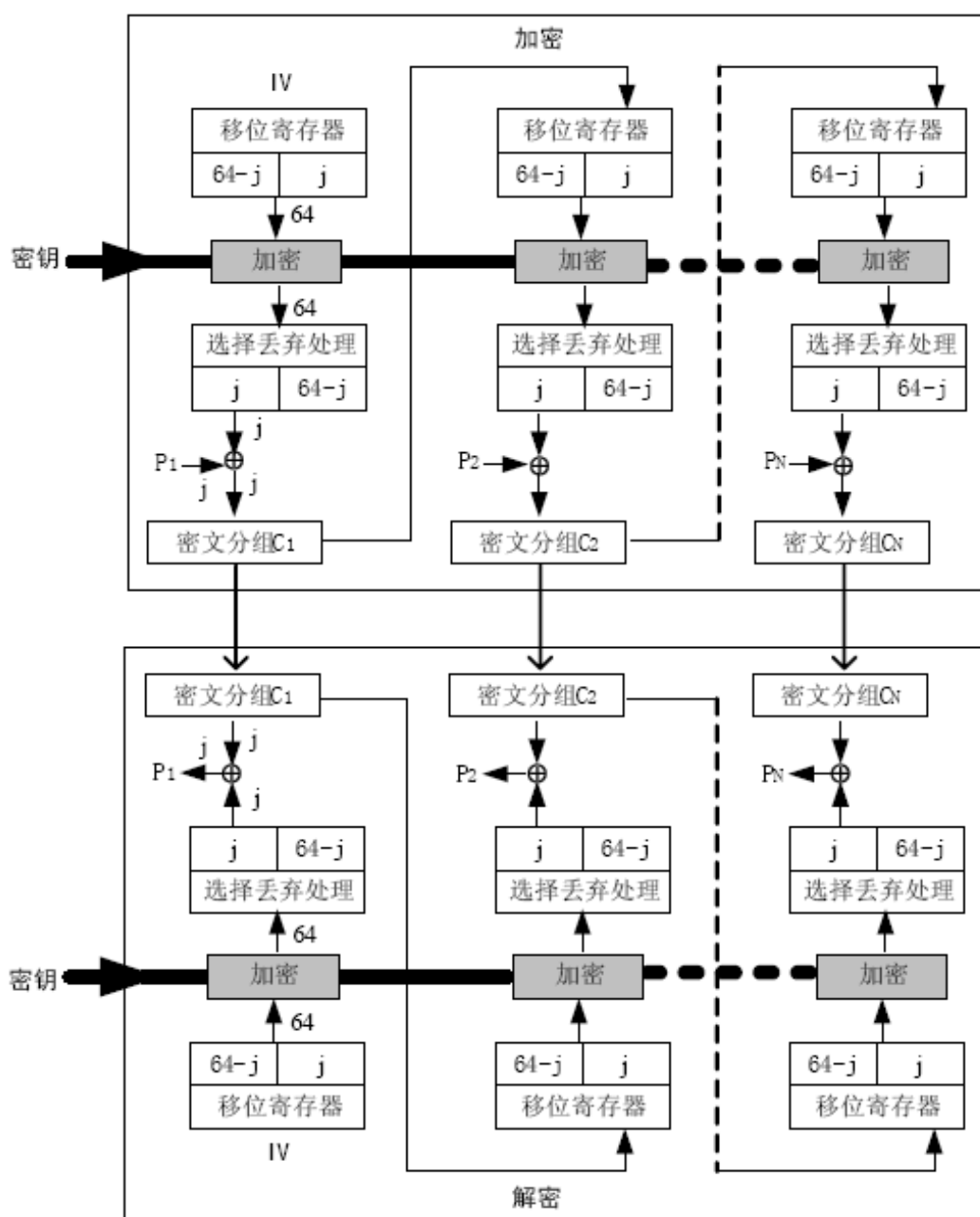
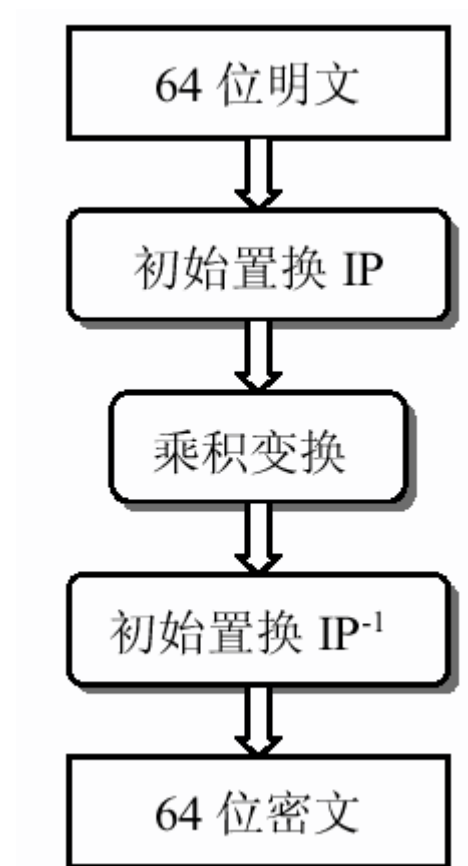


