



哈尔滨工业大学
HARBIN INSTITUTE OF TECHNOLOGY

立足航天，服务国防，面向国民经济主战场



计算机网络之危机四伏

主讲人：李全龙

本讲主题

密码学基础（3）



现代加密技术

- ❖ 现代加密技术的基本操作包括经典的替代和置换
 - 不再针对一个个字母，而是针对二进制位操作
- ❖ 现代加密技术主要分为：
 - 对称密钥加密
 - 非对称密钥加密（公开密钥加密）
- ❖ 对称密钥加密：
 - 流密码（stream ciphers）
 - 分组密码，也称块密码（block ciphers）



流密码

❖ 基本思想:

- 首先利用密钥 K 产生一个密钥流: $z=z_0 z_1 z_2 \dots$
- 然后使用如下规则对明文串 $x=x_0x_1x_2\dots$ 加密:

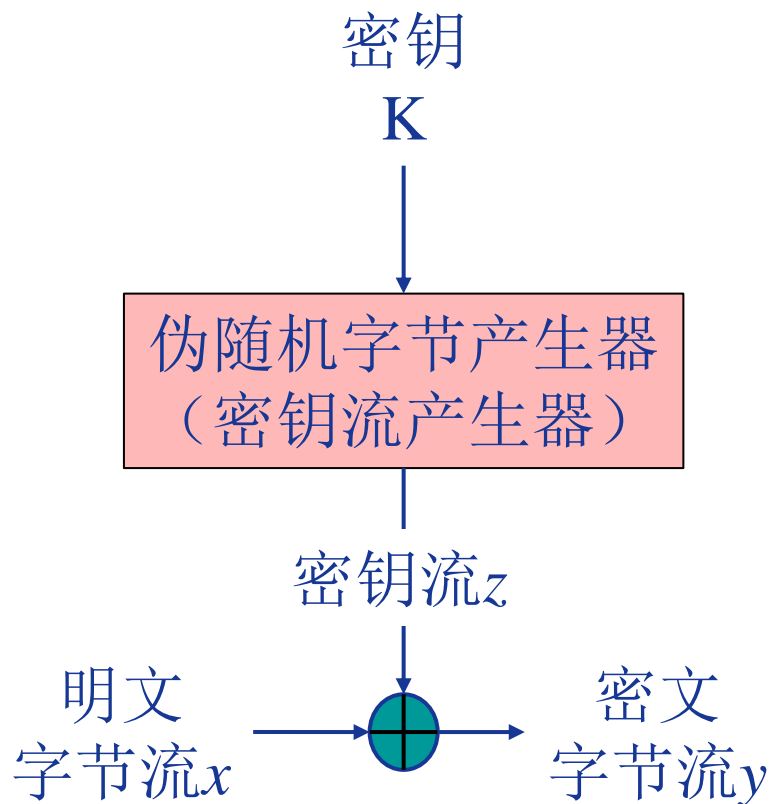
$$y=y_0y_1y_2\dots=E_{z_0}(x_0)E_{z_1}(x_1)E_{z_2}(x_2)\dots$$

❖ 解密时, 使用相同的密钥流与密文做运算 (XOR)

