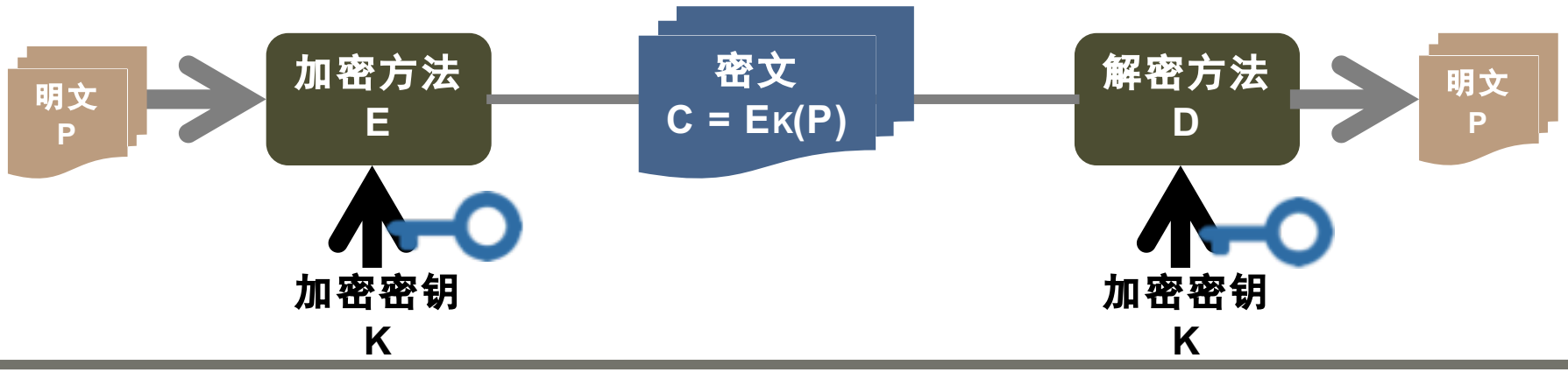
对称密钥系统

密码分析问题的三个层次

密文问题	已知明文问题	选择明文问题
密码分析者得到了一定量的密文，但是没有对应的明文。	密码分析者有了一些相匹配的密文和明文。	密码分析者能够加密某一些他自己选择的明文。



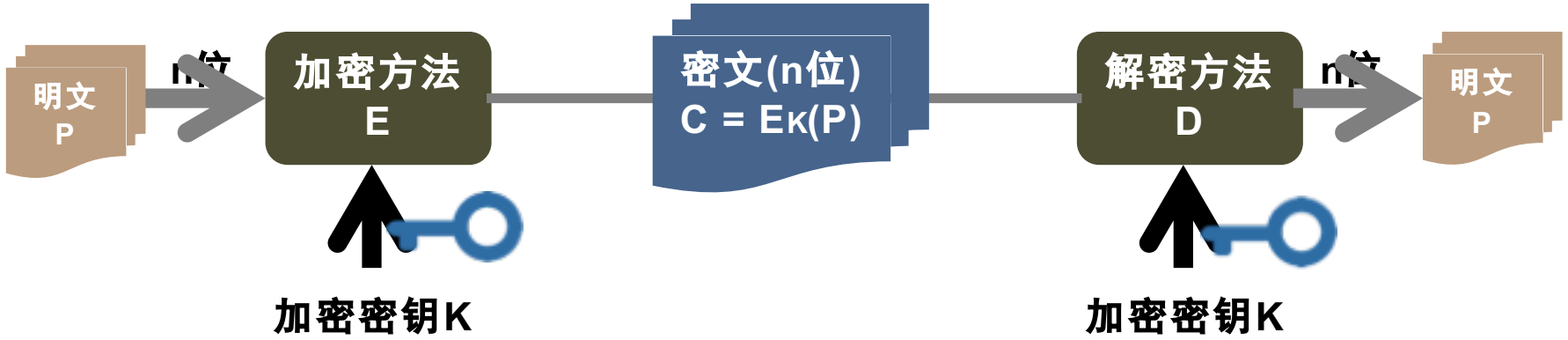
对称密钥(symmetric key)

