Jack Phillips
CRYPTO HW 1 P2:

Q1) for our simplified box we have:

$$S_0 = \begin{bmatrix} 1, 0, 3, 2 \\ 3, 2, 1, 0 \\ 0, 2, 1, 3 \\ 3, 1, 3, 2 \end{bmatrix}$$

Now there are 16 pairs for (x, x^*) in this box.

$$x' = x \oplus x^*$$

each spot varies to values up to 4

$$y = S(x), \quad y^* = S(x^*).$$

$$y' = y \oplus y^*$$

we can now make Differential Distribution table from all of these values:

input x'	output y' = 0	1	2	3
00	16	0	0	0
01	0	10	6	0
02	0	2	10	4
03	2	4	0	10
04	2	4	8	2
05	4	2	2	8
06	8	2	2	4
07	2	8	4	2
08	2	4	8	2
09	0	2	2	12
A	10	0	4	2
B	4	10	2	0
C	8	2	2	4
D	2	8	4	2
E	2	4	8	2
F	4	2	2	8

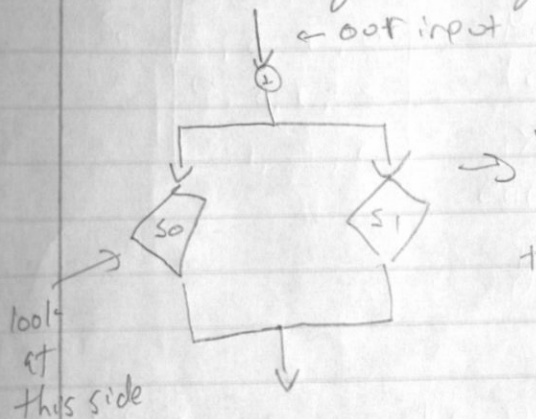
I used Python to make the DDTable to left using each x as 4 bit value. Picking all combos of x.

Now lets start to get the actual key :)

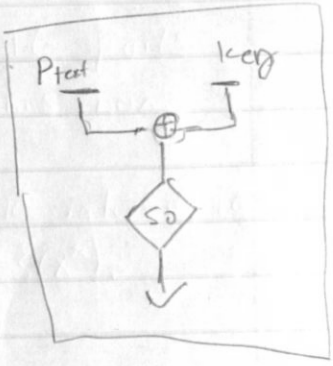
(on next page we continue)

Now that we have All the above lets pick 4 bit key: 0xa lets say.

we are gonna look at:



we can simplify to get consept



Lets Pick the input of:

1: 6, 2 to encrypt

our results will be:

- 6 & A = 13 look up → 3
- 2 & A = 9 look up → 0

Xor 4

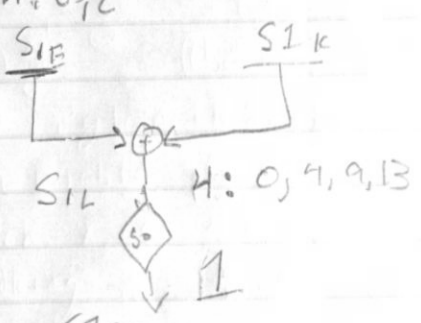
Output: 0 1 2 3

occurs: 2 4 0 2

→ Now values that (X, X⊕4)

4 → 1: 0, 4, 9, 13

Now to get key!



key:

S1K = S1E ⊕ S1L:

0 ⊕ 6 = 6	0 ⊕ 2 = 2
4 ⊕ 6 = 2	4 ⊕ 2 = 6
9 ⊕ 6 = 15	9 ⊕ 2 = 11
13 ⊕ 6 = 11	6 ⊕ 2 = 4

Posible_vals = {2, 4, 6, 11, 15}

we can continue doing this till we end up getting that the 11 is the key.

Basically the we could continue get another set and intersection. until we got 11 as key. with more complex system. This all can be expanded to work. Just more boxes and xois make gerelating harder.

Q2) $H(K|C) = H(K) + H(P) - H(C)$

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

$= -(\frac{1}{3}\log_2 1/3 + 1/6 \log_2 1/6 + 1/2 \log_2 1/2)$

$= 1.45$

$P = \{a, b, c\}$ with
$P_p(a) = 1/3$
$P_p(b) = 1/6$
$P_p(c) = 1/2$

$H(K) = -(1/2 \log_2 1/2 + 1/4 \log_2 1/4 + 1/4 \log_2 1/4)$

$= 1.5$

$e_{K_1}(a) = 1 \quad e_{K_1}(b) = 2 \quad e_{K_1}(c) = 3$

$e_{K_2}(a) = 2 \quad e_{K_2}(b) = 3 \quad e_{K_2}(c) = 1$

$e_{K_3}(a) = 3 \quad e_{K_3}(b) = 4 \quad e_{K_3}(c) = 4$

Prob dist P_c

$P_c(1) = (1/3 \cdot 1/2) + (1/2 \cdot 1/4)$

$= \frac{1}{6} + \frac{1}{8} = \frac{14}{48} = 7/24$

$P_c(2) = (1/3 \cdot 1/4) + (1/6 \cdot 1/2) + (1/2 \cdot 1/2)$

$= 1/12 + 1/12 + 1/4 = 5/12$

$P(3) = (1/4 \cdot 1/3) + (1/4 \cdot 1/6)$

$= 1/12 + 1/24 = 3/24 = 1/8$

$P(4) = (1/4 \cdot 1/6) + (1/4 \cdot 1/2)$

$= 1/24 + 1/8 = 4/24$

$H(C) = -(7/24 \log_2(7/24) + 5/12 \log_2(5/12) + 1/8 \log_2 1/8 + 4/24 \log_2(4/24))$

$= 1.85$

$H(K|D) = 1.5 + 1.45 - 1.797 = \boxed{1.85}$