chap05

[陈永俊] [522031910203]

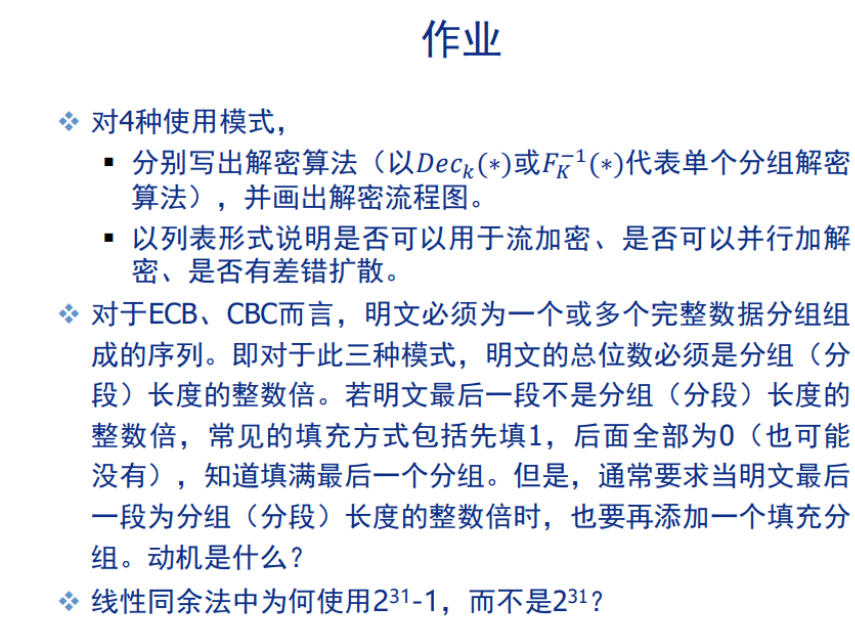

Figure 1: chap05

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}。

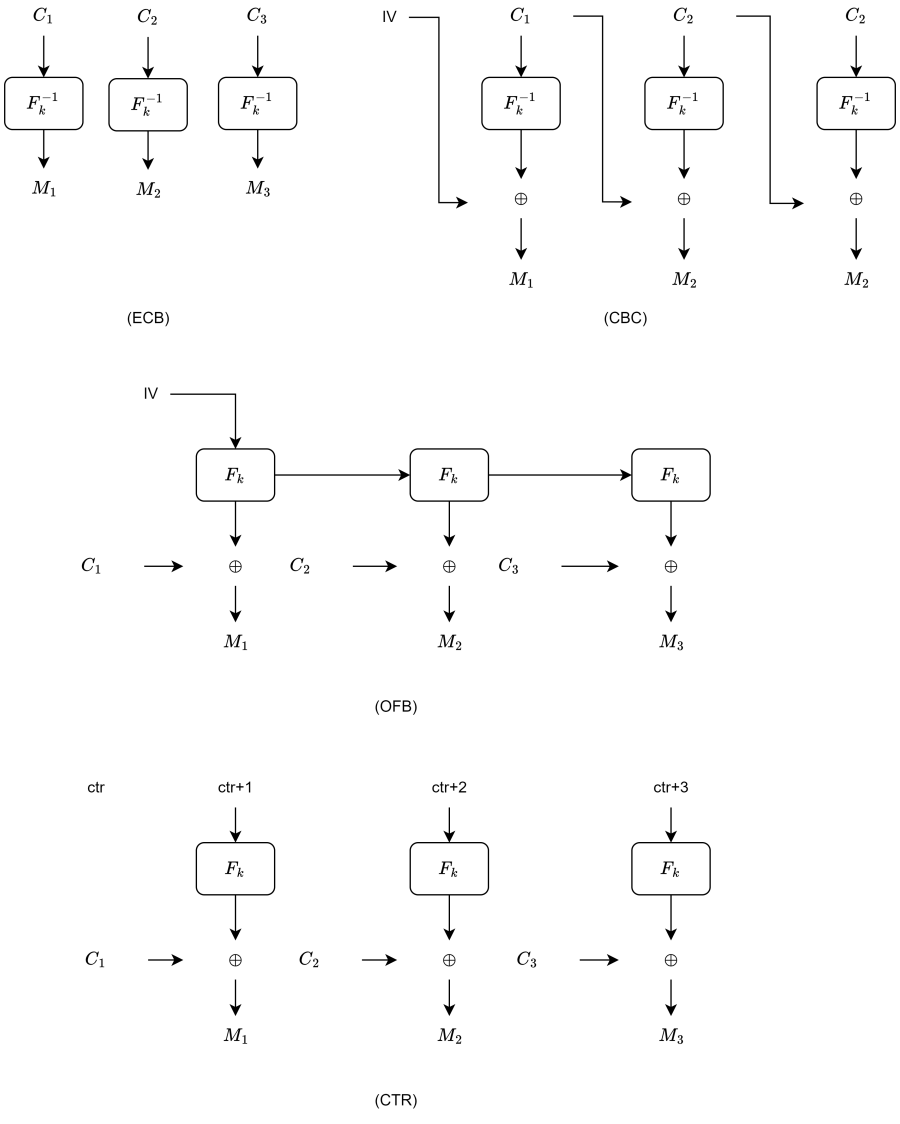
C_1
C_2
C_3
F_k^{-1}
M_1
M_2
M_3
(ECB)
IV
C_1
C_2
C_2
F_k^{-1}
$\oplus$
M_1
M_2
M_2
(CBC)
IV
F_k
C_1
C_2
C_3
$\oplus$
M_1
M_2
M_3
(OFB)
ctr
ctr+1
ctr+2
ctr+3
F_k
C_1
C_2
C_3
$\oplus$
M_1
M_2
M_3
(CTR)

Figure 2: 5.1