密码学概述

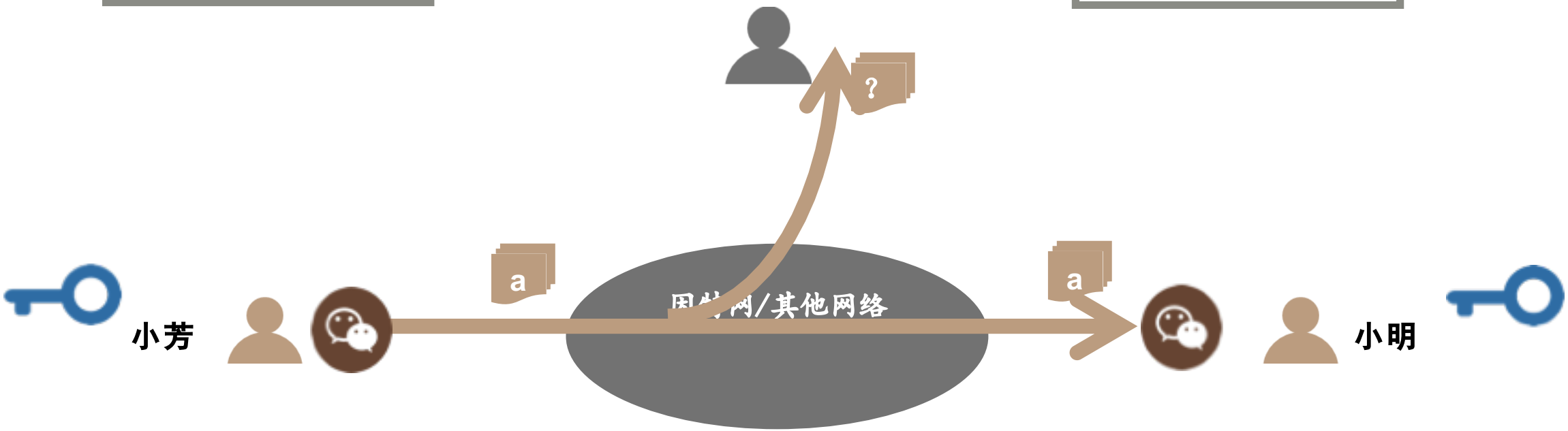
密码学(cryptography)

密码编码学

- 设计密码的技术
- 加密/解密算法

密码分析学

- 破解密码的技术



明文密文vs.加密解密

明文（plaintext）：待加密的原始消息
密文（ciphertext）：加密后的消息

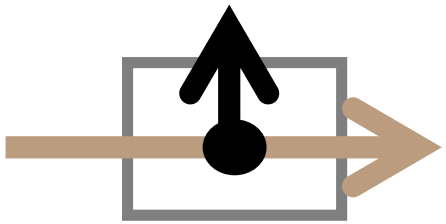
密钥（key）：生成加密算法所用的秘密信息。

$$C = E_k(P)$$
$$P = D_k(C)$$
$$D_k(E_k(P)) = P$$

- 明文经加密后变成密文
- 密文经解密后还原成明文
- 被加密后的密文能被解密还原成明文

- P：明文
- C：密文
- K：密钥
- E：加密算法(P, K)
- D：解密算法(C, K)

