数据加密标准

定义

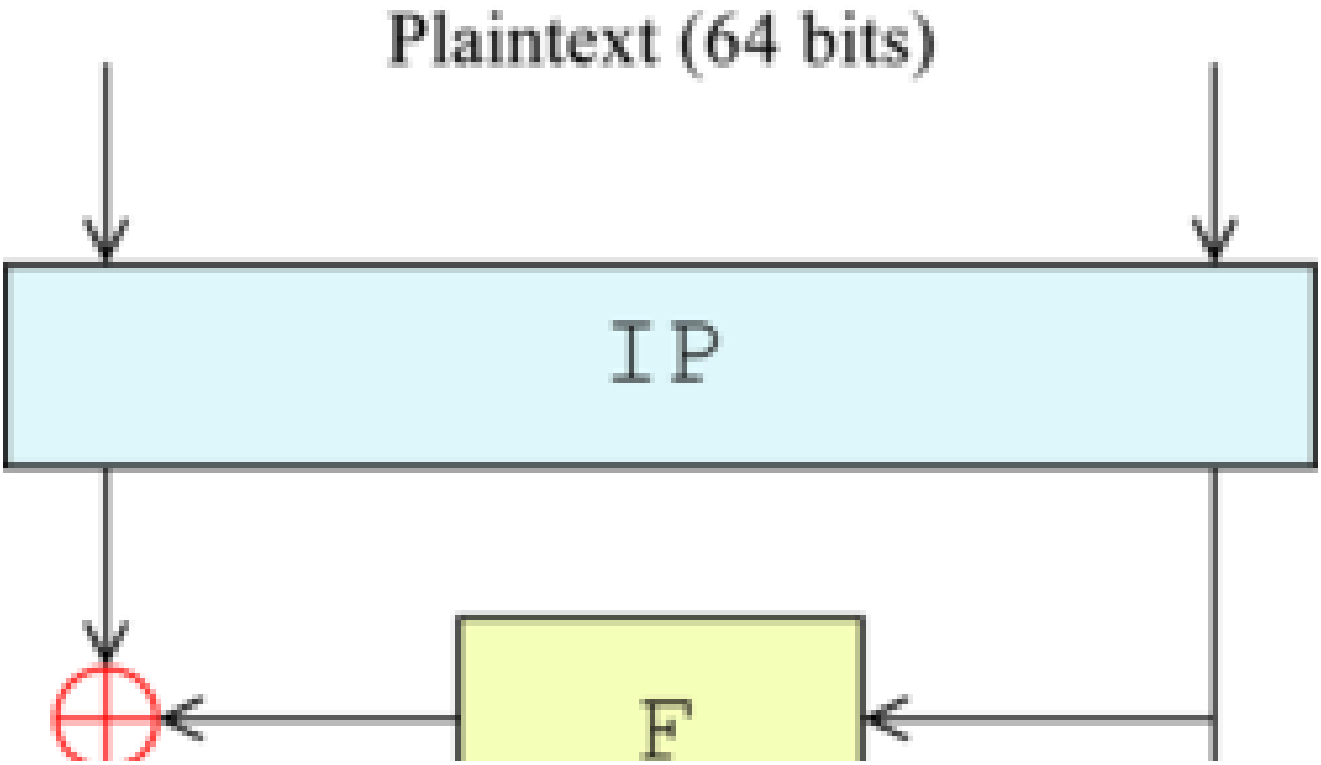
数据加密标准（英语：Data Encryption Standard，缩写为 DES）是一种对称密钥加密块密码算法，1976年被美国联邦政府的国家标准局确定为联邦资料处理标准（FIPS），随后在国际上广泛流传开来。它基于使用56位密钥的对称算法。