图5-13 密码反馈模式

影响密码操作模式选择的因素

- 安全性
- 高效性
- 所能实现的功能

5. DES 的加密处理略图



6. 3DES 的优、缺点

🌈 优点：

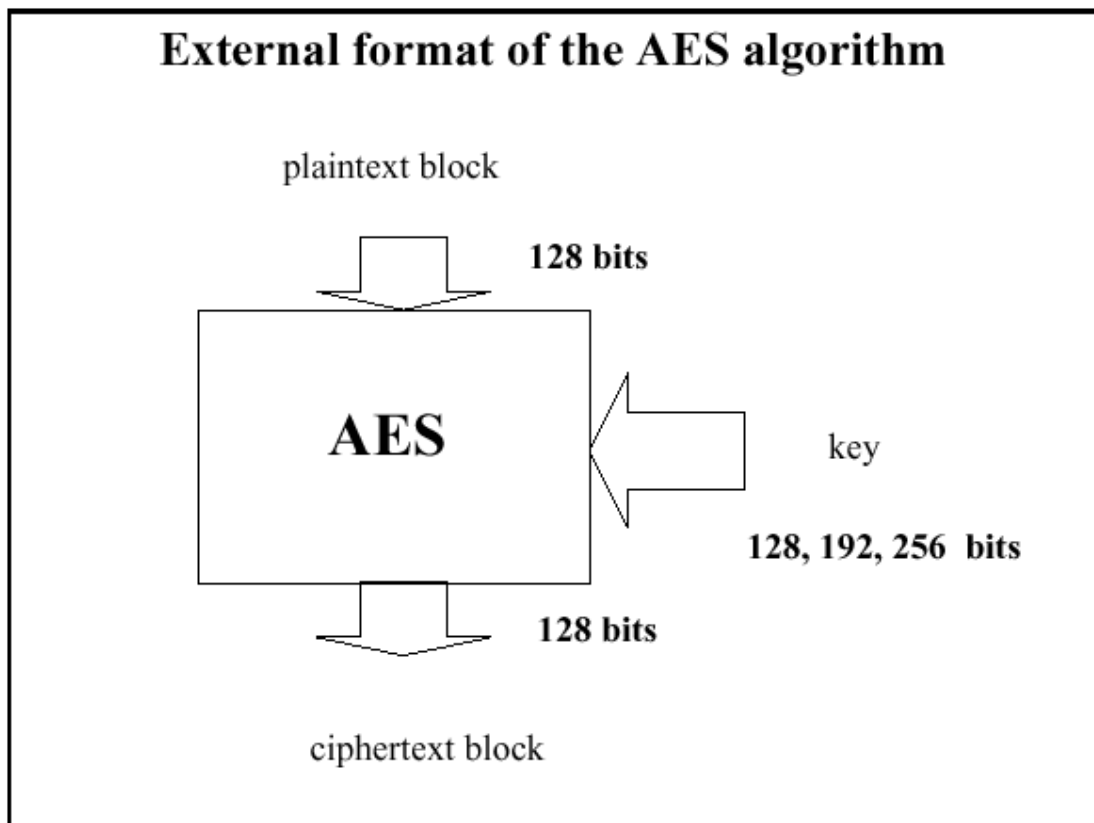
- 密钥长度增加到 112 位或 168 位，可以有效克服穷举搜索攻击；
- 相对于 DES，增强了抗差分分析和线性分析的能力；
- 具备继续使用现有的 DES 实现的可能。

🌈 缺点：

- 处理速度相对较慢，特别是对于软件实现。
- 明文分组的长度仍为 64 位，就效率 and 安全性而言，与密钥的增长不匹配。

7. 高级加密标准 (AES)