对称密钥系统：加密密钥与解密密钥是相同的密码体制。

块密码：不是逐位进行加密，而是以n位为一块进行加密处理。

密码设计目标

密码分析者获得部分密文在没有密钥时推测不出明文

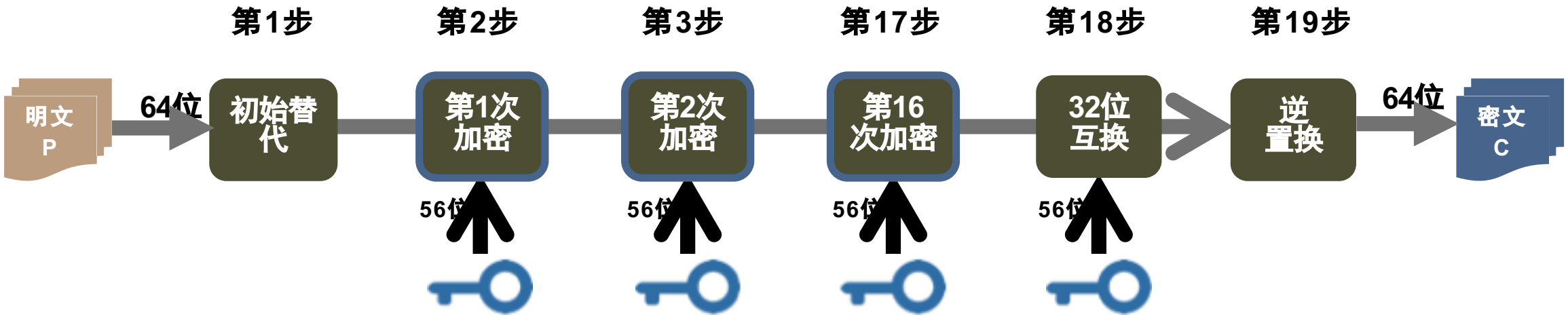


数据加密标准（DES）

数据加密标准(DES)：由IBM提出的块密码算法，1977年被美国政府采纳作为非机密信息的官方加密标准。

DES加密过程

① 对整个明文（64位）进行替代操作
② 针对每个64位的块，进行16次加密，密钥56位，是加密算法的参数
