信息安全复习

——林逸

第一章　绪论

1. 安全机制：

概念：用来保护系统免受侦听、阻止安全攻击及恢复系统的机制

特定的安全机制：加密、数字签名、访问控制、数据完整性、认证交换、流量填充…

通用的安全机制：　可信功能、安全标签、事件检测、安全审计跟踪、安全恢复。

2. 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

3. 安全攻击的主要形式：

(1)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。

(2)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。

(3)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

(4)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

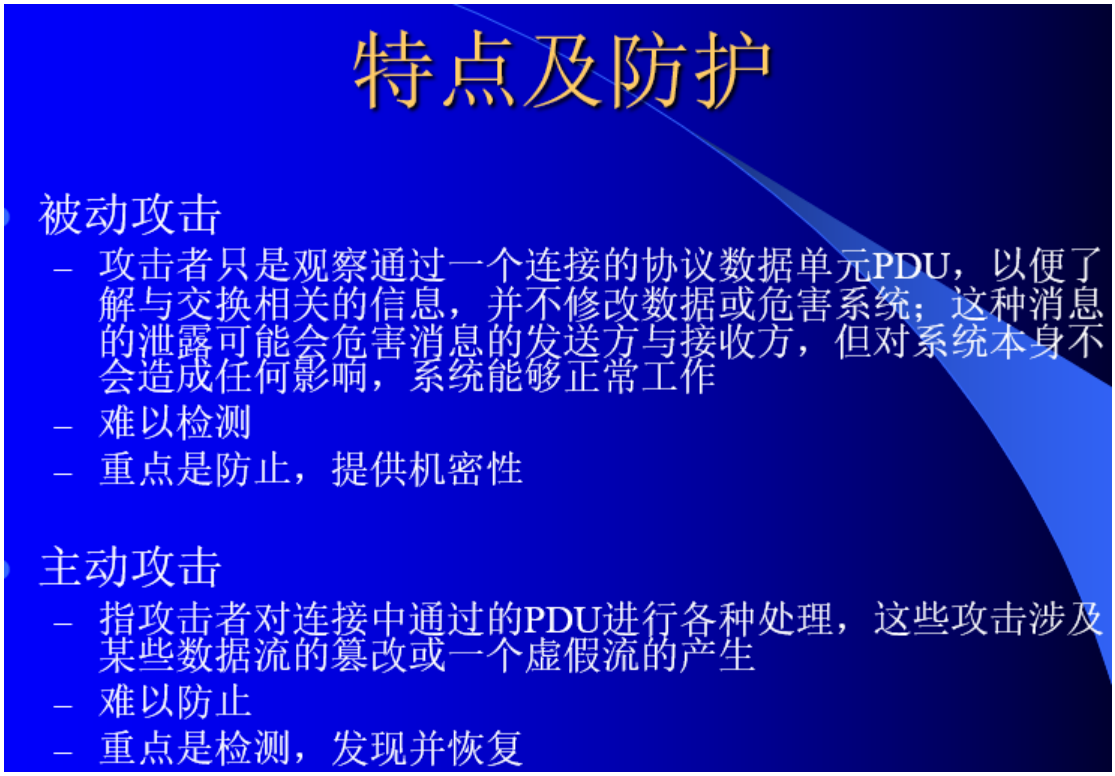
(5)重放（Replaying）

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

(6)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



第 2 章　密码学基础

1. 安全模型：

网络传输中的信息安全：

动态数据的安全

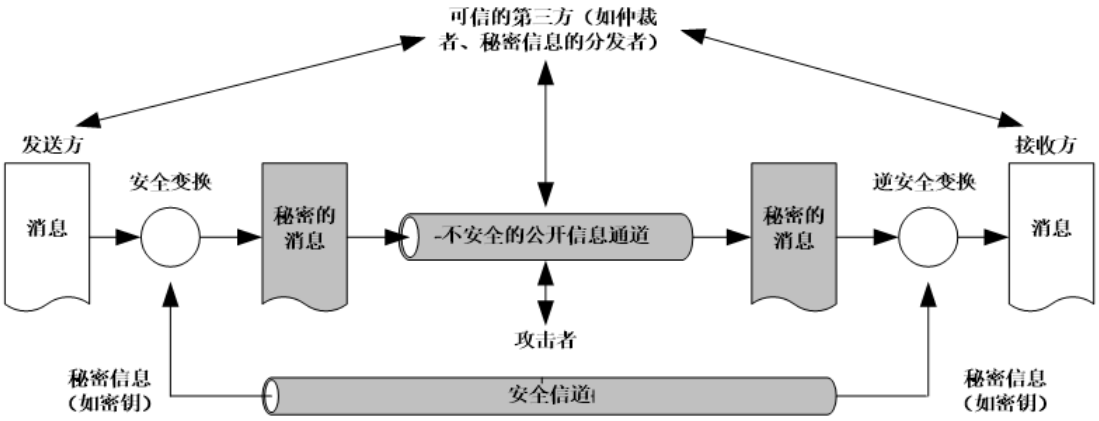
网络安全模型

计算机系统中的信息安全：

静态数据的安全

网络访问安全模型

网络通信安全模型



网络访问安全模型

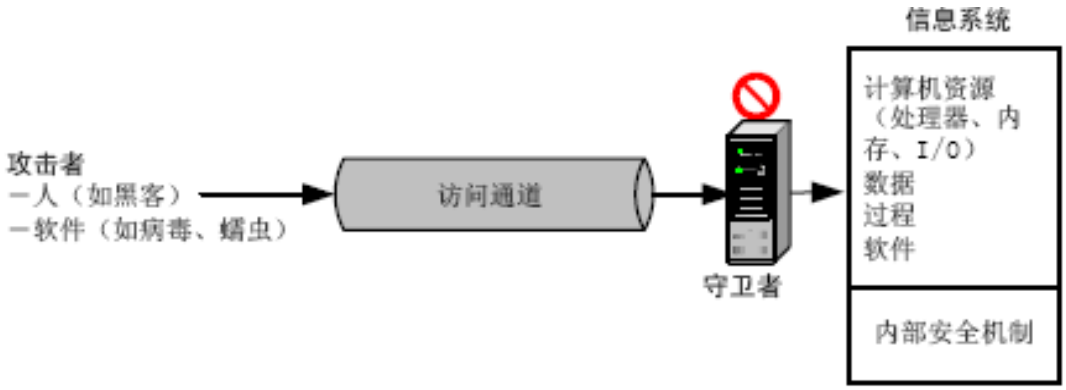


图2-3　网络访问安全模型

2. 密码系统的安全条件：

密码系统的安全性只寓于密钥，通常假定算法是公开的，这要求加密算法本身非常强壮。

3. 一个密码系统实际安全的条件：

(1)每一个加密函数和每一个解密函数 都能有效地计算

(2)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

(3)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

4. 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：

(1)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

(2)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

(3)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

(4)存在数字签名困难问题

5. 公开密钥密码体制的优、缺点：

优点：

(1)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

(2)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

(3)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

6. 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

第五章　对称密码体制

1. 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

2. 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

3. 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

4. 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”

5. 密钥扩展：

[1]根据输入密钥得到 w[0]、w[1]、w[2]、w[3]，作为扩展密钥的基础
[2]扩展密钥：
(1)对 w 数组中下标不为 4 的倍数的元素：w[i]=w[i-1]⊕w[i-4](i 不为 4 的倍数)
[2]对 w 数组中下标为 4 的倍数的元素：
将一个字的四个字节循环左移一个字节，即[b0,b1,b2,b3] - > [b1,b2,b3,b0]
基于 S 盒对输入字中的每个字节进行 S 代替
将步骤 1 和步骤 2 的结果再与轮常量 Rcon[i]相异或

