Cryptography & Network Security 1 HW 1.2

Coen Valk

1. For the S box S_0:

$$\begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix}$$

One can perform a differential cryptanalysis attack by considering the change in differential output y' as the differential input x' changes. Firstly, we must compute our possible input values and pairs. We have a 4x4 S box, which means the number of input values is $4 \times 4 = 16$, and the number of possible input pairs is $16^2 = 256$. Additionally, the S box output space is only 2 bits, so as the input varies over 16 values, the output values vary over 4 values. With this information we can construct the following differential distribution table:

$$\begin{bmatrix} 16 & 0 & 0 & 0 \\ 0 & 4 & 8 & 4 \\ 0 & 4 & 8 & 4 \\ 4 & 8 & 0 & 4 \\ 2 & 6 & 2 & 6 \\ 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 \\ 6 & 2 & 6 & 2 \\ 4 & 4 & 4 & 4 \\ 2 & 6 & 2 & 6 \\ 6 & 2 & 6 & 2 \\ 4 & 4 & 4 & 4 \\ 4 & 8 & 4 & 0 \\ 8 & 0 & 4 & 4 \\ 4 & 0 & 4 & 8 \\ 4 & 8 & 4 & 0 \end{bmatrix}$$

Looking at input XOR 1, the possible output is XOR 1, 2, or 3. The possible values for x and $x*$ are then:

$1 \rightarrow 1$: 14, 15

$1 \rightarrow 2$: 0, 12, 13, 1

$1 \rightarrow 3$: 2, 4, 6, 8, 10, 11, 9, 7, 5, 3

Consider the input 14, 15, results in XOR 1 as input, and XOR output through the S box is 2. We follow that

$$S_{1K} = S_{1I} \oplus S_{1E}$$

Which results in:

$$
\begin{array}{ll}
E \oplus 0 = E & F \oplus 0 = F \\
E \oplus C = 2 & F \oplus C = 3 \\
E \oplus D = 3 & F \oplus D = 2 \\
E \oplus 1 = F & F \oplus 1 = E
\end{array}
$$

Therefore the possible keys are: {2, 3, E, F}

This process can be repeated with more known input and output pairs until one possible key remains.

2.

$$H(K|C) = H(K) + H(P) - H(C)$$

$$H(X) = -\sum_{i=1}^{n} p(X = x_i) \log_2 p(X = x_i)$$

$$H(P) = -\left(\frac{1}{3}\log_2\left(\frac{1}{3}\right) + \frac{1}{6}\log_2\left(\frac{1}{6}\right) + \frac{1}{2}\log_2\left(\frac{1}{2}\right)\right)$$

$$H(K) = -\left(\frac{1}{2}\log_2\left(\frac{1}{2}\right) + \frac{1}{4}\log_2\left(\frac{1}{4}\right) + \frac{1}{4}\log_2\left(\frac{1}{4}\right)\right)$$

$$H(C) = -\left(\frac{2}{9}\log_2\left(\frac{2}{9}\right) + \frac{2}{9}\log_2\left(\frac{2}{9}\right) + \frac{2}{9}\log_2\left(\frac{2}{9}\right) + \frac{1}{3}\log_2\left(\frac{1}{3}\right)\right)$$

$$H(P) \approx 1.459,\ H(K) = 1.5,\ H(C) \approx 1.975$$

$$H(K|C) \approx 0.984$$