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

计算机网络之危机四伏

主讲人：李全龙

本讲主题

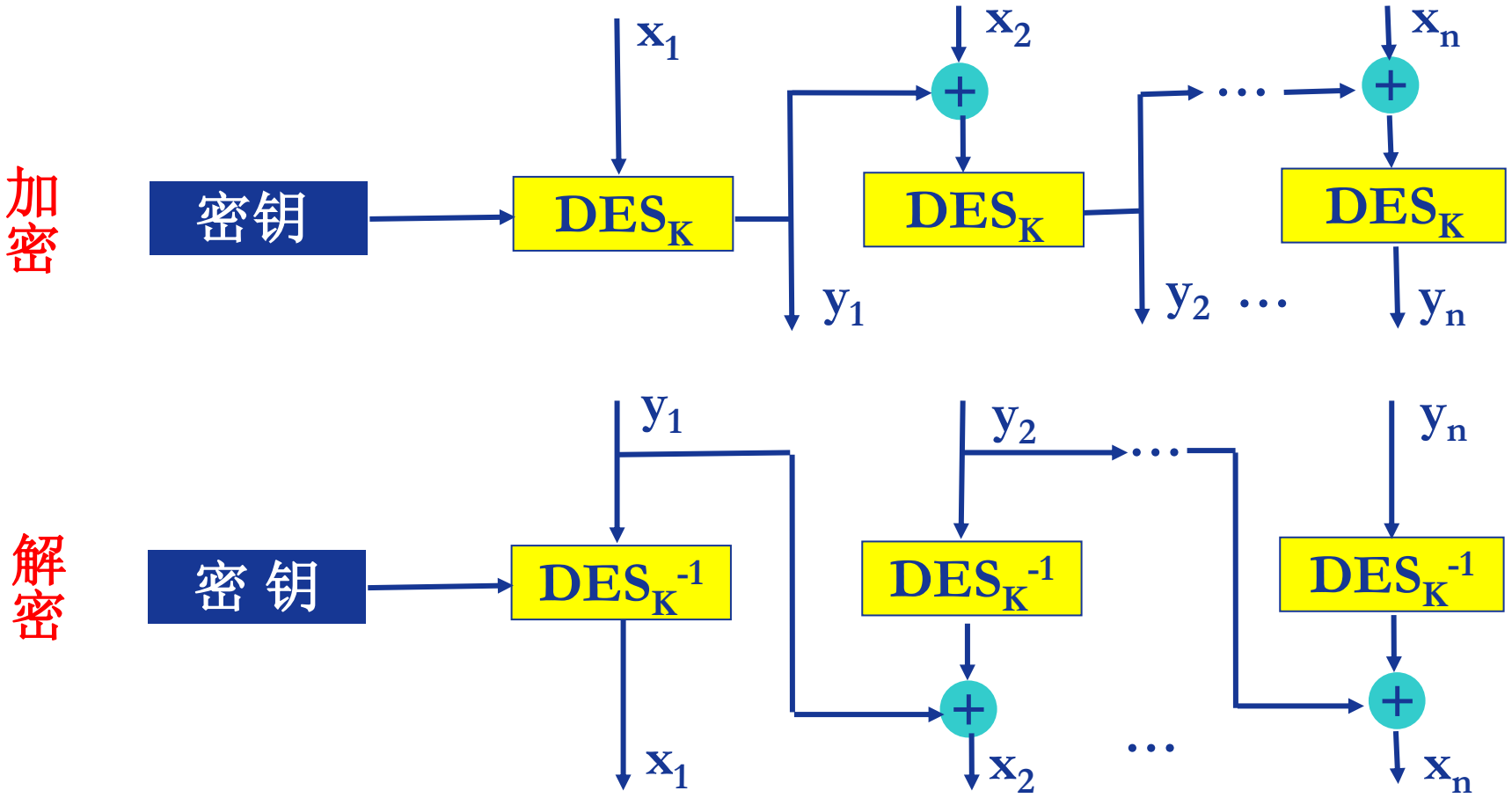
密码学基础（6）

DES的安全性

- DES的56位密钥可能太小
  - 1998年7月，EFE（电子前哨基金会）宣布攻破了DES算法，他们使用的是不到25万美元的特殊的“DES破译机”，这种攻击只需要不到3天的时间。
- DES的迭代次数可能太少
  - 16次恰巧能抵抗差分分析
- S盒（即替代函数S）中可能有不安全因素
- DES的一些关键部分不应当保密
- DES存在弱密钥和半弱密钥
- 针对DES的攻击方法：
  - 差分分析方法（Difference Analysis Method）
  - 线性分析方法（Linear Analysis Method）
  - 旁路攻击法（Side-Channel Attack）

DES的改进

- 密码分组链接（CBC-cipher block chaining）
  - 加密算法的输入是当前明文分组和前一次密文分组的异或
  - 重复的明文分组不会在密文中暴露出重复关系



DES的改进

- DES密钥过短（56bits）→多重DES
- 3DES使用3个密钥，执行3次DES算法，加密过程：
  - 加密-解密-加密（EDE），即：

$$C=E_{K3}(D_{K2}(E_{K1}(M)))$$

- 为了避免3DES使用3个密钥进行三阶段加密带来的密钥过长的缺点（168bit），Tuchman提出使用两个密钥的三重加密方法，这个方法只要求112bit密钥，即令其$K_1=K_3$：

$$C=E_{K1}(D_{K2}(E_{K1}(M)))$$

- 3DES的第二阶段的解密并没有密码编码学上的意义，唯一优点是可以使用3DES解密原来的单次DES加密的数据，即$K_1=K_2=K_3$

$$C=E_{K1}(D_{K1}(E_{K1}(M)))=E_{K1}(M)$$

高级加密标准AES

- AES: Advanced Encryption Standard
- NIST（美国国家标准技术研究所）对称密钥加密标准, 取代DES(2001年12月)
- 1997年NIST宣布征集AES算法，要求:
  - 可公开加密方法
  - 分组加密，分组长度为128位
  - 至少像3DES一样安全
  - 更加高效、快
  - 可提供128/192/256位密钥
- 比利时学者Joan Daemen和Vincent Rijmen提出的Rijndael加密算法最终被选为AES算法。
- NIST在2001年12月正式颁布了基于Rijndael算法AES标准

Rijndael加密算法简介

- 不属于Feistel结构
- 加密、解密相似但不完全对称
- 支持128/192/256数据块大小
- 支持128/192/256密钥长度
- 有较好的数学理论作为基础
- 结构简单、速度快
- Rijndael算法特点：
  - 分组长度和密钥长度均可变（128/192/256bits）
  - 循环次数允许在一定范围内根据安全要求进行修正
  - 汇聚了安全、效率、易用、灵活等优点
  - 抗线性攻击和抗差分攻击的能力大大增强
  - 如果1秒暴力破解DES，则需要149万亿年破解AES

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！