Homework 2 Solutions

- **Group Members: Yu Wang(wangy52 661834351)**
- **Collaborators: no**

Problem 1

Similar to the analysis in "Differential Cryptanalysis" by Çetin Kaya Koç, because the permutation block has inverse operation, we only consider the substitution box and the XOR operator.

For two 4-bit inputs x_1 and x_2 and their corresponding outputs from the S_0 box y_1 and y_2, let $x' = x_1 \oplus x_2$ and $y' = y_1 \oplus y_2$, Tab. 1 shows the relationship between x' and y'.

Input	Output y'			
x'	0	1	2	3
0	16	0	0	0
1	0	2	10	4
2	0	10	6	0
3	2	4	0	10
4	2	4	8	2
5	10	0	4	2
6	0	2	2	12
7	4	10	2	0
8	2	4	8	2
9	8	2	2	4
10	4	2	2	8
11	2	8	4	2
12	8	2	2	4
13	2	4	8	2
14	2	8	4	2
15	4	2	2	8

Table 1: S0 Differential Distribution Table

Suppose we know the two inputs are $S0_E = 1$ and $S0'_E = 2$ which XOR to $x' = S0_E \oplus S0'_E = 3$, and the outputs $S0_O = 0$ and $S0'_O = 1$ XOR to $y' = S0_O \oplus S0'_O = 1$.

- Step 1:

  We search the pairs of inputs to the S0 box and find that (8, 11) and (9, 10) satisfy: XOR or inputs is 3 and XOR of outputs is 1. Recall that, $S0_E \oplus S0'_E = (S0_E \oplus S0'_E) \oplus (K \oplus K) = (S0_E \oplus K) \oplus (S0'_E \oplus K) = S0_I \oplus S0'_I$. That's why we search the inputs to the S0 box with $x' = 3$.

- Step 2:

  For all possible inputs, we use property $K = S0_E \oplus (S0_I) = S0_E \oplus (S0_E \oplus K)$ to find the possible keys.

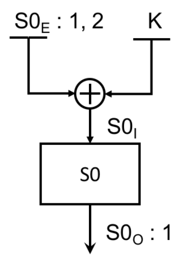
$$
\begin{array}{ll}
1 \oplus 8 = 9 & 2 \oplus 8 = 10 \\
1 \oplus 9 = 8 & 2 \oplus 9 = 11 \\
1 \oplus 10 = 11 & 2 \oplus 10 = 8 \\
1 \oplus 11 = 10 & 2 \oplus 11 = 9
\end{array}
$$

We now conclude that, the true key $K \in \{8, 9, 10, 11\}$

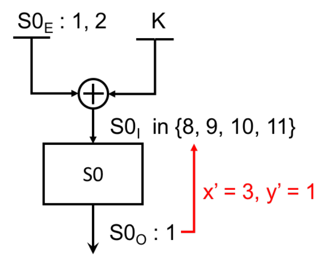
The steps are illustrated in Fig. 1.

Repeat the process for inputs $S0_E = 3$ and $S0_E = 4$, we find that $K \in \{0, 1, 2, 3, 4, 5, 6, 7, 9, 14\}$. Intersect the two sets we found,

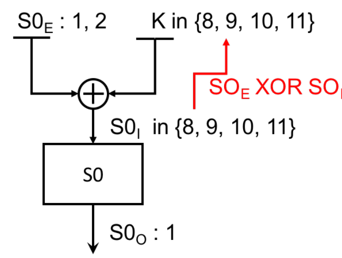
$$K \in \{8, 9, 10, 11\} \cap \{0, 1, 2, 3, 4, 5, 6, 7, 9, 14\} \Rightarrow K \in \{9\} \Rightarrow K = 9 \tag{1-1}$$



(a) initial knowledge



(b) step 1



(c) step 2

Figure 1: Use two known inputs to find candidate keys

Problem 2

The formula for conditional entropy is

$$\mathcal{H}(K|C) = \sum_{c \in C} \sum_{k \in K} p(c, k) \log \frac{p(c)}{p(c, k)} \tag{2-1}$$

Now our task turns to compute the marginal probability of $p(c)$ and the joint probability of $p(c, k)$. Also, cipher text c is a function (the encryption funcion) of plain text p and key k. We then have