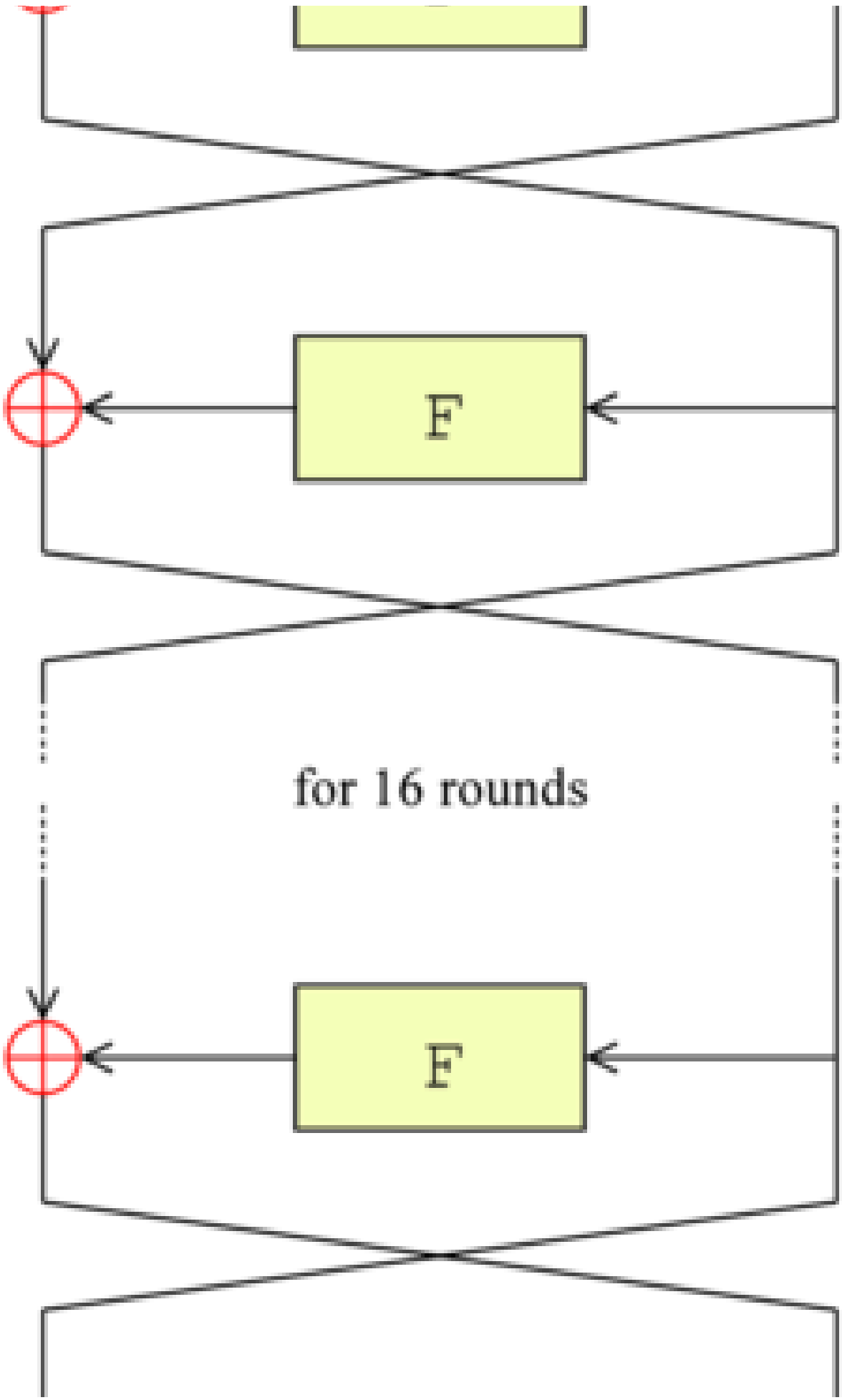
DES是一种典型的**块密码**—一种将固定长度的平文通过一系列复杂的操作变成同样长度的密文的算法。对DES而言，**块长度为64位**。密钥表面上是64位的，然而只有其中的**56位被实际用于算法，其余8位可以被用于奇偶校验**，并在算法中被丢弃。

