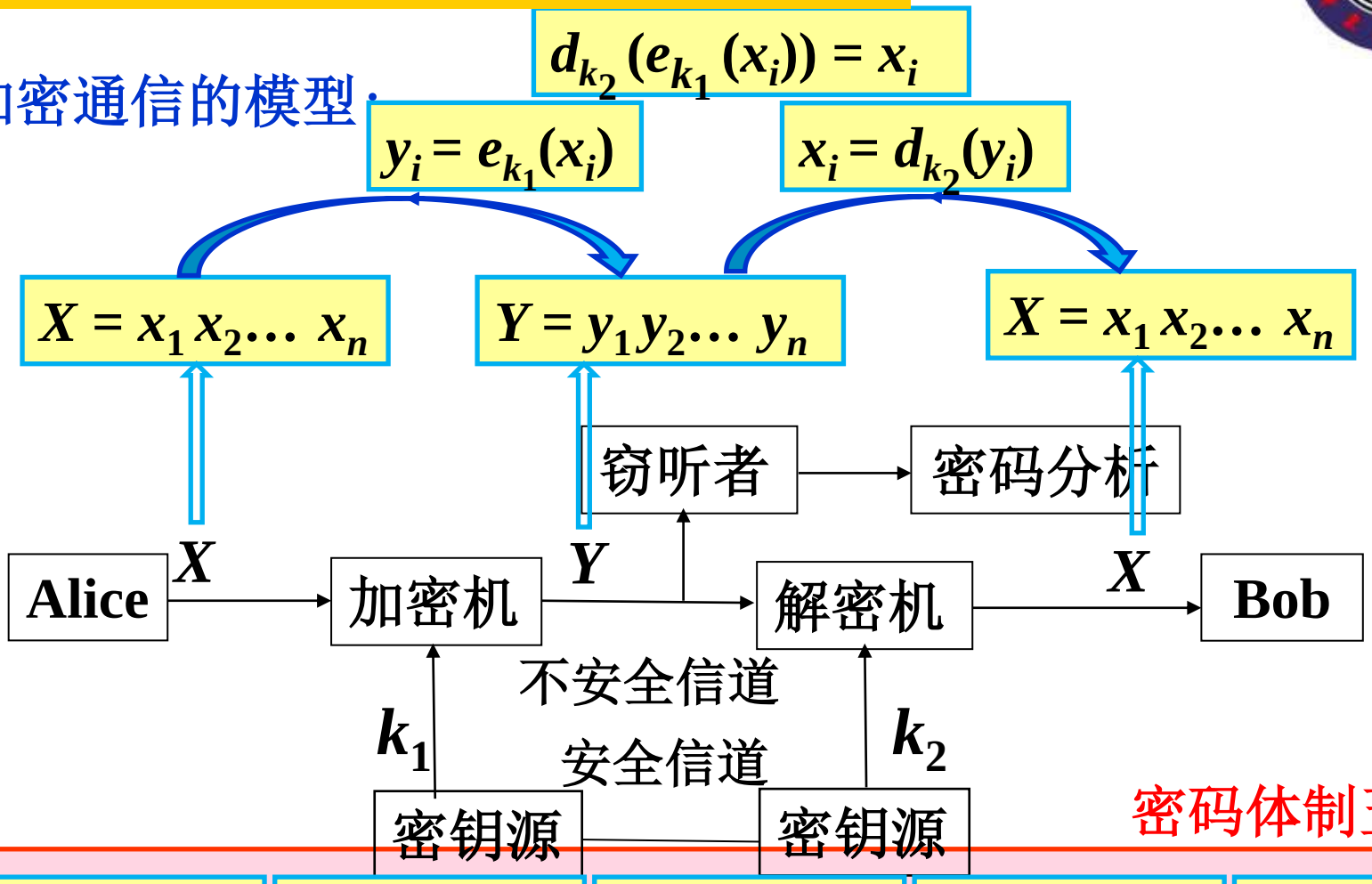
§2.1 密码学基本概念

加密通信的模型：



密码体制五元组

明文空间P	密文空间C	密钥空间K	加密算法E	解密算法D

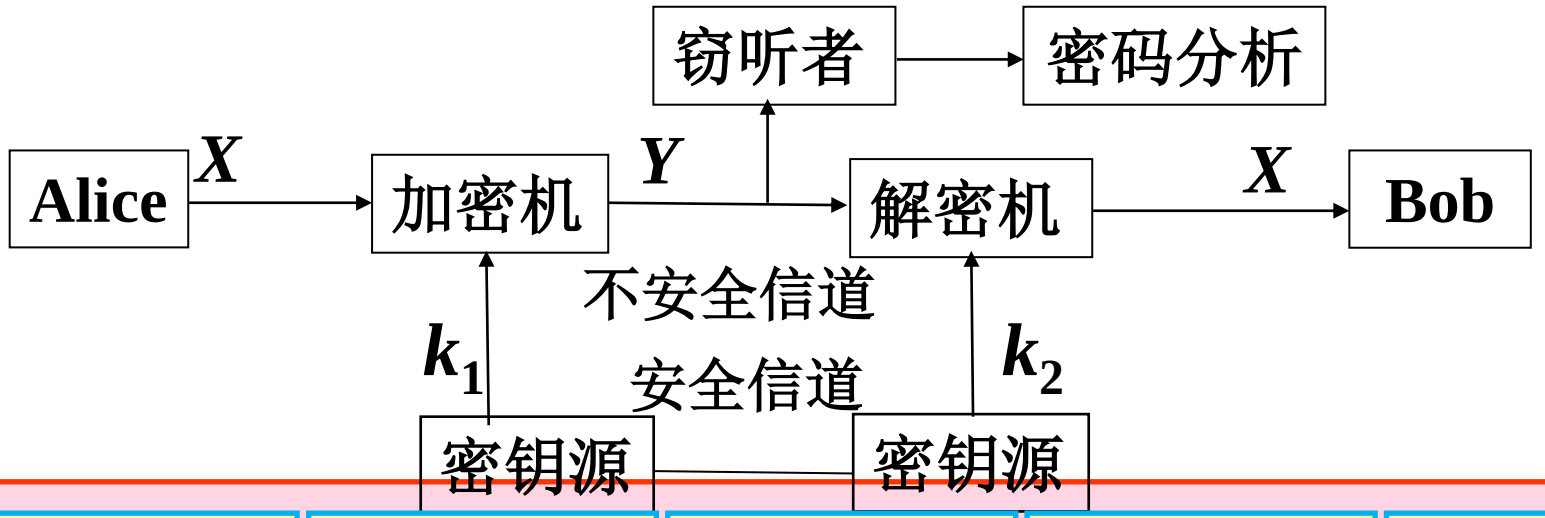
§2.1 密码学基本概念

加密通信的模型：

当$k_1=k_2$时，称为对称密码体制。

当$k_1\neq k_2$时，称为非对称密码体制。

唯密钥而保密



明文空间P | 密文空间C | 密钥空间K | 加密算法E | 解密算法D

§2.1 密码学基本概念

使消息保密的技术和科学叫做密码编码学(Cryptography)，从事此行的叫密码编码者（Cryptographer），密码分析者是从事密码分析的专业人员，密码分析学（Cryptanalysis）就是破译密文的科学和技术，即揭穿伪装。

密码学（Cryptology）作为数学的一个分支，包括密码编码学和密码分析学两部分，密码编码技术和密码分析技术是相互依存、相互支持、密不可分的两个方面。

§2.1 密码学基本概念

密码学除了提供机密性外，还有以下作用：