- 1997 年 9 月 12 日：美国 NIST 提出征集该算法的公告
 - 1998 年 8 月 20 日：NIST 召开了第一次候选大会，并公布了 15 个候选算法
 - 1999 年 3 月 22 日：NIST 从 15 个候选算法中公布了 5 个进入第二轮选择：
MARS , RC6 , Rijindael , SERPENT 和 Twofish
 - 2000 年 10 月 2 日：以安全性、性能、大小、实现特性为标准而最终选定了
Rijindael 算法
 - 2001 年：正式发布 AES 标准
- 外部格式的 AES 算法



8. AES 的基本运算

- ✚ 字节代替 SubBytes
- ✚ 列混淆 MixColumns
- ✚ 轮密钥加 AddRoundKey
- ✚ 行移位 ShiftRows

“三代替、一换位”

第六章 公钥密码体制

1. 三种典型的公钥密码体制

- ✚ DH 密钥交换算法
- ✚ RSA
- ✚ ECC

2. 对公钥密码体制的要求

- ✚ 参与方 B 容易通过计算产生一对密钥（公开密钥 KUb 和私有密钥 KRb）。
- ✚ 在知道公开密钥和待加密报文 M 的情况下，对于发送方 A，很容易通过计算产生对应的密文： $C = EKUb(M)$
- ✚ 接收方 B 使用私有密钥容易通过计算解密所得的密文以便恢复原来的报文： $M = DKRb(C) = DKRb(EKUb(M))$
- ✚ 敌对方即使知道公开密钥 KUb，要确定私有密钥 KRb 在计算上是不可行的。
- ✚ 敌对方即使知道公开密钥 KUb 和密文 C，要想恢复原来的报文 M 在计算上也是不可行的。

🌈 加密和解密函数可以以两个次序中的任何一个来使用:

$$M = D_{K_{Rb}} (E_{K_{Ub}} (M)) \quad M = E_{K_{Ub}} (D_{K_{Rb}} (M))$$

3. 陷门单向函数

🌈 是满足下列条件的函数 f :

- (1) 给定 x , 计算 $y=f(x)$ 是容易的
- (2) 给定 y , 计算 x 使 $y=f(x)$ 是困难的
- (3) 存在 δ , 已知 δ 时, 对给定的任何 y , 若相应的 x 存在 , 则计算 x 使 $y=f(x)$ 是容易的

注 :

1* . 仅满足(1)、(2)两条的称为单向函数 ; 第(3)条称为陷门性 , δ 称为陷门信息。

2* 加密密钥便称为公开密钥 , 记为 Pk 。 f 函数的设计者将 δ 保密 , 用作解密密钥 , 此时 δ 称为秘密密钥 , 记为 Sk 。 由于加密函数是公开的 , 任何人都可以将信息 x 加密成 $y=f(x)$, 然后送给函数的设计者 (当然可以通过不安全信道传送) ; 由于设计者拥有 Sk , 他自然可以解出 $x=f^{-1}(y)$ 。

3* . 单向陷门函数的第(2)条性质表明窃听者由截获的密文 $y=f(x)$ 推测 x 是不可行的。

4. 公钥密码系统的应用类型

🌈 加密/解密

🌈 数字签名

🌈 会话密钥交换

5. DH 例子 (计算题)

🌈 素数 $q=97$, 它的一个本原元 $a=5$

- ✚ A 和 B 分别选择随机数 $X_a=36$ 和 $X_b=58$
- ✚ A 计算公开密钥： $Y_a=536 \bmod 97=50 \bmod 97$
- ✚ B 计算公开密钥： $Y_b=558 \bmod 97=44 \bmod 97$
- ✚ A 计算会话密钥： $K=4436 \bmod 97=75 \bmod 97$
- ✚ B 计算会话密钥： $K=5058 \bmod 97=75 \bmod 97$

