Name:Chao Jiang
ECE5563 — Spring 2015 **HW 4** Due: Mar. 4

Problem 5.13

Demonstrate that Equation (5.9) is equivalent to Equation (5.4).

$$\begin{aligned} s'_{0,j} &= (2 \cdot s_{0,j}) \oplus (3 \cdot s_{1,j}) \oplus s_{2,j} \oplus s_{3,j} \\ s'_{1,j} &= s_{0,j} \oplus (2 \cdot s_{1,j}) \oplus (3 \cdot s_{2,j} \oplus s_{3,j}) \\ s'_{2,j} &= s_{0,j} \oplus s_{1,j} \oplus (2 \cdot s_{2,j}) \oplus (3 \cdot s_{3,j}) \\ s'_{3,j} &= (3 \cdot s_{0,j}) \oplus s_{1,j} \oplus s_{2,j} \oplus (2 \cdot s_{3,j}) \end{aligned} \tag{5.4}$$

$$\begin{aligned} Tmp &= s_{0,j} \oplus s_{1,j} \oplus s_{2,j} \oplus s_{3,j} \\ s'_{0,j} &= s_{0,j} \oplus Tmp \oplus [2 \cdot (s_{0,j} \oplus s_{1,j})] \\ s'_{1,j} &= s_{1,j} \oplus Tmp \oplus [2 \cdot (s_{1,j} \oplus s_{2,j})] \\ s'_{2,j} &= s_{2,j} \oplus Tmp \oplus [2 \cdot (s_{2,j} \oplus s_{3,j})] \\ s'_{3,j} &= s_{3,j} \oplus Tmp \oplus [2 \cdot (s_{3,j} \oplus s_{0,j})] \end{aligned} \tag{5.9}$$

Using the equation $03 \cdot x = (02 \cdot x) \oplus x$: For the $s'_{0,j}$ in the Equation (5.4):

$$\begin{aligned} s'_{0,j} &= (2 \cdot s_{0,j}) \oplus (3 \cdot s_{1,j}) \oplus s_{2,j} \oplus s_{3,j} \\ &= (2 \cdot s_{0,j}) \oplus (2 \cdot s_{1,j}) \oplus s_{1,j} \oplus s_{2,j} \oplus s_{3,j} \\ &= 2 \cdot (s_{0,j} \oplus s_{1,j}) \oplus s_{1,j} \oplus s_{2,j} \oplus s_{3,j} \\ &= s_{1,j} \oplus s_{2,j} \oplus s_{3,j} \oplus 2 \cdot (s_{0,j} \oplus s_{1,j}) \end{aligned}$$

For the $s'_{0,j}$ in the Equation (5.9):

$$\begin{aligned} s'_{0,j} &= s_{0,j} \oplus s_{0,j} \oplus s_{1,j} \oplus s_{2,j} \oplus s_{3,j} \oplus [2 \cdot (s_{0,j} \oplus s_{1,j})] \\ &= 0 \oplus s_{1,j} \oplus s_{2,j} \oplus s_{3,j} \oplus [2 \cdot (s_{0,j} \oplus s_{1,j})] \\ &= s_{1,j} \oplus s_{2,j} \oplus s_{3,j} \oplus 2 \cdot (s_{0,j} \oplus s_{1,j}) \end{aligned}$$

So using the same method, we can demonstrate that Equation (5.9) is equivalent to Equation (5.4).

Problem 6.1

You want to build a hardware device to do block encryption in the cipher block chaining (CBC) mode using an algorithm stronger than DES. 3DES is a good candidate. Figure 6.12 shows two possibilities, both of which follow from the definition of CBC.
Which of the two would you choose:

a. For security?
The One-loop CBC Mode is more secure.
For only One-loop the encryption function $C = E(k_1, D(k_2, E(k_1, p)))$. this makes the cryptanalysis like differential attack more difficult than doing it on a simple loop with encryption or decryption process because each loop in the Three-loop Mode approach appears like a simple DES that may be attacked alone in a chosen plain-text attack.

b. For performance?
The Three-loop Mode approach run more fast than the one-loop mode,this is because each block in each loop contains either encryption or decryption processes. But it is more vulnerable to cryptanalysis than the first approach because each loop is a single DES with differential attack possibility.

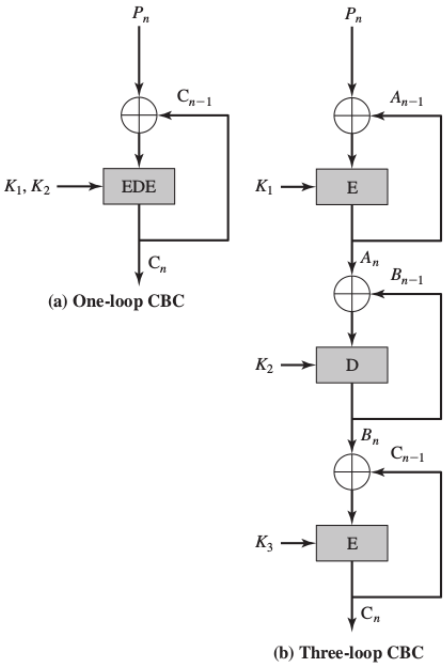

Figure 6.12 Use of Triple DES in CBC Mode

Problem 6.8

If a bit error occurs in the transmission of a ciphertext character in 8-bit CFB mode, how far does the error propagate?

The error will affect the decryption of the ciphertext block. In addition, the error block will stay in the IV for another $64/8 = 8$ blocks. In total, 9 blocks will be affected.