1、鉴别：消息的接收者能够确认消息的来源，入侵者不可能伪装成他人。

2、完整性：消息的接收者能够验证在传送过程中消息没有被修改，入侵者不可能用假消息代替合法消息。

3、抗抵赖：发送者事后不可能虚假地否认他发送的消息。

密码算法（Algorithm）也叫密码（Cipher），是用于加密和解密的数学函数。通常情况下，有两个相关的函数，一个用作加密，另一个用作解密。

密钥用K表示。K可以是很多数值里的任意值。密钥 K的可能值的范围叫做密钥空间。加密和解密运算都用它。

§2.1 密码学基本概念

密码体制在原理上分两类：对称密码（单钥）体制和非对称密码（公钥）体制。

对称密码体制中，收发双方使用同一密钥，系统的保密性主要取决于密钥的安全性。系统的密钥管理、传输和分配是重要且十分复杂的问题。密码算法按照对明文的处理方式分为：分组密码算法和序列密码算法。体制的缺点：密钥数目大，密钥分配困难，无法实现不可否认服务。

非对称密码体制中，加密密钥K_e是公开的，解密密钥K_d必须保密。密钥产生、分配和管理相对简单，尤适用于计算机网络系统中。特点：实现信息公开加密，实现不可否认服务。体制的缺点：加解密运算复杂其速度较慢。