6. RSA 数学基础

由 Rivest, Shamir 和 Adleman 在 1978 年提出来的

数学基础: Euler 定理，并建立在大整数因子分解的困难性之上

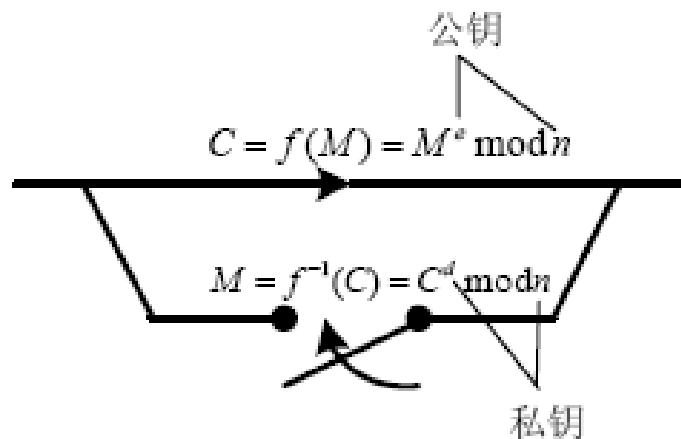


图6-5 RSA利用单向陷门函数的原理

7. RSA 密码体制描述

- ✚ 明文空间 P = 密文空间 $C = Z_n$
- ✚ 密钥的生成
 - 选择互异素数 p, q ，计算 $n = p * q$ ， $\varphi(n) = (p-1)(q-1)$ ，选择整数 e 使 $(\varphi(n), e) = 1, 1 < e < \varphi(n)$ ，计算 d ，使 $d = e^{-1} \bmod \varphi(n)$
 - 公钥 $Pk = \{e, n\}$
 - 私钥 $Sk = \{d, n\}$

🌈 加密 (用 e, n)

- 明文 : $M < n$ 密文 : $C = M^e \pmod n$

🌈 解密 (用 d, n)

- 密文 : C 明文 : $M = C^d \pmod n$

8. RSA 算法实现的三个基本问题

🌈 如何计算 $a^b \pmod n$?

要点 1 : $(a \times b) \pmod n = [(a \pmod n) \times (b \pmod n)] \pmod n$

要点 2 : $a^{16} = a^{2^4}$

$$= a^2, a^4, a^8, a^{16}$$

更一般性的问题 : a^m

m 的二进制表示为 $b_k b_{k-1} \dots b_0$, 则 $m = \sum_{i=0}^k b_i 2^i$

计算 $a^m \pmod n$

$$a^m \pmod n = \left[\prod_{b_i \neq 0} a^{(2^i)} \right] \pmod n$$

$$= \prod_{b_i \neq 0} [a^{(2^i)} \pmod n]$$

快速取模指数算法计算 $a^b \pmod n$

$c \leftarrow 0; d \leftarrow 1$

for $i \leftarrow k$ downto 0

```

do c  $\leftarrow$  2×c
  d  $\leftarrow$  (d × d) mod n
  if bi=1
    then c  $\leftarrow$  c+1
        d  $\leftarrow$  (d × a) mod n
return d

```

快速取模指数运算法二

要计算，更新一个三维数组 (X,M,Y)，该三维数组的初始值为 (a,m,1)。每一步的运算逻辑是：

- 如果 M 是奇数则用 $X*Y \bmod n$ 取代 Y、用 M-1 取代 M、X 的值不变；
- 如果 M 是偶数则用 $X*X \bmod n$ 取代 X、用 M/2 取代 M、Y 的值不变；
- 当 M=0 时，则对应应有 $Y=a^m \bmod n$

🌈 如何判定一个给定的整数是素数？

Miller and Rabin, WITNESS 算法

WITNESS(a,n) 判定 n 是否为素数，a 是某个小于 n 的整数

```

1. 令  $b_k b_{k-1} \dots b_0$  为 (n-1) 的二进制表示，
2. d  $\leftarrow$  1
3. for i  $\leftarrow$  k downto 0
4.     do x  $\leftarrow$  d
5.     d  $\leftarrow$  (d × d) mod n
6.     if d = 1 and x  $\neq$  1 and x  $\neq$  n-1
7.         then return TRUE
8.     if bi = 1
9.         then d  $\leftarrow$  (d × a) mod n
10. if d  $\neq$  1
11. then return TRUE
12. return FALSE

```

返回值：

TRUE: n 一定不是素数

FALSE: n 可能是素数

应用：

随机选择 $a < n$, 计算 s 次, 如果每次都返回 FALSE, 则这时 n 是素数的概率为 $(1 - 1/2^s)$

🚦 如何找到足够大的素数 p 和 q ?

