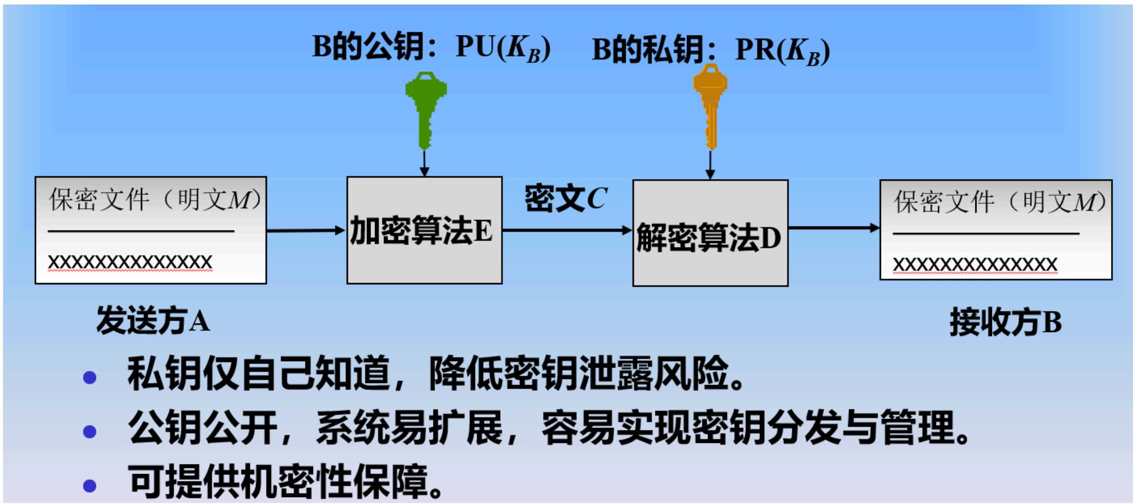
# 公钥密码

## 对称密码存在的限制

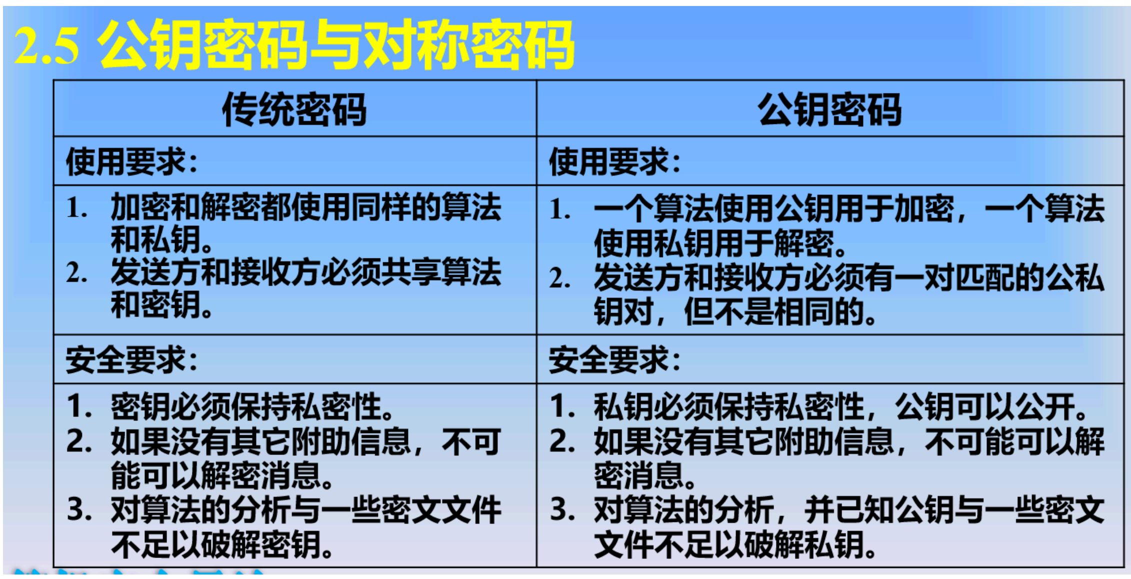
- 发送方和接收方共用一个密钥，当参与人数过多时，密钥的分发与管理是一个问题。
- 通讯双方地位平等，无法保证某一个消息由谁发送，缺少抗抵赖功能。

