Chapter 4 Homework 1, 4, 5, 8

1. Consider the following DES-like encryption method. Start with a message of $2n$ bits. Divide it into two blocks of length n (a left half and a right half); M_0M_1. The key K consists k bits, for some integer k. There is a function $f(K, M)$ that takes an input of k bits and n bits and gives an output of n bits. One round of encryption starts with a pair M_jM_{j+1}, where

$$M_{j+2} = M_j \oplus f(K, M_{j+1})$$

This is done for m rounds, so the ciphertext is M_mM_{m+1}.

(a) If you have a machine that does the m-round encryption just described, how would you use the same machine to decrypt the ciphertext M_mM_{m+1} (using the same key K)? Prove that your decryption method works.

Given the ciphertext $[M_m][M_{m+1}]$, switch sides to obtain $[M_{m+1}][M_m]$. We know from the encryption algorithm that

$$M_{m+1} = M_m \oplus f(K, M_m)$$

So, we can obtain M_{m-1} from M_{m+1} by

$$M_{m-1} \oplus f(K, M_m) \oplus f(K, M_m)$$

since $f(K, M_m) \oplus f(K, M_m)$ will have a net result of 0. By repeating this process we can deduce subsequent M_j until we reach $[M_1][M_0]$, which then by switching these halves gives the plaintext $[M_0][M_1]$.

(b) Suppose K has n bits and $f(K, M) = K \oplus M$, and suppose the encryption process consists of $m = 2$ rounds. If you know only a ciphertext, can you deduce the plaintext and the key? If you know a ciphertext and the corresponding plaintext, can you deduce the key? Justify your answers.

Round 1:

$$\begin{aligned}
[M_0][M_1] &= [M_1][M_0 \oplus f(K, M_1)] \\
&= [M_1][M_0 \oplus K \oplus M_1] \\
&= [M_1][M_2]
\end{aligned}$$

Round 2:

$$\begin{aligned}
[M_1][M_2] &= [M_2][M_1 \oplus f(K, M_2)] \\
&= [M_2][M_1 \oplus K \oplus M_2] \\
&= [M_2][M_1 \oplus K \oplus M_0 \oplus K \oplus M_1] \\
&= [M_0 \oplus K \oplus M_1][M_1 \oplus M_1 \oplus K \oplus K \oplus M_0] \\
&= [M_0 \oplus K \oplus M_1][M_0]
\end{aligned}$$

So, knowing the ciphertext, we could combine the two halves to obtain

$$M_0 \oplus K \oplus M_1 \oplus M_0 = K \oplus M_1$$

We would not have enough information to obtain K if we only knew the ciphertext at this point. However, if we also knew the plaintext then we would have $[M_0][M_1]$ and could combine $K \oplus M_1 \oplus M_1$ to obtain K.

(c) Suppose K has n bits and $f(K, M) = K \oplus M$, and suppose the encryption process consists of $m = 3$ rounds. Why is this system not secure?

Using (b), we can find the next round of encryption.

$$\begin{aligned} &[M_0][M_0 \oplus K \oplus M_1 \oplus f(K, M_0)] \\ = &[M_0][M_0 \oplus K \oplus M_1 \oplus K \oplus M_0] \\ &= [M_0][M_1] \end{aligned}$$

So, 3 rounds of encryption produces the plaintext message, making this method non-secure for 3 rounds.

4. For a string of bits $\mathcal{S}$, let $\overline{\mathcal{S}}$ denote the complementary string obtained by changing all of the 1s to 0s and all of the 0s to 1s (equivalently, $\overline{\mathcal{S}} = \mathcal{S} \oplus 111111\ldots$). Show that if the DES key K encrypts P to C, then $\overline{K}$ encrypts $\overline{P}$ to $\overline{C}$.

