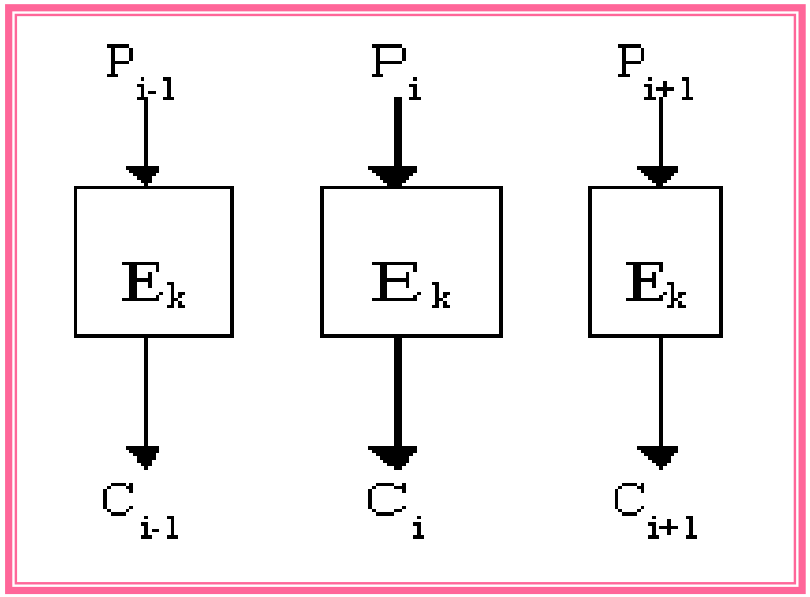
§3.4 分组密码工作模式

1、ECB（电子密码本）模式

各明文组独立地以同一密钥加密，传送短数据。

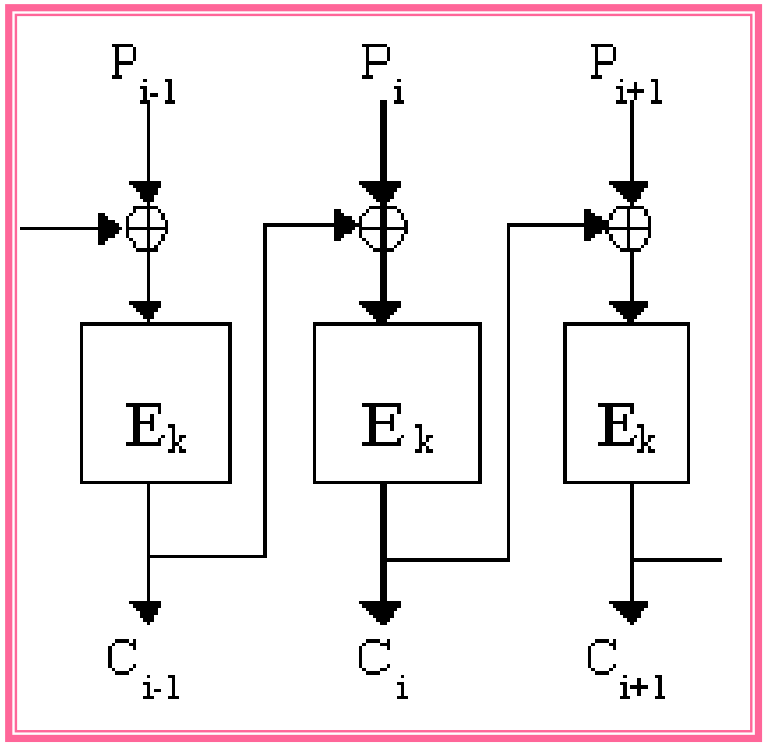
其缺点是组间同明文时，可能遇到同密钥，易暴露统计特性。



§3.4 分组密码工作模式

2、CBC（密码分组链接）模式

加解密算法的结果不仅与当前输入信息和密钥有关，还与先前的输入输出信息相关。



初始向量IV；

$C_0 = IV$；

$C_n = E_k[C_{n-1} \oplus P_n]$；

用途：传送数据分组；认证。

§3.4 分组密码工作模式

3、CFB（密码反馈）模式

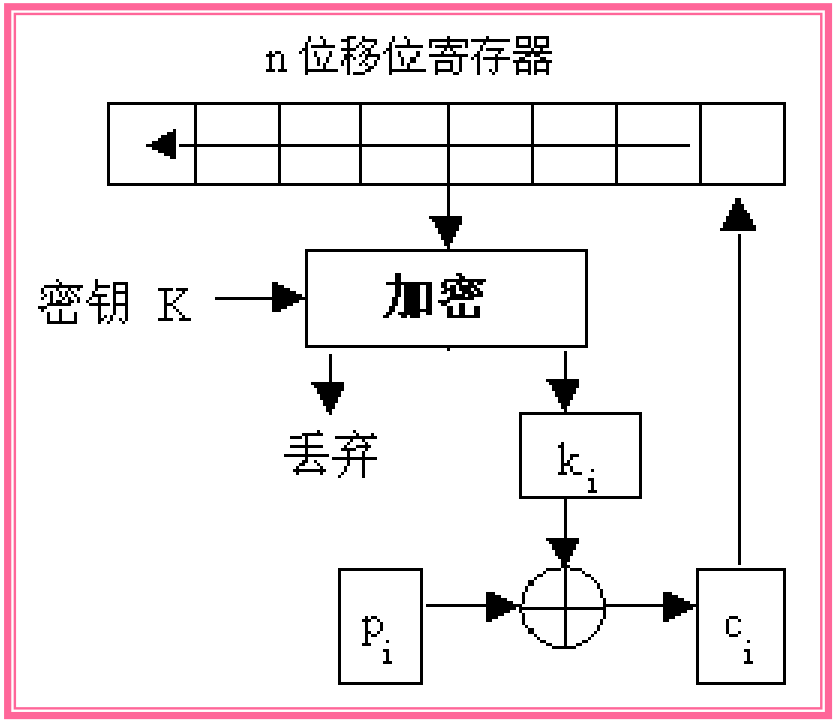
按字符或按比特处理明文，往往利用CFB模式，通过加密前的一个密文块产生密钥流元素$Z_i = E(C_{i-1}, k)$

初始向量IV；

$C_0 = IV$；

加密：$C_i = P_i \oplus Z_i$

解密：$P_i = C_i \oplus Z_i$



§3.4 分组密码工作模式

4、OFB（输出反馈）模式：

用分组密码产生一个随机密钥流，将此密钥流和明文流进行异或可得密文流。

初始向量IV；

$Z_0 = IV$；

$Z_i = E(Z_{i-1}, k)$

加密：$C_i = P_i \oplus Z_i$

解密：$P_i = C_i \oplus Z_i$