## 公钥密码

- 性质
  - 基于数学函数，而不是基于比特模式的简单操作
  - 使用两个密钥：一个公钥与一个私钥
  - 由于通讯双方使用密钥不一样，具有非对称结构
  - 公钥密码计算开锁大，作为对称加密方法的补充，而不是替换方案
- 解决的问题：1）密钥分发（在没有可信的分发通道的情况下保证通信安全）；2）数字签名：验证消息的发送方。
- 模型




- 公钥密码与传统密码的对比


2.5 公钥密码与对称密码

| 传统密码 | 公钥密码 |
| --- | --- |
| 使用要求： | 使用要求： |
| 1. 加密和解密都使用同样的算法和私钥。<br>2. 发送方和接收方必须共享算法和密钥。 | 1. 一个算法使用公钥用于加密，一个算法使用私钥用于解密。<br>2. 发送方和接收方必须有一对匹配的公私钥对，但不是相同的。 |
| 安全要求： | 安全要求： |
| 1. 密钥必须保持私密性。<br>2. 如果没有其它附助信息，不可能可以解密消息。<br>3. 对算法的分析与一些密文文件不足以破解密钥。 | 1. 私钥必须保持私密性，公钥可以公开。<br>2. 如果没有其它附助信息，不可能可以解密消息。<br>3. 对算法的分析，并已知公钥与一些密文文件不足以破解私钥。 |

- 应用：加密/解密、数字签名和密钥交换
- 公钥算法需要满足的要求：

- 接收方计算生成密钥对（公钥、私钥）是容易的。
- 已知公钥和明文消息$M$，发送方容易计算密文。
- 接收方用私钥解密密文时，比较容易恢复明文。
- 已知公钥，不可能通过计算推算出私钥。
- 已知公钥和密文，通过计算不可能恢复原始消息。
- 两个密钥，一个用于加密，另一个可以用于解密。

## RSA（重点）

$$C = M^e \bmod n,\ 这里\ 0 \le M < n$$

$$M = C^d \bmod n = M^{ed} \bmod n$$

**其中公钥** $PU = \{e, n\}$ **，私钥** $PR = \{d, n\}$ **。**

- 密钥设置要求：
  - 找到e, d, n的值，使得对所有的M<n, $M^{ed}\ mod\ n = M$。
  - 对所有满足M<n的值，计算$M^e$和$C^d$相对容易。（**快速幂**）
  - 给定e和n，不可能推出d。
- 密钥设置流程（**重点**）
  1. 随机选择两个大素数: $p$, $q$, 并计算他们的乘积 $n = p \times q$ 作为加密和解密时的模。
  2. 接着计算n的欧拉函数值 $\phi(n) = (p-1)(q-1)$
  3. 选择与n互素的加密密钥 e , 满足$1 < e < \phi(n), gcd(e, \phi(n)) = 1$。一般e会给出。
  4. 计算e关于模$\phi(n)$的乘法逆元d，作为解密密钥。（**扩展欧几里得算法**）
  5. 公布公钥: PU={e, n}， 保留私钥: PR={d, n}
- 密钥设置举例
  - **选择素数:** $p$=17 & $q$=11
  - **计算:** $n = pq$ =17 x 11=187
  - **计算:** $\phi(n)=(p-1)(q-1)$=16 x 10=160
  - **选择** $e$: gcd(e,160)=1; $e$=7
  - **决定** $d$: $de$=1 mod 160 **而且**$d$ < 160，**得出** $d$=23，**由于**23 x 7=161= 10 x 160+1
  - **公布公钥:** $PU$={7, 187}
  - **保留私钥:** $PR$={23, 187}
- 安全分析
  - 穷举搜索攻击：试遍所有可能的私钥，所以e和d的比特数越大，算法越安全，同时运算更复杂，系统运行更慢。
  - 分析RSA密码算法：主要重点在于如何分解n为两个素数。由于大数n具有很大的素因子，因式分解问题非常困难。目前1024比特的密钥安全强度足够了。