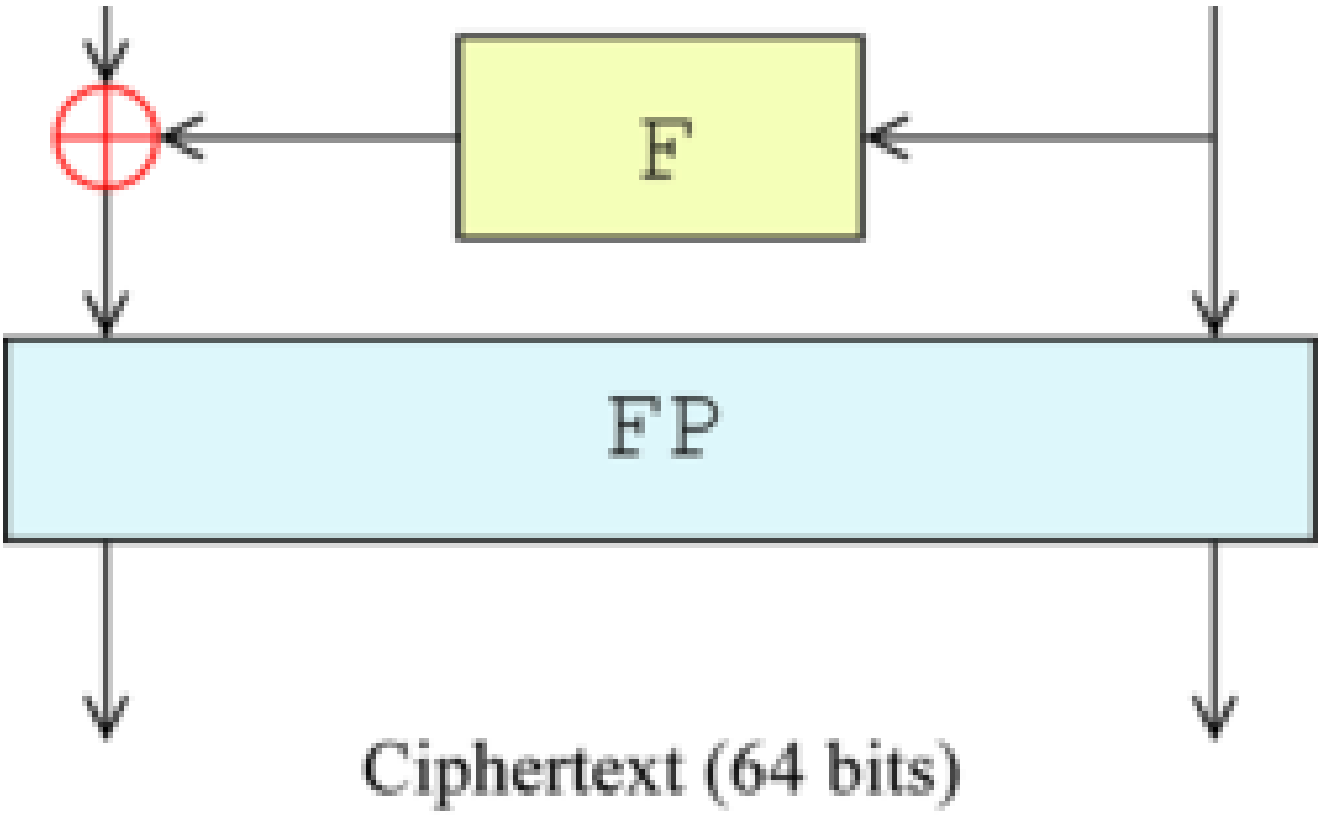
算法描述

回次

算法的整体结构有16个相同的处理过程，称为“回次”（*round*），并在首尾各有一次置换，称为**IP**与**FP**（或称IP^{-1}，FP为IP的反函数）（然而IP和FP几乎没有密码学上的重要性）如下图：




