

Jack Phillips

CRYPTO HW1 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'	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

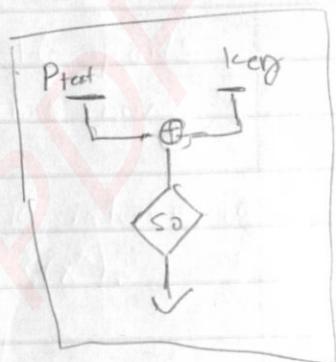
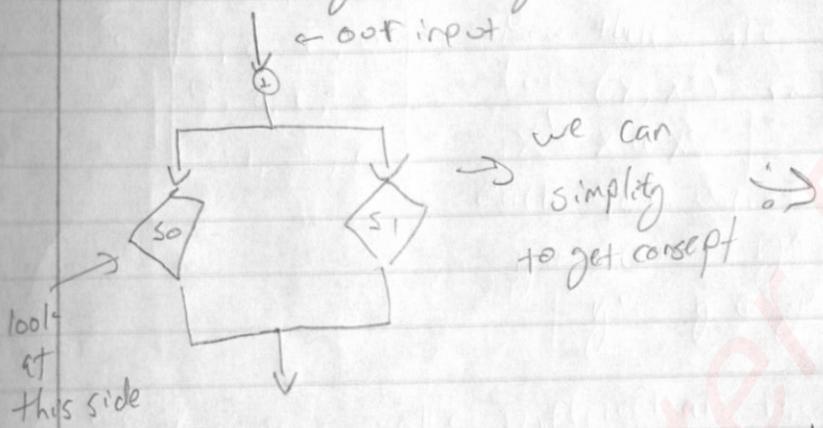
I used Python to make
the DPTable (0, left)
using each x as 4 bit
value. Picking all combos
of $(x,)$

Now let's start to
get the actual key :

On next page we
continue

Now that we have all the above lets pick 4 bit key = 0xa let's say.

We are gonna look at:



Let's Pick the input of:

1: 6, 2 to encrypt

our results will be:

$$- b \times A = 13 \text{ look up } \rightarrow 3$$

$$- 2 \times A = 9 \text{ look up } \rightarrow 0$$

xor 4

Output: $D(D) 2 \ 3$
occurs: $2(H) 0 \ 2$

Now values that (X, X^t)

$$4 \rightarrow 1: 0, 4, 9, 13$$

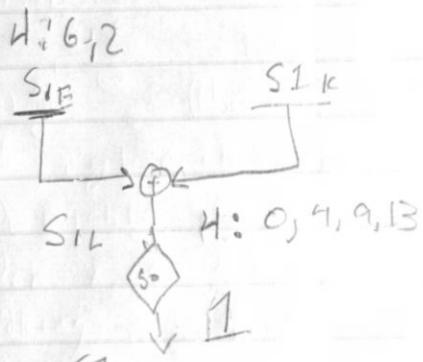
Now to find key:

S1E

weight:

0 and

0



Key:

$$S1K = S1E \oplus S1L:$$

$$0 \oplus 6 = 6 \quad | \quad 0 \oplus 2 = 2$$

$$4 \oplus 6 = 2 \quad | \quad 4 \oplus 2 = 6$$

$$9 \oplus 6 = 15 \quad | \quad 9 \oplus 2 = 11$$

$$13 \oplus 6 = 11 \quad | \quad 6 \oplus 2 = 4$$

Possible vals = {2, 4, 6, 11, 15}

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

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

$$Q2) H(k|c) = H(k) + H(p) - H(c)$$

$$\begin{aligned} H(p) &= - \sum_{i=1}^n p_i \log_2 p_i \\ &= - \left(\frac{1}{3} \log_2 \frac{1}{3} + \frac{1}{6} \log_2 \frac{1}{6} + \frac{1}{2} \log_2 \frac{1}{2} \right) \\ &= 1.45 \end{aligned}$$

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

$$\begin{aligned} H(k) &= - \left(\frac{1}{2} \log_2 \frac{1}{2} + \frac{1}{4} \log_2 \frac{1}{4} + \frac{1}{4} \log_2 \frac{1}{4} \right) \\ &= 1.5 \end{aligned}$$

$e_{k1}(a) = 1$	$e_{k1}(b) = 2$	$e_{k1}(c) = 3$
$e_{k2}(a) = 2$	$e_{k2}(b) = 3$	$e_{k2}(c) = 1$
$e_{k3}(a) = 3$	$e_{k3}(b) = 4$	$e_{k3}(c) = 4$

Prob dist P_c

$$\begin{aligned} P_c(1) &= \left(\frac{1}{3} \cdot \frac{1}{2} \right) + \left(\frac{1}{2} \cdot \frac{1}{4} \right) \\ &= \frac{1}{6} + \frac{1}{8} = \frac{14}{48} = 7/24 \end{aligned}$$

$$\begin{aligned} P_c(2) &= \left(\frac{1}{3} \cdot \frac{1}{4} \right) + \left(\frac{1}{6} \cdot \frac{1}{2} \right) + \left(\frac{1}{2} \cdot \frac{1}{2} \right) \\ &= \frac{1}{12} + \frac{1}{12} + \frac{1}{4} = 5/12 \end{aligned}$$

$$\begin{aligned} P_c(3) &= \left(\frac{1}{4} \cdot \frac{1}{3} \right) + \left(\frac{1}{4} \cdot \frac{1}{6} \right) \\ &= \frac{1}{12} + \frac{1}{24} = 3/24 = 1/8 \end{aligned}$$

$$\begin{aligned} P_c(4) &= \left(\frac{1}{4} \cdot \frac{1}{6} \right) + \left(\frac{1}{4} \cdot \frac{1}{2} \right) \\ &= \frac{1}{24} + \frac{1}{8} = 9/24 \end{aligned}$$

$$\begin{aligned} H(c) &= - \left(\frac{7}{24} \log_2 \left(\frac{7}{24} \right) + \frac{5}{12} \log_2 \left(\frac{5}{12} \right) + \frac{1}{8} \log_2 \left(\frac{1}{8} \right) \right. \\ &\quad \left. + \frac{9}{24} \log_2 \left(\frac{9}{24} \right) \right) \\ &= 1.85 \end{aligned}$$

$$H(k|c) = 1.5 + 1.45 - 1.85 = 1.11$$