Cryptology Exercise Week 4

Zijun Yu 202203581

September 2023

Exercise 6.2

Part 1

Let's first look at the f-function. Because the function E simply does permutation on its input (with some bits duplicated), we have $E(\overline{R}) = \overline{E(R)}$. So we further have that

$$f(\overline{R}, \overline{K}) = P(S(\overline{K} \oplus E(\overline{R}))) = P(S(\overline{K} \oplus \overline{E(R)})) = P(S(K \oplus E(R))) = f(R, K)$$

Now let's look at each round of DES (except the last round), we have $K'_i = \overline{K_i}$, $L'_0 = \overline{L_0}$ and $R'_0 = \overline{R_0}$. Now, suppose that we have $R'_{i-1} = \overline{R_{i-1}}$ and $L'_{i-1} = \overline{L_{i-1}}$, for $i > 1$, then we will have

$$L'_i = R'_{i-1} = \overline{R_{i-1}} = \overline{L_i}$$

$$\begin{aligned} R'_i &= L'_{i-1} \oplus f(R'_{i-1}, K'_i) \\ &= \overline{L_{i-1}} \oplus f(\overline{R_{i-1}}, \overline{K_i}) \\ &= \overline{L_{i-1}} \oplus f(R_{i-1}, K_i) \\ &= \overline{L_i \oplus f(R_{i-1}, K_i)} \\ &= \overline{R_i} \end{aligned}$$

Thus we have an induction proof that

$$L'_i = \overline{L_i} \text{ and } R'_i = \overline{R_i}$$

Then, for the last round, by applying the same reasoning, we have

$$R'_n = R'_{n-1} = \overline{R_{n-1}} = \overline{R_n}$$

$$L'_n = L'_{n-1} \oplus f(R'_{n-1}, K'_n) = \overline{L_n}$$

Therefore, we have

$$Y' = L'_n || R'_n = \overline{L_n} || \overline{R_n} = \overline{Y}$$

Part 2

We ask the oracle to give both $Y_1 = DES_K(X)$ and $Y_2 = DES_K(\overline{X})$. When we are checking a key k, we compute $y = DES_k(X)$. If y is neither Y_1 nor $\overline{Y_2}$, we can rule out both k and $\overline{k}$. If $y = Y_1$, then $K = k$, and if $y = \overline{Y_2}$, then $K = \overline{k}$.