Cryptography Homework 1(Part 2)

William Culver
Rensselaer Polytechnic Institute
(culvew@rpi.edu)

September 24, 2018

Problem 1

The first step is to run every combination of pairs of input values through the S-box without a key. Create a table with the rows being each Pairs XOR difference (16 rows in our toy DES) and each column being there outputs XOR difference (4 columns in our toy DES).

then choose a pair of 2 inputs to run through the S-box after XORing them with the key. Say these had previously given an XOR Difference of D_1, and now give a Difference of D_2. You would go to the table with the row of there input XOR difference, and Column D_2. This will have X different combinations of inputs that gave this difference in outputs. By XORing each of these numbers in this table location with each of the two different values that form our input pair, you will get a list of possible keys that is at max 2X long(could be shorter depending on duplicates).

This gets us a set of possible keys. We can repeat this process with different values to get a different set of keys. The true key would have to be in both these sets. Repeat this process until you have only 1 possible key.

Problem 2

The formula for $H(K|C)$ is fairly simple.

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

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

Calculating H(K) and H(P) are also simple since since the probabilities are given.

$$H(K) = -(\frac{1}{2}log_2(\frac{1}{2}) + \frac{1}{4}log_2(\frac{1}{4}) + \frac{1}{4}log_2(\frac{1}{4})) = 1.5$$

$$H(P) = -(\frac{1}{3}log_2(\frac{1}{3}) + \frac{1}{6}log_2(\frac{1}{6}) + \frac{1}{2}log_2(\frac{1}{2})) = 1.4592$$

Calculating H(C) is slightly harder since we need to calculate the probability of each C occurring. We can do this by looking at the output table and calculating the probability of each event occurring based on the probabilities of K and P.

$$P(1) = P(K_1)P(a) + P(K_2)P(c) = \frac{7}{24}$$

$$P(2) = P(K_1)P(b) + P(K_1)P(c) + +P(K_2)P(a) = \frac{10}{24}$$

$$P(3) = P(K_2)P(b) + P(K_3)P(a) = \frac{3}{24}$$

$$P(4) = P(K_3)P(b) + P(K_3)P(c) = \frac{4}{24}$$

When we plug these values in we get that H(C)=1.8506. We can then calculate $H(K|C)$ to be 1.1086.