

chap05

[陈永俊] [522031910203]

作业

- ❖ 对4种使用模式，
 - 分别写出解密算法（以 $Dec_k(*)$ 或 $F_k^{-1}(*)$ 代表单个分组解密算法），并画出解密流程图。
 - 以列表形式说明是否可以用于流加密、是否可以并行加解密、是否有差错扩散。
- ❖ 对于ECB、CBC而言，明文必须为一个或多个完整数据分组组成的序列。即对于此三种模式，明文的总位数必须是分组（分段）长度的整数倍。若明文最后一段不是分组（分段）长度的整数倍，常见的填充方式包括先填1，后面全部为0（也可能没有），知道填满最后一个分组。但是，通常要求当明文最后一段为分组（分段）长度的整数倍时，也要再添加一个填充分组。动机是什么？
- ❖ 线性同余法中为何使用 $2^{31}-1$ ，而不是 2^{31} ？

Figure 1: chap05

5.1

图片见 Figure 5.1

- ECB:

$$M_i = F_k^{-1}(C_i)$$

- CBC:

$$\begin{aligned} M_1 &= IV \oplus F_k^{-1}(C_1) \\ M_{i+1} &= C_i \oplus F_k^{-1}(C_{i+1}) \end{aligned}$$

- OFB:

$$\begin{aligned} O_0 &= IV \\ O_{i+1} &= F_k(O_i) \\ M_i &= C_i \oplus O_i \end{aligned}$$

- CTR:

$$M_i = C_i \oplus F_k(ctr + i)$$

Encryption	ECB	CBC	OFB	CTR
流加密	是	是	是	是
并行加解密	是	并行解密，但不并行加密	是	是
差错扩散	否	是	IV 有扩散	ctr 有扩散

5.2

- 错误校验：添加一个填充分组，可以检验填充分组是否出错。如无，则无法分别明文长度恰好和填充错误。
- 作为 EOF

5.3

因为计算机表示的最大非负整数为 $2^{31} - 1$ ，在 32 位计算机系统中，无法直接表示 2^{31} ， 2^{31} 是 -2^{31} 。

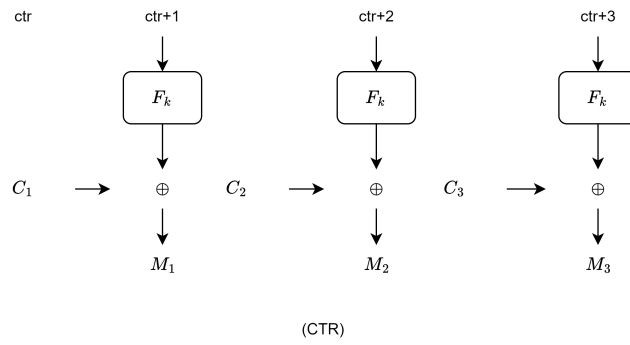
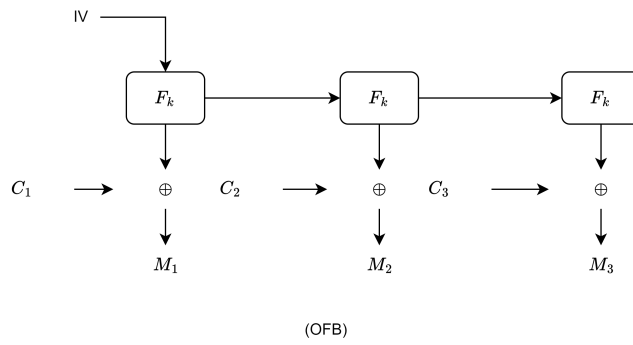
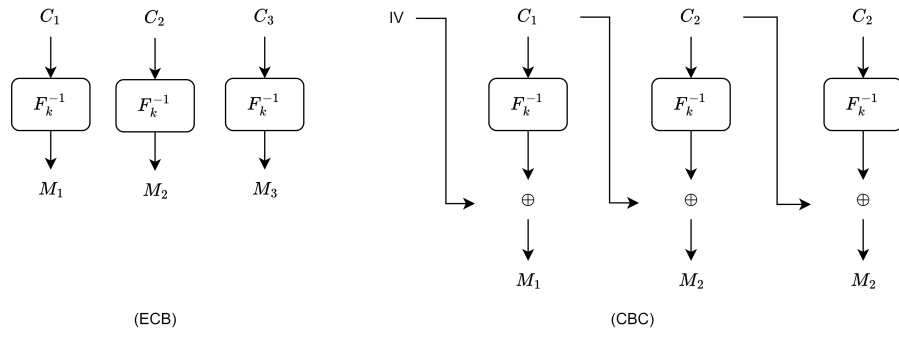


Figure 2: 5.1