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

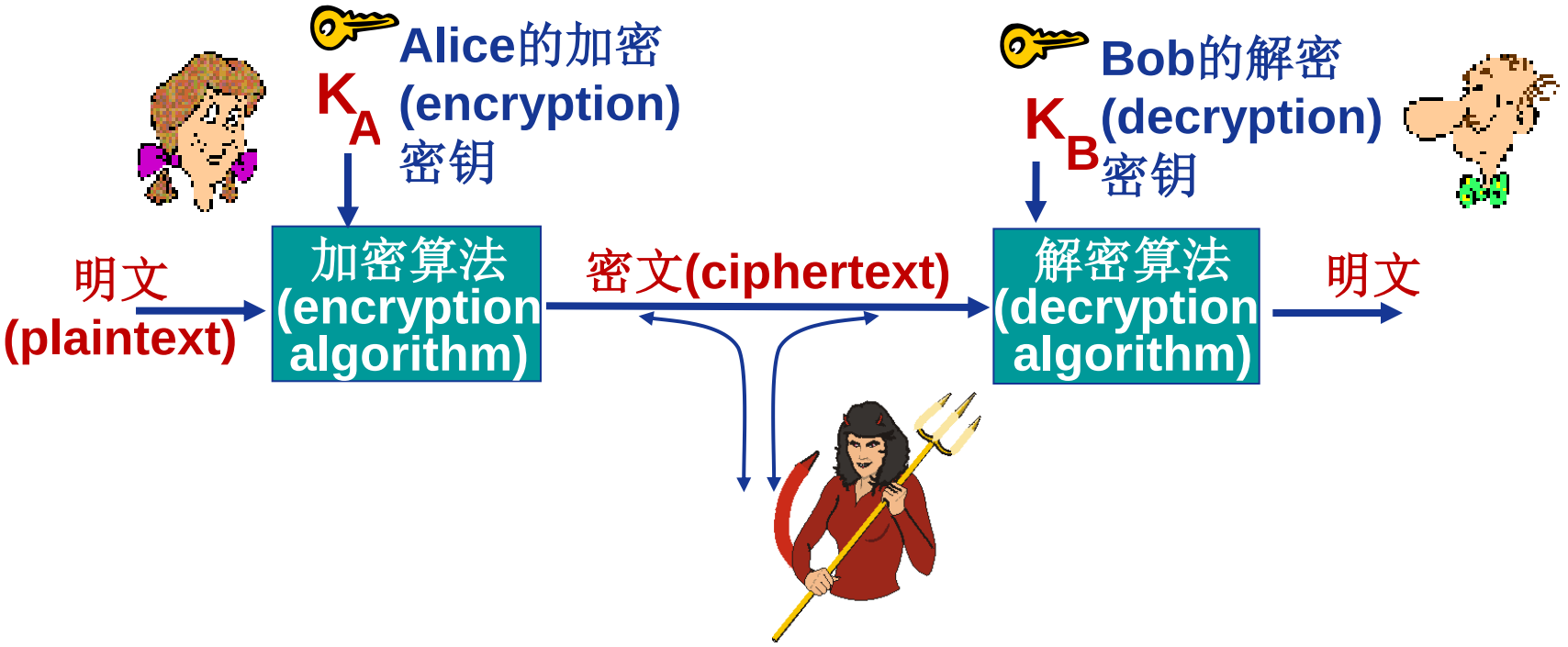
计算机网络之危机四伏

主讲人：李全龙

本讲主题

密码学基础（1）

密码学(cryptography)术语

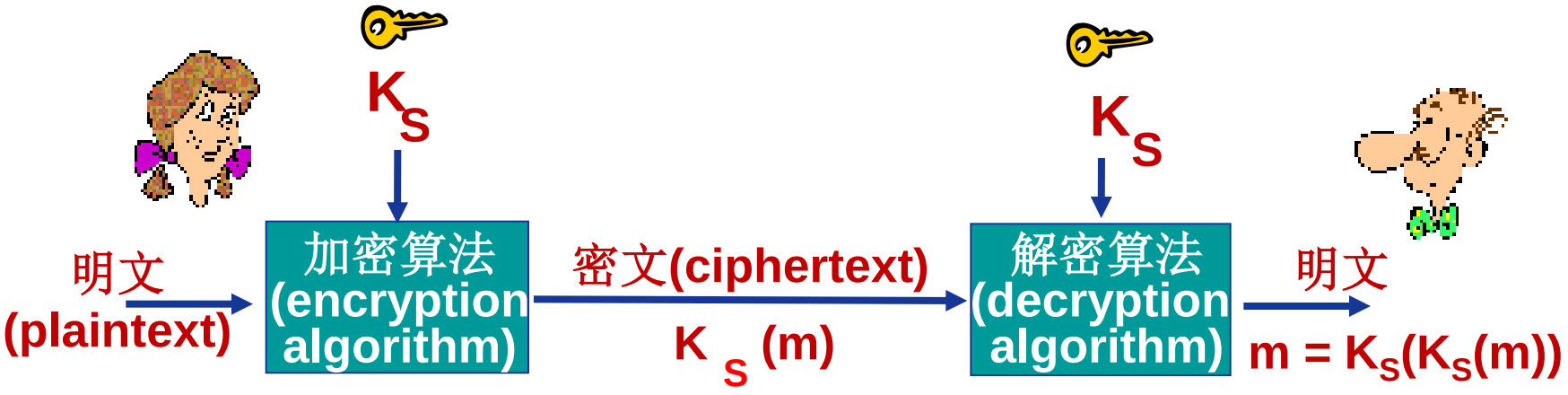


m：明文

$K_A(m)$：密文，利用秘钥K_A加密

$m = K_B(K_A(m))$：利用秘钥K_B解密

对称密钥加密

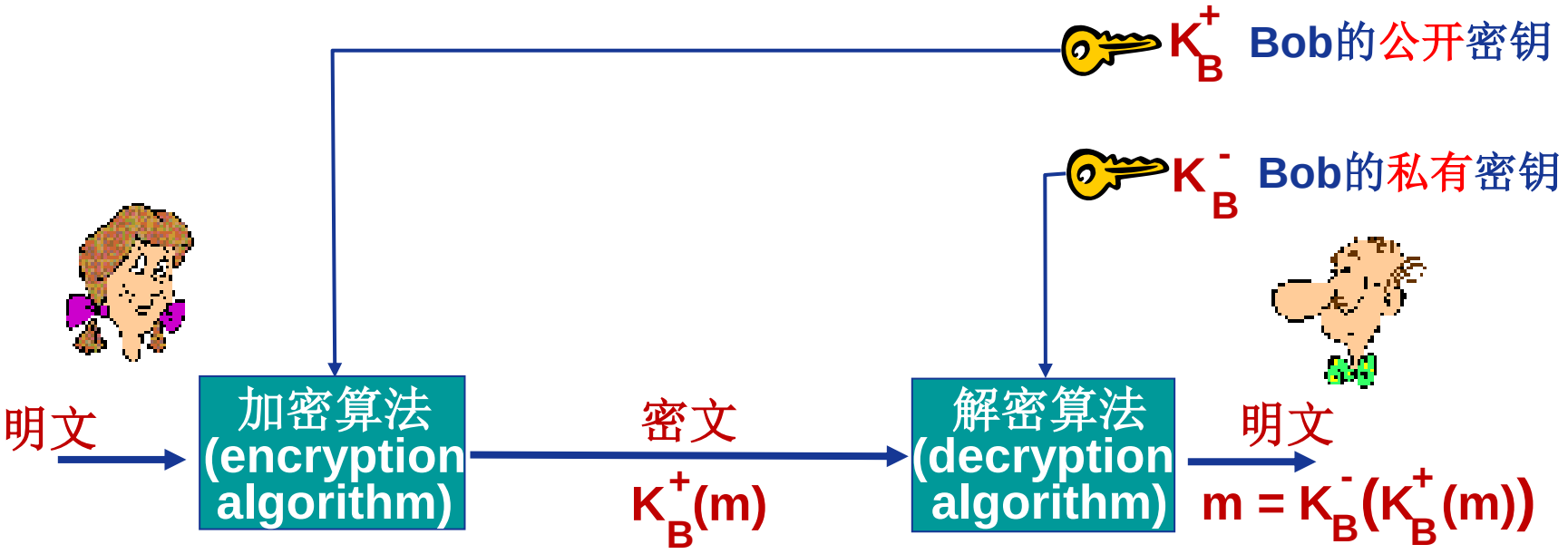


对称密钥加密: Bob和Alice共享相同(对称)密钥: K_S

- e.g., 单码替代密码的替代模式

Q: Bob和Alice如何确认密钥值（密钥分发）？

公开密钥加密


K_B^+ Bob的公开密钥
K_B^- Bob的私有密钥
明文
加密算法 (encryption algorithm)
密文
$K_B^+(m)$
解密算法 (decryption algorithm)
明文
$m = K_B^-(K_B^+(m))$

破解加密方法

- 唯密文攻击(cipher-text only attack): 入侵者(如Trudy)只截获到密文，基于对密文的分析进行破解
- 两条途径:
  - 暴力破解(brute force): 尝试所有可能的密钥
  - 统计分析
- 已知明文攻击(known-plaintext attack): 入侵者已知(部分)明文以及与之匹配的密文
  - e.g., 在单码替代密码(monoalphabetic cipher)中，入侵者已确认字母a,l,i,c,e,b,o的替换关系
- 选择明文攻击(chosen-plaintext attack): 入侵者可以获取针对选择的明文的密文

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！