1. 随机选一个奇数 n (伪随机数发生器)
2. 随机选择一个整数 $a < n$
3. 执行概率素数判定测试, 如果 n 未测试通过, 则 拒绝数值 n , 转向步骤 1
4. 如果 n 已通过足够的测试, 则接受 n , 否则转向步骤 2;

说明：① 随机选取大约用 $\ln(N)/2$ 的次数, 如 $\ln(2^{200})/2=70$

② 好在生成密钥对时才用到, 慢一点还可忍受。

③ 确定素数 p 和 q 以后, 只需选取 e , 满足 $\gcd(e, \phi(n))=1$, 计算 $d = e^{-1} \bmod \phi(n)$ (扩展的欧拉算法)

9. 椭圆曲线密码体制 ECC

🚦 椭圆曲线密码体制以高效性著称

🚦 由 Neal Koblitz 和 Victor Miller 在 1985 年分别提出

🚦 ECC 的安全性基于椭圆曲线离散对数问题的难解性

🚦 密钥长度大大地减小

🚦 是目前已知公钥密码体制中每位提供加密强度最高的一种体制

10. 椭圆曲线密码体制描述

1、系统的建立

2、密钥的生成

3、加密过程

4、解密过程

系统的建立

- 选取:
 - 一个基域 $GF(p)$
 - 定义在该基域上的椭圆曲线 $E_p(a,b)$
 - E 上的一个拥有素数阶 n 的点 P
- 其中有限域 $GF(p)$, 椭圆曲线参数 a,b , 点 P 和阶 n 都是公开信息

密钥的生成

- 在区间 $[1,n-1]$ 中随机选取一个整数 d
- 计算: $Q=d*P$
- 实体的
 - 公开密钥: 点 Q
 - 实体的私钥: 整数 d

加密过程

- 待发送消息 : $A \rightarrow B : M$
 - 查找 B 的公开密钥 : Q
 - 将消息 M 表示成一个域元素: m
 - 在区间 $[1, n-1]$ 中随机选取一个整数 k

- 计算点: $(x_1, y_1) = kP$
- 计算点: $(x_2, y_2) = kQ$, 如果 $x_2 = 0$, 则返回第(3)步
- 计算: $c = mx_2$
- 传送加密数据 (x_1, y_1, c) 给 B

解密过程

- 当实体 B 解密从 A 收到的密文 (x_1, y_1, c) 时, 执行步骤:
 - 使用私钥 d , 计算点: $(x_2, y_2) = d(x_1, y_1)$
 - 计算 $m = c \cdot x_2^{-1}$, 恢复出消息 m

11. 椭圆曲线密码体制与离散对数密码体制的比较

表6-2 离散对数密码体制和椭圆曲线密码体制的特征对比

特征	离散对数密码体制	椭圆曲线密码体制
条 件	$GF(p)^*$	$GF(p)$ 域上的椭圆曲线 E
基本操作	$GF(p)$ 域内的乘法	$GF(p)$ 域内点的加法
主要操作	(幂) 子数运算	标量乘运算
基本元素	生成元 g	基点 G
基本元素的阶	素数 p	素数 p
私 钥	整数 $d \pmod{p}$	整数 $d \pmod{p}$
公 钥	$GF(p)$ 域内元素 $e = g^d \pmod{p}$	椭圆曲线 E 上的点 $Q = d \times G \pmod{p}$