③ 将32位互换位置后进行替代的逆操作



DES加密过程的

初始化阶段

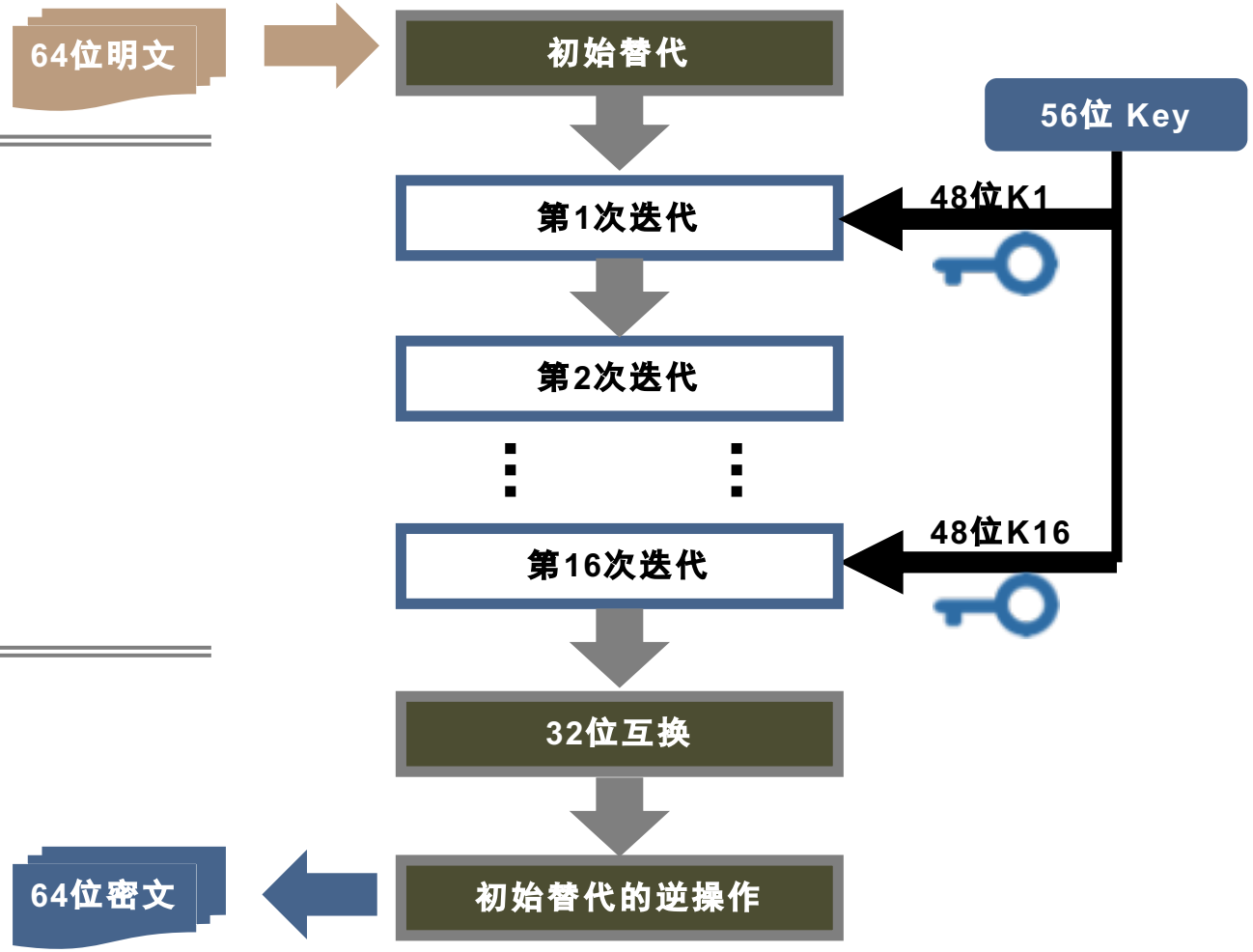
对整个明文（64位）进行替代操作（step1）

迭代加密阶段

- 针对每个64位的块，进行16次加密
- 密钥56位，每次加密取其中48位
- Step2~step17

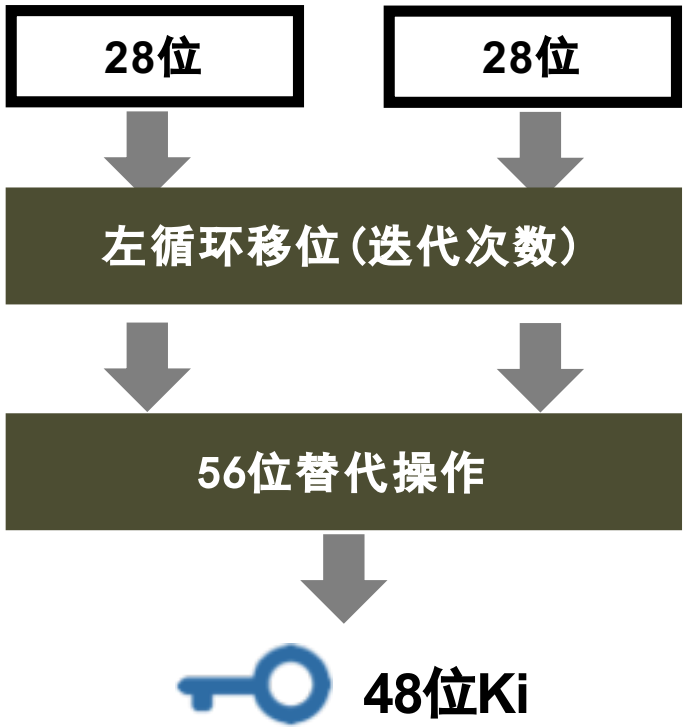
密文输出阶段