第 6 章　非对称密码体制

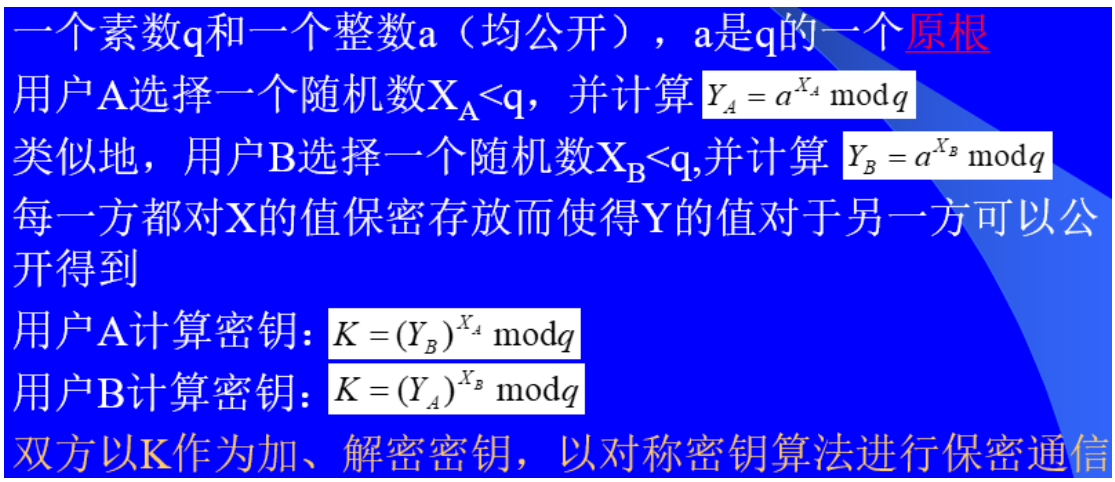
1. 公开密钥密码系统的分析方法：

强行攻击(对密钥)。
公开密钥算法本身可能被攻破。
可能报文攻击(对报文本身的强行攻击)。

2. 公钥密码系统的应用类型：

加密/解密
数字签名
密钥交换(混合密码体制)

3. Diffie-Hellman 密钥交换算法：



第 7 章　杂凑算法与消息认证

1. SHA-1 算法逻辑：

输入：最大长度为 264 位的消息；
输出：160 位消息摘要；
处理：输入以 512 位数据块为单位处理；

SHA-1　算法逻辑：

步骤 1：添加填充位。使数据位的长度　　448 mod 512
步骤 2：添加长度。一个 64 位块，表示原始消息长度
步骤 3：初始化 MD 缓冲区。160 位，表示为 5 个 32 位的寄存器
(A,B,C,D,E)。初始化为：
A = 67452301
B = EFCDAB89
C = 98BADCFE
D = 10325476
E = C3D2E1F0
big-endian format
步骤 4：以 512 位数据块为单位处理消息。四轮，每轮 20 步。四个基本逻辑函数：f1,f2,f3,f4.

步数	16进制
0<= t <=19	Kt=5A827999
20<=t<=39	Kt=6ED9EBA1
40<=t<=59	Kt=8F1BBCDC
60<=t<=79	Kt=CA62C1D6

步骤 5：输出。全部 L 个 512 位数据块处理完毕后，输出 160 位消息摘要。

2. 消息认证的目的：

(1)验证信息来源的真实性，即信源识别
(2)验证信息内容的完整性

3. 双向认证协议:

(1)最常用的协议
(2)该协议使得通信各方互相认证鉴别对方的身份，然后交换会话密钥
(3)认证的成功取决于：
声称者与它的密钥间绑定的证实
声称者基于随机数的数字签名的证实

第 8 章　数字签名

1. 数字签名的目的：

对数字对象的合法性、真实性进行标记
提供签名者的承诺

2. 数字签名应具有的性质：

签名是对文档的一种映射，签名与文档具有一一对应关系（**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**）

3. 数字签名的要求：

(1)接收者能够核实发送者对报文的签名
(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
(4)必须能够认证签名时刻的内容
(5)签名必须能够被第三方验证，以解决争议

4. 最基本的数字签名：

基于对称密钥密码算法：

本质是基于共享密钥的验证

签名算法－加密算法：$y = sig_k(m) = E_k(m)$

验证算法－解密算法：$ver(m, y) = true \Leftrightarrow m = D_k(y)$

或加密算法：$ver(m, y) = true \Leftrightarrow y = E_k(m)$

基于公钥密码算法：

本质上是公钥密码加密算法的逆应用

第 9 章　密钥管理

■ 重点：密钥、密钥管理等基本概念；密钥的生命周期；密钥的生成、安全存储和分发。 ■ 难点：密钥的协商与分发。
✓ 熟练掌握密钥、密钥管理等概念； ✓ 了解密钥管理的层次关系和生命周期； ✓ 掌握密钥的生成与安全存储的方法； ✓ 掌握密钥的协商与分发的实现方法。

1. 密钥的种类与层次结构：

会话密钥

- 在一次通信或数据交换中，直接用于向用户数据提供密码操作的密钥
- 短期会话密钥
- 长期会话密钥

一般密钥加密密钥

- 用于会话密钥或其下层密钥的加密，从而可实现这些密钥的在线分发

主密钥

- 位于整个密钥层次体系的最高层
- 可在较长时间内由用户所专用的秘密密钥
- 主要用于对密钥加密密钥或会话密钥的保护
- 主密钥的分发基于物理渠道或其他可靠的方法

