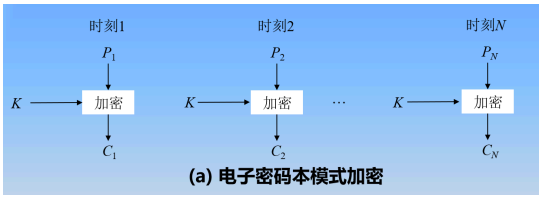
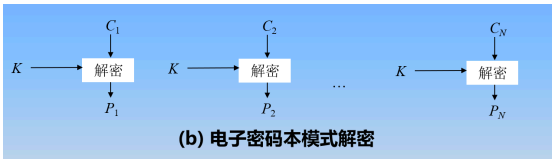
分组密码的运行模式（重点）

- 定义：分组密码一次加密一个固定长度的数据分组
- 除了电子密码本模式和分组密码链接模式，其他的模式都不对明文进行加密。

电子密码本模式

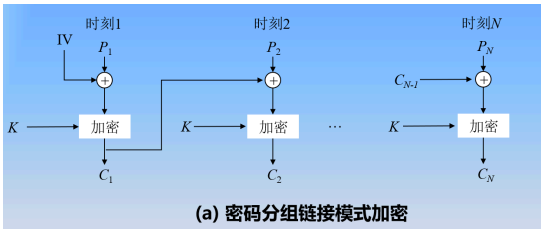
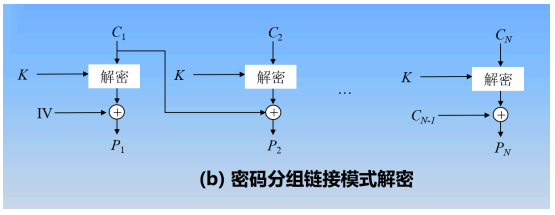
$$\text{加密：}\quad C_i = E_K(P_i)$$
$$\text{解密：}\quad P_i = E_K(C_i)$$

加密	解密
	

- 安全分析
  - 64-bit明文分组重复时在密文中也会重复出现
  - 主要是因为这些加密的消息是独立处理而造成

密码分组链接模式

$$\text{加密：}\quad C_i = E_K(P_i \text{ XOR } C_{i\text{-}1})$$
$$\text{解密：}\quad P_i = E_K(C_i) \text{ XOR } C_{i\text{-}1}$$

加密	解密
	

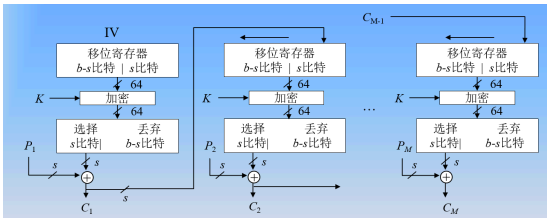
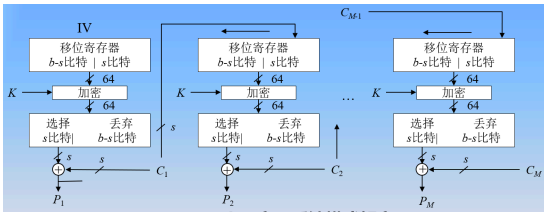
密码反馈模式

密码反馈模式能将任意分组密码转化成流密码，从而不需要对消息进行填充为分组的整数倍，还可以实时操作，充分利用传输信道。

加密：$C_i = P_i \text{ XOR } S[E_K(C_{i-1})]$

解密：$P_i = C_i \text{ XOR } S[E_K(C_{i-1})]$

其中S[X]是取X的最高有效 s bit，$C_0 = IV$ 是初始向量，需要保密。

加密	解密
	
(a) 密码反馈模式加密	(b) 密码反馈模式解密

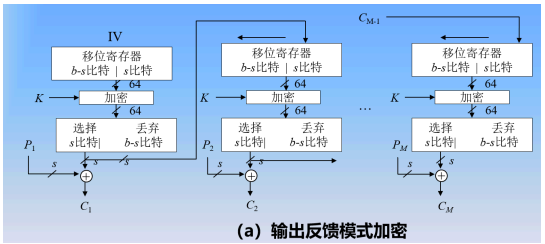
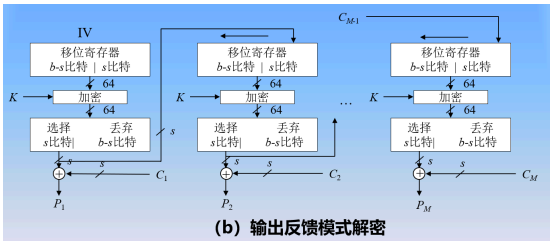
输出反馈模式

输出反馈模式类似于密码反馈模式，主要区别在于反馈的内容是加密器输出的随机数，而不是密文，因此不具有错误传播特性。

加密：$C_i = P_i \text{ XOR } S[E_K(IV)]$

解密：$P_i = C_i \text{ XOR } S[E_K(IV)]$

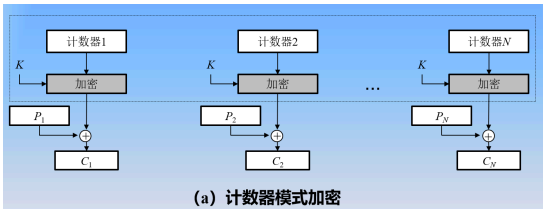
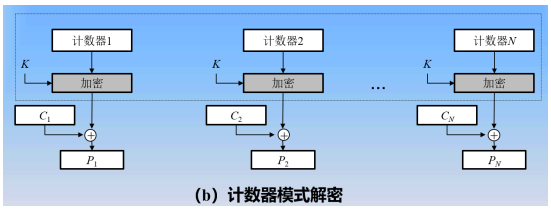
其中S[X]是取X的最高有效 s bit，IV 是初始向量需要保密,并随着加密一直更新（$IV=E_K(IV)$）。

加密	解密
	
(a) 输出反馈模式加密	(b) 输出反馈模式解密

计数器加密

$$\text{加密：}\ C_i = P_i \ \text{XOR}\ E_K(i)$$

$$\text{解密：}\ P_i = C_i \ \text{XOR}\ E_K(i)$$

加密	解密
	
(a) 计数器模式加密	(b) 计数器模式解密