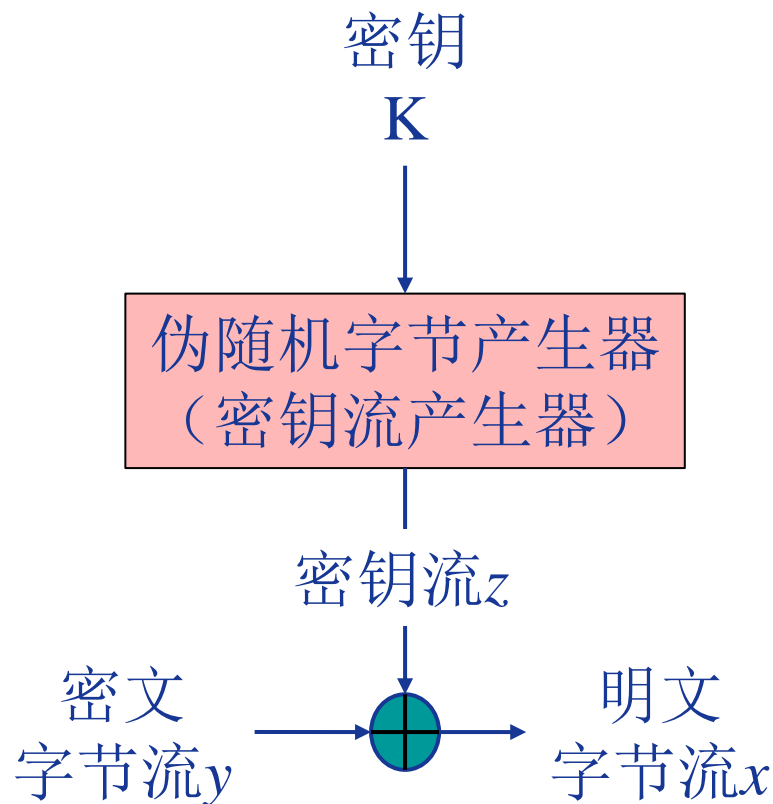


流密码工作流程

加密过程:



解密过程:



分组密码

- ❖ 将明文序列划分成长为 m 的明文组
- ❖ 各明文组在长为 i 的密钥组的控制下变换成长度为 n 的密文组
- ❖ 通常取 $n=m$
 - $n>m$ 扩展分组密码
 - $n<m$ 压缩分组密码
- ❖ 典型分组密码结构：Feistel分组密码结构
 - 在设计密码体制的过程中，Shannon提出了能够破坏对密码系统进行各种统计分析攻击的两个基本操作：扩散(diffusion)和混淆(confusion)
 - 基于1949年Shannon提出的交替使用替代和置换方式构造密码体制



Feistel分组密码结构

❖ 基于“扩散”和“混乱”的思考，Feistel提出通过替代和置换交替操作方式构造密码

❖ Feistel是一种设计原则，并非一个特殊的密码

❖ 加密：

- 将明文分成左、右两部分：

明文 = (L_0, R_0)

- 每一轮 $i=1, 2, \dots, n$ 计算：

$L_i = R_{i-1}$

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

其中 F 是轮函数； K_i 是子密钥

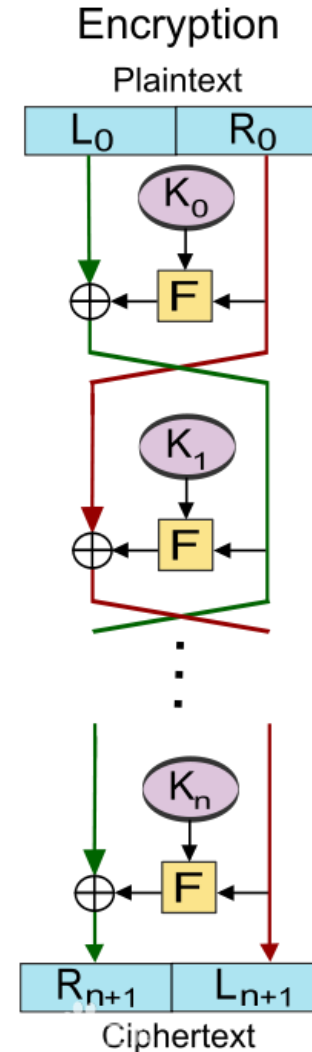
- 密文 = (L_n, R_n)



Feistel分组密码结构

❖ 解密:

- 密文 = (L_n, R_n)
- 每一轮 $i=n, n-1, \dots, 1$ 计算:
 $R_{i-1} = L_i$
 $L_{i-1} = R_i \oplus F(R_{i-1}, K_i)$
其中 F 是轮函数; K_i 是子密钥
- 密文 = (L_0, R_0)



Feistel分组密码结构

Feistel结构的分组密码安全性取决于：

❖ 分组长度

- 分组长度越**大**，安全性越**高**，加密速度越**慢**，效率越**低**
- 目前常用的分组加密算法的分组长度取**64位**

❖ 子密钥的大小

- 子密钥长度**增加**，安全性**提高**，加密速度**降低**
- 设计分组密码时需要在安全性和加密效率之间进行**平衡**

❖ 循环次数

- 循环越**多**，安全性越**高**，加密效率越**低**

❖ 子密钥产生算法

- 在初始密钥给定的情况下，产生子密钥的算法越**复杂**，安全性越**高**

❖ 轮函数

- 一般情况下，轮函数越**复杂**，加密算法的安全性越**高**





哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY



立足航天，服务国防，面向国民经济主战场

谢谢!