F
for 16 rounds
F

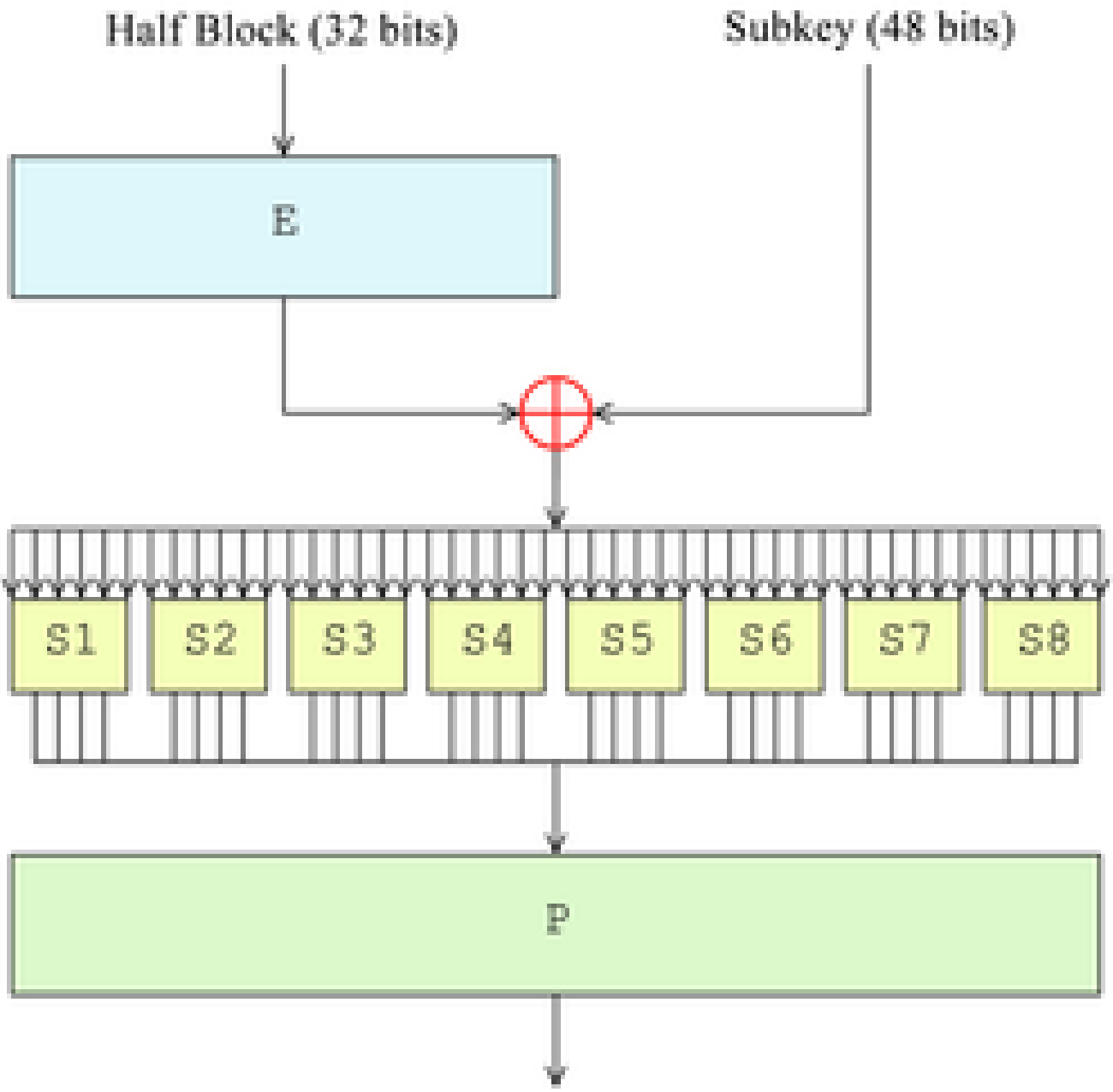


在主处理回次前，**数据块被分成两个32位的半块**，并被分别处理；这保证了加密和解密过程足够相似——唯一的区别在于子密钥在解密时是以反向的顺序应用的。大大简化了算法的实现，尤其是硬件实现，因为没有区分加密和解密算法的需要。

图中的⊕符号代表异或（XOR）操作。**“F函数”将数据半块A经过F函数与某个子密钥进行处理后，与另一个半块B异或产生下一个A，再与原本的半块A组合并交换顺序（原A当B用），进入下一个回次的处理。在最后一个回次完成时，两个半块需要交换顺序**，以保证加解密的过程相似。