第七章 Hash 函数与消息认证

1. 安全 HASH 函数的一般结构

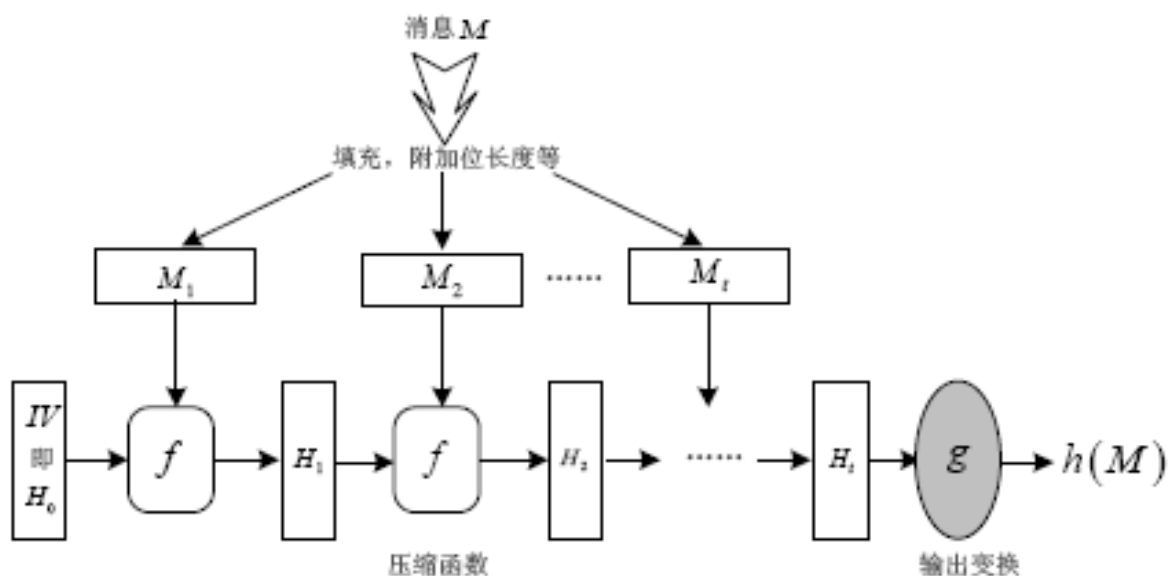


图7-1 安全散列函数的一般结构

第八章 数字签名

1. 数字签名应具有的性质

- 🌈 签名是对文档的一种映射，签名与文档具有——对应关系（精确性）
- 🌈 签名应基于签名者的唯一性特征（如私钥），从而确定签名的不可伪造性和不可否认性（唯一性）
- 🌈 签名应该具有时间特征，防止签名的重复使用（时效性）

2. 数字签名的要求

- 🌈 接收者能够核实发送者对报文的签名

- ✚ 发送者事后不能抵赖对报文的签名
- ✚ 接收者不能伪造对报文的签名
- ✚ 必须能够认证签名时刻的内容
- ✚ 签名必须能够被第三方验证，以解决争议

3. 数字签名方案描述

- ✚ 设 P 是消息的有限集合（明文空间）， S 是签名的有限集合（签名空间）， K 是密钥的有限集合（密钥空间），则：签名算法是一个映射：

$$sig : P \times K \rightarrow S, y = sig_k(x)$$

- ✚ 验证算法也是一个映射：

$$ver : P \times S \rightarrow \{(true, false) \mid \begin{array}{l} ver(x, y) = true, \text{ 如果 } y = sig_k(x) \\ ver(x, y) = false, \text{ 如果 } y \neq sig_k(x) \end{array}\}$$

- ✚ 五元组 $\{P, S, K, sig, ver\}$ 就称为一个签名方案

4. 两类数字签名函数（分别举 1 例）

- ✚ 直接数字签名

例 1

(1) $A \rightarrow B: E_{KR_a}[M]$

提供了认证与签名：

- 只有 A 具有 KR_a 进行加密
- 传输中无法被篡改
- 任何第三方可以用 KU_a 验证签名

(1') $A \rightarrow B: E_K [E_{KR_a}(M)]$

提供了保密(K)、认证与签名(KR_a)

例 2

(2) $A \rightarrow B: M || E_{K_{Ra}}[H(M)]$

提供认证及数字签名

- $H(M)$ 受到密码算法的保护
- 只有 A 能够生成 $E_{K_{Ra}}[H(M)]$
- $H(M)$ 有压缩功能

(2') $A \rightarrow B: E_K[M || E_{K_{Ra}}[H(M)]]$ 或 $E_K [M] || E_{K_{Ra}}[H(M)]$

提供保密性、认证和数字签名

🌈 可仲裁数字签名

例 1

(a) 单密钥加密方式，仲裁者可以看见消息：

(1) $X \rightarrow A: M || E_{K_{xa}}[ID_x || H(M)]$

(2) $A \rightarrow Y: E_{K_{ay}}[ID_x || M || E_{K_{xa}}[ID_x || H(M)] || T]$

X 与 A 之间共享密钥 K_{xa} ，Y 与 A 之间共享密钥 K_{ay} ；

X：准备消息 M，计算其散列码 $H(M)$ ，用 X 的标识符 ID_x 和散列值构成

签名，并将消息及签名经 K_{xa} 加密后发送给 A；

A：解密签名，用 $H(M)$ 验证消息 M，然后将 ID_x ，M，签名，和时间戳

一起经 K_{ay} 加密后发送给 Y；

Y：解密 A 发来的信息，并可将 M 和签名保存起来。

解决纠纷：

Y：向 A 发送 $E_{K_{ay}}[ID_x || M || E_{K_{xa}}[ID_x || H(M)]]$

A：用 K_{ay} 恢复 ID_x ，M，和签名（ $E_{K_{xa}}[ID_x || H(M)]$ ），然后用 K_{xa} 解密签名并验证散列码。

注意：

在这种模式下 Y 不能直接验证 X 的签名，Y 认为 A 的消息已认证，只因为它来自 A。因此，双方都需要高度相信 A：

- X 必须信任 A 没有暴露 K_{xa} ，并且没有自己生成签名

$$E_{K_{xa}}[ID_x || H(M)]$$

- Y 必须信任 A 验证了散列值正确并且签名确实是 X 产生的情况下才发送的 $E_{K_{ay}}[ID_x || M || E_{K_{xa}}[ID_x || H(M)] || T]$
- 双方都必须信任 A 处理争议是公正的。

