Brendan Forbes

Cryptography and Network Security

Homework 1 Part 2

Q1.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 00 | 01 | 10 | 11 |
| 0000 | 16 | 0 | 0 | 0 |
| 0001 | 0 | 4 | 8 | 4 |
| 0010 | 0 | 4 | 8 | 4 |
| 0011 | 4 | 8 | 0 | 4 |
| 0100 | 2 | 6 | 2 | 6 |
| 0101 | 4 | 4 | 4 | 4 |
| 0110 | 4 | 4 | 4 | 4 |
| 0111 | 6 | 2 | 6 | 2 |
| 1000 | 4 | 4 | 4 | 4 |
| 1001 | 2 | 6 | 2 | 6 |
| 1010 | 6 | 2 | 6 | 2 |
| 1011 | 4 | 4 | 4 | 4 |
| 1100 | 4 | 8 | 4 | 0 |
| 1101 | 8 | 0 | 4 | 4 |
| 1110 | 4 | 0 | 4 | 8 |
| 1111 | 4 | 8 | 4 | 0 |

The differential cryptanalysis of S0 begins by finding the results of all 256 possible pairs of inputs and outputs. The table above has the XOR of the two inputs in the rows, and the XOR of the two outputs in the columns. Let us assume that the table is correct.

For every entry on the table there will that many possible inputs organized as pairs. So for

(0000, 00) there will be 8 pairs.

Say we want to find the key. We know S1K = S1I XOR S1E and S1I’ = S1E’

If we input a pair, with let’s say XOR 1011, and the output y’ is 00, then there are 4 possible keys as indicated by the table. If we continue to do this, with different inputs, we will have different sets with possible key. The actual key will be in every single one, so we will find the intersection every time we test a new pair. We will test new pairs until our intersection contains only one value which will be the key

Q2.

H(K|C) = H(K) + H(P) – H(C)

H(K) =

H(P) =

Pc(1) = Pc(2)= Pc(3) = Pc(4) =

H(C) = = 1.85

H(K|C) = H(K) + H(P) – H(C) = 1.5 + 1.46 – 1.85 = 1.11