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.

$$\boxed{x' = x \oplus x^*}$$

each spot varies to values up to 4

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

$$\boxed{y' = y \oplus y^*}$$

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 |

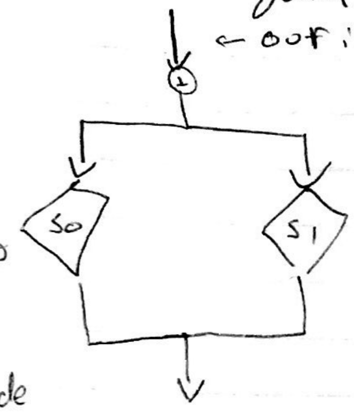
I used Pyton to make the DDTable to left using each x as 4 bit value, Picking all combos of x.

Now lets start to get the actual key :)

on next page we continue

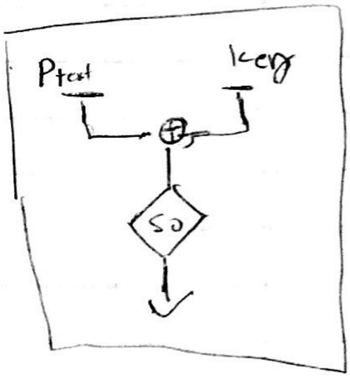
Now that we have All the above lets pick 4 bit key: 0xa lets say.

we are gonna look at!




look at this side

→ 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 → 2

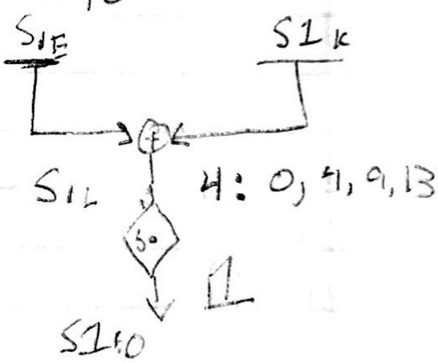
Xor 4

| Output : | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| occurs : | 2 | 4 | 8 | 2 |

→ Now values that (x, x*)

4 → 1: 0, 4, 9, 13

4: 6, 2




Key:

$S1_K = S1_E \oplus S1_L$:

| | |
|---|---|
| $0 \oplus 6 = 6$ | $0 \oplus 2 = 2$ |
| $4 \oplus 6 = 2$ | $4 \oplus 2 = 6$ |
| $9 \oplus 6 = 15$ | $9 \oplus 2 = 11$ |
| $13 \oplus 6 = 11$ | $6 \oplus 2 = 4$ |

$\boxed{\text{Posible\_vals} = \{2, 4, 6, 11, 15\}}$

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

Basically the we could continue get anosther set and intersecation until we got 11 as key. with more complex system. This all can be expanded to work. Just more boxes and xors make gereating harder.

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

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

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

$$= -\left(\tfrac{1}{3}\log_2 1/3 + 1/6 \log_2 1/6 + 1/2 \log_2 1/2\right)$$
$$= 1.45$$

$$H(K) = -\left(1/2 \log_2 1/2 + 1/4 \log_2 1/4 + 1/4 \log_2 1/4\right)$$
$$= 1.5$$

$e_{k_1}(a) = 1$ $e_{k_1}(b) = 2$ $e_{k_1}(c) = 3$
$e_{k_2}(a) = 2$ $e_{k_2}(b) = 3$ $e_{k_2}(c) =$
$e_{k_3}(a) = 3$ $e_{k_3}(b) = 4$ $e_{k_3}(c) =$

Prob dist $P_c$

$$P_c(1) = (1/3 \cdot 1/2) + (1/2 \cdot 1/4)$$
$$= \tfrac{1}{6} + \tfrac{1}{8} = \tfrac{14}{48} = 7/24$$

$$P_c(2) = (1/3 \cdot 1/4) + (1/6 \cdot 1/2) + (1/2 \cdot 1/2)$$
$$= 1/12 + 1/12 + 1/4 = 5/12$$

$$P(3) = (1/4 \cdot 1/3) + (1/4 \cdot 1/6)$$
$$= 1/12 + 1/24 = 3/24 = 1/8$$

$$P(4) = (1/4 \cdot 1/6) + (1/4 \cdot 1/2)$$
$$= 1/24 + 1/8 = 4/24$$

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

$$= \boxed{1.797}$$

$H(K|C) = 1,5 + 1,45 - 1,797 = \boxed{1,153}$