Glenn Smith

Q1. [25pnts] For the simplified DES, consider Sbox S0 and show how DiffCrypto attack would work. Show your work for partial credit.

The DiffCrypto attack abuses the non-uniform differential behavior of S-boxes. Even though the output for uniformly distributed single bits is uniformly distributed, the differential output between two uniformly distributed bits is not uniformly distributed.

The 4-bit input to Sbox S0 has 16 possible values. Assign variables,
x, x*, x' = x xor x*
The 2-bit output of Sbox S0 has 4 possible values. Assign variables,
y = S0(x), y* = S0(x*), y' = y xor y* = S0(x) xor S0(x*)

The differential distribution table for S0 is:

Input x'	**Output y'**			
	0	**1**	**2**	**3**
0	16	0	0	0
1	0	10	6	0
2	0	2	10	4
3	2	4	0	10
4	2	4	8	2
5	4	2	2	8
6	8	2	2	4
7	2	8	4	2
8	2	4	8	2
9	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

Note the highly non-uniform distribution of the output.
The first row is clearly explained because when x' = 0 then x = x* and clearly y = y*
But all other rows show a non-uniform distribution of outputs…

Consider the input XOR 2:
Here are the possible input values for S0 with input XOR 2
$2 \rightarrow 1$: D, F
$2 \rightarrow 2$: 0, 1, 2, 3, 8, 9, A, B, C, E
$2 \rightarrow 3$: 4, 5, 6, 7

Suppose we know two inputs to S0 as 4 and 6 which XORs to 2 and the output XOR as 1
The input XOR is 2 regardless of the key because the key does not change

$$
\begin{aligned}
S0'_I &= S0_I \text{ xor } S0^*_I \\
&= (S0_E \text{ xor } S0_K) \text{ xor } (S0^*_E \text{ xor } S0_K) \\
&= S0_E \text{ xor } S0^*_E \\
&= S0'_E
\end{aligned}
$$

And since $S0_I = S0_E$ xor $S0_K$
We know $S0_K = S0_I$ xor $S0_E$
Which means

D xor 4 = 9 D xor 6 = B
F xor 4 = B F xor 6 = 9
So the possible keys are {B, 9}

You can repeat this for each block of subkey to derive the entire subkey

Q2 [25pnts] Consider the crypto system below and compute $H(K|C)$
$P = \{a, b, c\}$ with $P_P(a) = 1/3$ $P_P(b) = 1/6$ $P_P(c) = 1/2$
$K = \{k_1, k_2, k_3\}$ with $P_K(k_1) = 1/2$ $P_K(k_2) = 1/4$ $P_K(k_3) = 1/4$
$C = \{1, 2, 3, 4\}$
$e_{k1}(a) = 1$ $e_{k1}(b) = 2$ $e_{k1}(c) = 2$
$e_{k2}(a) = 2$ $e_{k2}(b) = 3$ $e_{k2}(c) = 1$
$e_{k3}(a) = 3$ $e_{k3}(b) = 4$ $e_{k3}(c) = 4$
$P_C(1) = 1/6 + 1/8 = 7/24$
$P_C(2) = 1/12 + 1/4 + 1/12 = 5/12$
$P_C(3) = 1/24 + 1/12 = 1/8$
$P_C(4) = 1/24 + 1/8 = 1/6$

$H(P) = -(1/3 \log_2 1/3 + 1/6 \log_2 1/6 + 1/2 \log_2 1/2) = 1.459$
$H(K) = -(1/2 \log_2 1/2 + 1/4 \log_2 1/4 + 1/4 \log_2 1/4) = 1.500$
$H(C) = -(7/24 \log_2 7/24 + 5/12 \log_2 5/12 + 1/8 \log_2 1/8 + 1/6 \log_2 1/6) = 1.851$

$H(K|C) = 1.500 + 1.459 - 1.851 = 1.108$