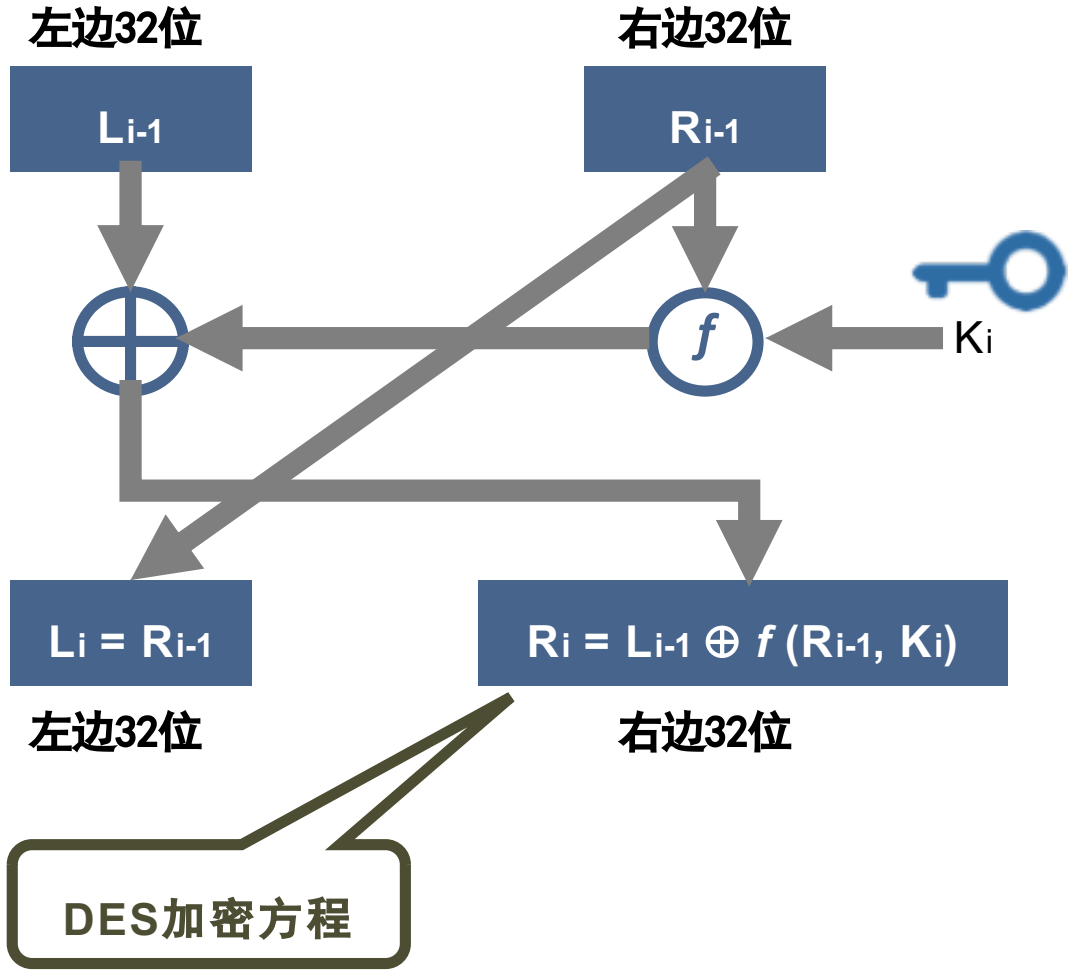
将32位互换位置后进行替代的逆操作（step18/19）



DES加密工作原理

- 每次加密所用密钥的生成过程

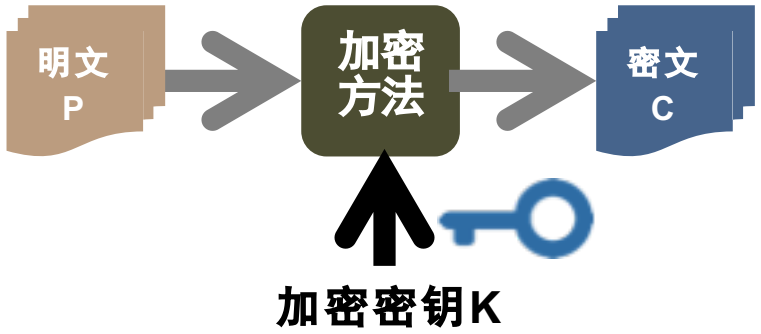




- 函数f为置换操作，将32位扩展至48位。

DES的特点和不足

本质上是一种单字母置换密码算法。



同样的明文加密100次得到同样的密文

100次→密码分析者提供了便利

- 密钥必须秘密保管
- 密钥必须分发出去