F函数

下图显示了费斯妥函数（F函数）的过程。其每次对半块（32位）进行操作，并包括四个步骤：

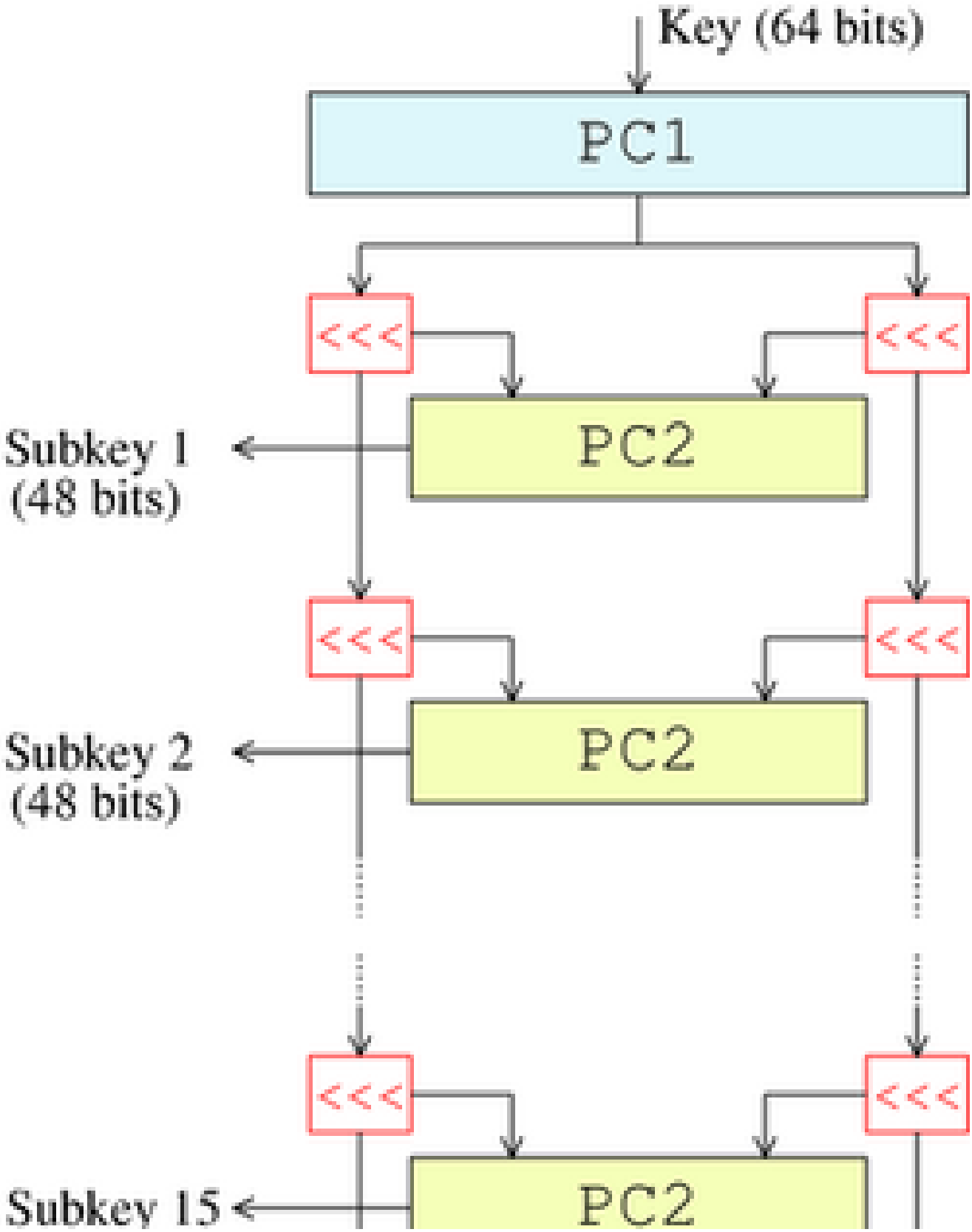


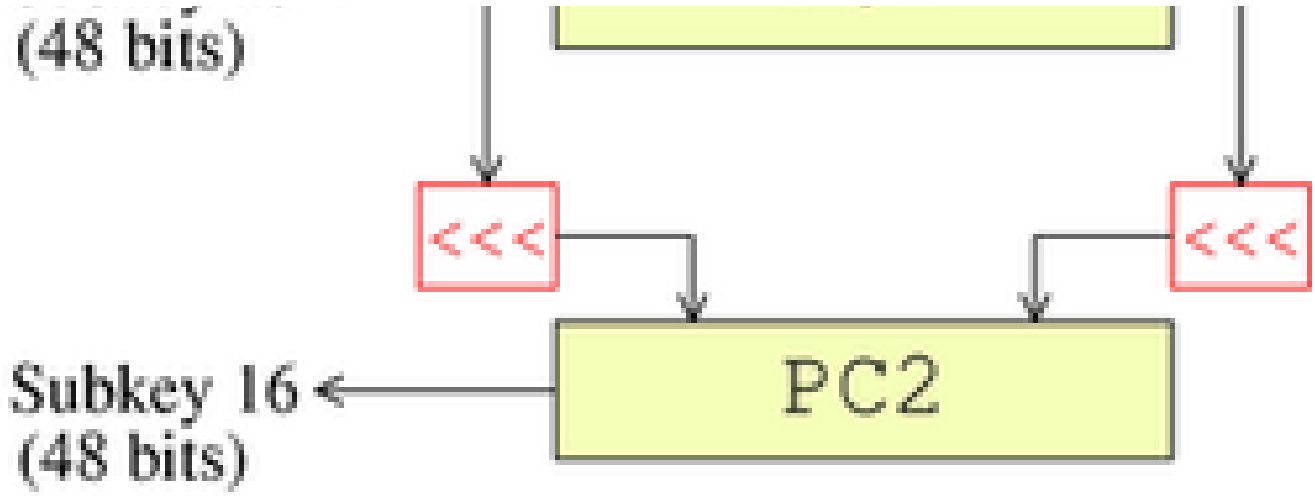
1. **扩张**：用扩张置换（图中的**E**）将32位的半块扩展到48位，其输出包括8个6位的块，每块包含4位对应的输入位，加上两个邻接的块中紧邻的位。
2. **与密钥混合**—用异或操作将扩张的结果和一个**子密钥**进行混合。16个48位的子密钥—每个用于一个回次的F变换—是利用密钥调度从主密钥生成的（见下文）。
3. **S盒**—在与子密钥混合之后，块被分成8个6位的块，然后使用S盒（置换盒）进行处理。8个S盒的每一个都使用以查找表方式提供的非线性的变换将它的6个输入位变成4个输出位。**S盒提供了DES的核心安全性**—如果没有S盒，密码会是线性的，很容易破解。
4. **P置换**—最后，S盒的32个输出位利用固定的置换进行重组。这个设计是为了将每个S盒的4位输出在下一回次的扩张后，使用4个不同的S盒进行处理。
5. S盒，P置换和E扩张各自满足了实用密码所需的必要条件，“混淆与扩散”。

密钥调度

下图显示了加密过程中的**密钥调度**—产生子密钥的算法。首先，使用**选择置换1**（PC-1）从64位输入密钥中选出56位的密钥—剩下的8位要么直接丢弃，要么作为奇偶校验位。然后，56位分成两个28位的半密钥；每个半密钥接下来都被分别处理。在接下来的回次中，两个半密钥都被左移1或2位（由回次数决定），然后通过**选择置换2**（PC-2）产生48位的子密钥—每个半密钥24位。移位（图中由`<<<`标示）表明每个子密钥中使用了不同的位，每个位大致在16个子密钥中的14个出现。

解密过程中，除了子密钥输出的顺序相反外，密钥调度的过程与加密完全相同。




(48 bits)
<<<
<<<
PC2
Subkey 16
(48 bits)