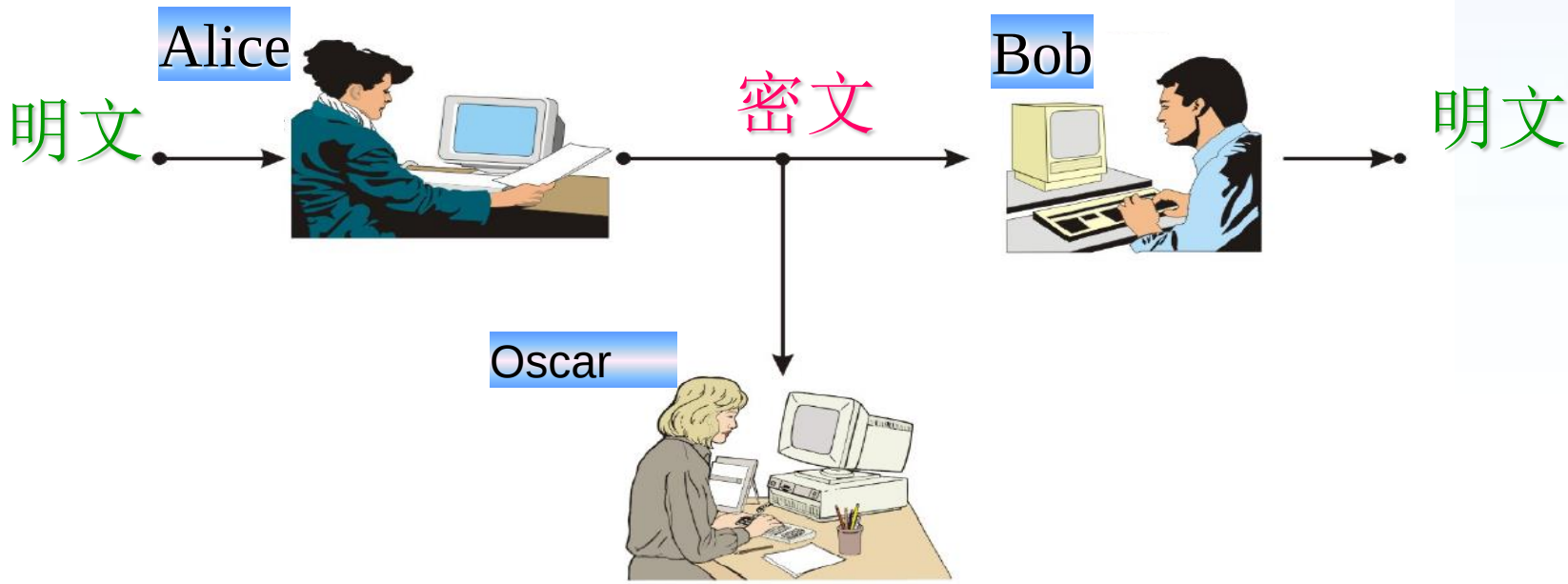
西安郵電大學
XI'AN UNIVERSITY OF POSTS & TELECOMMUNICATIONS

