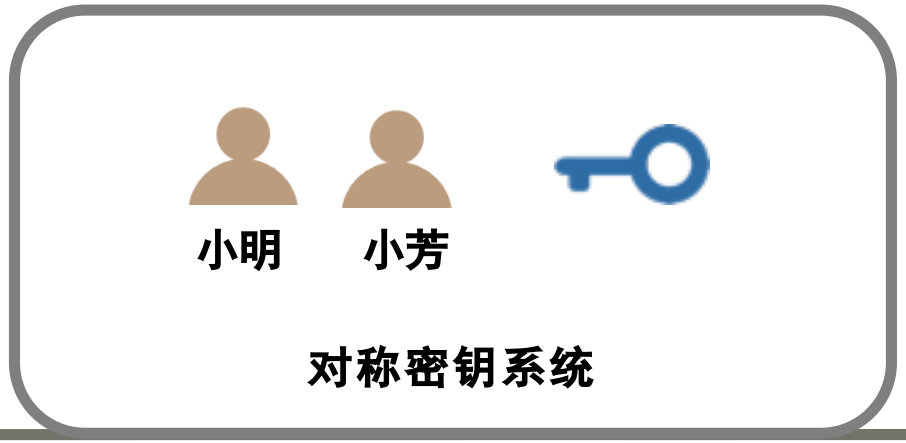
公开密钥系统

公开密钥密码体系

公开密钥密码：使用不同的加密密钥和解密密钥，是一种“由已知加密密钥推导出秘密密钥在计算上是不可性的”密码体系。

秘密密钥SK由公开密钥PK决定，但却不能根据PK计算出SK。

加密密钥	解密密钥
• 即公开密钥（PK） • 是公开信息 • 称为公钥	• 即隐密密钥（SK） • 接收者持有（隐秘） • 称为私钥



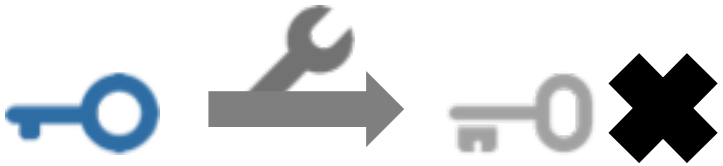
公开密钥密码体系特点

关于密钥

- 加密密钥是公开的，但无法用来解密
- 从公钥到私钥是“计算上不可能的”