只要 A 遵循上述要求，则 X 相信没有人可以伪造其签名；Y 相信 X 不能否认其签名。

上述情况还隐含着 A 可以看到 X 给 Y 的所有信息，因而所有的窃听者也能看到。

例 2

(b) 单密钥加密方式，仲裁者不可以看见消息：

$$(1) X \rightarrow A : ID_x || E_{K_{xy}}[M] || E_{K_{xa}}[ID_x || H(E_{K_{xy}}[M])]$$

$$(2) A \rightarrow Y : E_{K_{ay}}[ID_x || E_{K_{xy}}[M] || E_{K_{xa}}[ID_x || H(E_{K_{xy}}[M])]] || T]$$

在这种情况下，X 与 Y 之间共享密钥 K_{xy} ，

X：将标识符 ID_x ，密文 $E_{K_{xy}}[M]$ ，以及对 ID_x 和密文消息的

散列码用 K_{xa} 加密后形成签名发送给 A。

A：解密签名，用散列码验证消息，这时 A 只能验证消息的

密文而不能读取其内容。然后 A 将来自 X 的所有信息加上

时间戳并用 K_{ay} 加密后发送给 Y。

(a)和(b)共同存在一个共性问题：

A 和发送方联手可以否认签名的信息；

A 和接收方联手可以伪造发送方的签名；

例 3

(c) 双密钥加密方式，仲裁者不可以看见消息：

$$(1) X \rightarrow A : ID_x || E_{KR_x}[ID_x || E_{KU_y}(E_{KR_x}[M])]$$

$$(2) A \rightarrow Y : E_{KR_a}[ID_x || E_{KU_y}(E_{KR_x}[M]) || T]$$

X：对消息 M 双重加密：首先用 X 的私有密钥 KR_x ，然后用 Y 的公开

密钥 KU_y 。形成一个签名的、保密的消息。然后将该信息以及

X 的标识符一起用 KR_x 签名后与 ID_x 一起发送给 A。这种内部、

双重加密的消息对 A 以及对除 Y 以外的其它人都是安全的。

A：检查 X 的公开/私有密钥对是否仍然有效，是，则认证消息。并

将包含 ID_x 、双重加密的消息和时间戳构成的 消息用 KR_a 签名后

发送给 Y。

本模式比上述两个模式具有以下好处：

- 1、在通信之前各方之间无须共享任何信息，从而避免了联手作弊；
- 2、即使 KR_x 暴露，只要 KR_a 未暴露，不会有错误标定日期的消息被发送；
- 3、从 X 发送给 Y 的消息的内容对 A 和任何其他人是保密的。

5. 直接数字签名的缺点

🌈 验证模式依赖于发送方的私有密钥

- 发送方可能声称其私有密钥丢失或被窃，而抵赖发送过某一消息
- 需采用与私有密钥安全性相关的行政管理控制手段来制止或削弱这种情况，但威胁在某种程度上依然存在

🌈 X 的某些私有密钥确有可能在时间 T 被窃取，敌方可以伪造 X 的签名及早于或等于时间 T 的时间戳

🌈 改进的方式：对被签名的信息添加时间戳（日期与时间）

须将已暴露的密钥及时报告给一个授权中心（如 CRL）

6. 可仲裁数字签名原理

🌈 引入仲裁者

- 通常做法：所有 $X \rightarrow Y$ 的签名消息首先送到仲裁者 A，A 将消息及其签名进行一系列测试，以检查其来源和内容，然后将消息加上时间戳，并与已被验证通过的签名一起发给 Y

🌈 仲裁者在这一类签名模式中扮演裁判角色

- 所有参与者必须绝对相信这一仲裁机制工作正常（trusted system）

7. 数字签名标准(DSS)的主要参数

🌈 DSS 的主要参数：

(1)全局公开密钥分量，可以为用户公用

p ：素数，要求 $2^{L-1} < p < 2^L$, $512 \leq L < 1024$ ，且 L 为 64 的倍数

q ：($p-1$)的素因子， $2^{159} < q < 2^{160}$ ，即比特长度为 160 位

$g := h^{(p-1)/q} \bmod p$ 。其中 h 是一整数， $1 < h < (p-1)$ 且 $h^{(p-1)/q} \bmod p > 1$