加密模型——对称密钥密码



被动攻击模型

被动入侵者
侦听消息

没有密钥读不出密文的真实含义。

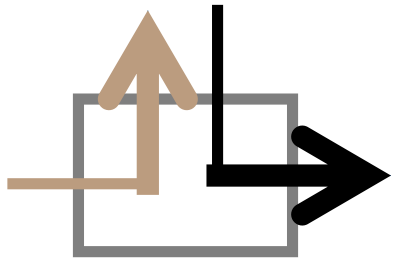
小芳

小明

加密密钥
K

加密密钥
K

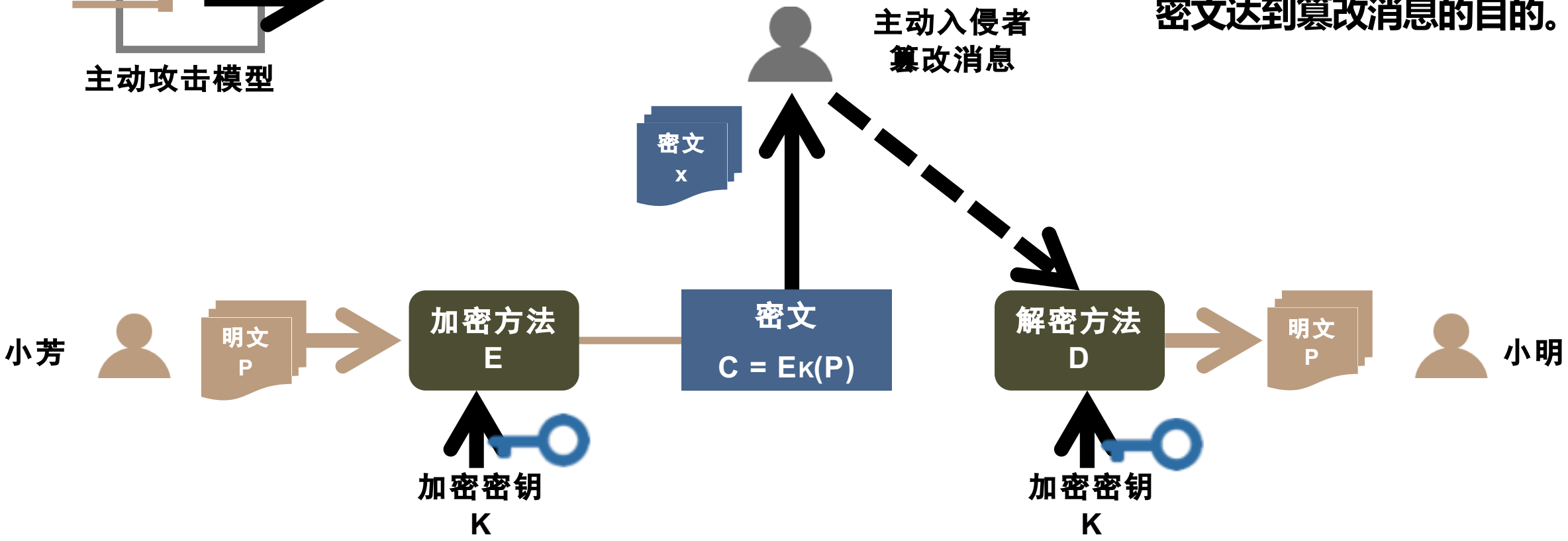
加密模型——对称密钥密码



主动攻击模型

密钥的保密至关重要!

没有密钥读不出密文的真实含义，就无法做到修改密文达到篡改消息的目的。



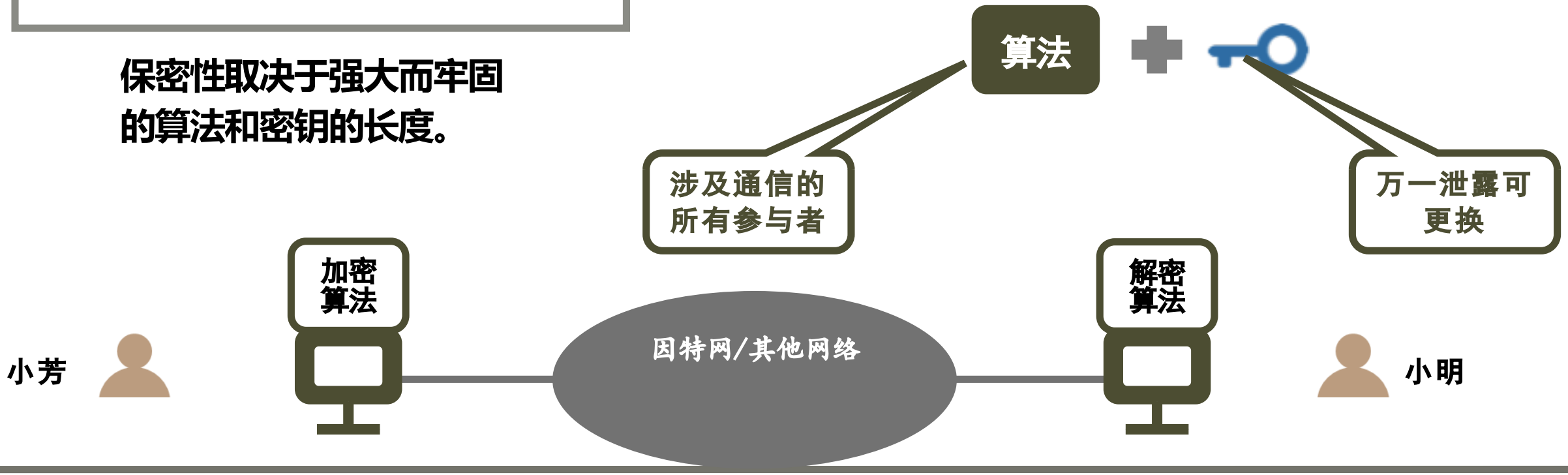
Kerckhoff原则

密码学的基本规则

假定密码分析者一定知道加密和解密方法，即知道E和D算法的所有细节。

保密性取决于强大而牢固的算法和密钥的长度。

Kerckhoff原则：所有的算法必须是公开的，而密钥是保密的。



Kerckhoff原则示例

示例：旅行航空箱的密码锁。

算法：输入若干位十进制数
KEY：数字正确的排列组合

破解密码系统的工作量随着密钥长度增加而呈指数递增。

算法 众所周知

X*Y*Z

- X：0-9的任意数字
- Y：0-9的任意数字
- Z：0-9的任意数字

① 密钥长度为2位数字，共有100种可能
② 密钥长度为3个数字，共有1000种可能
③ …
④ 密钥长度为6位数字，共有100万种可能