现代密码学

第十七讲 分组密码的基本概念

信息与软件工程学院

第十七讲 分组密码的基本概念

- ✓ 分组密码概述
- 分组密码的设计原则

分组密码概述

- 分组密码是许多系统安全的一个重要组成部分。可用于构造
  - 伪随机数生成器
  - 流密码
  - 消息认证码(MAC)和杂凑函数
  - 消息认证技术、数据完整性机制、实体认证协议以及单钥数字签字体制的核心组成部分。

应用中对于分组码的要求

- 安全性
- 运行速度
- 存储量(程序的长度、数据分组长度、高速缓存大小)
- 实现平台(硬、软件、芯片)
- 运行模式

尽可能快，但要满足安全性。

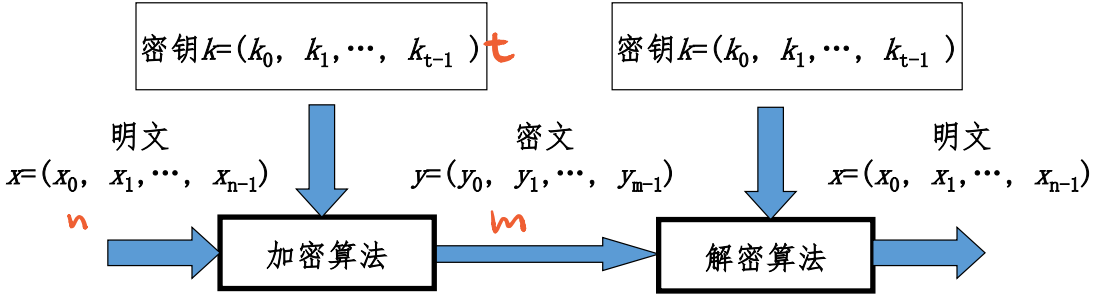
分组密码概述

明文序列 $x_0, x_1, \ldots, x_{n-1}, \ldots$，分组长度为n

加密函数 E: $V_n \times K \rightarrow V_m$ 明文空间与密钥相结合产生密文空间.

密文分组长度为m

这种密码实质上是字长为n的数字序列的代换密码。

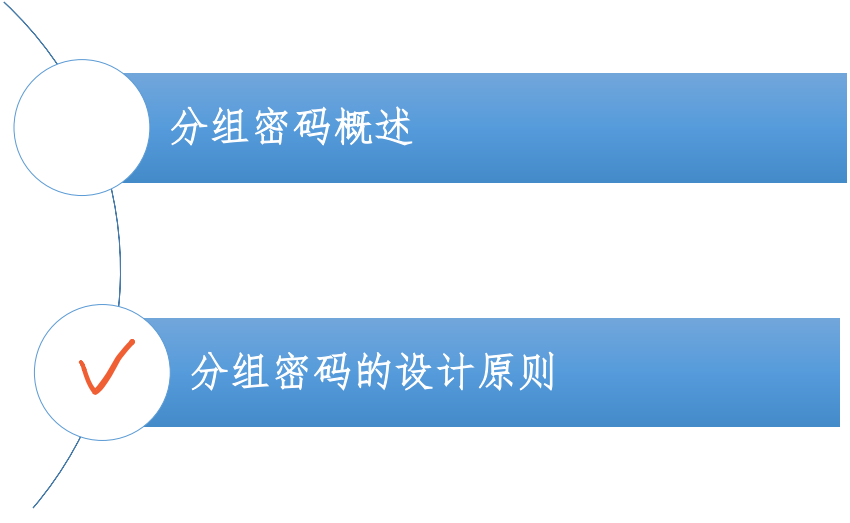


分组密码概述

- 通常取$n=m$。
- 若$n<m$，则为有数据扩展的分组密码。
- 若$n>m$，则为有数据压缩的分组密码。

> 实际中可不考

第十七讲 分组密码的基本概念



分组密码设计问题

分组密码的设计问题在于找到一种算法，能在密钥控制下从一个足够大且足够好的置换子集中，简单而迅速地选出一个置换，用来对当前输入的明文的数字组进行加密变换。

安全性设计原则

密求满足2T原则

香农提出

- **1. 混淆原则(Confusion)**

- 混淆原则就是将密文、明文、密钥三者之间的统计关系和代数关系变得尽可能复杂，使得敌手即使获得了密文和明文，也无法求出密钥的任何信息；即使获得了密文和明文的统计规律，也无法求出明文的新的信息。

- 可进一步理解为：

- （1）明文不能由已知的明文，密文及少许密钥比特代数地或统计地表示出来。

- （2）密钥不能由已知的明文，密文及少许密钥比特代数地或统计地表示出来。

安全性设计原则

- **2. 扩散原则(Diffusion)**
- 扩散原则就是应将明文的统计规律和结构规律散射到相当长的一段统计中去(Shannon的原话)。
- 也就是说让明文中的每一位影响密文中的尽可能多的位，或者说让密文中的每一位都受到明文中的尽可能多位的影响。
- 如果当明文变化一个比特时,密文有某些比特不可能发生变化,则这个明文就与那些密文无关,因而在攻击这个明文比比特时就可不利用那些密文比特.

密钥也该加入：密钥每一位影响密文尽可能多位

分组密码算法应满足的要求

1. 分组长度n要足够大：

防止明文穷举攻击法奏效。

2. 密钥量要足够大：

尽可能消除弱密钥并使所有密钥同等地好，以防止密钥穷举攻击奏效。

3. 由密钥确定置换的算法要足够复杂：

充分实现明文与密钥的扩散和混淆，没有简单的关系可循，要能抗击各种已知的攻击。

分组密码算法应满足的要求

4. 加密和解密运算简单：

易于软件和硬件高速实现。

5. 数据扩展：

一般无数据扩展，在采用同态置换和随机化加密技术时可引入数据扩展。

6. 差错传播尽可能地小。

一个密文分组的错误尽可能少的影响其他密文分组的解密

分组密码的实现原则

- 软件实现的原则：
  - 使用子块和简单的运算。如将分组n化分为子段，每段长为8、16或32。在以软件实现时，应选用简单的运算，使作用于子段上的密码运算易于以标准处理器的基本运算，如加、乘、移位等实现，避免用以软件难于实现的逐比特置换。
- 硬件实现的原则：
  - 加密解密可用同样的器件来实现。

感 谢 聆 听!

xynie@uestc.edu.cn