- $p(c)$ Use $\mathcal{R}(c)$ to denote all pairs of p and k such that $e_k(p) = c$. Then, apply the total probability formula,

$$p(c) = \sum_{\forall (p,k) \in \mathcal{R}(c) = c} p(p, k). \tag{2-2}$$

The selection of plain text p and key k is assumed to be independent, which means $p(p,k) = p(p) \cdot p(k)$

$$
\begin{aligned}
p_C(1) =& p_{PK}(P=a, K=k_1) + p_{PK}(P=c, K=k_2) \\
=& p_P(a)p_K(k_1) + p_P(c)p_K(k_2) \\
=& \frac{1}{3} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{4} = \frac{7}{24} \\
p_C(2) =& p_{PK}(P=b, K=k_1) + p_{PK}(P=c, K=k_1) + p_{PK}(P=a, K=k_2) \\
=& \frac{1}{6} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} + \frac{1}{3} \cdot \frac{1}{4} = \frac{5}{12} \\
p_C(3) =& p_{PK}(P=b, K=k_2) + p_{PK}(P=a, K=k_3) \\
=& \frac{1}{6} \cdot \frac{1}{4} + \frac{1}{3} \cdot \frac{1}{4} = \frac{1}{8} \\
p_C(4) =& p_{PK}(P=b, K=k_3) + p_{PK}(P=c, K=k_3) \\
=& \frac{1}{6} \cdot \frac{1}{4} + \frac{1}{2} \cdot \frac{1}{4} = \frac{1}{6}
\end{aligned}
$$

- $p(c,k)$ Conputing $p(c,k)$ directly is not easy. Let's use $p(c,k) = p(c|k) \cdot p(k)$ and compute $p(c|k)$ first.

$$
\begin{aligned}
& p_{C|K}(C=1|K=k_1) = p_{P|K}(P=a|K=k_1) = p_P(a) = \frac{1}{3} \\
& p_{C|K}(C=2|K=k_1) = p_{P|K}(P=b|K=k_1) + p_{C|K}(P=c|K=k_1) = p_P(b) + p_P(c) = \frac{1}{6} + \frac{1}{2} = \frac{2}{3} \\
& p_{C|K}(C=3|K=k_1) = 0 \\
& p_{C|K}(C=4|K=k_1) = 0 \\
& p_{C|K}(C=1|K=k_2) = p_{P|K}(P=c|K=k_2) = p_P(c) = \frac{1}{2} \\
& p_{C|K}(C=2|K=k_2) = p_{P|K}(P=a|K=k_2) = p_P(a) = \frac{1}{3} \\
& p_{C|K}(C=3|K=k_2) = p_{P|K}(P=b|K=k_2) = p_P(b) = \frac{1}{6} \\
& p_{C|K}(C=4|K=k_2) = 0 \\
& p_{C|K}(C=1|K=k_3) = 0 \\
& p_{C|K}(C=2|K=k_3) = 0 \\
& p_{C|K}(C=3|K=k_3) = p_{P|K}(P=a|K=k_3) = p_P(a) = \frac{1}{3} \\
& p_{C|K}(C=4|K=k_3) = p_{P|K}(P=b|K=k_3) + p_{P|K}(P=c|K=k_3) = p_P(b) + p_P(c) = \frac{2}{3}
\end{aligned}
$$

Then, we use $p(c,k) = p(c|k) \cdot p(k)$ and have Tab. 2.

C\K	k_1	k_2	k_3
1	1/6	1/8	0
2	1/3	1/12	0
3	0	1/24	1/12
4	0	0	1/6

Table 2: $p(c,k)$

Now, we apply the formula for conditional entropy and have

$$\begin{aligned}
\mathcal{H}(K|C) =& \sum_{c\in C}\sum_{k\in K} p(c,k)\log\frac{p(c)}{p(c,k)} \\
=& \frac{1}{6}\log\frac{7/24}{1/6} + \frac{1}{3}\log\frac{5/12}{1/3} + \frac{1}{8}\log\frac{7/24}{1/8} + \frac{1}{12}\log\frac{5/12}{1/12} \\
&+ \frac{1}{24}\log\frac{1/8}{1/24} + \frac{1}{12}\log\frac{1/8}{1/12} + \frac{1}{6}\log\frac{1/6}{1/6} \\
=& 0.7029\ bit
\end{aligned} \tag{2-3}$$