4、密码体制

主讲人：任方
网络空间安全学院

密码体制——目的

- 密码学的基本目的是面对攻击者Oscar，在被称为Alice和Bob的通信双方之间应用不安全的信道进行通信时，保证通信安全。



密码体制—定义

- 密码体制的定义

定义　密码体制：密码体制的构成包括以下要素：

（1）M：明文消息空间，表示所有可能的明文组成的有限集。

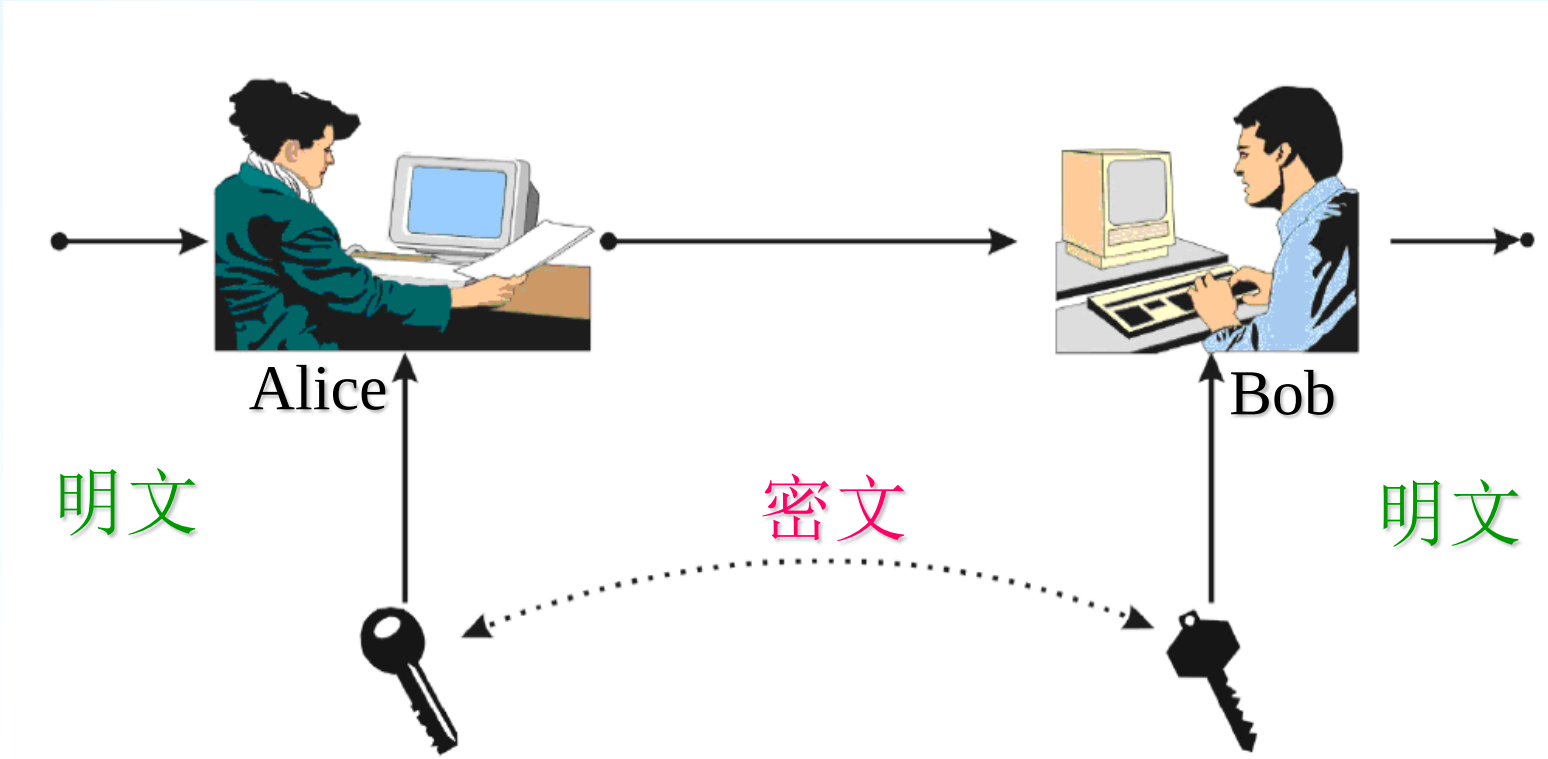
（2）C：密文消息空间，表示所有可能的密文组成的有限集。

（3）K：密钥空间，表示所有可能的密钥组成的有限集。

（4）E：加密算法集合。

