COMP90043: Cryptography and security:

Week 4 Workshop Activity

Activity: Working of Fiestel's algorithm for encryption and decryption.

Both encryption and decryption iteratively runs sixteen rounds of the same inner algorithm. The only difference is that the decryption rounds use a reversed key order. Verify that the decryption is the inverse operation of the encryption.

Plaintext: $\mathbf{LE_0 \| \ RE_0}$

Output of the 16th round (Encryption): $\mathbf{LE_{16} \| \ RE_{16}}$

$LE_{16} = RE_{15}$ $\quad\quad$ $RE_{16} = LE_{15} \oplus F(RE_{15}, K_{16})$

$LD_1 = RD_0 =$ _____

$RD_1 = LD_0 \oplus F(RD_0, K_{16})$

$= RE_{16} \oplus F($ $)$

$=$ _____ $\oplus F($ $) \oplus F($ $)$

$\mathbf{LD_1 =}$ **and** $\mathbf{RD_1 =}$

Output of 1st round of decryption :

$LE_i = RE_{i-1}$ $\quad\quad$ $RE_i = LE_{i-1} \oplus F(RE_{i-1}, K_i)$

$RE_{i-1} =$ _____

$LE_{i-1} =$ _____

Output of the 16th round (Decryption): $\mathbf{RE_0 \| \ LE_0}$

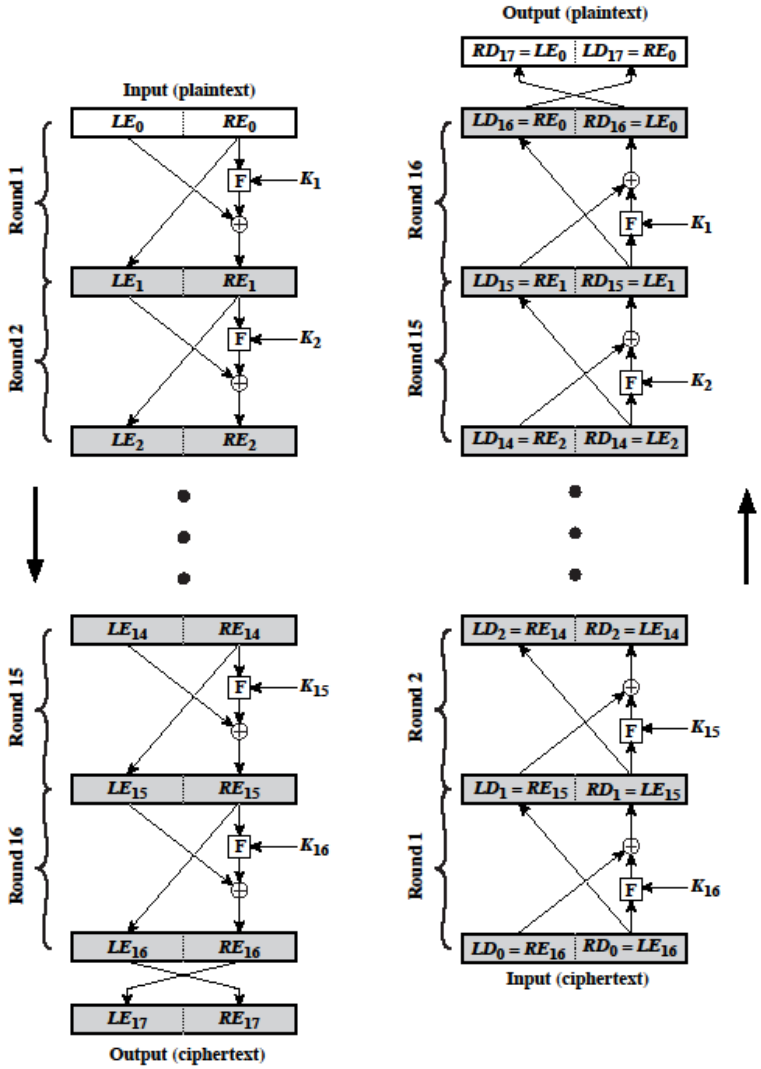

Figure 3.3 Feistel Encryption and Decryption (16 rounds)

Some Questions on Block Cipher modes:

- If a bit error occurs in the transmission of a ciphertext character in 8-bit CFB mode, how far does the error propagate? (Question 6.8)
- In discussing OFB, it was mentioned that if it was known that two different messages had an identical block of plaintext in the identical position, is it possible to recover the corresponding O block? (Question 6.9)
- Why do some block cipher modes of operations only use encryption while others use both encryption and decryption? (Question 6.5)
- Question 6.1 and 6.2 (see below)

Homework:

- What is reversible mapping? What is irreversible mapping? Think about why Fiestels algorithm works for any function F, even for the irreversible ones.
- What is the difference between a block cipher and a stream cipher?
- What is a product cipher?
- What is the difference between diffusion and confusion? How diffusion and confusion is achieved in Fiestels encryption algorithm?
- What parameters and design choices determine the actual algorithm of a Feistel Cipher?

The following are a list of questions for students to attempt at home to get a better grasp of the concepts discussed during the workshop.

- Complete any questions that were not completed during the workshop.
- What is avalanche effect? Why it is desired in encryption algorithms?
- Write the block diagram for DES decryption algorithm.

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 6.11 shows two possibilities, both of which follow from the definition of CBC. Which of the two would you choose:

a. For security?

b. For performance?

6.2 Can you suggest a security improvement to either option in Figure 6.11, using only three DES chips and some number of XOR functions? Assume you are still limited to two keys.

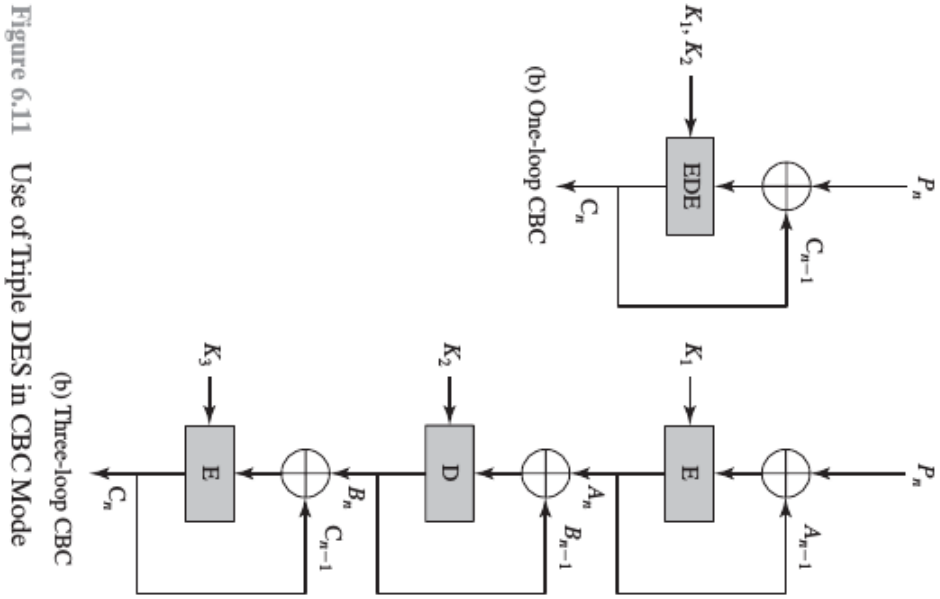

Figure 6.11 Use of Triple DES in CBC Mode