2. 密钥管理的层次式结构：

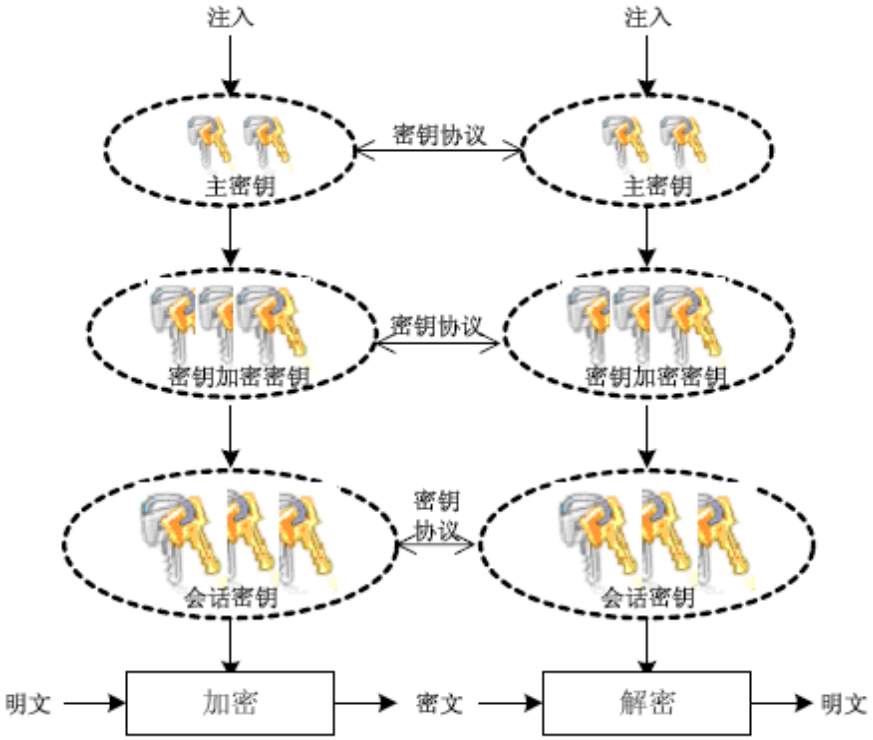


图9—1　密钥管理的层次结构

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

3. 密钥管理的生命周期：

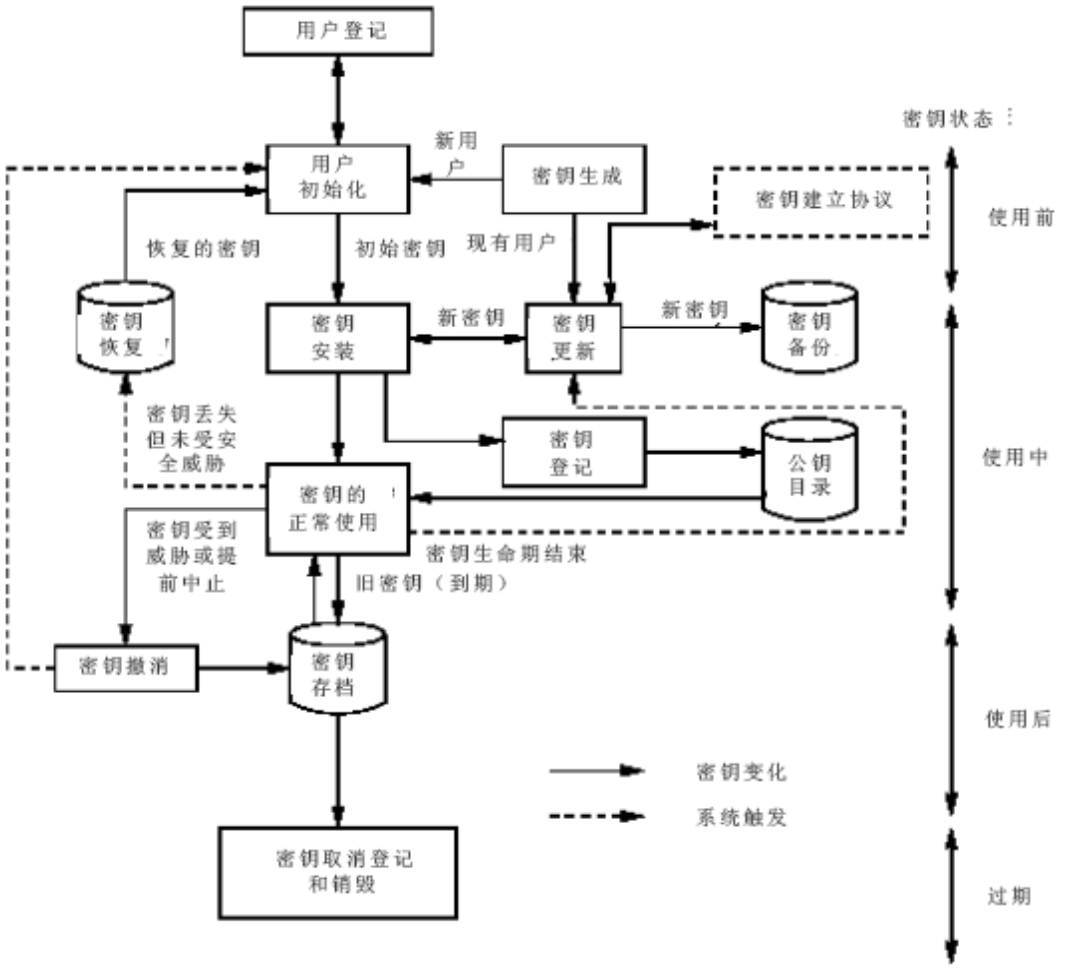


图9－2 密钥的生命周期

4. 密钥的生成与安全存储：

密钥的生成

密钥的大小与产生机制直接影响密码系统的安全

好的密钥应具有良好的随机性、避免弱密钥出现

生成过程：某种噪声源－＞有较好统计分布特性的序列－＞各种随机性检验：确保有较好的密码特性

一般，不同的密码体制有不同的具体密钥生成方法

密钥的安全存储

基于口令的软保护

基于硬件的物理保护

5. 密钥的协商与分发：

密钥的协商

是保密通信双方(或多方)通过公开信道的通信来共同形成秘密密钥的过程

密钥的分发

是保密通信中的一方生成并选择秘密密钥，然后把该密钥发送给通信参与的其他一

方或多方的机制

密钥分发协议

分类：网外分发、网内分发、秘密密钥的分发、公开密钥的分发

第 10 章　序列密码