(2)用户私有密钥

x ：随机或伪随机整数，要求 $0 < x < q$

(3)用户公开密钥

$y := g^x \bmod p$

(4) k ：随机或伪随机整数，要求 $0 < k < q$

第九章 密钥管理

1. 密钥管理的地位

- 🌈 密钥管理：在授权各方实现密钥关系的建立和维护的一整套技术和程序
- 🌈 密钥管理负责密钥的生成、存储、分配、使用、备份/恢复、更新、撤销和销毁等
- 🌈 现代密码系统的安全性并不取决于对密码算法的保密或者是对加密设备等的保护，一切秘密寓于密钥之中
- 🌈 注意：密钥管理要求管理与技术并重

2. 密钥管理的层次式结构

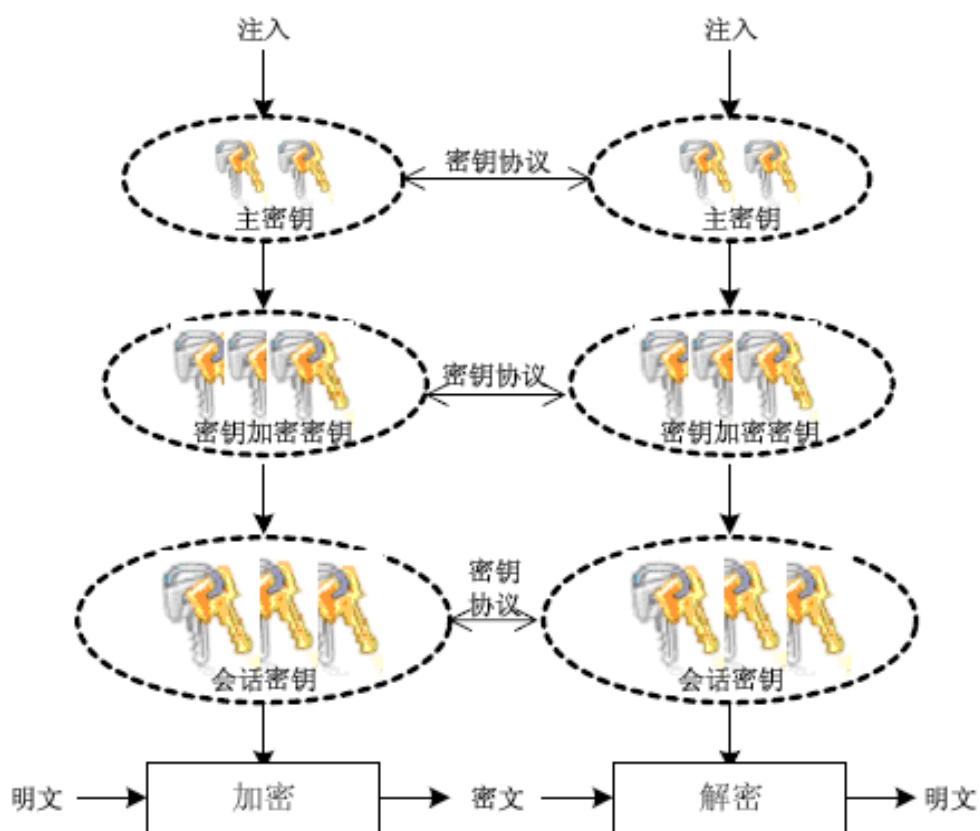


图9-1 密钥管理的层次结构

3. 层次式密钥管理的优势

安全性强

- 层次式管理形成一个动态的密钥系统

可实现密钥管理的自动化

- 除主密钥外，其他各层的密钥均可由系统按照某种协议进行自动化管理
- 大大提高了工作效率和数据安全性

4. 公开密钥的分发方式

建立公钥目录

带认证的公钥分发（在线服务器方式）

使用数字证书的公钥分发（离线服务器方式）

开放性试题

1. 举例说明生活或工作中的密码技术

二代身份证

内含有 RFID 芯片，特定的逻辑加密算法，无法复制，高度防伪，写入的信息可划分安全等级，分区存储、授权读写。

U盾

内置微型智能卡处理器，采用 1024 位非对称密钥算法对网上数据进行加密、解密和数字签名，确保网上交易的保密性、真实性、完整性和不可否认性。