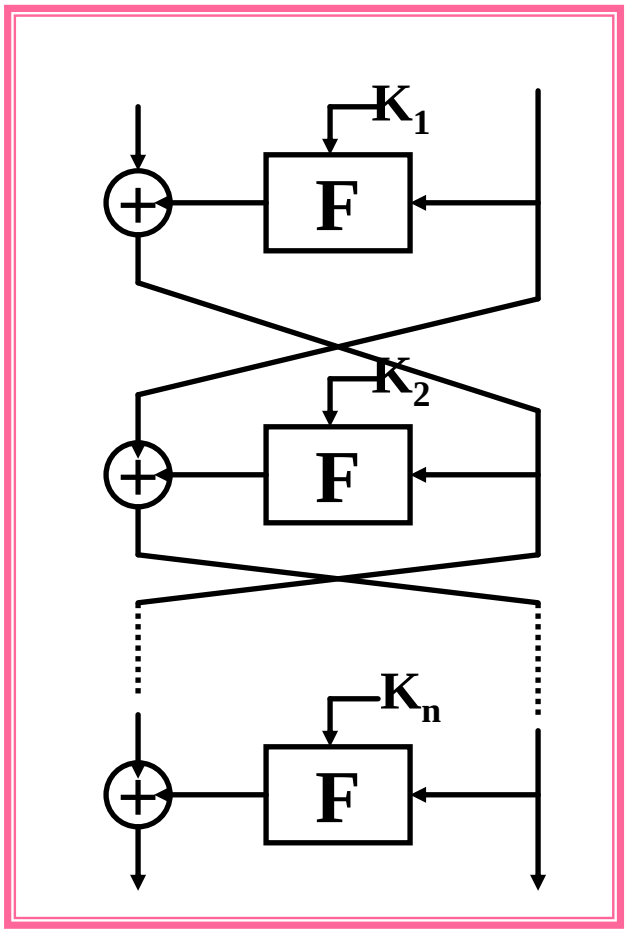
§3.2 分组密码概述

Feistel结构原理



加密：$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$

§3.2 分组密码概述

分组密码，也称为块密码，它是将明文消息经编码表示后的数字序列划分为若干固定长度的组，每组分别在密钥的控制下转换成等长度的密文分组输出。

分组密码易于构造拟随机数生成器、流密码、消息认证码和杂凑函数等，还可进而成为消息认证技术、数据完整性机构、实体认证协议以及单钥数字签名体制的核心组成部分。

§3.2 分组密码概述

置换：设S为一有限集合，ϕ 为S到S的一一映射，则ϕ 为S上的一个置换。

混淆：将作用于明文的密钥和密文之间的关系复杂化，使明文和密文之间、密文和密钥之间的统计相关性极小化，从而使统计分析攻击法不能奏效。

扩散：将每一位明文及密钥数字的影响尽可能迅速地散布到较多个输出的密文数字，以便隐蔽明文数字的统计特性。