重难点	■ 重点：序列密码模型、基于 LFSR 的序列密码。 ■ 难点：基于 LFSR 的序列密码体制。
学习要求	✓ 掌握序列密码、线性反馈移位寄存器的相关概念； ✓ 掌握基于 LFSR 的序列密码；

1. 序列密码模型：

序列密码又称为流密码。分为同步流密码和自同步流密码。

同步流密码特点：

同步要求

无错误传播

如果密钥流为无限随机序列，则成为一次一密

自同步流密码特点：

自同步

有限的错误传播

2. 流密码和分组密码：

流密码的优点：

转换速度快

低错误传播

流密码的缺点：

低扩散

有意插入及修改的不敏感性

分组密码的优点：

扩散性

插入的敏感性

分组密码的缺点：

加密速度慢

错误传播

3. 线性反馈移位寄存器：

（1）LFSR 非常适合硬件实现

（2）能产生大的周期流

（3）能产生好的统计特性的流

（4）其结构能够应用代数方法进行很好的分析

4. 基于 LFSR 的流密码：

基于LFSR的流密码生成器

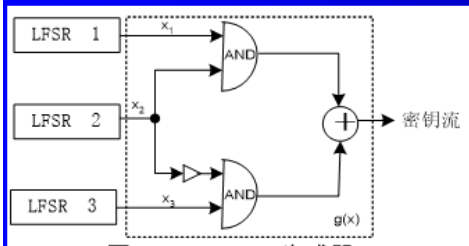


图10—8 Geffe生成器

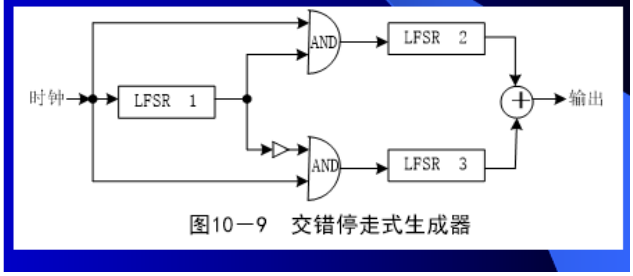


图10—9 交错停走式生成器