The DES encryption tells us to split P into two halves, L_0 and R_0. Then

$$[L_0][R_0] \xrightarrow{K} [R_0][L_0 \oplus f(R_0, K)]$$

where $L_1 = R_0$ and $R_1 = L_0 \oplus f(R_0, K)$.
Now consider the complements of K, C and P. Split $\overline{P}$ into two halves, $\overline{L_0}$ and $\overline{R_0}$. Then,

$$[\overline{L_0}][\overline{R_0}] \xrightarrow{\overline{K}} [\overline{R_0}][\overline{L_0} \oplus f(\overline{R_0}, \overline{K})]$$

where $\overline{R_0} = R_0 \oplus 111\cdots$, $\overline{L_0} = L_0 \oplus 111\ldots$ and $\overline{K} = K \oplus 111\ldots$.
Notice

$$\begin{aligned} &\overline{L_0} \oplus f(\overline{R_0}, \overline{K}) \\ = &\overline{L_0} \oplus R_0 \oplus 111\ldots \oplus K \oplus 111\ldots \\ &= \overline{L_0} \oplus R_0 \oplus K \\ &= \overline{L_0} \oplus f(R_0, K) \end{aligned}$$

and, since $\overline{L_0} = L_0 \oplus 111\ldots$, we have

$$\begin{aligned} \overline{L_0} \oplus f(\overline{R_0, \overline{K}}) &= L_0 \oplus 111\ldots \oplus R_0 \oplus K \\ &= L_0 \oplus R_0 \oplus K \oplus 111\ldots \\ &= L_0 \oplus f(R_0, K) \oplus 111\ldots \\ &= R_1 \oplus 111\ldots \\ &\overline{R_1} \end{aligned}$$

Putting this all together, we see

$$\begin{aligned}
[\overline{L_0}][\overline{R_0}] \xrightarrow{\overline{K}} [\overline{R_0}[\overline{L_0} \oplus f(\overline{R_0}, \overline{K})] \\
= [\overline{L_1}][\overline{R_1}] \\
= \overline{C}
\end{aligned}$$

5.

(a) Let $K = 111\ldots111$ be the DES key consisting of all 1s. Show that if $E_K(P) = C$, then $E_K(C) = P$, so encryption twice with this key returns the plaintext.

In the DES algorithm, a series of encryption steps are taken with K_i being the key K on the i^{th} step. Decryption is performed by using the same process but with the keys taken in reverse. If we allow $K = 111\ldots111$ to be used, encryption and decryption processes become the same. So, when the encryption process is used with this key, the decryption process is exactly the same. The fact that $K = 111\ldots111$, encryption produces the complement of the input text. When the same process is repeated, the complement of the complement is produced, which is the original text. So, if $E_K(P) = C$, then $E_K(C) = P$.

(b) Find another key with the same property as K in part (a).

Any symmetric K would work the same, since decryption is the same as encryption with the key reversed. The trivial $00\ldots00$ works but actually does no encryption at all.

8. Suppose we modify the Feistel setup as follows. Divide the plaintext into three equal blocks: L_0, M_0, R_0. Let the key for the i^{th} round be K_i and let f be some function that produces the appropriate size output. The i^{th} round of encryption is given by

$$L_i = R_{i-1}, \quad M_i = L_{i-1}, \quad R_i = f(K_i, R_{i-1}) \oplus M_{i-1}$$

This continues for n rounds. Consider the decryption algorithm that starts with the ciphertext A_n, B_n, C_n and uses the algorithm

$$A_{i-1} = B_i, \quad B_{i-1} = f(K_i, A_i) \oplus C_i, \quad C_{i-1} = A_i$$

Continue this for n rounds, down to A_0, B_0, C_0. Show that $A_i = L_i$, $B_i = M_i$, C_i, R_i for all i and that the decryption algorithm returns the plaintext.

Notice the relationship between the encryption and decryption processes. Encryption involves a shift right and decryption involves a shift left. So, the i^{th} encryption step is the same as the $n - i^{th}$ decryption step. It must be shown that the encryption and decryption functions 'undo' each other.
Consider the n^{th} round of encryption:

$$\begin{aligned}
[L_{n-1}][M_{n-1}][R_{n-1}] \xrightarrow{K} [R_{n-1}][L_{n-1}][f(K_n, R_{n-1}) \oplus M_{n-1}] \\
= [L_n][M_n][R_n] \\
= [A_n][B_n][C_n]
\end{aligned}$$

Decrypting now, we see:

$$\begin{aligned}
[A_n][B_n][C_n] &\xrightarrow{K} [B_n][f(K_n, A_n) \oplus C_n][A_n] \\
= [L_{n-1}][f(K_n, R_{n-1}) \oplus f(K_n, R_{n-1}) \oplus M_{n-1}][R_{n-1}] \\
= [L_{n-1}][M_{n-1}][R_{n-1}]
\end{aligned}$$

So, each round of decryption gives the prior round after encryption. Continuing gives $A_i = L_i$, $B_i = M_i$, $C_i = R_i$.