加密用公钥

解密用私钥



算法必须满足

- 发送者用加密密钥PK对明文P加密后，接收者用解密密钥SK解密，即可恢复明文P
- 从E推断出D极其困难
- E不可能被选择明文攻击破解

$$D_{SK}(E_{PK}(P)) = P$$

$$D_{PK}(E_{PK}(P)) \neq P$$

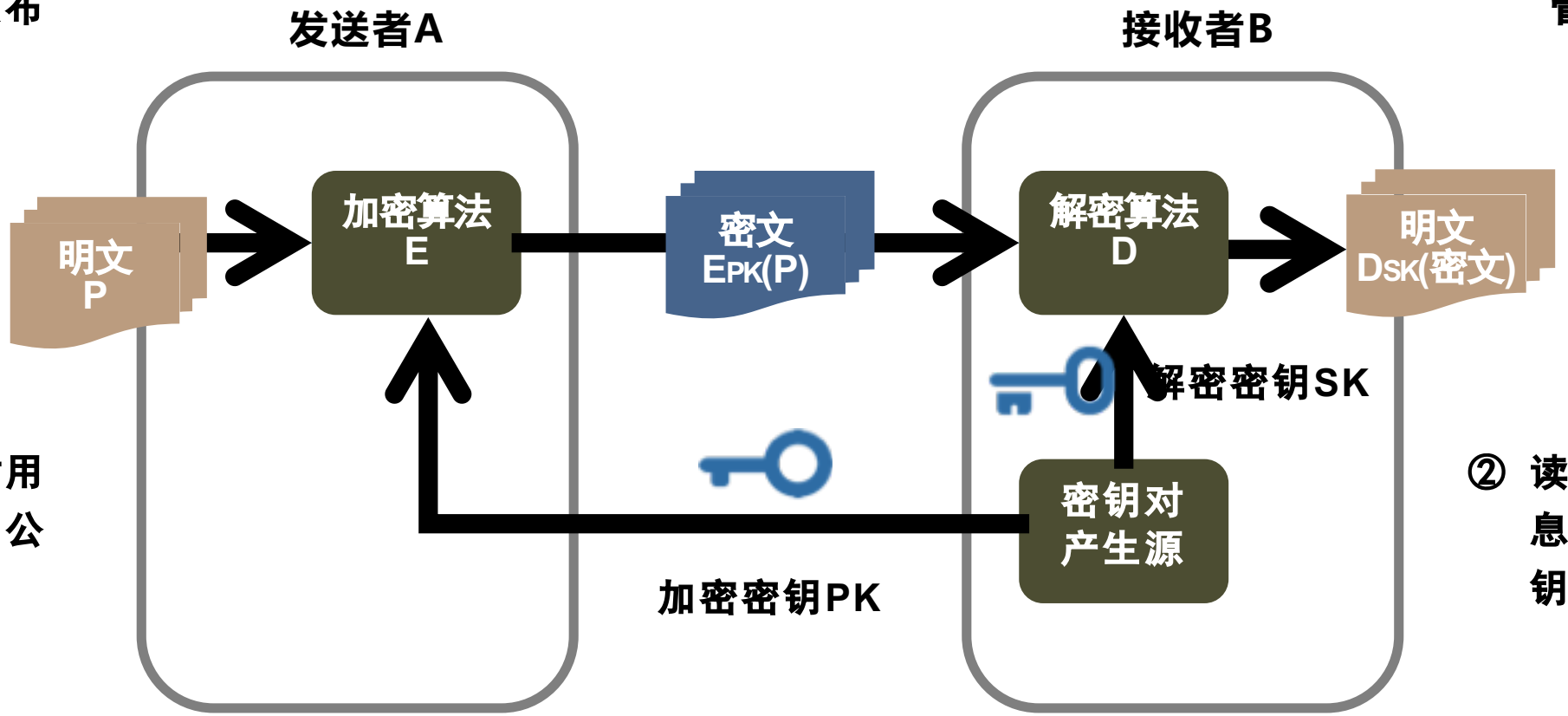
公开密钥密码体系工作原理

① 发送者获得接收者公开发布的公钥

② 发送消息时用公开密钥（公钥）加密

① 接收者自己保管隐秘的私钥

② 读取收到的消息时用隐密密钥(私钥)解密



加密用公钥　解密用私钥

RSA算法

RSA算法：由MIT的三位研究者于1978年公开密钥算法，并且算法由三位研究者名字的首字母命名。给三位研究者带来了2002年的ACM图灵奖殊荣。

n=p*q
p，q：是大素数
e，d：满足一定关系式

根据数论，寻求两个大素数比较简单，而将它们的乘积分解开则极其困难。

RSA算法特点

- 每个用户有两个密钥
  ① 加密密钥PK = {e, n}，公开
  ② 解密密钥SK = {d, n}，保密
- 系统中任何用户都可以使用公钥给该用户发送信息
- 攻击者知道e和n也无法推算出d
- 密钥长度至少需要2014位

RSA的加密和解密算法

加密算法

- 加密算法

$$C = P^e \ mod \ n$$

- 公开的加密用密钥

$$PK = \{e, n\}$$

- 整数P表示明文
- 整数C表示密文
- P和C均小于n

解密算法

- 解密算法

$$P = C^d \ mod \ n$$

- 保密的解密用密钥

$$SK = \{d, n\}$$

- 整数P表示明文
- 整数C表示密文
- P和C均小于n

RSA算法密钥的产生

计算n	计算欧拉函数	选择加密指数d	计算解密指数e	公钥和私钥
•秘密选择两个大素数p,q •计算n=p*q	•计算n的欧拉函数z •z = (p-1)*(q-1)	•从[0, z-1]中选择一个与z互素的数d作为公开的加密指数	•计算出满足 e*d = 1 *mod* z 的e作为解密指数	PK = {e, n} SK = {d, n}

- n公开，p和q保密
- p、q两个素数典型情况下为1024位

分解一个500位十进制数需要10^{25}年的时间(100万个处理器并行计算)

RSA算法示例

计算n	计算n的欧拉函数z	选择加密指数d	计算解密指数e	公钥和私钥
• p=7 • q=17 • n=p*q=119	z=(p-1)*(q-1) = 96	从[0,95]之间选择一个与96互素的数d，选d=5	根据公式 e*5 = 1 mod 96 解出e=77	公钥PK={5, 119} 私钥SK={77,119}

加密前必须先将明文划分为块，每个块的二进制位数不超过n。