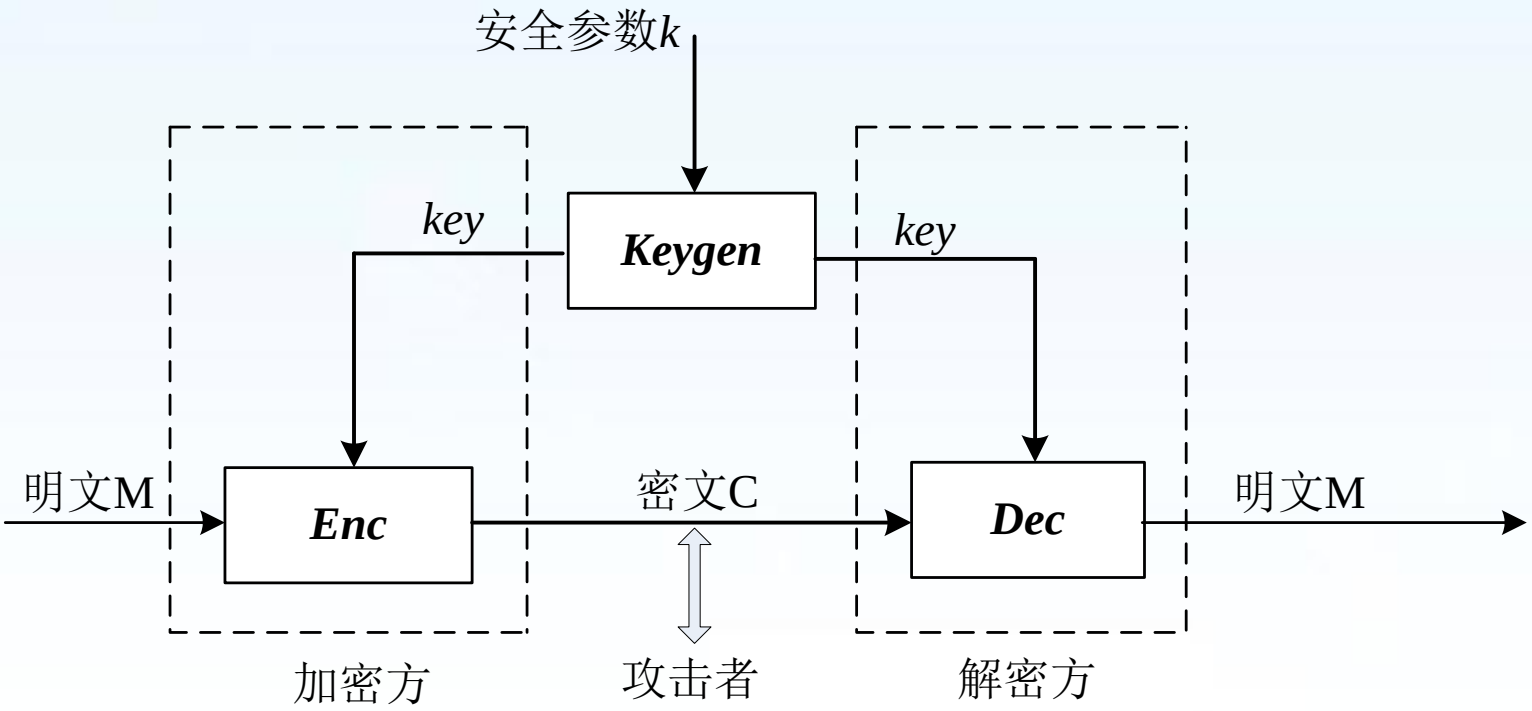
（5）D：解密算法集合。

密码体制—保密通信机制



保密通信的一般机制

密码体制—完整框图



密码体制—分类

- 密码体制的分类

对称密钥密码系统 加密密钥=解密密钥

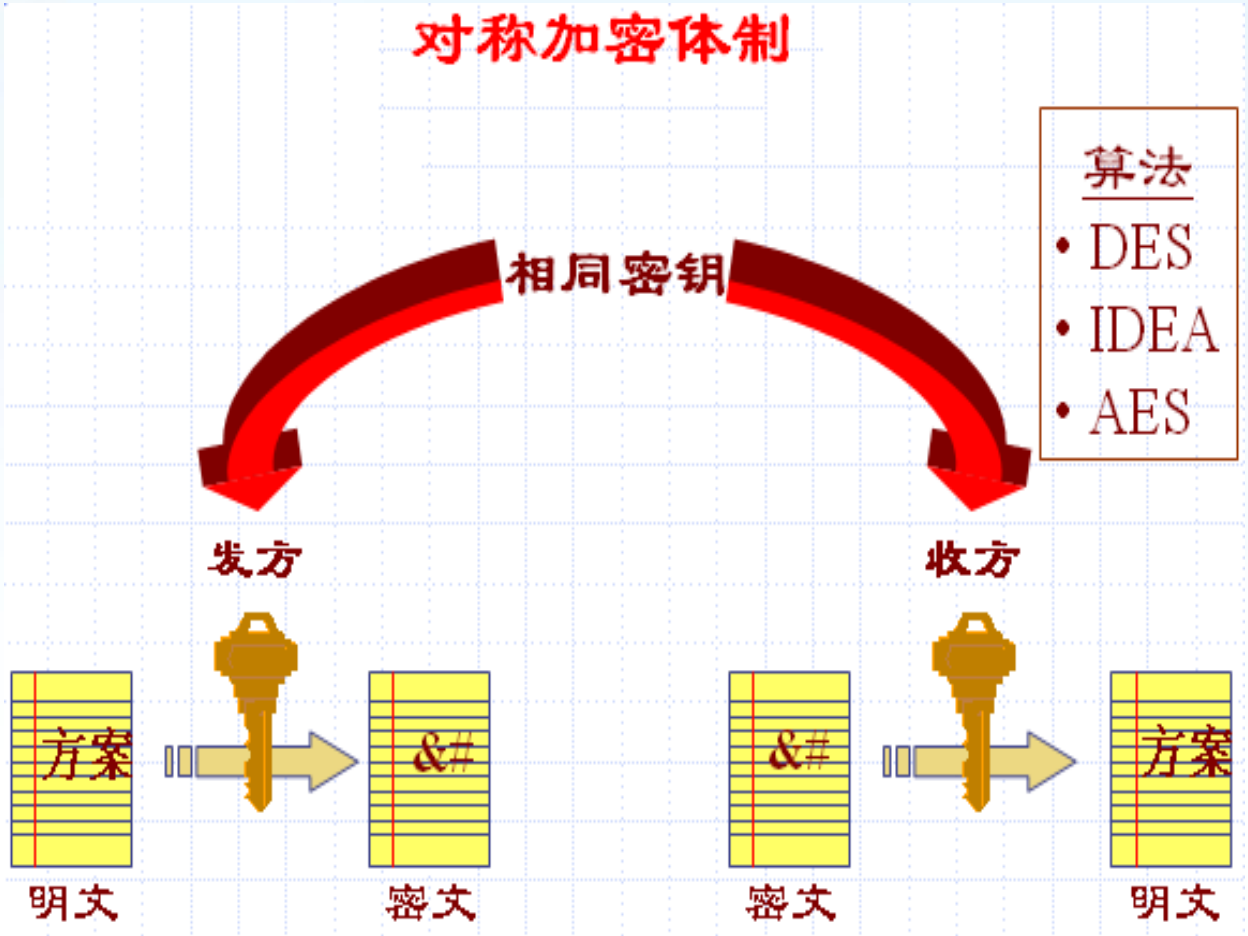
Symmetric Key Cryptosystem 密钥是保密的

非对称密钥密码系统 加密密钥≠解密密钥

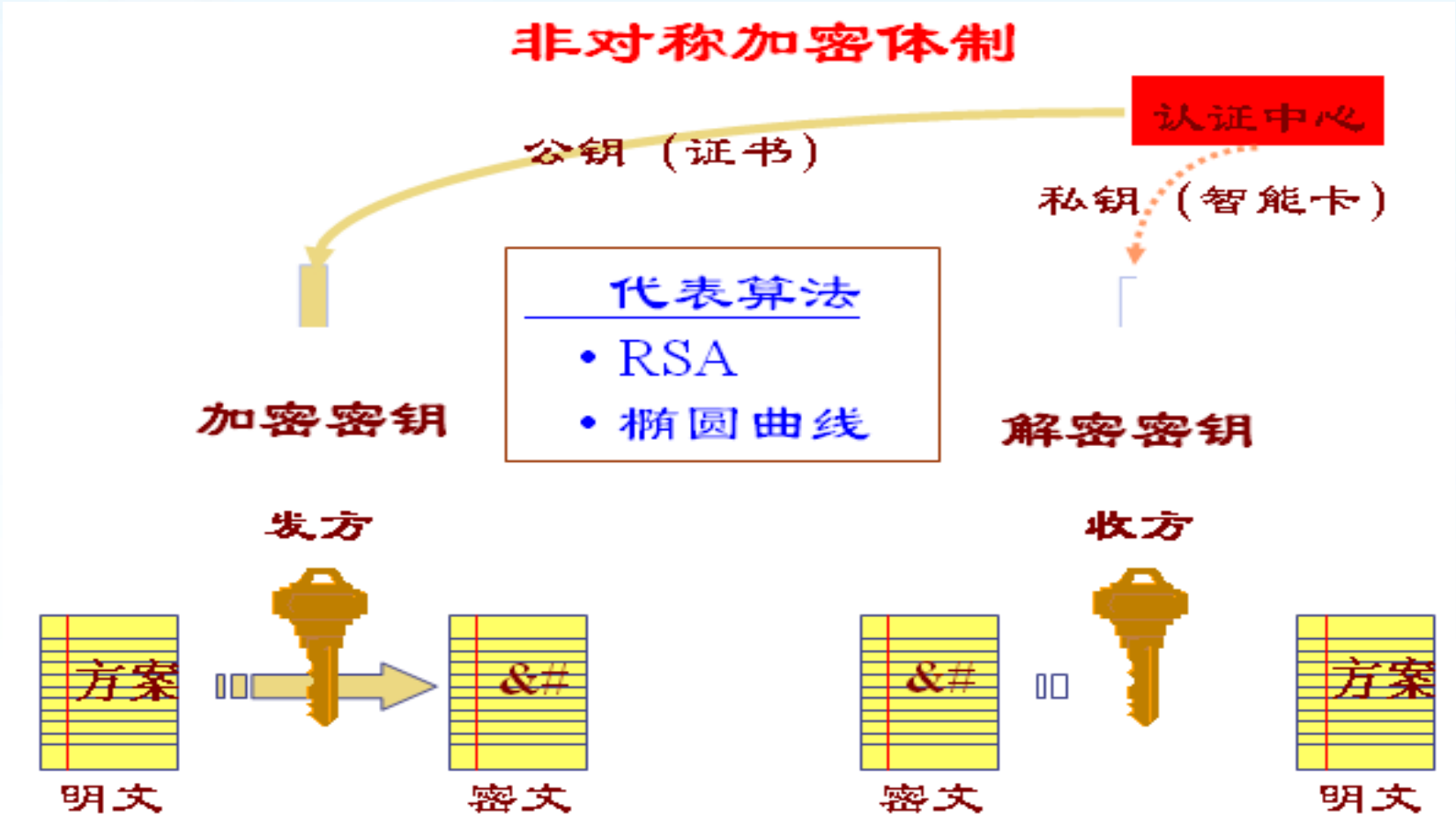
Asymmetric Key Cryptosystem

- 加密密钥为公钥（Public Key）
- 解密密钥为私钥（Private Key）

密码体制—分类



密码体制—分类



密码体制—攻击者

根据密码分析的Kerckhoffs原则：攻击者知道所用的加密算法的内部机理，不知道的仅仅是加密算法所采用的加密密钥

常用的密码分析攻击分为以下四类：

1.惟密文攻击(Ciphertext only attack)

2.已知明文攻击(Know plaintext attack)

3.选择明文攻击(Chosen plaintext attack)

4.选择密文攻击（Chosen ciphertext attack）

• 衡量密码体制安全性的基本准则：

•计算安全的（Computational security）

如果破译加密算法所需要的计算能力和计算时间是现实条件所不具备的，那么就认为相应的密码体制是满足计算安全性的。这意味着强力破解证明是安全的。

•可证明安全的（Provable security）

如果对一个密码体制的破译依赖于对某一个经过深入研究的数学难题的解决，就认为相应的密码体制是满足可证明安全性的。这意味着理论保证是安全的。

•无条件安全的（Unconditional security）

如果假设攻击者在用于无限计算能力和计算时间的前提下，也无法破译加密算法，就认为相应的密码体制是无条件安全性的。这意味着在极限状态上是安全的。

本节到此结束，谢谢！